

TÀI LIỆU THAM KHẢO NĂNG CAO

TOÁN 10 CHO GÀ CHỌI

Dành cho học sinh thi học sinh giỏi cấp tỉnh, cấp quốc gia và Olympic quốc tế

Olympiad Mathematics for Grade 10 — a bilingual guide

Đại số · Bất đẳng thức · Số học · Tổ hợp · Hình học phẳng

Định lý có chứng minh · Ví dụ có phân tích và lời giải

Bài tự luyện ba mức: tỉnh, quốc gia, quốc tế — lời giải đầy đủ

Song ngữ Việt – Anh · Vietnamese – English

Phiên bản 1.0 — Tháng 10 năm 2026

<https://globalmarket.vin>

M U C L U C

C O N T E N T S

Chương 1. Mệnh đề, tập hợp và các phương pháp chứng minh — Chapter 1. Logic, sets and methods of proof.....	7
1.1. Mệnh đề và lượng từ — <i>Statements and quantifiers</i>	7
1.2. Kéo theo, điều kiện cần và đủ, mệnh đề đảo và phản đảo — <i>Implication, necessary and sufficient conditions, converse and contrapositive</i>	9
1.3. Tập hợp, phép toán và lực lượng — <i>Sets, operations and cardinality</i>	11
1.4. Ánh xạ: đơn ánh, toàn ánh, song ánh — <i>Maps: injections, surjections, bijections</i>	15
1.5. Chứng minh trực tiếp, bằng phản đảo và bằng phản chứng — <i>Direct proof, contrapositive and contradiction</i>	17
1.6. Quy nạp và nguyên lý sắp thứ tự tốt — <i>Induction and the well-ordering principle</i> ...	21
1.7. Cách viết một chứng minh được chấm đủ điểm — <i>How to write a proof that earns full marks</i>	27
1.8. Bài tự luyện — <i>Practice problems</i>	31
1.9. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	33
Chương 2. Các bất đẳng thức cổ điển — Chapter 2. Classical inequalities.....	39
2.1. Thứ tự trên $\mathbb{R}$, biến đổi tương đương và bình phương — <i>Order on $\mathbb{R}$, equivalent transformations and squares</i>	39
2.2. Bất đẳng thức AM–GM và kỹ thuật điểm rơi — <i>The AM–GM inequality and the equality-point technique</i>	44
2.3. Bất đẳng thức Cauchy–Schwarz — <i>The Cauchy–Schwarz inequality</i>	49
2.4. Bất đẳng thức hoán vị và Chebyshev — <i>The rearrangement and Chebyshev inequalities</i>	54
2.5. Chuỗi trung bình và bất đẳng thức Bernoulli — <i>The chain of means and Bernoulli's inequality</i>	58
2.6. Trị tuyệt đối, bất đẳng thức tam giác và dạng căn Minkowski — <i>Absolute values, the triangle inequality and Minkowski's form</i>	61
2.7. Bất đẳng thức Nesbitt và bài toán cực trị có điều kiện — <i>Nesbitt's inequality and constrained extremum problems</i>	63
2.8. Kỹ thuật tách – ghép và các bổ đề nhỏ — <i>Splitting, pairing and small lemmas</i>	68
2.9. Bảng chiến lược chọn công cụ — <i>Strategy table: choosing the tool</i>	70
2.10. Bài tự luyện — <i>Practice problems</i>	73
2.11. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	74
Chương 3. Kỹ thuật chứng minh bất đẳng thức nâng cao — Chapter 3. Advanced techniques for inequalities	79
3.1. Thuần nhất hóa và chuẩn hóa — <i>Homogenisation and normalisation</i>	79
3.2. Bất đẳng thức Schur — <i>Schur's inequality</i>	82
3.3. Phương pháp SOS (tổng các bình phương) — <i>The SOS method (sums of squares)</i> ...	84
3.4. Phương pháp tiếp tuyến — <i>The tangent-line method</i>	86

3.5. Dồn biến về hai biến bằng nhau — <i>Mixing variables</i>	89
3.6. Đổi biến p, q, r — <i>The p, q, r substitution</i>	91
3.7. Đổi biến Ravi cho cạnh tam giác — <i>The Ravi substitution</i>	95
3.8. Hàm lồi và bất đẳng thức Jensen rời rạc — <i>Convex functions and discrete Jensen</i> ...	98
3.9. Bảng dấu hiệu và kỹ thuật — <i>Signs and techniques at a glance</i>	101
3.10. Bài tự luyện — <i>Practice problems</i>	104
3.11. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	105

Chương 4. Phương trình, bất phương trình và hệ phương trình — Chapter 4.

<i>Equations, inequations and systems</i>	112
4.1. Hàm số bậc hai và dấu của tam thức bậc hai — <i>The quadratic function and the sign of a quadratic trinomial</i>	112
4.2. Định lý Viète và so sánh nghiệm với một số α — <i>Viète's theorem and comparing roots with a number α</i>	115
4.3. Phương trình vô tỉ — <i>Irrational equations</i>	119
4.4. Phương trình bậc cao: đối xứng, hồi quy và đặt ẩn — <i>Higher-degree equations: symmetric, reciprocal and grouped substitution</i>	123
4.5. Hệ phương trình: đối xứng, đẳng cấp, bậc nhất ba ẩn — <i>Systems: symmetric, homogeneous, linear in three unknowns</i>	126
4.6. Hàm đơn điệu và phương trình $f(u) = f(v)$ — <i>Monotone functions and the equation $f(u) = f(v)$</i>	130
4.7. Bất phương trình vô tỉ — <i>Irrational inequations</i>	134
4.8. Bảng chiến lược — <i>Strategy table</i>	135
4.9. Bài tự luyện — <i>Practice problems</i>	138
4.10. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	139

Chương 5. Phương trình hàm, đa thức và dãy số — Chapter 5. Functional equations, polynomials and sequences

.....	145
5.1. Phương trình hàm và nguyên tắc hai pha — <i>Functional equations and the two-phase principle</i>	145
5.2. Hàm cộng tính và phương trình Cauchy — <i>Additive functions and Cauchy's equation</i>	148
5.3. Đơn ánh, toàn ánh và điểm bất động — <i>Injectivity, surjectivity and fixed points</i>	151
5.4. Đa thức: phép chia, định lý Bézout và nghiệm — <i>Polynomials: division, Bézout's theorem and roots</i>	155
5.5. Đa thức hệ số nguyên và nội suy Lagrange — <i>Integer polynomials and Lagrange interpolation</i>	160
5.6. Dãy số truy hồi tuyến tính — <i>Linear recurrence sequences</i>	163
5.7. Dãy tuần hoàn, tổng sai phân và dãy nguyên — <i>Periodic sequences, telescoping sums and integer sequences</i>	165
5.8. Bảng chiến lược và thuật ngữ — <i>Strategy table and glossary</i>	169
5.9. Bài tự luyện — <i>Practice problems</i>	172
5.10. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	173

Chương 6. Chia hết, ước chung lớn nhất và số nguyên tố — Chapter 6. Divisibility, gcd and primes.....	180
6.1. Chia hết và phép chia có dư — <i>Divisibility and division with remainder</i>	180
6.2. Ước chung lớn nhất, bội chung nhỏ nhất và thuật toán Euclid — <i>Greatest common divisor, least common multiple and the Euclidean algorithm</i>	182
6.3. Định lý Bézout và bổ đề Euclid — <i>Bézout's theorem and Euclid's lemma</i>	185
6.4. Số nguyên tố và định lý cơ bản của số học — <i>Primes and the fundamental theorem of arithmetic</i>	191
6.5. Số mũ p-adic và công thức Legendre — <i>The p-adic valuation and Legendre's formula</i>	194
6.6. Số ước, tổng ước và số hoàn hảo — <i>Number of divisors, sum of divisors and perfect numbers</i>	197
6.7. Số chính phương và phép thử bằng số dư — <i>Perfect squares and tests by remainders</i>	200
6.8. Hằng đẳng thức và tính chia hết của $a^n \pm b^n$ — <i>Identities and divisibility of $a^n \pm b^n$</i>	203
6.9. Bài tự luyện — <i>Practice problems</i>	208
6.10. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	209
Chương 7. Đồng dư và các định lý Fermat, Euler, Wilson — Chapter 7. Congruences; Fermat, Euler and Wilson theorems.....	216
7.1. Đồng dư và các tính chất cơ bản — <i>Congruences and their basic properties</i>	216
7.2. Nghịch đảo modulo m và phương trình đồng dư bậc nhất — <i>Inverses modulo m and linear congruences</i>	218
7.3. Định lý số dư Trung Hoa — <i>The Chinese remainder theorem</i>	221
7.4. Hàm φ , các định lý Euler, Fermat và Wilson — <i>The function φ and the theorems of Euler, Fermat and Wilson</i>	224
7.5. Cấp của một số modulo n — <i>The order of a number modulo n</i>	231
7.6. Thặng dư bình phương sơ cấp và số nguyên tố dạng $4k + 1$ — <i>Elementary quadratic residues and primes of the form $4k + 1$</i>	234
7.7. Bổ đề nâng số mũ (LTE) — <i>The lifting-the-exponent lemma (LTE)</i>	236
7.8. Chữ số tận cùng, lũy thừa tầng và bảng chiến lược — <i>Last digits, tower powers and a strategy table</i>	238
7.9. Bài tự luyện — <i>Practice problems</i>	243
7.10. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	244
Chương 8. Phương trình nghiệm nguyên và phần nguyên — Chapter 8. Diophantine equations and the floor function.....	249
8.1. Phương trình bậc nhất hai ẩn $ax + by = c$ — <i>The linear equation $ax + by = c$</i>	249
8.2. Phân tích thành nhân tử — <i>Factorisation</i>	252
8.3. Đánh giá, kẹp giữa hai số chính phương liên tiếp — <i>Estimation: squeezing between consecutive squares</i>	254
8.4. Xét đồng dư để chứng minh vô nghiệm — <i>Residues as an obstruction</i>	257
8.5. Lùi vô hạn, bước nhảy Vieta và nguyên lý cực hạn — <i>Infinite descent, Vieta jumping and the extremal principle</i>	260

8.6. Bộ ba Pythagore — <i>Pythagorean triples</i>	262
8.7. Phương trình Pell — <i>The Pell equation</i>	266
8.8. Phần nguyên và phần lẻ — <i>The floor function and the fractional part</i>	270
8.9. Bài tự luyện — <i>Practice problems</i>	278
8.10. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	280
Chương 9. Phép đếm nâng cao, nhị thức Newton và xác suất — Chapter 9. Advanced counting, binomial theorem and probability	287
9.1. Quy tắc cộng, quy tắc nhân và các cấu hình cơ bản — <i>The sum and product rules and the basic configurations</i>	287
9.2. Hoán vị lặp, tổ hợp lặp và phương pháp sao – vạch — <i>Permutations with repetition, multisets and stars and bars</i>	290
9.3. Song ánh trong phép đếm — <i>Bijections in counting</i>	293
9.4. Bao hàm – loại trừ và hoán vị không điểm bất động — <i>Inclusion–exclusion and derangements</i>	294
9.5. Đếm bằng hai cách và các đẳng thức tổ hợp — <i>Double counting and combinatorial identities</i>	297
9.6. Nhị thức Newton — <i>The binomial theorem</i>	299
9.7. Hệ thức truy hồi, dãy Fibonacci và số Catalan — <i>Recurrences, Fibonacci numbers and Catalan numbers</i>	302
9.8. Xác suất cổ điển — <i>Classical probability</i>	306
9.9. Bảng chiến lược và thuật ngữ — <i>Strategy table and glossary</i>	308
9.10. Bài tự luyện — <i>Practice problems</i>	311
9.11. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	312
Chương 10. Nguyên lý Dirichlet, bất biến và cực hạn — Chapter 10. Pigeonhole principle, invariants and extremal principle	319
10.1. Nguyên lý Dirichlet cơ bản và tổng quát — <i>The pigeonhole principle: basic and general forms</i>	319
10.2. Nguyên lý Dirichlet trong hình học — <i>The pigeonhole principle in geometry</i>	323
10.3. Nguyên lý Dirichlet trong số học — <i>The pigeonhole principle in arithmetic</i>	327
10.4. Dãy con đơn điệu: định lý Erdős–Szekeres — <i>Monotone subsequences: the Erdős–Szekeres theorem</i>	330
10.5. Bất biến và đơn biến — <i>Invariants and monovariants</i>	333
10.6. Nguyên lý cực hạn — <i>The extremal principle</i>	337
10.7. Tô màu bàn cờ và phủ hình — <i>Colouring boards and tilings</i>	339
10.8. Bảng chiến lược — <i>Strategy table</i>	345
10.9. Bài tự luyện — <i>Practice problems</i>	348
10.10. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	349
Chương 11. Đồ thị, tô màu và trò chơi — Chapter 11. Graphs, colourings and games	357
11.1. Đồ thị, bậc của đỉnh và bổ đề bắt tay — <i>Graphs, degrees and the handshake lemma</i>	357
11.2. Đường đi, chu trình, liên thông và cây — <i>Paths, cycles, connectivity and trees</i>	360
11.3. Tô màu đỉnh và đồ thị hai phía — <i>Vertex colouring and bipartite graphs</i>	366

11.4. Chu trình Euler — <i>Euler circuits</i>	369
11.5. Bài toán quen biết, Ramsey $R(3,3) = 6$ và định lý Mantel — <i>Acquaintance problems, Ramsey $R(3,3) = 6$ and Mantel's theorem</i>	372
11.6. Trò chơi hai người: vị trí thắng, vị trí thua — <i>Two-player games: winning and losing positions</i>	376
11.7. Trò chơi Nim và tổng XOR — <i>The game of Nim and the XOR sum</i>	382
11.8. Bài toán thuật toán: tồn tại cách làm và số bước tối thiểu — <i>Algorithmic problems: existence and the least number of steps</i>	386
11.9. Bài tự luyện — <i>Practice problems</i>	392
11.10. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	394

Chương 12. Vector và hệ thức lượng trong tam giác — Chapter 12. Vectors and metric relations in triangles..... 401

12.1. Vector, tích vô hướng và định lý cos — <i>12.1. Vectors, the dot product and the cosine rule</i>	401
12.2. Tâm tỉ cự và hệ thức Leibniz — <i>12.2. Barycentres and Leibniz's relation</i>	403
12.3. Trục tâm, tâm ngoại tiếp và đường thẳng Euler — <i>12.3. Orthocentre, circumcentre and the Euler line</i>	406
12.4. Định lý sin, trung tuyến, phân giác và công thức Stewart — <i>12.4. Sine rule, medians, bisectors and Stewart's theorem</i>	409
12.5. Diện tích, bán kính nội tiếp, ngoại tiếp và hệ thức Euler — <i>12.5. Area, inradius, circumradius and Euler's relation</i>	415
12.6. Định lý Menelaus và định lý Ceva — <i>12.6. The theorems of Menelaus and Ceva</i>	422
12.7. Nhận dạng tam giác bằng hệ thức lượng — <i>12.7. Identifying a triangle from metric relations</i>	429
12.8. Bảng chiến lược và thuật ngữ — <i>12.8. Strategy table and glossary</i>	431
12.9. Bài tự luyện — <i>Practice problems</i>	433
12.10. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	434

Chương 13. Đường tròn: góc, phương tích, tứ giác nội tiếp — Chapter 13. Circles: angles, power of a point, cyclic quadrilaterals 441

13.1. Góc nội tiếp, góc giữa tiếp tuyến và dây, cung chứa góc — <i>Inscribed angles, the tangent–chord angle and the arc of a given angle</i>	441
13.2. Tứ giác nội tiếp và góc định hướng — <i>Cyclic quadrilaterals and directed angles</i>	446
13.3. Phương tích, trục đẳng phương và tâm đẳng phương — <i>Power of a point, radical axis and radical centre</i>	453
13.4. Định lý Ptolemy — <i>Ptolemy's theorem</i>	460
13.5. Đường thẳng Simson và đường tròn chín điểm — <i>The Simson line and the nine-point circle</i>	464
13.6. Định lý Miquel — <i>Miquel's theorem</i>	470
13.7. Đường tròn nội tiếp, bàng tiếp và bổ đề đỉnh ba — <i>Incircles, excircles and the incentre–excentre lemma</i>	473
13.8. Bảng chiến lược và thuật ngữ — <i>Strategy table and glossary</i>	481
13.9. Bài tự luyện — <i>Practice problems</i>	484
13.10. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	486

Chương 14. Phương pháp tọa độ, ba đường conic và cực trị hình học — Chapter 14.	
<i>Coordinate methods, conics and geometric extremes</i>	492
14.1. Đường thẳng, khoảng cách và diện tích trong tọa độ — <i>Lines, distances and areas in coordinates</i>	492
14.2. Đường tròn: tiếp tuyến và trục đẳng phương — <i>Circles: tangents and the radical axis</i>	495
14.3. Tọa độ hóa bài hình học — <i>Setting up coordinates for geometry problems</i>	497
14.4. Elip — <i>The ellipse</i>	501
14.5. Hyperbol — <i>The hyperbola</i>	506
14.6. Parabol — <i>The parabola</i>	509
14.7. Cực trị hình học — <i>Geometric extremum problems</i>	514
14.8. Các tính chất bổ sung của elip và hyperbol — <i>Further properties of the ellipse and the hyperbola</i>	520
14.9. Bảng tổng hợp ba conic — <i>Summary of the three conics</i>	523
14.10. Bảng chiến lược — <i>Strategy table</i>	523
14.11. Bảng thuật ngữ — <i>Glossary</i>	525
14.12. Bài tự luyện — <i>Practice problems</i>	526
14.13. Lời giải bài tự luyện — <i>Solutions to practice problems</i>	528
Phụ lục A. Ba đề luyện thi tự soạn — Appendix A. Three original practice papers	534
A.1. Đề số 1 — mức học sinh giỏi cấp tỉnh — <i>Paper 1 — provincial level</i>	534
A.2. Lời giải và thang điểm đề số 1 — <i>Solutions and marking scheme for Paper 1</i>	535
A.3. Đề số 2 — mức quốc gia — <i>Paper 2 — national level</i>	540
A.4. Lời giải và thang điểm đề số 2 — <i>Solutions and marking scheme for Paper 2</i>	542
A.5. Đề số 3 — mức quốc tế — <i>Paper 3 — international level</i>	550
A.6. Lời giải và thang điểm đề số 3 — <i>Solutions and marking scheme for Paper 3</i>	552
Phụ lục B. Tra cứu định lý và kết quả có tên — Appendix B. Index of named theorems and results	562
B.1. Bảng tra theo chương — <i>B.1. Index by chapter</i>	562
Phụ lục C. Thuật ngữ Việt – Anh — Appendix C. Vietnamese – English glossary	580
C.1. Bảng tra từ A đến Z — <i>C.1. A to Z index</i>	580
Phụ lục D. Tài liệu đọc thêm — Appendix D. Further reading	591
D.1. Sách tiếng Anh và sách giáo khoa — <i>D.1. Books in English and textbooks</i>	591

Chương 1. Mệnh đề, tập hợp và các phương pháp chứng minh

— Chapter 1. Logic, sets and methods of proof

Mục tiêu chương — Chapter objectives

- Lập phủ định chính xác của mệnh đề có lượng từ $\forall$, $\exists$ và phân biệt điều kiện cần với điều kiện đủ.
Negate statements with the quantifiers $\forall$ and $\exists$ exactly, and tell necessary conditions from sufficient ones.
- Đếm phần tử của hợp ba tập bằng bao hàm – loại trừ; nhận ra đơn ánh, toàn ánh, song ánh và dùng chúng để đếm.
Count the elements of a union of three sets by inclusion–exclusion; recognise injections, surjections and bijections and use them to count.
- Chọn đúng một trong năm cách chứng minh: trực tiếp, phản đảo, phản chứng, phản ví dụ, quy nạp.
Choose the right one of five methods of proof: direct, contrapositive, contradiction, counterexample, induction.
- Dùng quy nạp thường, quy nạp mạnh, quy nạp Cauchy và nguyên lý sắp thứ tự tốt, với bước cơ sở viết đủ.
Use ordinary, strong and Cauchy induction and the well-ordering principle, with the base cases written out in full.
- Viết lời giải theo cấu trúc mà giám khảo chấm đủ điểm: giả thiết, kế hoạch, từng bước có lý do, kết luận.
Write a solution in the structure that earns full marks: hypotheses, plan, each step with its reason, conclusion.

1.1. Mệnh đề và lượng từ — Statements and quantifiers

Bài chứng minh được chấm từng câu, nên mỗi câu trong lời giải phải là một khẳng định đúng hoặc sai rõ ràng.

A proof is marked sentence by sentence, so every sentence in a solution must be a claim that is definitely true or definitely false.

ĐỊNH NGHĨA 1.1 (Mệnh đề) / DEFINITION 1.1 (Statement) — Mệnh đề là một câu khẳng định có giá trị chân lý xác định: đúng hoặc sai, không thể vừa đúng vừa sai. Câu chứa biến, như “ n là số chẵn”, chưa là mệnh đề; nó trở thành mệnh đề khi gán giá trị cho biến hoặc gán lượng từ. Phủ định của P ký hiệu $\neg P$: $\neg P$ đúng khi P sai và ngược lại. Hợp $P \vee Q$ đúng khi ít nhất một trong hai đúng; hội $P \wedge Q$ đúng khi cả hai đúng.

A statement is a declarative sentence with a definite truth value: true or false, never both. A sentence with a free variable, such as “ n is even”, is not yet a statement; it becomes one once the variable is given a value or bound by a quantifier. The negation $\neg P$ is true exactly when P is false. The disjunction $P \vee Q$ is true when at least one of the two is true; the conjunction $P \wedge Q$ is true when both are.

ĐỊNH NGHĨA 1.2 (Lượng từ) / DEFINITION 1.2 (Quantifier) — Lượng từ “với mọi” $\forall$ và “tồn tại” $\exists$. Mệnh đề $\forall x \in X: P(x)$ đúng khi $P(x)$ đúng với mọi phần tử x của X . Mệnh đề

$\exists x \in X: P(x)$ đúng khi có ít nhất một phần tử x của X làm $P(x)$ đúng.

The quantifiers “for all” $\forall$ and “there exists” $\exists$. The statement $\forall x \in X: P(x)$ is true when $P(x)$ holds for every element x of X . The statement $\exists x \in X: P(x)$ is true when at least one element x of X makes $P(x)$ true.

ĐỊNH LÝ 1.3 (Phủ định lượng từ) / THEOREM 1.3 (Negation of quantifiers) — Phủ

định đổi $\forall$ thành $\exists$, đổi $\exists$ thành $\forall$, rồi phủ định phần còn lại:

$\neg(\forall x \in X: P(x))$ là $\exists x \in X: \neg P(x)$; $\neg(\exists x \in X: P(x))$ là $\forall x \in X: \neg P(x)$.

Với hai mệnh đề: $\neg(P \vee Q)$ là $(\neg P) \wedge (\neg Q)$; $\neg(P \wedge Q)$ là $(\neg P) \vee (\neg Q)$.

Negation turns $\forall$ into $\exists$ and $\exists$ into $\forall$, then negates what remains:

$\neg(\forall x \in X: P(x))$ is $\exists x \in X: \neg P(x)$; $\neg(\exists x \in X: P(x))$ is $\forall x \in X: \neg P(x)$.

For two statements: $\neg(P \vee Q)$ is $(\neg P) \wedge (\neg Q)$; $\neg(P \wedge Q)$ is $(\neg P) \vee (\neg Q)$.

Chứng minh. / Proof.

Mệnh đề $\forall x: P(x)$ sai khi và chỉ khi không phải mọi x đều thỏa P , tức là có ít nhất một x không thỏa P . Đó chính là $\exists x: \neg P(x)$.

The statement $\forall x: P(x)$ is false exactly when not every x satisfies P , that is, when at least one x fails P . That is precisely $\exists x: \neg P(x)$.

Mệnh đề $\exists x: P(x)$ sai khi và chỉ khi không có x nào thỏa P , tức là mọi x đều không thỏa P : $\forall x: \neg P(x)$.

The statement $\exists x: P(x)$ is false exactly when no x satisfies P , that is, every x fails P : $\forall x: \neg P(x)$.

$P \vee Q$ sai khi và chỉ khi cả P lẫn Q cùng sai, tức $(\neg P) \wedge (\neg Q)$ đúng. $P \wedge Q$ sai khi và chỉ khi ít nhất một trong hai sai, tức $(\neg P) \vee (\neg Q)$ đúng.

$P \vee Q$ is false exactly when both P and Q are false, that is, $(\neg P) \wedge (\neg Q)$ is true. $P \wedge Q$ is false exactly when at least one of them is false, that is, $(\neg P) \vee (\neg Q)$ is true. ■

PHẢI THUỘC / MEMORISE — Phủ định của “với mọi x , $P(x)$ ” là “tồn tại x , không $P(x)$ ”; để bác bỏ một khẳng định “với mọi” chỉ cần một phản ví dụ.

The negation of “for all x , $P(x)$ ” is “there is an x with not $P(x)$ ”; one counterexample is enough to refute a “for all” claim.

VÍ DỤ 1.1 (Thứ tự lượng từ) / EXAMPLE 1.1 (Order of quantifiers) — Xét hai mệnh đề

P : “với mọi số thực $y \neq 0$ tồn tại số thực x sao cho $y^2 + xy + 1 = 0$ ” và Q : “tồn tại số thực x sao cho với mọi số thực $y \neq 0$ ta có $y^2 + xy + 1 = 0$ ”. Viết phủ định của P và của Q , rồi xác định giá trị đúng – sai của cả bốn mệnh đề.

Consider P : “for every real $y \neq 0$ there is a real x with $y^2 + xy + 1 = 0$ ” and Q : “there is a real x such that $y^2 + xy + 1 = 0$ for every real $y \neq 0$ ”. Write the negations of P and Q , then decide the truth value of all four statements.

Lời giải. / Solution.

Phủ định theo Định lý 1.3. $\neg P$: tồn tại $y \neq 0$ sao cho với mọi x , $y^2 + xy + 1 \neq 0$. $\neg Q$: với mọi x tồn tại $y \neq 0$ sao cho $y^2 + xy + 1 \neq 0$.

Negations by Theorem 1.3. $\neg P$: there is $y \neq 0$ such that $y^2 + xy + 1 \neq 0$ for every x . $\neg Q$: for every x there is $y \neq 0$ with $y^2 + xy + 1 \neq 0$.

P đúng: với $y \neq 0$ cho trước, chọn $x = -(y^2 + 1)/y$ thì $y^2 + xy + 1 = y^2 - (y^2 + 1) + 1 = 0$. Do đó $\neg P$ sai.

P is true: for a given $y \neq 0$ take $x = -(y^2 + 1)/y$; then $y^2 + xy + 1 = y^2 - (y^2 + 1) + 1 = 0$. Hence $\neg P$ is false.

Q sai: nếu một x thỏa mãn thì $y = 1$ cho $x = -2$, còn $y = 2$ cho $5 + 2x = 0$, tức $x = -5/2$; hai giá trị này khác nhau. Vậy không có x chung, Q sai và $\neg Q$ đúng.

Q is false: if one x worked, then $y = 1$ would force $x = -2$, while $y = 2$ gives $5 + 2x = 0$, so $x = -5/2$; the two values differ. So no common x exists, Q is false and $\neg Q$ is true.

Vậy P đúng, Q sai, $\neg P$ sai, $\neg Q$ đúng. Hai mệnh đề P và Q chỉ khác thứ tự lượng từ nhưng khác giá trị chân lý.

Hence P is true, Q is false, $\neg P$ is false, $\neg Q$ is true. P and Q differ only in the order of the quantifiers, yet have different truth values. ■

NHẬN XÉT / REMARK — Đổi chỗ $\forall$ và $\exists$ làm đổi nghĩa mệnh đề. “ $\forall y \exists x$ ” cho phép x phụ thuộc y ; “ $\exists x \forall y$ ” đòi một x dùng chung cho mọi y . Khi x phụ thuộc y , hãy viết $x = x(y)$ để thấy rõ.

Swapping $\forall$ and $\exists$ changes the meaning. “ $\forall y \exists x$ ” lets x depend on y ; “ $\exists x \forall y$ ” demands one x serving every y . When x depends on y , write $x = x(y)$ to make this visible.

LỖI HAY GẶP / COMMON MISTAKE — Phủ định “mọi học sinh trong đội đều giải được bài 1” thành “mọi học sinh trong đội đều không giải được bài 1”. Phủ định đúng là “có một học sinh không giải được bài 1”.

Negating “every member of the squad solved problem 1” as “every member failed problem 1”. The correct negation is “some member did not solve problem 1”.

1.2. Kéo theo, điều kiện cần và đủ, mệnh đề đảo và phản đảo — Implication, necessary and sufficient conditions, converse and contrapositive

ĐỊNH NGHĨA 1.4 (Kéo theo, đảo, phản đảo) / DEFINITION 1.4 (Implication, converse, contrapositive) — Mệnh đề kéo theo $P \Rightarrow Q$ (“nếu P thì Q ”) sai duy nhất khi P đúng còn Q sai. Với $P \Rightarrow Q$ cho trước: mệnh đề đảo là $Q \Rightarrow P$; mệnh đề phản đảo là $(\neg Q) \Rightarrow (\neg P)$. $P \Leftrightarrow Q$ nghĩa là cả $P \Rightarrow Q$ lẫn $Q \Rightarrow P$ đúng. Khi $P \Rightarrow Q$ đúng, P là điều kiện đủ của Q và Q là điều kiện cần của P .

The implication $P \Rightarrow Q$ (“if P then Q ”) is false only when P is true and Q is false. For a given $P \Rightarrow Q$, the converse is $Q \Rightarrow P$ and the contrapositive is $(\neg Q) \Rightarrow (\neg P)$. $P \Leftrightarrow Q$ means that both $P \Rightarrow Q$ and $Q \Rightarrow P$ hold. When $P \Rightarrow Q$ is true, P is a sufficient condition for Q and Q is a necessary condition for P .

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$ (đảo) $Q \Rightarrow P$ (converse)	$(\neg Q) \Rightarrow (\neg P)$ (phản đảo) $(\neg Q) \Rightarrow (\neg P)$ (contrapositive)
Đ T	Đ T	Đ T	Đ T	Đ T
Đ T	S F	S F	Đ T	S F

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$ (đảo) $Q \Rightarrow P$ (converse)	$(\neg Q) \Rightarrow (\neg P)$ (phản đảo) $(\neg Q) \Rightarrow (\neg P)$ (contrapositive)
S F	Đ T	Đ T	S F	Đ T
S F	S F	Đ T	Đ T	Đ T

ĐỊNH LÝ 1.5 (Phản đảo tương đương) / THEOREM 1.5 (Contrapositive equivalence)

— Mệnh đề $P \Rightarrow Q$ và mệnh đề phản đảo $(\neg Q) \Rightarrow (\neg P)$ luôn có cùng giá trị chân lý. Mệnh đề đảo $Q \Rightarrow P$ thì không bị ràng buộc bởi $P \Rightarrow Q$.

The statement $P \Rightarrow Q$ and its contrapositive $(\neg Q) \Rightarrow (\neg P)$ always have the same truth value. The converse $Q \Rightarrow P$ is not tied to $P \Rightarrow Q$.

Chứng minh. / Proof.

$P \Rightarrow Q$ sai khi và chỉ khi P đúng và Q sai. $(\neg Q) \Rightarrow (\neg P)$ sai khi và chỉ khi $\neg Q$ đúng và $\neg P$ sai, tức là Q sai và P đúng. Hai điều kiện giống nhau, nên hai mệnh đề cùng đúng hoặc cùng sai.

$P \Rightarrow Q$ is false exactly when P is true and Q is false. $(\neg Q) \Rightarrow (\neg P)$ is false exactly when $\neg Q$ is true and $\neg P$ is false, that is, Q is false and P is true. The two conditions coincide, so the two statements are true together or false together.

Với mệnh đề đảo: lấy P : “ $x = 2$ ”, Q : “ $x^2 = 4$ ”. $P \Rightarrow Q$ đúng nhưng $Q \Rightarrow P$ sai ($x = -2$).

For the converse: take P : “ $x = 2$ ” and Q : “ $x^2 = 4$ ”. Then $P \Rightarrow Q$ is true but $Q \Rightarrow P$ is false ($x = -2$). ■

PHÂN TÍCH / ANALYSIS — Đề hỏi “tìm điều kiện cần và đủ” thì phải làm đủ hai chiều.

Với số nguyên, chiều thuận thường dùng tính chất của số nguyên tố, chiều đảo thường là phép tính trực tiếp.

A problem asking for a “necessary and sufficient condition” needs both directions. For integers the forward direction usually uses a property of primes and the reverse is usually a direct computation.

VÍ DỤ 1.2 (Điều kiện cần và đủ) / EXAMPLE 1.2 (Necessary and sufficient condition) —

Cho số nguyên n . Chứng minh rằng 12 chia hết n^2 khi và chỉ khi 6 chia hết n . Từ đó cho biết “ $6 \mid n$ ” là điều kiện gì của “ $12 \mid n^2$ ”, và nêu mệnh đề đảo của “ $12 \mid n^2 \Rightarrow 12 \mid n$ ” có đúng không.

Let n be an integer. Prove that 12 divides n^2 if and only if 6 divides n . Hence say what kind of condition “ $6 \mid n$ ” is for “ $12 \mid n^2$ ”, and decide whether “ $12 \mid n^2 \Rightarrow 12 \mid n$ ” is true.

Lời giải. / Solution.

- Chiều thuận. Giả sử $12 \mid n^2$. Vì $4 \mid n^2$: nếu n lẻ thì n^2 lẻ, vô lý; nên n chẵn. Vì $3 \mid n^2$ và 3 nguyên tố, theo bổ đề Euclid $3 \mid n$.

Forward direction. Suppose $12 \mid n^2$. Since $4 \mid n^2$: if n were odd then n^2 would be odd, absurd; so n is even. Since $3 \mid n^2$ and 3 is prime, Euclid’s lemma gives $3 \mid n$.

- n chẵn và $3 \mid n$, mà 2 và 3 nguyên tố cùng nhau, nên $6 \mid n$.

n is even and $3 \mid n$, and 2 and 3 are coprime, so $6 \mid n$.

3. Chiều đảo. Nếu $n = 6m$ thì $n^2 = 36m^2 = 12 \cdot 3m^2$, chia hết cho 12.

Reverse direction. If $n = 6m$ then $n^2 = 36m^2 = 12 \cdot 3m^2$, which is divisible by 12.

Vậy $12 \mid n^2 \Leftrightarrow 6 \mid n$, nên $6 \mid n$ là điều kiện cần và đủ. Mệnh đề “ $12 \mid n^2 \Rightarrow 12 \mid n$ ” sai: $n = 6$ cho $n^2 = 36$ chia hết cho 12 nhưng $12 \nmid 6$.

Hence $12 \mid n^2 \Leftrightarrow 6 \mid n$, so $6 \mid n$ is a necessary and sufficient condition. The statement “ $12 \mid n^2 \Rightarrow 12 \mid n$ ” is false: $n = 6$ gives $n^2 = 36$, divisible by 12, but $12 \nmid 6$. ■

VÍ DỤ 1.3 (Phản ví dụ) / EXAMPLE 1.3 (Counterexample) — Bác bỏ ba khẳng định bằng phản ví dụ: (a) $n^2 + n + 17$ là số nguyên tố với mọi số tự nhiên n ; (b) nếu $6 \mid ab$ thì $6 \mid a$ hoặc $6 \mid b$; (c) nếu $a^2 > b^2$ thì $a > b$.

Refute each of the three claims with a counterexample: (a) $n^2 + n + 17$ is prime for every natural number n ; (b) if $6 \mid ab$ then $6 \mid a$ or $6 \mid b$; (c) if $a^2 > b^2$ then $a > b$.

Lời giải. / Solution.

1. (a) Với $n = 16$: $16^2 + 16 + 17 = 289 = 17^2$, hợp số. Các giá trị $n = 0, 1, \dots, 15$ đều cho số nguyên tố nên phản ví dụ nhỏ nhất là $n = 16$.

(a) For $n = 16$: $16^2 + 16 + 17 = 289 = 17^2$, composite. The values $n = 0, 1, \dots, 15$ all give primes, so the smallest counterexample is $n = 16$.

2. (b) Với $a = 2, b = 3$: $ab = 6$ chia hết cho 6, nhưng $6 \nmid 2$ và $6 \nmid 3$.

(b) With $a = 2, b = 3$: $ab = 6$ is divisible by 6, but $6 \nmid 2$ and $6 \nmid 3$.

3. (c) Với $a = -3, b = 1$: $a^2 = 9 > 1 = b^2$ nhưng $a < b$.

(c) With $a = -3, b = 1$: $a^2 = 9 > 1 = b^2$ but $a < b$.

Vậy cả ba khẳng định đều sai.

Hence all three claims are false. ■

NHẬN XÉT / REMARK — Một chuỗi giá trị đầu đúng không chứng minh được gì: $n^2 + n + 17$ nguyên tố 16 lần liên tiếp rồi mới sập. Quy nạp không đầy đủ là nguồn của nhiều “định lý” sai.

A run of true initial values proves nothing: $n^2 + n + 17$ is prime sixteen times in a row and then fails. Incomplete induction is the source of many false “theorems”.

NHẬN XÉT / REMARK — Khi nghi ngờ một khẳng định “với mọi”, thử trước các giá trị biên và các giá trị suy biến (0, 1, số âm, hai biến bằng nhau, hai biến chênh lệch cực lớn).

When a “for all” claim looks doubtful, try the boundary and degenerate values first (0, 1, negatives, equal variables, wildly different variables).

1.3. Tập hợp, phép toán và lực lượng — Sets, operations and cardinality

ĐỊNH NGHĨA 1.6 (Phép toán tập hợp) / DEFINITION 1.6 (Set operations) — Với hai tập A, B : hợp $A \cup B$ gồm các phần tử thuộc A hoặc thuộc B ; giao $A \cap B$ gồm các phần tử thuộc cả hai; hiệu $A \setminus B$ gồm các phần tử thuộc A mà không thuộc B ; $A \subset B$ nghĩa là mọi phần tử của A thuộc B . Trong tập nền X , phần bù của A là $A^c = X \setminus A$. Số phần tử của tập hữu hạn A (lực lượng) ký hiệu $|A|$. Hai tập bằng nhau khi mỗi tập là con của tập kia: để chứng minh $A = B$ ta chứng minh $x \in A \Rightarrow x \in B$ và $x \in B \Rightarrow x \in A$.

For sets A, B : the union $A \cup B$ consists of elements in A or in B ; the intersection $A \cap B$ of elements in

both; the difference $A \setminus B$ of elements in A but not in B ; $A \subset B$ means every element of A lies in B . Inside a universe X the complement of A is $A^c = X \setminus A$. The number of elements (cardinality) of a finite set A is written $|A|$. Two sets are equal when each is a subset of the other: to prove $A = B$ show $x \in A \Rightarrow x \in B$ and $x \in B \Rightarrow x \in A$.

ĐỊNH LÝ 1.7 (Công thức De Morgan) / THEOREM 1.7 (De Morgan's laws) — Với các tập A, B, C trong tập nền X : $(A \cup B)^c = A^c \cap B^c$ và $(A \cap B)^c = A^c \cup B^c$. Ngoài ra $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

For sets A, B, C in a universe X : $(A \cup B)^c = A^c \cap B^c$ and $(A \cap B)^c = A^c \cup B^c$. Also $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Chứng minh. / Proof.

Lấy $x \in X$. $x \in (A \cup B)^c \Leftrightarrow$ không $(x \in A$ hoặc $x \in B) \Leftrightarrow x \notin A$ và $x \notin B \Leftrightarrow x \in A^c \cap B^c$. Đây là phủ định của “hoặc” theo Định lý 1.3.

Take $x \in X$. $x \in (A \cup B)^c \Leftrightarrow$ not $(x \in A$ or $x \in B) \Leftrightarrow x \notin A$ and $x \notin B \Leftrightarrow x \in A^c \cap B^c$. This is the negation of “or” from Theorem 1.3.

Công thức thứ hai: $x \in (A \cap B)^c \Leftrightarrow$ không $(x \in A$ và $x \in B) \Leftrightarrow x \notin A$ hoặc $x \notin B \Leftrightarrow x \in A^c \cup B^c$.

Second law: $x \in (A \cap B)^c \Leftrightarrow$ not $(x \in A$ and $x \in B) \Leftrightarrow x \notin A$ or $x \notin B \Leftrightarrow x \in A^c \cup B^c$.

Phân phối: $x \in A \cap (B \cup C) \Leftrightarrow x \in A$ và $(x \in B$ hoặc $x \in C) \Leftrightarrow (x \in A$ và $x \in B)$ hoặc $(x \in A$ và $x \in C) \Leftrightarrow x \in (A \cap B) \cup (A \cap C)$.

Distributivity: $x \in A \cap (B \cup C) \Leftrightarrow x \in A$ and $(x \in B$ or $x \in C) \Leftrightarrow (x \in A$ and $x \in B)$ or $(x \in A$ and $x \in C) \Leftrightarrow x \in (A \cap B) \cup (A \cap C)$. ■

ĐỊNH LÝ 1.8 (Bao hàm – loại trừ hai tập) / THEOREM 1.8 (Inclusion–exclusion for two sets) — Với hai tập hữu hạn A, B : $|A \cup B| = |A| + |B| - |A \cap B|$.

For finite sets A and B : $|A \cup B| = |A| + |B| - |A \cap B|$.

$$|A \cup B| = |A| + |B| - |A \cap B| \quad (1.1)$$

Chứng minh. / Proof.

Hợp $A \cup B$ là hợp rời của ba tập $A \setminus B$, $A \cap B$, $B \setminus A$. Do đó $|A \cup B| = |A \setminus B| + |A \cap B| + |B \setminus A|$.

$A \cup B$ is the disjoint union of the three sets $A \setminus B$, $A \cap B$, $B \setminus A$. Hence $|A \cup B| = |A \setminus B| + |A \cap B| + |B \setminus A|$.

Mặt khác $|A| = |A \setminus B| + |A \cap B|$ và $|B| = |B \setminus A| + |A \cap B|$. Cộng hai đẳng thức: $|A| + |B| = |A \setminus B| + |B \setminus A| + 2|A \cap B|$.

Also $|A| = |A \setminus B| + |A \cap B|$ and $|B| = |B \setminus A| + |A \cap B|$. Adding: $|A| + |B| = |A \setminus B| + |B \setminus A| + 2|A \cap B|$.

Trừ $|A \cap B|$ hai vế được $|A| + |B| - |A \cap B| = |A \setminus B| + |B \setminus A| + |A \cap B| = |A \cup B|$.

Subtracting $|A \cap B|$ from both sides gives $|A| + |B| - |A \cap B| = |A \setminus B| + |B \setminus A| + |A \cap B| = |A \cup B|$. ■

ĐỊNH LÝ 1.9 (Bao hàm – loại trừ ba tập) / THEOREM 1.9 (Inclusion–exclusion for three sets) — Với ba tập hữu hạn A, B, C :

For three finite sets A, B, C :

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |B \cap C| - |C \cap A| + |A \cap B \cap C| \quad (1.2)$$

Chứng minh. / Proof.

Áp dụng Định lý 1.8 cho hai tập $A \cup B$ và C :

Apply Theorem 1.8 to the two sets $A \cup B$ and C :

$$|A \cup B \cup C| = |A \cup B| + |C| - |(A \cup B) \cap C|$$

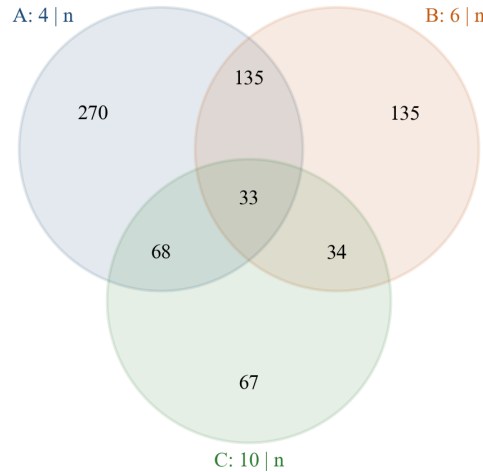
Theo Định lý 1.8, $|A \cup B| = |A| + |B| - |A \cap B|$. Theo tính phân phối (Định lý 1.7), $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$, nên áp dụng Định lý 1.8 lần nữa:

By Theorem 1.8, $|A \cup B| = |A| + |B| - |A \cap B|$. By distributivity (Theorem 1.7), $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$, so Theorem 1.8 once more gives:

$$|(A \cup B) \cap C| = |A \cap C| + |B \cap C| - |A \cap B \cap C|$$

Giao của $A \cap C$ và $B \cap C$ là $A \cap B \cap C$. Thay hai kết quả vào dòng đầu được công thức (1.2).

The intersection of $A \cap C$ and $B \cap C$ is $A \cap B \cap C$. Substituting both results into the first line gives (1.2). ■



Hình 1.1. Số phần tử mỗi vùng khi A, B, C là các bội của 4, 6, 10 trong tập $\{1, \dots, 2024\}$; ngoài ba hình tròn có 1282 số.

Figure 1.1. Number of elements in each region when A, B, C are the multiples of 4, 6, 10 in $\{1, \dots, 2024\}$; outside the three discs lie 1282 numbers.

Hai sự kiện về bội dùng trong cả chương: trong $\{1, \dots, N\}$ có $\lfloor N/m \rfloor$ bội của m , và số vừa chia hết cho m vừa chia hết cho l là bội của $\text{BCNN}(m, l)$.

Two facts about multiples are used throughout: $\{1, \dots, N\}$ contains $\lfloor N/m \rfloor$ multiples of m , and a number divisible by both m and l is a multiple of $\text{lcm}(m, l)$.

$$|\{n \leq N : m \mid n\}| = \lfloor N/m \rfloor, |\{n \leq N : m \mid n \text{ và } l \mid n\}| = \lfloor N/\text{BCNN}(m, l) \rfloor \quad (1.3)$$

PHÂN TÍCH / ANALYSIS — Đề hỏi “ít nhất một trong ba” nên nghĩ ngay tới hợp ba tập. Mỗi tập là tập các bội của một số, còn giao của các tập là tập bội của BCNN: $A \cap B$ là bội của 12, $A \cap C$ bội của 20, $B \cap C$ bội của 30, $A \cap B \cap C$ bội của 60. Mỗi lực lượng là một phần nguyên của phép chia.

“At least one of three” points straight to a union of three sets. Each set is the set of multiples of a number, and intersections are multiples of the lcm: $A \cap B$ are multiples of 12, $A \cap C$ of 20, $B \cap C$ of 30, $A \cap B \cap C$ of 60. Each cardinality is the integer part of a quotient.

VÍ DỤ 1.4 (Bao hàm – loại trừ) / EXAMPLE 1.4 (Inclusion–exclusion) — Có bao nhiêu số nguyên dương không vượt quá 2024 chia hết cho ít nhất một trong các số 4, 6, 10? Có bao nhiêu số trong đó không chia hết cho số nào?

How many positive integers not exceeding 2024 are divisible by at least one of 4, 6, 10? How many are divisible by none of them?

Lời giải. / Solution.

Gọi A, B, C là tập các số trong $\{1, \dots, 2024\}$ chia hết cho 4, 6, 10. Số bội của m trong tập này là $\lfloor 2024/m \rfloor$.

Let A, B, C be the sets of numbers in $\{1, \dots, 2024\}$ divisible by 4, 6, 10. The number of multiples of m is $\lfloor 2024/m \rfloor$.

$$|A| = 506, |B| = 337, |C| = 202$$

$\text{BCNN}(4, 6) = 12, \text{BCNN}(4, 10) = 20, \text{BCNN}(6, 10) = 30, \text{BCNN}(4, 6, 10) = 60$ nên:
 $\text{lcm}(4, 6) = 12, \text{lcm}(4, 10) = 20, \text{lcm}(6, 10) = 30, \text{lcm}(4, 6, 10) = 60$, so:

$$|A \cap B| = 168, |A \cap C| = 101, |B \cap C| = 67, |A \cap B \cap C| = 33$$

Theo (1.2): $|A \cup B \cup C| = 506 + 337 + 202 - 168 - 101 - 67 + 33 = 742$.

By (1.2): $|A \cup B \cup C| = 506 + 337 + 202 - 168 - 101 - 67 + 33 = 742$.

Số không chia hết cho cả ba số là $2024 - 742 = 1282$.

The numbers divisible by none of them number $2024 - 742 = 1282$.

Vậy có 742 số chia hết cho ít nhất một trong ba số và 1282 số không chia hết cho số nào.

Hence 742 numbers are divisible by at least one of the three and 1282 by none. ■

NHẬN XÉT / REMARK — Lỗi hay gặp khi áp dụng (1.2) là bỏ sót số hạng cuối $|A \cap B \cap C|$. Kiểm nhanh: nếu A, B, C đôi một rời nhau thì mọi giao bằng rỗng và (1.2) trở về tổng $|A| + |B| + |C|$.

A common slip with (1.2) is to drop the last term $|A \cap B \cap C|$. Quick check: if A, B, C are pairwise disjoint all intersections are empty and (1.2) reduces to the sum $|A| + |B| + |C|$.

NHẬN XÉT / REMARK — Dạng tổng quát cho n tập có dấu xen kẽ: tổng các $|A_i|$, trừ tổng các giao đôi, cộng tổng các giao ba, và cứ thế. Trường hợp $n = 3$ là đủ cho đa số bài ở mức tỉnh; mức quốc gia cần dạng tổng quát (chương Phép đếm nâng cao).

The general formula for n sets alternates signs: sum of the $|A_i|$, minus the sum of pairwise

intersections, plus the sum of triple intersections, and so on. The case $n = 3$ covers most provincial-level problems; national level needs the general form (chapter on advanced counting).

NHẬN XÉT / REMARK — Chứng minh hai tập bằng nhau luôn gồm hai chiều: lấy x tùy ý trong tập thứ nhất và chứng minh x thuộc tập thứ hai, rồi làm ngược lại. Chỉ chứng minh một chiều thì mới được $A \subset B$.

A proof that two sets are equal always has two directions: take an arbitrary x in the first set and show it lies in the second, then do the reverse. One direction only gives $A \subset B$.

1.4. Ánh xạ: đơn ánh, toàn ánh, song ánh — Maps: injections, surjections, bijections

ĐỊNH NGHĨA 1.10 (Đơn ánh, toàn ánh, song ánh) / DEFINITION 1.10 (Injection, surjection, bijection) — Ánh xạ f từ tập A vào tập B đặt mỗi $x \in A$ ứng với đúng một $f(x) \in B$. f là đơn ánh nếu $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, tức $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. f là toàn ánh nếu mọi $y \in B$ đều có $x \in A$ với $f(x) = y$. f là song ánh nếu vừa đơn ánh vừa toàn ánh; khi đó với mỗi $y \in B$ có đúng một $x \in A$ sao cho $f(x) = y$, và ánh xạ ngược $y \mapsto x$ được ký hiệu f^{-1} .

A map f from a set A into a set B assigns to each $x \in A$ exactly one $f(x) \in B$. f is injective if $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$, equivalently $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$. f is surjective if every $y \in B$ has some $x \in A$ with $f(x) = y$. f is bijective if it is both; then each $y \in B$ has exactly one $x \in A$ with $f(x) = y$, and the inverse map $y \mapsto x$ is written f^{-1} .

ĐỊNH LÝ 1.11 (Đơn ánh – toàn ánh trên tập hữu hạn) / THEOREM 1.11 (Injective iff surjective on finite sets) — Cho A, B là hai tập hữu hạn có cùng số phần tử và f là ánh xạ từ A vào B . Ba điều sau tương đương: f là đơn ánh; f là toàn ánh; f là song ánh. Hệ quả: nếu có song ánh giữa hai tập hữu hạn thì chúng có cùng số phần tử.

Let A, B be finite sets with the same number of elements and f a map from A into B . The following are equivalent: f is injective; f is surjective; f is bijective. Consequently, if there is a bijection between two finite sets they have the same number of elements.

Chứng minh. / Proof.

Đặt $n = |A| = |B|$. Nếu f là đơn ánh, các giá trị $f(x)$ với $x \in A$ đôi một khác nhau nên ảnh $f(A)$ có đúng n phần tử, là tập con của B có n phần tử, nên $f(A) = B$: f là toàn ánh.

Let $n = |A| = |B|$. If f is injective, the values $f(x)$, $x \in A$, are pairwise distinct, so the image $f(A)$ has exactly n elements; it is a subset of B , which has n elements, hence $f(A) = B$ and f is surjective.

Ngược lại, giả sử f là toàn ánh. Nếu f không là đơn ánh, tồn tại $x_1 \neq x_2$ cùng ảnh, nên ảnh $f(A)$ có nhiều nhất $n - 1$ phần tử, nhỏ hơn $|B| = n$, mâu thuẫn với toàn ánh. Vậy f là đơn ánh.

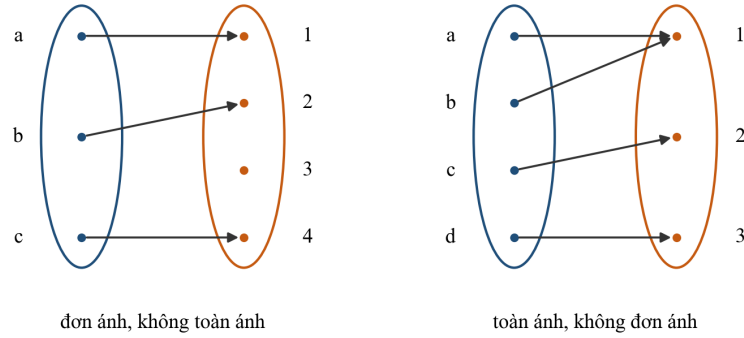
Conversely, let f be surjective. If f were not injective, some $x_1 \neq x_2$ would share an image, so $f(A)$ would have at most $n - 1$ elements, fewer than $|B| = n$, contradicting surjectivity. So f is injective.

Vậy ba tính chất tương đương. Phần hệ quả: song ánh g từ A lên B cho $n = |A| = |f(A)| = |B|$, vì g đơn ánh nên $|g(A)| = |A|$ và g toàn ánh nên $g(A) = B$.

So the three properties are equivalent. For the consequence: a bijection g from A onto B gives $|A| = |g(A)| = |B|$, since g is injective (so $|g(A)| = |A|$) and surjective (so $g(A) = B$). ■

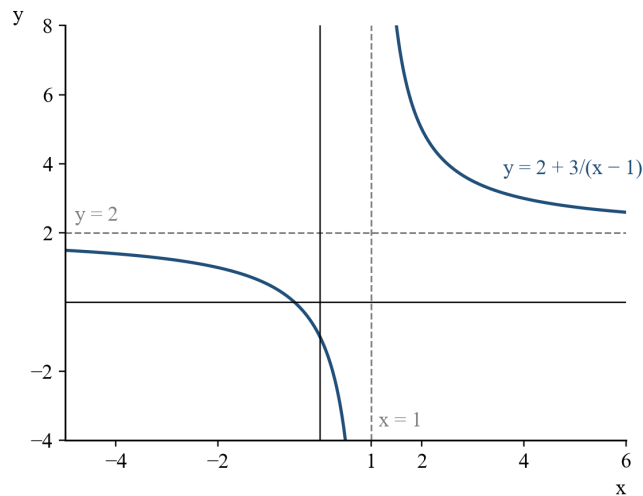
NHẬN XÉT / REMARK — Định lý 1.11 sai cho tập vô hạn: $n \mapsto n + 1$ trên $\mathbb{Z}^+$ là đơn ánh nhưng không toàn ánh (không nhận giá trị 1). Mọi lập luận “đơn ánh nên toàn ánh” phải ghi rõ tập hữu hạn và hai tập cùng cỡ.

Theorem 1.11 fails for infinite sets: $n \mapsto n + 1$ on $\mathbb{Z}^+$ is injective but not surjective (it never takes the value 1). Every argument “injective, hence surjective” must state that the sets are finite and of equal size.



Hình 1.2. Trái: ánh xạ đơn ánh nhưng không toàn ánh (phần tử 3 không được nhận). Phải: ánh xạ toàn ánh nhưng không đơn ánh (a và b cùng ảnh 1).

Figure 1.2. Left: an injective map that is not surjective (element 3 is never hit). Right: a surjective map that is not injective (a and b share the image 1).



Hình 1.3. Đồ thị $y = (2x + 1)/(x - 1) = 2 + 3/(x - 1)$: mỗi đường ngang $y = c$ với $c \neq 2$ cắt đồ thị đúng một điểm, đường $y = 2$ không cắt.

Figure 1.3. Graph of $y = (2x + 1)/(x - 1) = 2 + 3/(x - 1)$: each horizontal line $y = c$ with $c \neq 2$ meets the graph exactly once; the line $y = 2$ never does.

VÍ DỤ 1.5 (Chứng minh song ánh) / EXAMPLE 1.5 (Proving bijectivity) — Cho $X = \mathbb{R} \setminus \{1\}$ và $Y = \mathbb{R} \setminus \{2\}$, $f(x) = (2x + 1)/(x - 1)$. Chứng minh f là song ánh từ X lên Y và tìm ánh xạ ngược.

Let $X = \mathbb{R} \setminus \{1\}$, $Y = \mathbb{R} \setminus \{2\}$ and $f(x) = (2x + 1)/(x - 1)$. Prove that f is a bijection from X onto Y and find the inverse.

Lời giải. / Solution.

1. Giá trị thuộc Y : $f(x) = 2 + 3/(x - 1)$ và $3/(x - 1) \neq 0$ nên $f(x) \neq 2$.
Values lie in Y : $f(x) = 2 + 3/(x - 1)$ and $3/(x - 1) \neq 0$, so $f(x) \neq 2$.
2. Đơn ánh. Giả sử $f(a) = f(b)$ với $a, b \in X$. Khi đó $3/(a - 1) = 3/(b - 1)$, suy ra $a - 1 = b - 1$, tức $a = b$.
Injective. Suppose $f(a) = f(b)$ with $a, b \in X$. Then $3/(a - 1) = 3/(b - 1)$, so $a - 1 = b - 1$, that is $a = b$.
3. Toàn ánh. Lấy $y \in Y$. Đặt $x = (y + 1)/(y - 2)$, có nghĩa vì $y \neq 2$. Khi đó $x - 1 = 3/(y - 2) \neq 0$ nên $x \in X$, và $f(x) = 2 + 3/(x - 1) = 2 + (y - 2) = y$.
Surjective. Take $y \in Y$. Put $x = (y + 1)/(y - 2)$, defined since $y \neq 2$. Then $x - 1 = 3/(y - 2) \neq 0$, so $x \in X$, and $f(x) = 2 + 3/(x - 1) = 2 + (y - 2) = y$.

Vậy f là song ánh từ X lên Y , ánh xạ ngược $f^{-1}(y) = (y + 1)/(y - 2)$ với $y \neq 2$.

Hence f is a bijection from X onto Y with inverse $f^{-1}(y) = (y + 1)/(y - 2)$ for $y \neq 2$. ■

LỖI HAY GẶP / COMMON MISTAKE — Chứng minh toàn ánh bằng cách giải phương trình $f(x) = y$ rồi không kiểm tra nghiệm x tìm được có thuộc tập xác định hay không. Ở Ví dụ 1.5, nếu bỏ qua $x \neq 1$ thì không biết $y = 2$ phải bị loại.

Proving surjectivity by solving $f(x) = y$ and not checking that the solution x lies in the domain. In Example 1.5, ignoring $x \neq 1$ hides why $y = 2$ must be excluded.

1.5. Chứng minh trực tiếp, bằng phản đảo và bằng phản chứng — Direct proof, contrapositive and contradiction

Chứng minh trực tiếp đi từ giả thiết tới kết luận bằng các suy luận liên tiếp; với số nguyên, kỹ thuật chính là xét số dư và phân tích thành nhân tử. Chứng minh bằng phản đảo thay $P \Rightarrow Q$ bằng $(\neg Q) \Rightarrow (\neg P)$, hợp lệ theo Định lý 1.5. Chứng minh phản chứng giả sử điều cần chứng minh sai, rồi suy ra một điều vô lý; điều vô lý có thể là trái giả thiết, trái một sự thật đã biết, hoặc tự mâu thuẫn.

A direct proof runs from the hypotheses to the conclusion through successive deductions; for integers the main tools are residues and factorisation. A proof by contrapositive replaces $P \Rightarrow Q$ by $(\neg Q) \Rightarrow (\neg P)$, which is legitimate by Theorem 1.5. A proof by contradiction assumes the claim is false and derives an absurdity: a clash with a hypothesis, with a known fact, or with itself.

VÍ DỤ 1.6 (Xét số dư) / EXAMPLE 1.6 (Case analysis by residues) — Cho các số nguyên a, b . Chứng minh rằng nếu $a^2 + b^2$ chia hết cho 3 thì cả a và b đều chia hết cho 3.

Let a, b be integers. Prove that if $a^2 + b^2$ is divisible by 3 then both a and b are divisible by 3.

Lời giải. / Solution.

1. Bình phương của một số nguyên chia 3 dư 0 hoặc 1: $n = 3k$ cho $n^2 = 9k^2 \equiv 0$; $n = 3k \pm 1$ cho $n^2 = 9k^2 \pm 6k + 1 \equiv 1 \pmod{3}$.
A square leaves remainder 0 or 1 on division by 3: $n = 3k$ gives $n^2 = 9k^2 \equiv 0$; $n = 3k \pm 1$ gives $n^2 = 9k^2 \pm 6k + 1 \equiv 1 \pmod{3}$.

2. Xét tổng $a^2 + b^2$ theo các dư của hai bình phương: $0 + 0 \equiv 0, 0 + 1 \equiv 1, 1 + 0 \equiv 1, 1 + 1 \equiv 2 \pmod{3}$. Chỉ trường hợp đầu cho tổng chia hết cho 3.

Add the residues of the two squares: $0 + 0 \equiv 0, 0 + 1 \equiv 1, 1 + 0 \equiv 1, 1 + 1 \equiv 2 \pmod{3}$.

Only the first case gives a sum divisible by 3.

Vậy $a^2 \equiv b^2 \equiv 0 \pmod{3}$, tức $3 \mid a^2$ và $3 \mid b^2$, nên $3 \mid a$ và $3 \mid b$ (vì nếu n không chia hết cho 3 thì n^2 chia 3 dư 1).

Hence $a^2 \equiv b^2 \equiv 0 \pmod{3}$, so $3 \mid a^2$ and $3 \mid b^2$, and therefore $3 \mid a$ and $3 \mid b$ (a number not divisible by 3 has a square leaving remainder 1). ■

VÍ DỤ 1.7 (Phản đảo) / EXAMPLE 1.7 (Contrapositive) — Cho số nguyên dương n . Chứng minh rằng nếu $n^2 - 1$ không chia hết cho 8 thì n là số chẵn.

Let n be a positive integer. Prove that if $n^2 - 1$ is not divisible by 8 then n is even.

Lời giải. / Solution.

1. Chứng minh phản đảo: nếu n lẻ thì $8 \nmid n^2 - 1$. Cách này tiện vì giả thiết “ n lẻ” cho được dạng tường minh, còn giả thiết gốc “không chia hết” thì không.

Prove the contrapositive: if n is odd then $8 \nmid n^2 - 1$. This is convenient because “ n is odd” gives an explicit form, whereas the original hypothesis “not divisible” does not.

2. Nếu n lẻ, $n = 2k + 1$ với k nguyên, $k \geq 0$. Khi đó $n^2 - 1 = 4k^2 + 4k = 4k(k + 1)$.

If n is odd, $n = 2k + 1$ with k an integer, $k \geq 0$. Then $n^2 - 1 = 4k^2 + 4k = 4k(k + 1)$.

3. Trong hai số nguyên liên tiếp k và $k + 1$ có một số chẵn nên $k(k + 1)$ chia hết cho 2, suy ra $4k(k + 1)$ chia hết cho 8.

Of the consecutive integers k and $k + 1$ one is even, so $2 \mid k(k + 1)$, and hence $8 \mid 4k(k + 1)$.

Vậy phản đảo đúng, và theo Định lý 1.5 mệnh đề đã cho đúng.

So the contrapositive holds, and by Theorem 1.5 the given statement is true. ■

BỔ ĐỀ 1.12 (Ước nguyên tố, bổ đề Euclid) / LEMMA 1.12 (Prime divisor, Euclid’s lemma) — Mọi số nguyên $n > 1$ đều có ước nguyên tố. Hơn nữa, nếu p là số nguyên tố và $p \mid ab$ thì $p \mid a$ hoặc $p \mid b$ (bổ đề Euclid).

Every integer $n > 1$ has a prime divisor. Moreover, if p is a prime and $p \mid ab$ then $p \mid a$ or $p \mid b$ (Euclid’s lemma).

Chứng minh. / Proof.

Tập các ước lớn hơn 1 của n khác rỗng (chứa n), nên theo nguyên lý sắp thứ tự tốt (Mục 1.6) có phần tử nhỏ nhất d . Nếu d có ước e với $1 < e < d$ thì e cũng là ước của n nhỏ hơn d , vô lý. Vậy d nguyên tố.

The set of divisors of n exceeding 1 is non-empty (it contains n), so by the well-ordering principle (Section 1.6) it has a least element d . If d had a divisor e with $1 < e < d$ then e would be a smaller divisor of n , absurd. So d is prime.

Bổ đề Euclid: giả sử $p \mid ab$ và $p \nmid a$. Vì p nguyên tố nên ước chung lớn nhất của p và a bằng 1, theo định lý Bézout có các số nguyên u, v với $up + va = 1$. Nhân với b : $upb + vab = b$. Cả hai số hạng bên trái chia hết cho p , nên $p \mid b$. Định lý Bézout dùng ở đây được chứng minh trong chương về chia hết, ƯCLN và số nguyên tố.

Euclid's lemma: suppose $p \mid ab$ and $p \nmid a$. Since p is prime, $\gcd(p, a) = 1$, and by Bézout's theorem there are integers u, v with $up + va = 1$. Multiplying by b : $upb + vab = b$. Both terms on the left are divisible by p , so $p \mid b$. Bézout's theorem used here is proved in the chapter on divisibility, gcd and primes. ■

ĐỊNH LÝ 1.13 (Tính vô tỉ của $\sqrt{2}$) / THEOREM 1.13 (Irrationality of $\sqrt{2}$) — Số $\sqrt{2}$ là số vô tỉ.

The number $\sqrt{2}$ is irrational.

Chứng minh. / Proof.

Giả sử $\sqrt{2} = p/q$ với p, q nguyên dương và phân số p/q tối giản (ước chung lớn nhất của p và q bằng 1).

Suppose $\sqrt{2} = p/q$ with p, q positive integers and p/q in lowest terms ($\gcd(p, q) = 1$).

Bình phương: $p^2 = 2q^2$, nên p^2 chẵn. Nếu p lẻ thì p^2 lẻ, nên p chẵn: $p = 2r$.

Squaring: $p^2 = 2q^2$, so p^2 is even. If p were odd then p^2 would be odd, so p is even: $p = 2r$.

Thay vào: $4r^2 = 2q^2$, tức $q^2 = 2r^2$, nên q chẵn theo cùng lập luận. Khi đó 2 là ước chung của p và q , mâu thuẫn với $\gcd(p, q) = 1$. Vậy $\sqrt{2}$ vô tỉ.

Substituting: $4r^2 = 2q^2$, that is $q^2 = 2r^2$, so q is even by the same argument. Then 2 is a common divisor of p and q , contradicting $\gcd(p, q) = 1$. Hence $\sqrt{2}$ is irrational. ■

ĐỊNH LÝ 1.14 (Định lý Euclid về số nguyên tố) / THEOREM 1.14 (Euclid's theorem on primes) — Có vô hạn số nguyên tố.

There are infinitely many primes.

Chứng minh. / Proof.

Giả sử chỉ có hữu hạn số nguyên tố $p_1, p_2, \dots, p_k$. Đặt $N = p_1 p_2 \dots p_k + 1 > 1$.

Suppose there are only finitely many primes $p_1, p_2, \dots, p_k$. Put $N = p_1 p_2 \dots p_k + 1 > 1$.

Theo Bổ đề 1.12, N có ước nguyên tố q . Vì mọi số nguyên tố đều nằm trong danh sách, $q = p_i$ với một i nào đó.

By Lemma 1.12, N has a prime divisor q . Every prime is in the list, so $q = p_i$ for some i .

Khi đó q chia hết cả N lẫn tích $p_1 \dots p_k$, nên q chia hết hiệu của chúng là 1, vô lý vì $q \geq 2$. Vậy có vô hạn số nguyên tố.

Then q divides both N and the product $p_1 \dots p_k$, hence their difference 1, absurd since $q \geq 2$. So there are infinitely many primes. ■

PHÂN TÍCH / ANALYSIS — Trực tiếp thì chỉ có một số hữu tỉ $r = \sqrt{2} + \sqrt{3}$ để dùng. Giả sử r hữu tỉ rồi tìm một biểu thức hữu tỉ khác chứa riêng $\sqrt{3}$ hoặc riêng $\sqrt{2}$. Biểu thức liên hợp $1/r = \sqrt{3} - \sqrt{2}$ là lối ra: r và $1/r$ cho hai phương trình bậc nhất với hai ẩn $\sqrt{2}, \sqrt{3}$.

Directly there is only the number $r = \sqrt{2} + \sqrt{3}$ to work with. Assume r is rational and look for another rational expression that isolates $\sqrt{3}$ or $\sqrt{2}$. The conjugate $1/r = \sqrt{3} - \sqrt{2}$ is the way out: r and $1/r$ give two linear equations in the two unknowns $\sqrt{2}, \sqrt{3}$.

VÍ DỤ 1.8 (Phản chứng với liên hợp) / EXAMPLE 1.8 (Contradiction with the conjugate) — Chứng minh $\sqrt{2} + \sqrt{3}$ là số vô tỉ.

Prove that $\sqrt{2} + \sqrt{3}$ is irrational.

Lời giải. / Solution.

1. Trước hết $\sqrt{3}$ vô tỉ. Giả sử $\sqrt{3} = p/q$ tối giản, p, q nguyên dương. Khi đó $p^2 = 3q^2$, nên $3 \mid p^2$, theo bổ đề Euclid $3 \mid p$, $p = 3r$. Suy ra $9r^2 = 3q^2$, $q^2 = 3r^2$, nên $3 \mid q$. Hai số p, q cùng chia hết cho 3, mâu thuẫn tính tối giản.

First, $\sqrt{3}$ is irrational. Suppose $\sqrt{3} = p/q$ in lowest terms, p, q positive integers. Then $p^2 = 3q^2$, so $3 \mid p^2$, and by Euclid's lemma $3 \mid p$, $p = 3r$. It follows that $9r^2 = 3q^2$, $q^2 = 3r^2$, so $3 \mid q$. Both p and q are divisible by 3, contradicting lowest terms.

2. Giả sử $s = \sqrt{2} + \sqrt{3}$ là số hữu tỉ; rõ ràng $s > 0$. Do $(\sqrt{3} - \sqrt{2})(\sqrt{3} + \sqrt{2}) = 3 - 2 = 1$ nên $\sqrt{3} - \sqrt{2} = 1/s$ cũng hữu tỉ.

Suppose $s = \sqrt{2} + \sqrt{3}$ is rational; clearly $s > 0$. Since $(\sqrt{3} - \sqrt{2})(\sqrt{3} + \sqrt{2}) = 3 - 2 = 1$, the number $\sqrt{3} - \sqrt{2} = 1/s$ is also rational.

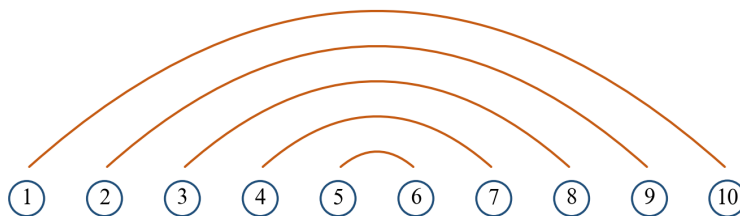
3. Cộng s và $1/s$: $s + 1/s = 2\sqrt{3}$, nên $\sqrt{3} = (s + 1/s)/2$ là số hữu tỉ, mâu thuẫn với bước 1.

Adding s and $1/s$: $s + 1/s = 2\sqrt{3}$, so $\sqrt{3} = (s + 1/s)/2$ would be rational, contradicting step 1.

Vậy $\sqrt{2} + \sqrt{3}$ là số vô tỉ.

Hence $\sqrt{2} + \sqrt{3}$ is irrational. ■

mỗi cung nối hai số có tổng 11



Hình 1.4. Năm cặp có tổng 11 chia tập $\{1, \dots, 10\}$; sáu số được chọn buộc có hai số trong cùng một cặp.

Figure 1.4. Five pairs with sum 11 split $\{1, \dots, 10\}$; six chosen numbers force two into the same pair.

PHÂN TÍCH / ANALYSIS — Con số 11 xuất hiện vì $1 + 10 = 2 + 9 = \dots = 5 + 6$. Mười số chia thành năm cặp “bù nhau”. Chọn sáu số mà không có hai số nào cùng cặp thì cần ít nhất sáu cặp. Đây là phản chứng gắn với phép đếm: giả sử không có hai số nào có tổng 11 rồi đếm tối đa số phần tử chọn được.

The number 11 appears because $1 + 10 = 2 + 9 = \dots = 5 + 6$. The ten numbers split into five complementary pairs. Six chosen numbers with no two in one pair would need at least six pairs. This is contradiction tied to counting: assume no two numbers sum to 11 and count the largest possible selection.

VÍ DỤ 1.9 (Phản chứng và đếm) / EXAMPLE 1.9 (Contradiction and counting) — Chọn sáu số nguyên phân biệt từ tập $\{1, 2, \dots, 10\}$. Chứng minh rằng trong sáu số đó có hai số có

tổng bằng 11. Khẳng định còn đúng khi chỉ chọn năm số không?

Choose six distinct integers from $\{1, 2, \dots, 10\}$. Prove that two of them have sum 11. Does the claim remain true if only five numbers are chosen?

Lời giải. / Solution.

1. Chia tập thành năm cặp $P_i = \{i, 11 - i\}$, $i = 1, \dots, 5$: $\{1, 10\}$, $\{2, 9\}$, $\{3, 8\}$, $\{4, 7\}$, $\{5, 6\}$. Mỗi số của tập thuộc đúng một cặp, và hai số trong cùng một cặp có tổng 11.
Split the set into five pairs $P_i = \{i, 11 - i\}$, $i = 1, \dots, 5$: $\{1, 10\}$, $\{2, 9\}$, $\{3, 8\}$, $\{4, 7\}$, $\{5, 6\}$. Each element lies in exactly one pair, and the two numbers in one pair sum to 11.
2. Giả sử trong sáu số được chọn không có hai số nào tổng 11. Khi đó mỗi cặp chứa nhiều nhất một số được chọn, nên số số được chọn nhiều nhất là 5, mâu thuẫn với 6.
Suppose no two of the six chosen numbers sum to 11. Then each pair contains at most one chosen number, so at most 5 numbers are chosen, contradicting 6.
3. Với năm số: $\{1, 2, 3, 4, 5\}$ không có hai số nào tổng 11 (tổng lớn nhất là $4 + 5 = 9$), nên khẳng định sai.
With five numbers: $\{1, 2, 3, 4, 5\}$ has no two numbers with sum 11 (the largest sum is $4 + 5 = 9$), so the claim fails.

Vậy sáu số luôn có hai số tổng 11, và con số sáu là nhỏ nhất có tính chất này.

Hence any six numbers contain two with sum 11, and six is the least number with this property.

NHẬN XÉT / REMARK — Phản chứng chỉ dùng khi phủ định của kết luận cho thêm một dữ kiện có ích (như “tối giản”, “ N là tích của mọi số nguyên tố”). Nếu lập luận cuối chỉ là chứng minh trực tiếp nằm giữa hai câu “giả sử” và “mâu thuẫn”, hãy viết lại bằng chứng minh trực tiếp.

Use contradiction only when negating the conclusion hands you a useful extra fact (such as “lowest terms” or “ N is built from all the primes”). If the argument is just a direct proof sandwiched between “suppose” and “contradiction”, rewrite it as a direct proof.

LỖI HAY GẶP / COMMON MISTAKE — Phản chứng $\sqrt{2}$ mà quên nêu giả thiết p/q tối giản: khi đó “ p và q cùng chẵn” không mâu thuẫn với điều gì.

Proving $\sqrt{2}$ irrational by contradiction without stating that p/q is in lowest terms: “ p and q are both even” then contradicts nothing.

LỖI HAY GẶP / COMMON MISTAKE — Phủ định sai kết luận khi phản chứng. Phủ định của “tồn tại nghiệm nguyên dương” là “không có nghiệm nguyên dương nào”, không phải “mọi nghiệm đều âm”.

Negating the conclusion wrongly in a proof by contradiction. The negation of “a positive integer solution exists” is “no positive integer solution exists”, not “every solution is negative”.

1.6. Quy nạp và nguyên lý sắp thứ tự tốt — Induction and the well-ordering principle

ĐỊNH NGHĨA 1.15 (Nguyên lý sắp thứ tự tốt) / DEFINITION 1.15 (Well-ordering principle) — Nguyên lý sắp thứ tự tốt: mọi tập con khác rỗng của tập các số tự nhiên $\mathbb{N} = \{0, 1, 2, \dots\}$ đều có số nhỏ nhất.

$1, 2, \dots\}$ đều có phần tử nhỏ nhất. Đây là tính chất cơ bản của số tự nhiên và được thừa nhận; mọi dạng quy nạp trong mục này được suy ra từ nó.

The well-ordering principle: every non-empty subset of the natural numbers $\mathbb{N} = \{0, 1, 2, \dots\}$ has a least element. It is a basic property of the natural numbers and is taken as given; every form of induction below follows from it.

Quy nạp giống một hàng quân cờ domino: bước cơ sở đẩy quân đầu tiên, bước quy nạp bảo đảm quân nào đổ thì quân kế tiếp đổ. Thiếu một trong hai thì hàng không đổ hết.

Induction works like a row of dominoes: the base case tips the first one, the inductive step guarantees that whenever one falls the next falls too. Without either, the row does not all fall.

ĐỊNH LÝ 1.16 (Nguyên lý quy nạp) / THEOREM 1.16 (Principle of induction) — Quy nạp thường. Cho $P(n)$ là một mệnh đề với n là số nguyên $n \geq n_0$. Nếu (i) $P(n_0)$ đúng (bước cơ sở) và (ii) với mọi $k \geq n_0$, $P(k)$ đúng kéo theo $P(k+1)$ đúng (bước quy nạp), thì $P(n)$ đúng với mọi $n \geq n_0$.

Ordinary induction. Let $P(n)$ be a statement about an integer $n \geq n_0$. If (i) $P(n_0)$ is true (base case) and (ii) for every $k \geq n_0$, $P(k)$ true implies $P(k+1)$ true (inductive step), then $P(n)$ is true for all $n \geq n_0$.

Chứng minh. / Proof.

Giả sử kết luận sai. Tập S các số $n \geq n_0$ mà $P(n)$ sai khác rỗng, nên theo Định nghĩa 1.15 có phần tử nhỏ nhất m .

Suppose the conclusion fails. The set S of integers $n \geq n_0$ for which $P(n)$ is false is non-empty, so by Definition 1.15 it has a least element m .

Theo (i), $m \neq n_0$, nên $m-1 \geq n_0$. Do m nhỏ nhất trong S nên $P(m-1)$ đúng. Theo (ii) với $k = m-1$, $P(m)$ đúng, mâu thuẫn với $m \in S$. Vậy S rỗng.

By (i), $m \neq n_0$, so $m-1 \geq n_0$. As m is least in S , $P(m-1)$ is true. By (ii) with $k = m-1$, $P(m)$ is true, contradicting $m \in S$. So S is empty. ■

ĐỊNH LÝ 1.17 (Quy nạp mạnh) / THEOREM 1.17 (Strong induction) — Quy nạp mạnh (nhiều cơ sở). Cho $r \geq 1$. Nếu $P(n_0), P(n_0+1), \dots, P(n_0+r-1)$ đều đúng (r bước cơ sở), và với mọi $k \geq n_0+r$, từ giả thiết $P(m)$ đúng với mọi m có $n_0 \leq m < k$ suy ra $P(k)$ đúng, thì $P(n)$ đúng với mọi $n \geq n_0$.

Strong induction (several base cases). Let $r \geq 1$. If $P(n_0), P(n_0+1), \dots, P(n_0+r-1)$ are all true (r base cases), and for every $k \geq n_0+r$, the truth of $P(m)$ for all m with $n_0 \leq m < k$ implies $P(k)$, then $P(n)$ is true for all $n \geq n_0$.

Chứng minh. / Proof.

Đặt $Q(n)$: “ $P(m)$ đúng với mọi m có $n_0 \leq m \leq n$ ”. Ta chứng minh $Q(n)$ đúng với $n \geq n_0+r-1$ bằng quy nạp thường (Định lý 1.16).

Let $Q(n)$ be: “ $P(m)$ is true for all m with $n_0 \leq m \leq n$ ”. We prove $Q(n)$ for $n \geq n_0+r-1$ by ordinary induction (Theorem 1.16).

Cơ sở: $Q(n_0+r-1)$ đúng vì đó chính là r bước cơ sở. Bước quy nạp: nếu $Q(k-1)$ đúng với $k \geq n_0+r$ thì $P(m)$ đúng với mọi $n_0 \leq m < k$, nên theo giả thiết $P(k)$ đúng, suy ra $Q(k)$ đúng.

Base: $Q(n_0 + r - 1)$ holds, being exactly the r base cases. Step: if $Q(k - 1)$ holds for some $k \geq n_0 + r$ then $P(m)$ holds for every $n_0 \leq m < k$, so $P(k)$ holds by hypothesis and $Q(k)$ follows.

Mọi $P(n)$ với $n \geq n_0$ nằm trong một $Q(n)$ nên đúng.

Every $P(n)$ with $n \geq n_0$ sits inside some $Q(n)$, so it is true. ■

ĐỊNH LÝ 1.18 (Quy nạp Cauchy) / THEOREM 1.18 (Cauchy induction) — Quy nạp Cauchy (tiến – lùi). Cho $P(n)$ là mệnh đề với số nguyên $n \geq 2$. Nếu (i) $P(2)$ đúng; (ii) với mọi $n \geq 2$, $P(n)$ đúng kéo theo $P(2n)$ đúng; (iii) với mọi $n \geq 3$, $P(n)$ đúng kéo theo $P(n - 1)$ đúng; thì $P(n)$ đúng với mọi $n \geq 2$.

Cauchy induction (forward–backward). Let $P(n)$ be a statement about integers $n \geq 2$. If (i) $P(2)$ is true; (ii) for every $n \geq 2$, $P(n)$ implies $P(2n)$; (iii) for every $n \geq 3$, $P(n)$ implies $P(n - 1)$; then $P(n)$ is true for all $n \geq 2$.

Chứng minh. / Proof.

Từ (i) và (ii), bằng quy nạp thường theo k : $P(2^k)$ đúng với mọi $k \geq 1$ ($P(2^k)$ kéo theo $P(2^{k+1})$).

From (i) and (ii), by ordinary induction on k : $P(2^k)$ is true for all $k \geq 1$ ($P(2^k)$ implies $P(2^{k+1})$).

Với $n \geq 2$ bất kỳ, chọn k sao cho $2^k \geq n$. $P(2^k)$ đúng; áp dụng (iii) liên tiếp với $2^k, 2^k - 1, \dots, n + 1$ (đều ≥ 3) ta nhận $P(2^k - 1), \dots, P(n)$ đúng.

For any $n \geq 2$ choose k with $2^k \geq n$. $P(2^k)$ is true; applying (iii) successively at $2^k, 2^k - 1, \dots, n + 1$ (all ≥ 3) yields $P(2^k - 1), \dots, P(n)$. ■

PHẢI THUỘC / MEMORISE — Lời giải quy nạp gồm bốn phần viết riêng: phát biểu $P(n)$; bước cơ sở (với mọi giá trị đầu cần thiết); giả thiết quy nạp; chứng minh bước quy nạp có dùng giả thiết; kết luận.

An induction write-up has separate parts: state $P(n)$; the base case (every starting value needed); the inductive hypothesis; the inductive step, visibly using the hypothesis; the conclusion.

VÍ DỤ 1.10 (Quy nạp thường) / EXAMPLE 1.10 (Ordinary induction) — Chứng minh rằng với mọi số nguyên dương n : $1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + \dots + n \cdot 2^n = (n - 1) \cdot 2^{n+1} + 2$.

Prove that for every positive integer n : $1 \cdot 2^1 + 2 \cdot 2^2 + 3 \cdot 2^3 + \dots + n \cdot 2^n = (n - 1) \cdot 2^{n+1} + 2$.

Lời giải. / Solution.

1. Gọi $P(n)$ là đẳng thức đã cho. Cơ sở $n = 1$: vế trái bằng $1 \cdot 2 = 2$, vế phải bằng $0 \cdot 4 + 2 = 2$. $P(1)$ đúng.

Let $P(n)$ be the stated identity. Base $n = 1$: the left side is $1 \cdot 2 = 2$, the right side is $0 \cdot 4 + 2 = 2$. $P(1)$ holds.

2. Giả thiết $P(k)$ đúng với một $k \geq 1$: $1 \cdot 2^1 + \dots + k \cdot 2^k = (k - 1) \cdot 2^{k+1} + 2$.

Hypothesis: $P(k)$ holds for some $k \geq 1$: $1 \cdot 2^1 + \dots + k \cdot 2^k = (k - 1) \cdot 2^{k+1} + 2$.

3. Cộng $(k + 1) \cdot 2^{k+1}$ vào hai vế: vế phải trở thành $(k - 1) \cdot 2^{k+1} + 2 + (k + 1) \cdot 2^{k+1} = 2k \cdot 2^{k+1} + 2 = k \cdot 2^{k+2} + 2$.

Add $(k + 1) \cdot 2^{k+1}$ to both sides: the right side becomes $(k - 1) \cdot 2^{k+1} + 2 + (k + 1) \cdot 2^{k+1} = 2k \cdot 2^{k+1} + 2 = k \cdot 2^{k+2} + 2$.

Đó chính là vế phải của $P(k+1)$, vì $((k+1)-1) \cdot 2^{(k+1)+1} + 2 = k \cdot 2^{k+2} + 2$. Theo nguyên lý quy nạp, đẳng thức đúng với mọi $n \geq 1$.

That is exactly the right side of $P(k+1)$, because $((k+1)-1) \cdot 2^{(k+1)+1} + 2 = k \cdot 2^{k+2} + 2$. By induction the identity holds for all $n \geq 1$. ■

PHÂN TÍCH / ANALYSIS — Hệ thức truy hồi nối a_{n+2} với hai số hạng trước, nên bước quy nạp cần cả $P(n)$ lẫn $P(n+1)$. Vì thế bước cơ sở phải kiểm hai giá trị $n=1$ và $n=2$. Kiểm một giá trị là thiếu, và là lỗi mất điểm kinh điển.

The recurrence ties a_{n+2} to the two previous terms, so the inductive step needs both $P(n)$ and $P(n+1)$. The base case must therefore check two values, $n=1$ and $n=2$. Checking one is not enough, and it is the classic way to lose marks.

VÍ DỤ 1.11 (Quy nạp hai bước) / EXAMPLE 1.11 (Two-step induction) — Cho dãy $a_1 = 1, a_2 = 5, a_{n+2} = 5a_{n+1} - 6a_n$ với $n \geq 1$. Chứng minh $a_n = 3^n - 2^n$ với mọi số nguyên dương n .

The sequence satisfies $a_1 = 1, a_2 = 5, a_{n+2} = 5a_{n+1} - 6a_n$ for $n \geq 1$. Prove that $a_n = 3^n - 2^n$ for every positive integer n .

Lời giải. / Solution.

1. Cơ sở: $a_1 = 1 = 3 - 2$ và $a_2 = 5 = 9 - 4$. Hai giá trị đầu đúng.

Base: $a_1 = 1 = 3 - 2$ and $a_2 = 5 = 9 - 4$. The first two values hold.

2. Giả thiết: $a_k = 3^k - 2^k$ và $a_{k+1} = 3^{k+1} - 2^{k+1}$ với một $k \geq 1$.

Hypothesis: $a_k = 3^k - 2^k$ and $a_{k+1} = 3^{k+1} - 2^{k+1}$ for some $k \geq 1$.

3. Khi đó $a_{k+2} = 5(3^{k+1} - 2^{k+1}) - 6(3^k - 2^k) = 3^k(15 - 6) - 2^k(10 - 6) = 9 \cdot 3^k - 4 \cdot 2^k = 3^{k+2} - 2^{k+2}$.

Then $a_{k+2} = 5(3^{k+1} - 2^{k+1}) - 6(3^k - 2^k) = 3^k(15 - 6) - 2^k(10 - 6) = 9 \cdot 3^k - 4 \cdot 2^k = 3^{k+2} - 2^{k+2}$.

Vậy công thức đúng cho $n = k+2$ khi đúng cho k và $k+1$; kết hợp hai giá trị đầu, theo quy nạp mạnh (Định lý 1.17 với $r=2$) $a_n = 3^n - 2^n$ với mọi $n \geq 1$.

So the formula holds for $k+2$ whenever it holds for k and $k+1$; with the first two values, strong induction (Theorem 1.17 with $r=2$) gives $a_n = 3^n - 2^n$ for all $n \geq 1$. ■

PHÂN TÍCH / ANALYSIS — Thử các số nhỏ: $4a+7b$ có thể là 0, 4, 7, 8, 11, 12, 14, 15, 16, 18, 19, 20, 21, ... và bỏ qua 17. Sau 17 dường như không còn lỗ hổng. Nếu 18, 19, 20, 21 đều biểu diễn được thì thêm 4 cho ta bốn số kế tiếp, và cứ thế bốn số một lần phủ kín mọi số lớn hơn. Số cơ sở bằng 4 vì bước nhảy là 4.

Try small values: $4a+7b$ can be 0, 4, 7, 8, 11, 12, 14, 15, 16, 18, 19, 20, 21, ... and it skips 17. After 17 there seem to be no more gaps. If 18, 19, 20, 21 are all representable, adding 4 gives the next four numbers, and four at a time covers everything above. There are 4 base cases because the step size is 4.

VÍ DỤ 1.12 (Quy nạp nhiều cơ sở) / EXAMPLE 1.12 (Induction with several base cases) — Chứng minh rằng mọi số nguyên $n \geq 18$ đều viết được dưới dạng $n = 4a + 7b$ với a, b là số nguyên không âm, và 17 không viết được dưới dạng đó.

Prove that every integer $n \geq 18$ can be written as $n = 4a + 7b$ with non-negative integers a, b , and that 17 cannot.

Lời giải. / Solution.

1. Cơ sở (bốn giá trị): $18 = 4 \cdot 1 + 7 \cdot 2$, $19 = 4 \cdot 3 + 7 \cdot 1$, $20 = 4 \cdot 5 + 7 \cdot 0$, $21 = 4 \cdot 0 + 7 \cdot 3$.
Base (four values): $18 = 4 \cdot 1 + 7 \cdot 2$, $19 = 4 \cdot 3 + 7 \cdot 1$, $20 = 4 \cdot 5 + 7 \cdot 0$, $21 = 4 \cdot 0 + 7 \cdot 3$.
2. Bước quy nạp mạnh: với $n \geq 22$, số $n - 4 \geq 18$ nên theo giả thiết $n - 4 = 4a + 7b$. Khi đó $n = 4(a + 1) + 7b$.
Strong step: for $n \geq 22$, the number $n - 4 \geq 18$, so by hypothesis $n - 4 = 4a + 7b$. Then $n = 4(a + 1) + 7b$.
3. Với 17: nếu $17 = 4a + 7b$ thì $b \in \{0, 1, 2\}$ vì $7b \leq 17$. Khi đó $17 - 7b$ bằng 17, 10, 3, không số nào chia hết cho 4.
For 17: if $17 = 4a + 7b$ then $b \in \{0, 1, 2\}$ since $7b \leq 17$. Then $17 - 7b$ equals 17, 10, 3, none divisible by 4.

Vậy mọi $n \geq 18$ biểu diễn được theo Định lý 1.17 ($r = 4$), còn 17 thì không.

Hence every $n \geq 18$ is representable by Theorem 1.17 ($r = 4$), while 17 is not. ■

PHÂN TÍCH / ANALYSIS — Quy nạp từ n lên $n + 1$ khó vì phải thêm một số mà vẫn kiểm soát được tổng. Lùi từ n xuống $n - 1$ dễ hơn: thêm vào $n - 1$ số một số bằng trung bình của chúng thì cả hai vế đổi theo cách tính được. Trường hợp hai số là hằng đẳng thức $(x - y)^2 \geq 0$, và ghép hai nhóm cho bước nhân đôi. Cặp “nhân đôi, lùi một” của Định lý 1.18 phù hợp.
Induction from n to $n + 1$ is hard because a new number must be added while the sum stays under control. Going down from n to $n - 1$ is easier: append to the $n - 1$ numbers one equal to their mean and both sides change in a computable way. Two numbers give the identity $(x - y)^2 \geq 0$, and joining two groups gives the doubling step. The “double, step back” pair of Theorem 1.18 fits.

VÍ DỤ 1.13 (Quy nạp Cauchy) / EXAMPLE 1.13 (Cauchy induction) — Chứng minh rằng với mọi số nguyên $n \geq 2$ và mọi số thực $x_1, x_2, \dots, x_n$: $n(x_1^2 + x_2^2 + \dots + x_n^2) \geq (x_1 + x_2 + \dots + x_n)^2$.
Prove that for every integer $n \geq 2$ and all real numbers $x_1, x_2, \dots, x_n$: $n(x_1^2 + x_2^2 + \dots + x_n^2) \geq (x_1 + x_2 + \dots + x_n)^2$.

Lời giải. / Solution.

1. Gọi $P(n)$ là bất đẳng thức. $P(2)$: $2(x^2 + y^2) - (x + y)^2 = (x - y)^2 \geq 0$.
Let $P(n)$ be the inequality. $P(2)$: $2(x^2 + y^2) - (x + y)^2 = (x - y)^2 \geq 0$.
2. $P(n) \Rightarrow P(2n)$. Chia $2n$ số thành hai nhóm n số có tổng S_1, S_2 và tổng bình phương Q_1, Q_2 . Theo $P(n)$: $nQ_1 \geq S_1^2$, $nQ_2 \geq S_2^2$. Theo $P(2)$ cho hai số S_1, S_2 : $2(S_1^2 + S_2^2) \geq (S_1 + S_2)^2$. Vậy $2n(Q_1 + Q_2) \geq 2(S_1^2 + S_2^2) \geq (S_1 + S_2)^2$, tức $P(2n)$.
 $P(n) \Rightarrow P(2n)$. Split the $2n$ numbers into two groups of n with sums S_1, S_2 and sums of squares Q_1, Q_2 . By $P(n)$: $nQ_1 \geq S_1^2$, $nQ_2 \geq S_2^2$. By $P(2)$ for the two numbers S_1, S_2 : $2(S_1^2 + S_2^2) \geq (S_1 + S_2)^2$. Hence $2n(Q_1 + Q_2) \geq 2(S_1^2 + S_2^2) \geq (S_1 + S_2)^2$, which is $P(2n)$.
3. $P(n) \Rightarrow P(n - 1)$ với $n \geq 3$. Cho $x_1, \dots, x_{n-1}$ có tổng S và $Q = x_1^2 + \dots + x_{n-1}^2$. Đặt $m = S/(n - 1)$ và $x_n = m$. Theo $P(n)$: $n(Q + m^2) \geq (S + m)^2 = (nm)^2$. Chia cho n : $Q + m^2 \geq nm^2$, tức $Q \geq (n - 1)m^2$. Nhân với $n - 1$: $(n - 1)Q \geq (n - 1)^2 m^2 = S^2$, tức $P(n - 1)$.
 $P(n) \Rightarrow P(n - 1)$ for $n \geq 3$. Take $x_1, \dots, x_{n-1}$ with sum S and $Q = x_1^2 + \dots + x_{n-1}^2$. Put $m = S/(n - 1)$ and $x_n = m$. By $P(n)$: $n(Q + m^2) \geq (S + m)^2 = (nm)^2$. Divide by n : $Q + m^2 \geq nm^2$, that is $Q \geq (n - 1)m^2$. Multiply by $n - 1$: $(n - 1)Q \geq (n - 1)^2 m^2 = S^2$, which is $P(n - 1)$.

Ba điều kiện của Định lý 1.18 thỏa mãn, nên bất đẳng thức đúng với mọi $n \geq 2$.

All three conditions of Theorem 1.18 hold, so the inequality is true for every $n \geq 2$. ■

NHẬN XÉT / REMARK — Dấu bằng trong ví dụ 1.13 xảy ra khi và chỉ khi $x_1 = x_2 = \dots = x_n$. Bất đẳng thức này là hệ quả của bất đẳng thức Cauchy–Schwarz (chương Các bất đẳng thức cổ điển) với bộ $(1, \dots, 1)$; cách chứng minh ở đây chỉ dùng phép toán đại số lớp 8 và dùng kỹ thuật tiến – lùi.

Equality in Example 1.13 holds exactly when $x_1 = x_2 = \dots = x_n$. The inequality also follows from the Cauchy–Schwarz inequality (chapter on classical inequalities) with the tuple $(1, \dots, 1)$; the proof here uses only school algebra and uses the forward–backward technique.

PHÂN TÍCH / ANALYSIS — Các hệ số 1, 2, 4 làm tính chẵn lẻ lan ra: x phải chẵn, rồi y chẵn, rồi z chẵn, và chia cả ba số cho 2 thì ra đúng phương trình cũ. Một nghiệm khác 0 sinh ra nghiệm khác 0 nhỏ hơn, mãi mãi. Nguyên lý sắp thứ tự tốt chặn quá trình này: lấy nghiệm có $|x| + |y| + |z|$ nhỏ nhất.

The coefficients 1, 2, 4 make parity spread: x must be even, then y , then z , and halving all three returns the same equation. One non-zero solution produces a smaller non-zero solution, for ever. The well-ordering principle stops this: take the solution with $|x| + |y| + |z|$ least.

VÍ DỤ 1.14 (Lùi vô hạn) / EXAMPLE 1.14 (Infinite descent) — Tìm tất cả các bộ số nguyên (x, y, z) thỏa mãn $x^3 + 2y^3 = 4z^3$.

Find all integer triples (x, y, z) satisfying $x^3 + 2y^3 = 4z^3$.

Lời giải. / Solution.

1. Bộ $(0, 0, 0)$ là nghiệm. Giả sử có nghiệm khác $(0, 0, 0)$. Tập các giá trị $|x| + |y| + |z|$ của các nghiệm khác $(0, 0, 0)$ là tập con khác rỗng của $\mathbb{Z}^+$, nên có phần tử nhỏ nhất; lấy nghiệm (x, y, z) đạt giá trị nhỏ nhất đó.
The triple $(0, 0, 0)$ is a solution. Suppose there is a solution other than $(0, 0, 0)$. The values $|x| + |y| + |z|$ over such solutions form a non-empty subset of $\mathbb{Z}^+$, so there is a least one; take a solution (x, y, z) attaining it.
2. $x^3 = 4z^3 - 2y^3$ chẵn nên x chẵn: $x = 2u$. Thay vào: $8u^3 + 2y^3 = 4z^3$, suy ra $y^3 = 2z^3 - 4u^3$ chẵn, nên y chẵn: $y = 2v$.
 $x^3 = 4z^3 - 2y^3$ is even, so x is even: $x = 2u$. Substituting: $8u^3 + 2y^3 = 4z^3$, hence $y^3 = 2z^3 - 4u^3$ is even, so y is even: $y = 2v$.
3. Thay $y = 2v$: $8u^3 + 16v^3 = 4z^3$, suy ra $z^3 = 2u^3 + 4v^3$ chẵn, nên z chẵn: $z = 2w$.
Substituting $y = 2v$: $8u^3 + 16v^3 = 4z^3$, hence $z^3 = 2u^3 + 4v^3$ is even, so z is even: $z = 2w$.
4. Thay $x = 2u, y = 2v, z = 2w$ và chia cho 8: $u^3 + 2v^3 = 4w^3$. Vậy (u, v, w) cũng là nghiệm, khác $(0, 0, 0)$, với $|u| + |v| + |w| = (|x| + |y| + |z|)/2$, nhỏ hơn giá trị nhỏ nhất. Mâu thuẫn.
Substituting $x = 2u, y = 2v, z = 2w$ and dividing by 8: $u^3 + 2v^3 = 4w^3$. So (u, v, w) is also a solution, different from $(0, 0, 0)$, with $|u| + |v| + |w| = (|x| + |y| + |z|)/2$, smaller than the least value. Contradiction.

Vậy phương trình chỉ có nghiệm nguyên $(x, y, z) = (0, 0, 0)$.

Hence the only integer solution is $(x, y, z) = (0, 0, 0)$. ■

NHẬN XÉT / REMARK — Cách lùi vô hạn cũng viết được như quy nạp: chứng minh bằng quy nạp mạnh theo $N = |x| + |y| + |z|$ rằng không có nghiệm khác $(0, 0, 0)$ với tổng bằng N . Hai cách tương đương; chọn cách nào thì viết trọn vẹn cách đó.

Infinite descent can be written as induction too: prove by strong induction on $N = |x| + |y| + |z|$ that no solution other than $(0, 0, 0)$ has total N . The two are equivalent; whichever is chosen, write it out in full.

LỖI HAY GẶP / COMMON MISTAKE — Quy nạp thiếu bước cơ sở: chứng minh “ $2^n > n^2$ với $n \geq 1$ ” bằng bước quy nạp rồi kết luận, trong khi bất đẳng thức sai ở $n = 2, 3, 4$ (với $n = 2, 3, 4$ vế trái là 4, 8, 16 còn vế phải là 4, 9, 16). Bước cơ sở đúng là $n = 5$.

Induction without a base case: proving “ $2^n > n^2$ for $n \geq 1$ ” by the inductive step alone and concluding, although the inequality fails at $n = 2, 3, 4$ (for $n = 2, 3, 4$ the left side is 4, 8, 16 and the right side 4, 9, 16). The right base case is $n = 5$.

LỖI HAY GẶP / COMMON MISTAKE — Bước quy nạp có dùng giả thiết $P(k)$ nhưng ở bước cuối viết “tương tự” hoặc “hiển nhiên” cho đúng phép biến đổi khó nhất. Giám khảo trừ điểm chính chỗ đó.

An inductive step that quotes $P(k)$ but writes “similarly” or “clearly” for exactly the hardest manipulation. The marker deducts at that very place.

LỖI HAY GẶP / COMMON MISTAKE — Quy nạp “chứng minh” rằng mọi con ngựa cùng màu: bước từ n lên $n + 1$ dùng hai nhóm n con ngựa có chung phần tử, nhưng với $n = 1$ hai nhóm không có phần tử chung. Bước quy nạp phải đúng với mọi k kể cả giá trị nhỏ nhất, chứ không riêng các k lớn.

The “proof” by induction that all horses have the same colour: the step from n to $n + 1$ uses two overlapping groups of n horses, but for $n = 1$ the groups do not overlap. The inductive step must hold for every k including the smallest, not only for large k .

PHẢI THUỘC / MEMORISE — Quy nạp mạnh: số cơ sở bằng số bước lùi của hệ thức. Hệ thức dùng $P(n - 1)$, $P(n - 2)$ thì cần hai cơ sở; hệ thức nhảy bước 4 thì cần bốn cơ sở.

Strong induction: the number of base cases equals the number of steps back used by the argument. A relation using $P(n - 1)$ and $P(n - 2)$ needs two bases; a step of size 4 needs four.

1.7. Cách viết một chứng minh được chấm đủ điểm — *How to write a proof that earns full marks*

Thang điểm cho từng ý riêng, nên lời giải đúng nhưng thiếu một ý của thang vẫn mất điểm. Ví dụ sau viết cùng một kết quả theo hai cách.

The marking scheme awards marks for individual ideas, so a correct solution that omits one scheme item still loses marks. The example below writes the same result in two ways.

Bài toán: chứng minh với mọi số nguyên dương n , số $n^3 + 5n$ chia hết cho 6.

Problem: prove that for every positive integer n , the number $n^3 + 5n$ is divisible by 6.

LỖI HAY GẶP / COMMON MISTAKE — Bản viết hỏng: “Với $n = 1$ được 6, $n = 2$ được 18, $n = 3$ được 42, đều chia hết cho 6, nên đúng với mọi n .” Ba giá trị đúng không chứng minh được khẳng định về mọi n (xem Ví dụ 1.3).

A failing write-up: “ $n = 1$ gives 6, $n = 2$ gives 18, $n = 3$ gives 42, all divisible by 6, so it holds for all n .” Three true values do not prove a claim about every n (see Example 1.3).

Chứng minh. / Proof.

Tách $n^3 + 5n = (n^3 - n) + 6n = (n - 1)n(n + 1) + 6n$.

Split $n^3 + 5n = (n^3 - n) + 6n = (n - 1)n(n + 1) + 6n$.

Trong ba số nguyên liên tiếp $n - 1$, n , $n + 1$ có một số chia hết cho 3 và có ít nhất một số chẵn, nên tích chia hết cho 2 và cho 3. Vì 2 và 3 nguyên tố cùng nhau, tích chia hết cho 6.

Among the three consecutive integers $n - 1$, n , $n + 1$ one is divisible by 3 and at least one is even, so the product is divisible by 2 and by 3. Since 2 and 3 are coprime, the product is divisible by 6.

Số hạng $6n$ chia hết cho 6, nên tổng $(n - 1)n(n + 1) + 6n$ chia hết cho 6. Vậy $n^3 + 5n$ chia hết cho 6 với mọi số nguyên dương n .

The term $6n$ is divisible by 6, so the sum $(n - 1)n(n + 1) + 6n$ is divisible by 6. Hence $n^3 + 5n$ is divisible by 6 for every positive integer n . ■

Năm việc làm trước khi nộp bài chứng minh:

Five checks before handing in a proof:

- Nêu rõ cái được phép dùng (giả thiết) và cái cần chứng minh; với bài có lượng từ, viết lại bằng ký hiệu $\forall$, $\exists$ để không đổi nghĩa.

State what may be used (hypotheses) and what is to be proved; for quantified claims, rewrite with $\forall$, $\exists$ so the meaning does not drift.

- Khai báo phương pháp ngay từ đầu: “Chứng minh bằng phản chứng”, “Quy nạp theo n ”. Giám khảo đọc nhanh hơn và biết tìm bước cơ sở ở đâu.

Announce the method at the start: “Proof by contradiction”, “Induction on n ”. The marker reads faster and knows where to look for the base case.

- Mỗi dòng suy ra từ dòng trước hoặc từ giả thiết; ghi lý do cạnh dòng nếu lý do không hiển nhiên (bổ đề Euclid, bình phương không âm, tính phân phối).

Each line follows from an earlier line or a hypothesis; write the reason beside the line when it is not obvious (Euclid’s lemma, squares are non-negative, distributivity).

- Kiểm các điểm kỳ dị: chia cho biểu thức có thể bằng 0, căn của số âm, lấy ngược bất đẳng thức khi nhân với số âm, các trường hợp bị bỏ sót.

Check the singular points: division by an expression that may vanish, roots of negative numbers, reversing an inequality when multiplying by a negative, missed cases.

- Kết thúc bằng câu kết luận trả lời đúng câu hỏi của đề: “Vậy mọi nghiệm là ...”, “Vậy giá trị nhỏ nhất bằng ...”.

End with a conclusion that answers the question actually asked: “Hence all solutions are ...”, “Hence the minimum equals ...”.

Dấu hiệu trong đề <i>Sign in the problem</i>	Phương pháp nên thử <i>Method to try</i>	Ví dụ <i>Example</i>
Công thức, đẳng thức hay bất đẳng thức chứa n , đúng với mọi $n \geq n_0$ <i>Formula, identity or inequality containing n, for all $n \geq n_0$</i>	Quy nạp thường <i>Ordinary induction</i>	1.10
Hệ thức truy hồi nối nhiều số hạng, hoặc bước nhảy k <i>Recurrence over several terms, or a jump of size k</i>	Quy nạp mạnh, k cơ sở <i>Strong induction, k base cases</i>	1.11, 1.12
Bất đẳng thức cho n số, dễ làm với 2 số <i>Inequality for n numbers, easy for 2 numbers</i>	Quy nạp Cauchy tiến – lùi <i>Cauchy forward–backward induction</i>	1.13
“Chứng minh không tồn tại”, “vô tỉ”, “vô hạn” <i>“Prove there is no ...”, “irrational”, “infinitely many”</i>	Phản chứng <i>Contradiction</i>	1.8, 1.9
Giả thiết dạng phủ định (“không chia hết”), kết luận dạng tường minh (“ n lẻ”) <i>Negative hypothesis (“not divisible”), explicit conclusion (“n odd”)</i>	Phản đảo <i>Contrapositive</i>	1.7
Phải bác bỏ khẳng định “với mọi” <i>A “for all” claim must be refuted</i>	Phản ví dụ <i>Counterexample</i>	1.3
Số nguyên và bình phương, lập phương, chia hết cho 3, 4, 8 <i>Integers with squares, cubes, divisibility by 3, 4, 8</i>	Xét số dư <i>Residues</i>	1.6
“Ít nhất một trong ba điều kiện”, đếm theo điều kiện chia hết <i>“At least one of three conditions”, counting by divisibility</i>	Bao hàm – loại trừ <i>Inclusion–exclusion</i>	1.4
Phương trình nghiệm nguyên, chẵn lẻ lặp lại sau khi chia 2 hoặc 3 <i>Integer equation whose parity or divisibility repeats after halving or thirding</i>	Lùi vô hạn, sắp thứ tự tốt <i>Infinite descent, well-ordering</i>	1.14

Dấu hiệu trong đề <i>Sign in the problem</i>	Phương pháp nên thử <i>Method to try</i>	Ví dụ <i>Example</i>
Chứng minh hai tập bằng nhau hoặc cùng số phần tử <i>Two sets equal, or of the same size</i>	Hai chiều $\subset$, hoặc song ánh <i>Two inclusions, or a bijection</i>	1.5, 1.9

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Mệnh đề	Statement (proposition)	Câu khẳng định đúng hoặc sai <i>A sentence that is true or false</i>
Lượng từ	Quantifier	$\forall$ (với mọi) và $\exists$ (tồn tại) <i>$\forall$ (for all) and $\exists$ (there exists)</i>
Phủ định	Negation	Mệnh đề đúng khi mệnh đề đã cho sai <i>True exactly when the given statement is false</i>
Kéo theo	Implication	$P \Rightarrow Q$ sai khi P đúng, Q sai <i>$P \Rightarrow Q$ is false only when P is true and Q false</i>
Điều kiện cần	Necessary condition	Q cần cho P khi $P \Rightarrow Q$ <i>Q is necessary for P when $P \Rightarrow Q$</i>
Điều kiện đủ	Sufficient condition	P đủ cho Q khi $P \Rightarrow Q$ <i>P is sufficient for Q when $P \Rightarrow Q$</i>
Mệnh đề đảo	Converse	$Q \Rightarrow P$ so với $P \Rightarrow Q$ <i>$Q \Rightarrow P$ compared with $P \Rightarrow Q$</i>
Mệnh đề phản đảo	Contrapositive	$(\neg Q) \Rightarrow (\neg P)$, tương đương $P \Rightarrow Q$ <i>$(\neg Q) \Rightarrow (\neg P)$, equivalent to $P \Rightarrow Q$</i>
Phản ví dụ	Counterexample	Một trường hợp làm sai khẳng định “với mọi” <i>One case that breaks a “for all” claim</i>
Hợp, giao, hiệu	Union, intersection, difference	$A \cup B, A \cap B, A \setminus B$
Phần bù	Complement	Phần tử của tập nền không thuộc A <i>Elements of the universe not in A</i>
Lực lượng	Cardinality	Số phần tử của tập hữu hạn <i>Number of elements of a finite set</i>
Bao hàm – loại trừ	Inclusion–exclusion	Công thức đếm phần tử của hợp các tập <i>Formula for the size of a union</i>
Ánh xạ	Map (function)	Quy tắc đặt mỗi phần tử ứng với một ảnh <i>A rule giving each element one image</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Đơn ánh	Injection	Hai phần tử khác nhau có ảnh khác nhau <i>Distinct elements have distinct images</i>
Toàn ánh	Surjection	Mọi phần tử đích đều là ảnh <i>Every target element is an image</i>
Song ánh	Bijection	Vừa đơn ánh vừa toàn ánh <i>Both injective and surjective</i>
Chứng minh phản chứng	Proof by contradiction	Giả sử sai rồi suy ra vô lý <i>Assume false and derive an absurdity</i>
Quy nạp	Induction	Cơ sở cộng bước quy nạp <i>Base case plus inductive step</i>
Quy nạp mạnh	Strong induction	Dùng mọi giá trị trước đó <i>Uses all earlier values</i>
Sắp thứ tự tốt	Well-ordering	Tập con khác rỗng của $\mathbb{N}$ có phần tử nhỏ nhất <i>Every non-empty subset of $\mathbb{N}$ has a least element</i>
Lùi vô hạn	Infinite descent	Từ nghiệm sinh nghiệm nhỏ hơn mãi mãi <i>A solution producing ever smaller solutions</i>
Bước cơ sở	Base case	Giá trị đầu tiên cần kiểm tra trực tiếp <i>The starting values checked directly</i>

1.8. Bài tự luyện — Practice problems

Mức 1 — Học sinh giỏi cấp tỉnh — Level 1 — Provincial olympiad

Bài 1.1 / Problem 1.1 — Cho P: “với mọi số thực x tồn tại số thực y sao cho $x + y = xy$ ” và Q: “tồn tại số thực y sao cho với mọi số thực x ta có $x + y = xy$ ”. Viết phủ định của P, của Q và xác định đúng – sai của P, Q.

Let P: “for every real x there is a real y with $x + y = xy$ ” and Q: “there is a real y such that $x + y = xy$ for every real x ”. Write the negations of P and Q and decide whether P, Q are true.

Bài 1.2 / Problem 1.2 — Có bao nhiêu số nguyên dương không vượt quá 300 mà không chia hết cho 3, không chia hết cho 5 và không chia hết cho 7?

How many positive integers not exceeding 300 are divisible by none of 3, 5, 7?

Bài 1.3 / Problem 1.3 — Chứng minh bằng quy nạp rằng với mọi số nguyên dương n , số $5^n + 2 \cdot 3^{n-1} + 1$ chia hết cho 8.

Prove by induction that for every positive integer n , the number $5^n + 2 \cdot 3^{n-1} + 1$ is divisible by 8.

Bài 1.4 / Problem 1.4 — Cho $f: \mathbb{Z} \rightarrow \mathbb{Z}$ xác định bởi $f(n) = n + 1$ nếu n chẵn và $f(n) = n - 1$ nếu n lẻ. Chứng minh f là song ánh, tìm ánh xạ ngược và chứng minh f không có điểm bất động (không có n để $f(n) = n$).

Let $f: \mathbb{Z} \rightarrow \mathbb{Z}$ be given by $f(n) = n + 1$ for even n and $f(n) = n - 1$ for odd n . Prove that f is a bijection, find its inverse, and prove that f has no fixed point (no n with $f(n) = n$).

Mức 2 — Học sinh giỏi quốc gia — Level 2 — National olympiad

Bài 1.5 / Problem 1.5 — Gọi a_n là số tập con (kể cả tập rỗng) của $\{1, 2, \dots, n\}$ không chứa hai số nguyên liên tiếp. Chứng minh $a_1 = 2$, $a_2 = 3$ và $a_n = a_{n-1} + a_{n-2}$ với $n \geq 3$. Tính a_{10} .
Let a_n be the number of subsets (the empty set included) of $\{1, 2, \dots, n\}$ containing no two consecutive integers. Prove $a_1 = 2$, $a_2 = 3$ and $a_n = a_{n-1} + a_{n-2}$ for $n \geq 3$. Compute a_{10} .

Bài 1.6 / Problem 1.6 — Chứng minh $n^4 + 4$ là hợp số với mọi số nguyên $n > 1$. Từ đó tìm tất cả số nguyên dương n để $n^4 + 4$ là số nguyên tố.
Prove that $n^4 + 4$ is composite for every integer $n > 1$. Hence find all positive integers n for which $n^4 + 4$ is prime.

Bài 1.7 / Problem 1.7 — Tìm tất cả bộ số nguyên (a, b, c) thỏa mãn $a^2 + b^2 = 3c^2$.
Find all integer triples (a, b, c) with $a^2 + b^2 = 3c^2$.

Bài 1.8 / Problem 1.8 — Cho tập X có 100 phần tử và $A, B, C \subset X$ với $|A| = 60$, $|B| = 70$, $|C| = 80$. Tìm giá trị nhỏ nhất và giá trị lớn nhất của $|A \cap B \cap C|$.
Let X be a set of 100 elements and $A, B, C \subset X$ with $|A| = 60$, $|B| = 70$, $|C| = 80$. Find the least and the greatest value of $|A \cap B \cap C|$.

Mức 3 — Olympic quốc tế — Level 3 — International olympiad

Bài 1.9 / Problem 1.9 — Với mỗi số nguyên dương n , xét 2^n số có đúng n chữ số mà mọi chữ số đều bằng 1 hoặc 2. Chứng minh rằng trong các số đó có đúng một số chia hết cho 2^n .
For each positive integer n consider the 2^n numbers with exactly n digits, every digit being 1 or 2. Prove that exactly one of them is divisible by 2^n .

Bài 1.10 / Problem 1.10 — Gọi $F_1 = F_2 = 1$, $F_{k+1} = F_k + F_{k-1}$ (dãy Fibonacci: 1, 1, 2, 3, 5, 8, ...). Chứng minh rằng mọi số nguyên dương n đều viết được thành tổng của một số hữu hạn các số F_k với $k \geq 2$, các chỉ số k đôi một khác nhau và không có hai chỉ số nào liên tiếp.
Let $F_1 = F_2 = 1$, $F_{k+1} = F_k + F_{k-1}$ (the Fibonacci sequence 1, 1, 2, 3, 5, 8, ...). Prove that every positive integer n is a sum of finitely many numbers F_k with $k \geq 2$, the indices being pairwise distinct and no two of them consecutive.

Bài 1.11 / Problem 1.11 — Chứng minh rằng với mọi số nguyên dương n : $1 + 1/2^2 + 1/3^2 + \dots + 1/n^2 < 5/3$.
Prove that for every positive integer n : $1 + 1/2^2 + 1/3^2 + \dots + 1/n^2 < 5/3$.

Bài 1.12 / Problem 1.12 — Tính số ánh xạ từ tập $\{1, 2, \dots, n\}$ lên tập $\{1, 2, 3\}$ (toàn ánh) theo n bằng bao hàm – loại trừ, rồi chứng minh số đó chia hết cho 6 với mọi $n \geq 1$. Tính giá trị khi $n = 8$.
Count the surjective maps from $\{1, 2, \dots, n\}$ onto $\{1, 2, 3\}$ in terms of n by inclusion–exclusion, then prove the count is divisible by 6 for every $n \geq 1$. Evaluate for $n = 8$.

1.9. Lời giải bài tự luyện — Solutions to practice problems

Bài 1.1 — Problem 1.1

1. $\neg P$: tồn tại số thực x sao cho với mọi số thực y , $x + y \neq xy$. $\neg Q$: với mọi số thực y tồn tại số thực x sao cho $x + y \neq xy$.
 $\neg P$: there is a real x such that $x + y \neq xy$ for every real y . $\neg Q$: for every real y there is a real x with $x + y \neq xy$.
2. P sai. Với $x = 1$: $x + y = 1 + y$ và $xy = y$, nên $x + y - xy = 1 \neq 0$ với mọi y . Vậy $\neg P$ đúng.
 P is false. For $x = 1$: $x + y = 1 + y$ and $xy = y$, so $x + y - xy = 1 \neq 0$ for every y . Hence $\neg P$ is true.
3. Q sai. Nếu có y thỏa mãn với mọi x thì $x = 0$ cho $y = 0$; khi đó $x = 1$ cho $1 + 0 = 0$, vô lý. Vậy $\neg Q$ đúng.
 Q is false. If some y worked for every x then $x = 0$ would force $y = 0$; then $x = 1$ would give $1 + 0 = 0$, absurd. Hence $\neg Q$ is true.

Vậy P và Q đều sai.

Hence P and Q are both false. ■

Bài 1.2 — Problem 1.2

1. Gọi A, B, C là tập các số trong $\{1, \dots, 300\}$ chia hết cho 3, 5, 7. $|A| = 100$, $|B| = 60$, $|C| = 42$.
Let A, B, C be the sets of numbers in $\{1, \dots, 300\}$ divisible by 3, 5, 7. $|A| = 100$, $|B| = 60$, $|C| = 42$.
2. Các số 3, 5, 7 đôi một nguyên tố cùng nhau nên giao tương ứng là bội của 15, 21, 35, 105: $|A \cap B| = 20$, $|A \cap C| = 14$, $|B \cap C| = 8$, $|A \cap B \cap C| = 2$.
The numbers 3, 5, 7 are pairwise coprime, so the intersections are multiples of 15, 21, 35, 105: $|A \cap B| = 20$, $|A \cap C| = 14$, $|B \cap C| = 8$, $|A \cap B \cap C| = 2$.
3. Theo (1.2): $|A \cup B \cup C| = 100 + 60 + 42 - 20 - 14 - 8 + 2 = 162$.
By (1.2): $|A \cup B \cup C| = 100 + 60 + 42 - 20 - 14 - 8 + 2 = 162$.

Vậy có $300 - 162 = 138$ số thỏa mãn.

Hence $300 - 162 = 138$ numbers qualify. ■

Bài 1.3 — Problem 1.3

1. Đặt $u_n = 5^n + 2 \cdot 3^{n-1} + 1$. Cơ sở: $u_1 = 5 + 2 + 1 = 8$ chia hết cho 8.
Put $u_n = 5^n + 2 \cdot 3^{n-1} + 1$. Base: $u_1 = 5 + 2 + 1 = 8$, divisible by 8.
2. Giả thiết $8 \mid u_k$. Ta có $5u_k = 5^{k+1} + 10 \cdot 3^{k-1} + 5$ và $u_{k+1} = 5^{k+1} + 6 \cdot 3^{k-1} + 1$.
Hypothesis $8 \mid u_k$. We have $5u_k = 5^{k+1} + 10 \cdot 3^{k-1} + 5$ and $u_{k+1} = 5^{k+1} + 6 \cdot 3^{k-1} + 1$.

$$u_{k+1} = 5u_k - 4(3^{k-1} + 1)$$
3. 3^{k-1} lẻ nên $3^{k-1} + 1$ chẵn, do đó $4(3^{k-1} + 1)$ chia hết cho 8. Cả hai số hạng của hiệu đều chia hết cho 8 nên $8 \mid u_{k+1}$.
 3^{k-1} is odd, so $3^{k-1} + 1$ is even and $4(3^{k-1} + 1)$ is divisible by 8. Both terms of the difference are divisible by 8, so $8 \mid u_{k+1}$.

Vậy $8 \mid u_n$ với mọi $n \geq 1$ theo nguyên lý quy nạp.

Hence $8 \mid u_n$ for all $n \geq 1$ by induction. ■

Bài 1.4 — Problem 1.4

1. Nếu n chẵn thì $f(n) = n + 1$ lẻ, nên $f(f(n)) = (n + 1) - 1 = n$. Nếu n lẻ thì $f(n) = n - 1$ chẵn, nên $f(f(n)) = (n - 1) + 1 = n$. Vậy $f(f(n)) = n$ với mọi n .
If n is even then $f(n) = n + 1$ is odd, so $f(f(n)) = (n + 1) - 1 = n$. If n is odd then $f(n) = n - 1$ is even, so $f(f(n)) = (n - 1) + 1 = n$. Hence $f(f(n)) = n$ for all n .
2. Đơn ánh: $f(a) = f(b)$ suy ra $a = f(f(a)) = f(f(b)) = b$. Toàn ánh: với mọi $m \in \mathbb{Z}$, $m = f(f(m))$ nên m là ảnh của $f(m)$. Vậy f là song ánh và $f^{-1} = f$.
Injective: $f(a) = f(b)$ gives $a = f(f(a)) = f(f(b)) = b$. Surjective: for every $m \in \mathbb{Z}$, $m = f(f(m))$ so m is the image of $f(m)$. So f is bijective and $f^{-1} = f$.
3. Điểm bất động: $f(n)$ luôn khác n về tính chẵn lẻ ($n + 1$ và $n - 1$ khác tính chẵn lẻ với n), nên $f(n) \neq n$.
Fixed points: $f(n)$ always has the opposite parity to n ($n + 1$ and $n - 1$ differ in parity from n), so $f(n) \neq n$.

Vậy f là song ánh, $f^{-1} = f$, và f không có điểm bất động.

Hence f is a bijection, $f^{-1} = f$, and f has no fixed point. ■

Bài 1.5 — Problem 1.5

1. $n = 1$: các tập con là $\emptyset$ và $\{1\}$, nên $a_1 = 2$. $n = 2$: $\emptyset, \{1\}, \{2\}$ (tập $\{1, 2\}$ bị loại), nên $a_2 = 3$.
 $n = 1$: the subsets are $\emptyset$ and $\{1\}$, so $a_1 = 2$. $n = 2$: $\emptyset, \{1\}, \{2\}$ (the set $\{1, 2\}$ is excluded), so $a_2 = 3$.
2. Với $n \geq 3$, chia các tập con hợp lệ của $\{1, \dots, n\}$ thành hai nhóm. Nhóm 1: không chứa n ; đó chính là các tập con hợp lệ của $\{1, \dots, n - 1\}$, có a_{n-1} tập.
For $n \geq 3$, split the valid subsets of $\{1, \dots, n\}$ into two groups. Group 1: not containing n ; these are exactly the valid subsets of $\{1, \dots, n - 1\}$, so there are a_{n-1} .
3. Nhóm 2: chứa n . Khi đó không chứa $n - 1$, và phần còn lại là một tập con hợp lệ bất kỳ của $\{1, \dots, n - 2\}$. Phép đặt tương ứng (bỏ n) là song ánh từ nhóm 2 lên tập các tập con hợp lệ của $\{1, \dots, n - 2\}$, nên nhóm 2 có a_{n-2} tập.
Group 2: containing n . Then $n - 1$ is absent, and the rest is an arbitrary valid subset of $\{1, \dots, n - 2\}$. Deleting n is a bijection from group 2 onto the valid subsets of $\{1, \dots, n - 2\}$, so group 2 has a_{n-2} sets.
4. Do đó $a_n = a_{n-1} + a_{n-2}$. Tính tiếp: $a_3 = 5, a_4 = 8, a_5 = 13, a_6 = 21, a_7 = 34, a_8 = 55, a_9 = 89, a_{10} = 144$.
Hence $a_n = a_{n-1} + a_{n-2}$. Continuing: $a_3 = 5, a_4 = 8, a_5 = 13, a_6 = 21, a_7 = 34, a_8 = 55, a_9 = 89, a_{10} = 144$.

Vậy $a_{10} = 144$.

Hence $a_{10} = 144$. ■

Bài 1.6 — Problem 1.6

1. Phân tích: $n^4 + 4 = (n^2 + 2)^2 - 4n^2 = (n^2 + 2n + 2)(n^2 - 2n + 2)$.
Factorise: $n^4 + 4 = (n^2 + 2)^2 - 4n^2 = (n^2 + 2n + 2)(n^2 - 2n + 2)$.
2. Nhân tử thứ hai bằng $(n - 1)^2 + 1 \geq 2$ khi $n \geq 2$. Nhân tử thứ nhất bằng $(n + 1)^2 + 1 > 2$. Cả hai nhân tử lớn hơn 1 nên tích là hợp số.
The second factor equals $(n - 1)^2 + 1 \geq 2$ for $n \geq 2$. The first equals $(n + 1)^2 + 1 > 2$. Both factors exceed 1, so the product is composite.
3. Còn $n = 1$: $1 + 4 = 5$ là số nguyên tố.
Remaining case $n = 1$: $1 + 4 = 5$ is prime.

Vậy $n^4 + 4$ là số nguyên tố khi và chỉ khi $n = 1$.

Hence $n^4 + 4$ is prime if and only if $n = 1$. ■

Bài 1.7 — Problem 1.7

1. Bộ $(0, 0, 0)$ là nghiệm. Giả sử có nghiệm khác $(0, 0, 0)$; lấy nghiệm có $|a| + |b| + |c|$ nhỏ nhất (tồn tại theo nguyên lý sắp thứ tự tốt).
The triple $(0, 0, 0)$ is a solution. Suppose another solution exists; take one with $|a| + |b| + |c|$ least (it exists by the well-ordering principle).
2. Vì $3 \mid a^2 + b^2$, theo Ví dụ 1.6 cả a và b chia hết cho 3: $a = 3a_1, b = 3b_1$.
Since $3 \mid a^2 + b^2$, Example 1.6 shows that a and b are divisible by 3: $a = 3a_1, b = 3b_1$.
3. Khi đó $9a_1^2 + 9b_1^2 = 3c^2$, tức $c^2 = 3(a_1^2 + b_1^2)$, nên $3 \mid c^2$ và $3 \mid c$: $c = 3c_1$.
Then $9a_1^2 + 9b_1^2 = 3c^2$, that is $c^2 = 3(a_1^2 + b_1^2)$, so $3 \mid c^2$ and $3 \mid c$: $c = 3c_1$.
4. Thay vào và chia cho 9: $a_1^2 + b_1^2 = 3c_1^2$. Bộ (a_1, b_1, c_1) là nghiệm khác $(0, 0, 0)$ với tổng giá trị tuyệt đối bằng một phần ba tổng ban đầu, nhỏ hơn giá trị nhỏ nhất, mâu thuẫn.
Substituting and dividing by 9: $a_1^2 + b_1^2 = 3c_1^2$. The triple (a_1, b_1, c_1) is a solution different from $(0, 0, 0)$ whose sum of absolute values is a third of the original, below the least value: a contradiction.

Vậy nghiệm duy nhất là $(a, b, c) = (0, 0, 0)$.

Hence the only solution is $(a, b, c) = (0, 0, 0)$. ■

Bài 1.8 — Problem 1.8

1. Giá trị nhỏ nhất. Theo công thức De Morgan, $(A \cap B \cap C)^c = A^c \cup B^c \cup C^c$, với $|A^c| = 40, |B^c| = 30, |C^c| = 20$. Số phần tử của hợp không vượt quá tổng $40 + 30 + 20 = 90$, nên $|A \cap B \cap C| \geq 100 - 90 = 10$.
Least value. By De Morgan's law, $(A \cap B \cap C)^c = A^c \cup B^c \cup C^c$, with $|A^c| = 40, |B^c| = 30, |C^c| = 20$. The union has at most $40 + 30 + 20 = 90$ elements, so $|A \cap B \cap C| \geq 100 - 90 = 10$.
2. Đạt được: lấy $X = \{1, \dots, 100\}, A^c = \{1, \dots, 40\}, B^c = \{41, \dots, 70\}, C^c = \{71, \dots, 90\}$. Ba phần bù đôi một rời nhau nên $A \cap B \cap C = \{91, \dots, 100\}$ có 10 phần tử.
Attained: take $X = \{1, \dots, 100\}, A^c = \{1, \dots, 40\}, B^c = \{41, \dots, 70\}, C^c = \{71, \dots, 90\}$. The three complements are pairwise disjoint, so $A \cap B \cap C = \{91, \dots, 100\}$ has 10 elements.

3. Giá trị lớn nhất. $A \cap B \cap C \subset A$ nên $|A \cap B \cap C| \leq 60$. Đạt được khi $A = \{1, \dots, 60\} \subset B = \{1, \dots, 70\} \subset C = \{1, \dots, 80\}$, khi đó $A \cap B \cap C = A$ có 60 phần tử.
Greatest value. $A \cap B \cap C \subset A$ gives $|A \cap B \cap C| \leq 60$. It is attained for $A = \{1, \dots, 60\} \subset B = \{1, \dots, 70\} \subset C = \{1, \dots, 80\}$, where $A \cap B \cap C = A$ has 60 elements.

Vậy giá trị nhỏ nhất là 10 và giá trị lớn nhất là 60.

Hence the least value is 10 and the greatest is 60. ■

Bài 1.9 — Problem 1.9

- Mỗi số có dạng $N(e) = \sum (1 + e_i) \cdot 10^i$ với i chạy từ 0 đến $n - 1$ và $e_i \in \{0, 1\}$; có 2^n dãy $e = (e_0, \dots, e_{n-1})$, ứng với 2^n số khác nhau.
Each such number has the form $N(e) = \sum (1 + e_i) \cdot 10^i$, i running from 0 to $n - 1$ with $e_i \in \{0, 1\}$; there are 2^n sequences $e = (e_0, \dots, e_{n-1})$, giving 2^n different numbers.
- Lấy hai dãy khác nhau $e \neq e'$ và gọi j là chỉ số nhỏ nhất mà $e_j \neq e'_j$. Khi đó $N(e) - N(e') = \pm 10^j + \sum_{i>j} (e_i - e'_i) \cdot 10^i$. Mọi số hạng trong tổng này chia hết cho 2^{j+1} (vì $10^i = 2^i \cdot 5^i$ với $i \geq j + 1$).
Take two different sequences $e \neq e'$ and let j be the least index with $e_j \neq e'_j$. Then $N(e) - N(e') = \pm 10^j + \sum_{i>j} (e_i - e'_i) \cdot 10^i$. Every term of the sum is divisible by 2^{j+1} (since $10^i = 2^i \cdot 5^i$ with $i \geq j + 1$).
- Còn $10^j = 2^j \cdot 5^j$ với 5^j lẻ, nên 10^j chia hết cho 2^j nhưng không chia hết cho 2^{j+1} . Suy ra hiệu $N(e) - N(e')$ không chia hết cho 2^{j+1} , mà $j + 1 \leq n$ nên cũng không chia hết cho 2^n .
And $10^j = 2^j \cdot 5^j$ with 5^j odd, so 10^j is divisible by 2^j but not by 2^{j+1} . Hence $N(e) - N(e')$ is not divisible by 2^{j+1} , and since $j + 1 \leq n$ it is not divisible by 2^n either.
- Vậy 2^n số trên có 2^n số dư khác nhau khi chia cho 2^n . Ánh xạ từ tập 2^n số vào tập 2^n số dư $\{0, 1, \dots, 2^n - 1\}$ là đơn ánh nên theo Định lý 1.11 là song ánh: mỗi số dư, kể cả 0, xuất hiện đúng một lần.
So the 2^n numbers leave 2^n different remainders on division by 2^n . The map from the set of 2^n numbers into the set of 2^n remainders $\{0, 1, \dots, 2^n - 1\}$ is injective, hence bijective by Theorem 1.11: each remainder, 0 included, occurs exactly once.

Vậy có đúng một số trong 2^n số chia hết cho 2^n .

Hence exactly one of the 2^n numbers is divisible by 2^n . ■

Bài 1.10 — Problem 1.10

- Dãy $F_2 = 1 < F_3 = 2 < F_4 = 3 < \dots$ tăng ngặt (vì $F_{k+1} = F_k + F_{k-1} > F_k$). Ta quy nạp mạnh theo n . Cơ sở: $1 = F_2$.
The sequence $F_2 = 1 < F_3 = 2 < F_4 = 3 < \dots$ is strictly increasing (since $F_{k+1} = F_k + F_{k-1} > F_k$). Use strong induction on n . Base: $1 = F_2$.
- Cho $n \geq 2$ và giả sử khẳng định đúng với mọi số nguyên dương nhỏ hơn n . Vì $F_3 = 2 \leq n$ và dãy tăng không giới hạn, tồn tại $k \geq 3$ lớn nhất sao cho $F_k \leq n$; khi đó $F_k \leq n < F_{k+1}$.
Let $n \geq 2$ and assume the claim for all smaller positive integers. Since $F_3 = 2 \leq n$ and the sequence is unbounded, there is a largest $k \geq 3$ with $F_k \leq n$; then $F_k \leq n < F_{k+1}$.

3. Nếu $n = F_k$ thì xong. Nếu không, đặt $m = n - F_k$; khi đó $1 \leq m < F_{k+1} - F_k = F_{k-1}$, và $m < n$. Theo giả thiết quy nạp, m là tổng các số Fibonacci có chỉ số đôi một cách nhau ít nhất 2. Gọi F_j là số hạng có chỉ số lớn nhất trong tổng đó.

If $n = F_k$ we are done. Otherwise put $m = n - F_k$; then $1 \leq m < F_{k+1} - F_k = F_{k-1}$, and $m < n$. By the hypothesis m is a sum of Fibonacci numbers whose indices are pairwise at least 2 apart. Let F_j be the term with the largest index in that sum.

4. Do $F_j \leq m < F_{k-1}$ và dãy tăng ngặt từ chỉ số 2 (mà $k - 1 \geq 2$), ta có $j < k - 1$, tức $j \leq k - 2$. Thêm F_k vào tổng của m : chỉ số k cách chỉ số lớn nhất j ít nhất 2, các chỉ số còn lại vẫn cách nhau ít nhất 2.

Since $F_j \leq m < F_{k-1}$ and the sequence is strictly increasing from index 2 (with $k - 1 \geq 2$), we get $j < k - 1$, that is $j \leq k - 2$. Add F_k to the sum for m : the index k is at least 2 above the largest index j , and the other indices remain at least 2 apart.

Vậy $n = F_k + m$ có biểu diễn cần tìm, và theo quy nạp mạnh khẳng định đúng với mọi $n \geq 1$.

Hence $n = F_k + m$ has the required representation, and by strong induction the claim holds for every $n \geq 1$. ■

Bài 1.11 — Problem 1.11

1. Đặt $S_n = 1 + 1/2^2 + \dots + 1/n^2$. Quy nạp trực tiếp với $S_n < 5/3$ không đi được: từ $S_k < 5/3$ không suy ra $S_k + 1/(k+1)^2 < 5/3$. Cần tăng cường: chứng minh với mọi $n \geq 1$
- Put $S_n = 1 + 1/2^2 + \dots + 1/n^2$. Direct induction on $S_n < 5/3$ fails: $S_k < 5/3$ does not give $S_k + 1/(k+1)^2 < 5/3$. Strengthen the claim: prove for every $n \geq 1$*

$$S_n \leq 5/3 - 2/(2n+1) \quad (1.4)$$

2. Cơ sở $n = 1$: $S_1 = 1$ và $5/3 - 2/3 = 1$, đẳng thức đúng.
- Base $n = 1$: $S_1 = 1$ and $5/3 - 2/3 = 1$, so (1.4) holds with equality.*
3. Giả thiết (1.4) đúng với k . Khi đó $S_{k+1} \leq 5/3 - 2/(2k+1) + 1/(k+1)^2$. Ta cần số này không vượt quá $5/3 - 2/(2k+3)$, tức là $1/(k+1)^2 \leq 2/(2k+1) - 2/(2k+3) = 4/((2k+1)(2k+3))$.

Assume (1.4) for k . Then $S_{k+1} \leq 5/3 - 2/(2k+1) + 1/(k+1)^2$. We need this not to exceed $5/3 - 2/(2k+3)$, that is, $1/(k+1)^2 \leq 2/(2k+1) - 2/(2k+3) = 4/((2k+1)(2k+3))$.

4. Bất đẳng thức đó tương đương $(2k+1)(2k+3) \leq 4(k+1)^2$, hay $4k^2 + 8k + 3 \leq 4k^2 + 8k + 4$, đúng. Vậy (1.4) đúng với $k+1$.

That inequality is equivalent to $(2k+1)(2k+3) \leq 4(k+1)^2$, that is $4k^2 + 8k + 3 \leq 4k^2 + 8k + 4$, which is true. So (1.4) holds for $k+1$.

Vậy với mọi $n \geq 1$: $S_n \leq 5/3 - 2/(2n+1) < 5/3$.

Hence for every $n \geq 1$: $S_n \leq 5/3 - 2/(2n+1) < 5/3$. ■

Bài 1.12 — Problem 1.12

1. Có 3^n ánh xạ từ $\{1, \dots, n\}$ vào $\{1, 2, 3\}$. Gọi A_i là tập các ánh xạ không nhận giá trị i ($i = 1, 2, 3$). Ánh xạ không toàn ánh khi và chỉ khi thuộc $A_1 \cup A_2 \cup A_3$.

There are 3^n maps from $\{1, \dots, n\}$ into $\{1, 2, 3\}$. Let A_i be the set of maps never taking the value i ($i = 1, 2, 3$). A map fails to be surjective exactly when it lies in $A_1 \cup A_2 \cup A_3$.

2. $|A_i| = 2^n$ (mỗi phần tử có 2 giá trị cho phép); $A_i \cap A_j$ ($i \neq j$) chỉ gồm ánh xạ hằng bằng giá trị còn lại, nên $|A_i \cap A_j| = 1$; $A_1 \cap A_2 \cap A_3 = \emptyset$ vì $n \geq 1$ và ánh phải là một giá trị nào đó.
 $|A_i| = 2^n$ (each element has 2 allowed values); $A_i \cap A_j$ ($i \neq j$) consists only of the constant map onto the remaining value, so $|A_i \cap A_j| = 1$; $A_1 \cap A_2 \cap A_3 = \emptyset$ since $n \geq 1$ and an element must map somewhere.
3. Theo (1.2): $|A_1 \cup A_2 \cup A_3| = 3 \cdot 2^n - 3 \cdot 1 + 0$. Do đó số toàn ánh bằng $3^n - 3 \cdot 2^n + 3$.
By (1.2): $|A_1 \cup A_2 \cup A_3| = 3 \cdot 2^n - 3 \cdot 1 + 0$. Hence the number of surjections is $3^n - 3 \cdot 2^n + 3$.
4. Chia hết cho 2: 3^n lẻ, $3 \cdot 2^n$ chẵn, 3 lẻ nên lẻ – chẵn + lẻ là số chẵn. Chia hết cho 3: với $n \geq 1$, $3 \mid 3^n$, $3 \mid 3 \cdot 2^n$ và $3 \mid 3$. Vì 2 và 3 nguyên tố cùng nhau nên số đó chia hết cho 6.
Divisible by 2: 3^n is odd, $3 \cdot 2^n$ is even, 3 is odd, so odd – even + odd is even. Divisible by 3: for $n \geq 1$, $3 \mid 3^n$, $3 \mid 3 \cdot 2^n$ and $3 \mid 3$. As 2 and 3 are coprime the count is divisible by 6.
5. Với $n = 8$: $3^8 - 3 \cdot 2^8 + 3 = 6561 - 768 + 3 = 5796 = 6 \cdot 966$.
For $n = 8$: $3^8 - 3 \cdot 2^8 + 3 = 6561 - 768 + 3 = 5796 = 6 \cdot 966$.

Vậy số toàn ánh bằng $3^n - 3 \cdot 2^n + 3$, chia hết cho 6, và bằng 5796 khi $n = 8$.

Hence the number of surjections is $3^n - 3 \cdot 2^n + 3$, divisible by 6, and equals 5796 for $n = 8$. ■

Chương 2. Các bất đẳng thức cổ điển — Chapter 2. Classical inequalities

Mục tiêu chương — Chapter objectives

- Biến đổi tương đương và dùng bình phương để chứng minh một bất đẳng thức, kể cả khi phải thêm bớt hạng tử.
Prove an inequality by equivalent transformations and by completing squares, including when terms must be added and subtracted.
- Chứng minh và dùng AM–GM cho 2, 3 và n số, chọn điểm rơi đúng trước khi tách hạng tử.
Prove and use AM–GM for 2, 3 and n numbers, choosing the equality point before splitting terms.
- Dùng Cauchy–Schwarz (dạng tổng và dạng Engel), bất đẳng thức hoán vị và Chebyshev.
Use Cauchy–Schwarz (the sum form and the Engel form), the rearrangement inequality and Chebyshev's inequality.
- Nắm chuỗi trung bình $HM \leq GM \leq AM \leq QM$, bất đẳng thức Bernoulli, trị tuyệt đối, bất đẳng thức tam giác và Nesbitt.
Know the chain $HM \leq GM \leq AM \leq QM$, Bernoulli's inequality, absolute values, the triangle inequality and Nesbitt's inequality.
- Giải bài tìm giá trị lớn nhất, nhỏ nhất có điều kiện và chứng minh giá trị đó thật sự đạt được.
Solve constrained maximum and minimum problems and prove that the extreme value is actually attained.

2.1. Thứ tự trên $\mathbb{R}$, biến đổi tương đương và bình phương — Order on $\mathbb{R}$, equivalent transformations and squares

Chứng minh một bất đẳng thức quy về một nhận xét: hiệu hai vế có dấu xác định. Ta bắt đầu từ định nghĩa thứ tự và các phép biến đổi giữ nguyên chiều bất đẳng thức.

Proving an inequality comes down to one observation: the difference of the two sides has a definite sign. We start from the definition of the order and the operations that keep the direction of an inequality.

ĐỊNH NGHĨA 2.1 (Thứ tự trên $\mathbb{R}$) / DEFINITION 2.1 (Order on $\mathbb{R}$) — Với hai số thực a, b , ta viết $a \geq b$ nếu $a - b \geq 0$, và viết $a > b$ nếu $a - b > 0$. Chứng minh $a \geq b$ nghĩa là chứng minh hiệu $a - b$ không âm.

For real numbers a, b we write $a \geq b$ if $a - b \geq 0$, and $a > b$ if $a - b > 0$. To prove $a \geq b$ means to prove that the difference $a - b$ is non-negative.

TÍNH CHẤT 2.2 (Các phép biến đổi bảo toàn bất đẳng thức) / PROPERTY 2.2 (Operations that preserve an inequality) — Với a, b, c, d là các số thực:

- (i) Nếu $a \geq b$ thì $a + c \geq b + c$. Nếu $a \geq b$ và $c \geq d$ thì $a + c \geq b + d$.
- (ii) Nếu $a \geq b$ và $c > 0$ thì $ac \geq bc$; nếu $a \geq b$ và $c < 0$ thì $ac \leq bc$.

- (iii) Nếu $a \geq b \geq 0$ và $c \geq d \geq 0$ thì $ac \geq bd$.
 (iv) Nếu $a \geq b > 0$ thì $1/a \leq 1/b$.
 (v) Với $a, b \geq 0$ và $n \in \mathbb{Z}^+$: $a \geq b$ khi và chỉ khi $a^n \geq b^n$.

For real numbers a, b, c, d :

- (i) If $a \geq b$ then $a + c \geq b + c$. If $a \geq b$ and $c \geq d$ then $a + c \geq b + d$.
 (ii) If $a \geq b$ and $c > 0$ then $ac \geq bc$; if $a \geq b$ and $c < 0$ then $ac \leq bc$.
 (iii) If $a \geq b \geq 0$ and $c \geq d \geq 0$ then $ac \geq bd$.
 (iv) If $a \geq b > 0$ then $1/a \leq 1/b$.
 (v) For $a, b \geq 0$ and $n \in \mathbb{Z}^+$: $a \geq b$ if and only if $a^n \geq b^n$.

Chứng minh. / Proof.

(i) Hiệu $(a + c) - (b + c)$ bằng $a - b \geq 0$. Với bất đẳng thức thứ hai, $(a + c) - (b + d) = (a - b) + (c - d)$, tổng hai số không âm.

(i) The difference $(a + c) - (b + c)$ equals $a - b \geq 0$. For the second inequality, $(a + c) - (b + d) = (a - b) + (c - d)$, a sum of two non-negative numbers.

(ii) $ac - bc = c(a - b)$; dấu của tích là dấu của c khi $a - b > 0$, và bằng 0 khi $a = b$.

(ii) $ac - bc = c(a - b)$; this has the sign of c when $a - b > 0$, and equals 0 when $a = b$.

(iii) $ac - bd = c(a - b) + b(c - d)$. Vì $c \geq 0, b \geq 0$ nên cả hai số hạng không âm.

(iii) $ac - bd = c(a - b) + b(c - d)$. Since $c \geq 0$ and $b \geq 0$, both terms are non-negative.

(iv) $1/b - 1/a = (a - b)/(ab) \geq 0$ vì $a - b \geq 0$ và $ab > 0$.

(iv) $1/b - 1/a = (a - b)/(ab) \geq 0$ because $a - b \geq 0$ and $ab > 0$.

(v) Chiều thuận: áp dụng (iii) $n - 1$ lần. Chiều đảo: nếu $a < b$ thì $b > 0$, và $a^n < b^n$ (với $a = 0$ hiển nhiên, với $a > 0$ nhân n bất đẳng thức chặt giữa các số dương), trái với $a^n \geq b^n$. Vậy $a \geq b$.

(v) Forward direction: apply (iii) $n - 1$ times. Converse: if $a < b$ then $b > 0$ and $a^n < b^n$ (trivial for $a = 0$; for $a > 0$ multiply n strict inequalities between positive numbers), contradicting $a^n \geq b^n$. Hence $a \geq b$. ■

TÍNH CHẤT 2.3 (Ba đồng nhất thức hay dùng) / PROPERTY 2.3 (Three frequently used identities) — Với mọi số thực a, b, c , đặt $p = a + b + c$ và $q = ab + bc + ca$:

(a) $(a + b + c)^2 = a^2 + b^2 + c^2 + 2q$;

(b) $a^3 + b^3 = (a + b)^3 - 3ab(a + b)$;

(c) $(a + b)(b + c)(c + a) = p \cdot q - abc$.

For all real a, b, c , put $p = a + b + c$ and $q = ab + bc + ca$:

(a) $(a + b + c)^2 = a^2 + b^2 + c^2 + 2q$;

(b) $a^3 + b^3 = (a + b)^3 - 3ab(a + b)$;

(c) $(a + b)(b + c)(c + a) = p \cdot q - abc$.

Chứng minh. / Proof.

(a) Khai triển trực tiếp ba bình phương và ba tích đôi. (b) $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + b^3 + 3ab(a + b)$.

(a) Expand the three squares and the three cross terms directly. (b) $(a + b)^3 = a^3 + 3a^2b + 3ab^2 + b^3 = a^3 + b^3 + 3ab(a + b)$.

(c) Vì $a + b = p - c$, $b + c = p - a$, $c + a = p - b$, nên tích bằng $(p - a)(p - b)(p - c) = p^3 - p^2 \cdot (a + b + c) + p \cdot q - abc = p \cdot q - abc$.

(c) Since $a + b = p - c$, $b + c = p - a$, $c + a = p - b$, the product equals $(p - a)(p - b)(p - c) = p^3 - p^2 \cdot (a + b + c) + p \cdot q - abc = p \cdot q - abc$. ■

TÍNH CHẤT 2.4 (So sánh phân số) / PROPERTY 2.4 (Comparing fractions) — Với $b, d > 0$: (i) $a/b \geq c/d$ khi và chỉ khi $ad \geq bc$; (ii) nếu $a/b \geq c/d$ thì $a/b \geq (a + c)/(b + d) \geq c/d$.
For $b, d > 0$: (i) $a/b \geq c/d$ if and only if $ad \geq bc$; (ii) if $a/b \geq c/d$ then $a/b \geq (a + c)/(b + d) \geq c/d$.

Chứng minh. / Proof.

(i) Nhân hai vế với $bd > 0$ (Tính chất 2.2(ii), hai chiều vì nhân với số dương và chia cho số dương đều giữ chiều).

(i) Multiply both sides by $bd > 0$ (Property 2.2(ii); it works both ways since multiplying and dividing by a positive number keep the direction).

(ii) Theo (i), $ad \geq bc$. Vì $b + d > 0$: $a/b - (a + c)/(b + d) = (a(b + d) - b(a + c))/(b(b + d)) = (ad - bc)/(b(b + d)) \geq 0$, và $(a + c)/(b + d) - c/d = (d(a + c) - c(b + d))/(d(b + d)) = (ad - bc)/(d(b + d)) \geq 0$.

(ii) By (i), $ad \geq bc$. Since $b + d > 0$: $a/b - (a + c)/(b + d) = (a(b + d) - b(a + c))/(b(b + d)) = (ad - bc)/(b(b + d)) \geq 0$, and $(a + c)/(b + d) - c/d = (d(a + c) - c(b + d))/(d(b + d)) = (ad - bc)/(d(b + d)) \geq 0$. ■

Bình phương của số thực không âm là nguồn gốc của hầu hết bất đẳng thức sơ cấp. Ba bất đẳng thức sau xử lý được nhiều bài ở mức tỉnh.

The square of a real number is non-negative, and this is the source of most elementary inequalities. The next three inequalities handle many provincial-level problems.

BỔ ĐỀ 2.5 (Bình phương không âm) / LEMMA 2.5 (Squares are non-negative) — Với mọi số thực x, y, z :

(a) $x^2 + y^2 \geq 2xy$, dấu bằng khi và chỉ khi $x = y$;

(b) $(x + y)^2 \geq 4xy$, dấu bằng khi và chỉ khi $x = y$;

(c) $x^2 + y^2 + z^2 \geq xy + yz + zx$, dấu bằng khi và chỉ khi $x = y = z$.

For all real x, y, z :

(a) $x^2 + y^2 \geq 2xy$, with equality if and only if $x = y$;

(b) $(x + y)^2 \geq 4xy$, with equality if and only if $x = y$;

(c) $x^2 + y^2 + z^2 \geq xy + yz + zx$, with equality if and only if $x = y = z$.

Chứng minh. / Proof.

(a) $x^2 + y^2 - 2xy = (x - y)^2 \geq 0$. (b) $(x + y)^2 - 4xy = (x - y)^2 \geq 0$. (c) Ta có đồng nhất thức
(a) $x^2 + y^2 - 2xy = (x - y)^2 \geq 0$. (b) $(x + y)^2 - 4xy = (x - y)^2 \geq 0$. (c) We have the identity

$$x^2 + y^2 + z^2 - xy - yz - zx = (1/2) \cdot [(x - y)^2 + (y - z)^2 + (z - x)^2] \quad (2.1)$$

Vế phải không âm. Nó bằng 0 khi và chỉ khi $x - y = y - z = z - x = 0$, tức $x = y = z$.

The right-hand side is non-negative. It equals 0 if and only if $x - y = y - z = z - x = 0$, that is $x = y = z$. ■

PHÂN TÍCH / ANALYSIS — Đề cho x, y, z cùng với hạng tử $2z^2$ và tích $z(x + y)$: hai tích xz, yz xuất hiện cạnh x^2, y^2, z^2 . Ghép mỗi tích với một bình phương: z^2 đứng cạnh x^2 và xz , z^2 đứng cạnh y^2 và yz . Mỗi nhóm có dạng $a^2 + b^2 - 2ab$.

The statement contains x, y, z with the term $2z^2$ and the product $z(x + y)$: the products xz and yz appear next to x^2, y^2 and z^2 . Pair each product with a square: one z^2 sits with x^2 and xz , the other z^2 with y^2 and yz . Each group has the shape $a^2 + b^2 - 2ab$.

VÍ DỤ 2.1 (Nhóm thành bình phương) / EXAMPLE 2.1 (Grouping into squares) —

Chứng minh rằng với mọi số thực x, y, z : $x^2 + y^2 + 2z^2 \geq 2z(x + y)$. Tìm các bộ (x, y, z) để dấu bằng xảy ra.

Prove that for all real x, y, z : $x^2 + y^2 + 2z^2 \geq 2z(x + y)$. Find all triples (x, y, z) for which equality holds.

Lời giải. / Solution.

Tách $2z^2 = z^2 + z^2$ và nhóm lại:

Split $2z^2 = z^2 + z^2$ and regroup:

$$x^2 + y^2 + 2z^2 - 2zx - 2zy = (x^2 - 2zx + z^2) + (y^2 - 2zy + z^2) = (x - z)^2 + (y - z)^2$$

Tổng hai bình phương không âm nên bất đẳng thức đúng.

A sum of two squares is non-negative, so the inequality holds.

Dấu bằng khi và chỉ khi $x - z = 0$ và $y - z = 0$, tức $x = y = z$.

Equality holds if and only if $x - z = 0$ and $y - z = 0$, that is $x = y = z$.

Vậy bất đẳng thức đúng với mọi x, y, z và dấu bằng đạt khi $x = y = z$.

Hence the inequality holds for all x, y, z , with equality exactly when $x = y = z$. ■

VÍ DỤ 2.2 (Dùng bổ đề hai lần) / EXAMPLE 2.2 (Using a lemma twice) — Chứng minh rằng với mọi số thực a, b, c : $a^4 + b^4 + c^4 \geq abc(a + b + c)$.

Prove that for all real a, b, c : $a^4 + b^4 + c^4 \geq abc(a + b + c)$.

Lời giải. / Solution.

Áp dụng Bổ đề 2.5(c) hai lần. Lần thứ nhất với bộ ba $(x, y, z) = (a^2, b^2, c^2)$:

Apply Lemma 2.5(c) twice. First with the triple $(x, y, z) = (a^2, b^2, c^2)$:

$$a^4 + b^4 + c^4 \geq a^2b^2 + b^2c^2 + c^2a^2$$

Lần thứ hai với bộ ba $(x, y, z) = (ab, bc, ca)$, chú ý $xy + yz + zx = ab \cdot bc + bc \cdot ca + ca \cdot ab = abc(b + c + a)$:

Then with the triple $(x, y, z) = (ab, bc, ca)$, noting $xy + yz + zx = ab \cdot bc + bc \cdot ca + ca \cdot ab = abc(b + c + a)$:

$$a^2b^2 + b^2c^2 + c^2a^2 \geq ab \cdot bc + bc \cdot ca + ca \cdot ab = abc(a + b + c)$$

Nói hai bất đẳng thức ta được điều phải chứng minh. Dấu bằng khi $a^2 = b^2 = c^2$ và $ab = bc = ca$, chẳng hạn $a = b = c$.

Chaining the two inequalities gives the claim. Equality needs $a^2 = b^2 = c^2$ and $ab = bc = ca$, for instance $a = b = c$. ■

NHẬN XÉT / REMARK — Với x, y, z không âm, Bổ đề 2.5(c) còn viết được dưới dạng $(x + y + z)^2 \geq 3(xy + yz + zx)$. Dạng này tiện khi biết tổng $x + y + z$ và cần chặn trên tổng các tích đôi một.

For non-negative x, y, z , Lemma 2.5(c) can be written as $(x + y + z)^2 \geq 3(xy + yz + zx)$. This form is convenient when the sum $x + y + z$ is known and the sum of pairwise products must be bounded above.

NHẬN XÉT / REMARK — Cân bằng hệ số trước khi dùng $x^2 + y^2 \geq 2xy$. Với $\alpha > 0$, áp dụng cho $\sqrt{\alpha} \cdot x$ và $y/\sqrt{\alpha}$: $\alpha x^2 + y^2/\alpha \geq 2xy$. Ví dụ $3x^2 + 2y^2 \geq 2\sqrt{6} \cdot xy$ với mọi x, y thực: lấy $\alpha = \sqrt{(3/2)}$; dấu bằng khi $3x^2 = 2y^2$. Hệ số α được chọn để hai bình phương bằng nhau tại điểm rơi. Balance the coefficients before using $x^2 + y^2 \geq 2xy$. For $\alpha > 0$, apply it to $\sqrt{\alpha} \cdot x$ and $y/\sqrt{\alpha}$: $\alpha x^2 + y^2/\alpha \geq 2xy$. For example $3x^2 + 2y^2 \geq 2\sqrt{6} \cdot xy$ for all real x, y : take $\alpha = \sqrt{(3/2)}$; equality when $3x^2 = 2y^2$. The coefficient α is chosen so that the two squares are equal at the equality point.

ĐỊNH LÝ 2.6 (Dấu tam thức bậc hai) / THEOREM 2.6 (Sign of a quadratic trinomial)

— Cho tam thức $f(x) = ax^2 + bx + c$ với $a > 0$. Khi đó $f(x) \geq 0$ với mọi số thực x khi và chỉ khi $\Delta = b^2 - 4ac \leq 0$.

Let $f(x) = ax^2 + bx + c$ with $a > 0$. Then $f(x) \geq 0$ for every real x if and only if $\Delta = b^2 - 4ac \leq 0$.

Chứng minh. / Proof.

Hoàn thành bình phương: $f(x) = a \cdot [(x + b/(2a))^2 - \Delta/(4a^2)]$. Nếu $\Delta \leq 0$ thì ngoặc bằng $(x + b/(2a))^2 + (-\Delta)/(4a^2)$, tổng hai số không âm, nên $f(x) \geq 0$. Nếu $\Delta > 0$, tại $x = -b/(2a)$ giá trị $f = -\Delta/(4a) < 0$.

Complete the square: $f(x) = a \cdot [(x + b/(2a))^2 - \Delta/(4a^2)]$. If $\Delta \leq 0$ the bracket equals $(x + b/(2a))^2 + (-\Delta)/(4a^2)$, a sum of two non-negative numbers, and $f(x) \geq 0$. If $\Delta > 0$, at $x = -b/(2a)$ the value is $f = -\Delta/(4a) < 0$. ■

NHẬN XÉT / REMARK — Dùng Định lý 2.6 như một công cụ chứng minh: $x^2 + y^2 + 1 \geq xy + x + y$ với mọi x, y thực. Xem về hiệu như tam thức theo x : $x^2 - (y + 1)x + (y^2 - y + 1)$, hệ số cao nhất $1 > 0$, $\Delta = (y + 1)^2 - 4(y^2 - y + 1) = -3y^2 + 6y - 3 = -3(y - 1)^2 \leq 0$. Vậy hiệu không âm, và dấu bằng cần $y = 1$ rồi $x = (y + 1)/2 = 1$.

Using Theorem 2.6 as a proof tool: $x^2 + y^2 + 1 \geq xy + x + y$ for all real x, y . View the difference as a trinomial in x : $x^2 - (y + 1)x + (y^2 - y + 1)$, leading coefficient $1 > 0$, $\Delta = (y + 1)^2 - 4(y^2 - y + 1) = -3y^2 + 6y - 3 = -3(y - 1)^2 \leq 0$. So the difference is non-negative, and equality needs $y = 1$ and then $x = (y + 1)/2 = 1$.

LỖI HAY GẶP / COMMON MISTAKE — Bình phương hai vế khi một vế có thể âm. Từ $a > b$ không suy ra $a^2 > b^2$: $a = 1, b = -2$ cho $1 < 4$. Chỉ được bình phương khi cả hai vế không âm (tính chất (v) ở trên).

Squaring both sides when one side may be negative. From $a > b$ one cannot deduce $a^2 > b^2$: $a = 1, b = -2$ gives $1 < 4$. Squaring is allowed only when both sides are non-negative (property (v) above).

2.2. Bất đẳng thức AM–GM và kỹ thuật điểm rơi — *The AM–GM inequality and the equality-point technique*

ĐỊNH LÝ 2.7 (AM–GM hai số) / THEOREM 2.7 (Two-term AM–GM) — Với mọi $a, b \geq 0$: $(a + b)/2 \geq \sqrt{ab}$. Dấu bằng khi và chỉ khi $a = b$.
For all $a, b \geq 0$: $(a + b)/2 \geq \sqrt{ab}$, with equality if and only if $a = b$.

Chứng minh. / *Proof.*

Đặt $x = \sqrt{a}$, $y = \sqrt{b}$. Theo Bổ đề 2.5(a): $a + b = x^2 + y^2 \geq 2xy = 2\sqrt{ab}$, dấu bằng khi $x = y$, tức $a = b$.

Put $x = \sqrt{a}$, $y = \sqrt{b}$. By Lemma 2.5(a): $a + b = x^2 + y^2 \geq 2xy = 2\sqrt{ab}$, with equality when $x = y$, that is $a = b$. ■

ĐỊNH LÝ 2.8 (AM–GM ba số) / THEOREM 2.8 (Three-term AM–GM) — Với mọi $a, b, c \geq 0$: $(a + b + c)/3 \geq \sqrt[3]{abc}$. Dấu bằng khi và chỉ khi $a = b = c$.
For all $a, b, c \geq 0$: $(a + b + c)/3 \geq \sqrt[3]{abc}$, with equality if and only if $a = b = c$.

Chứng minh. / *Proof.*

Đặt $x = \sqrt[3]{a}$, $y = \sqrt[3]{b}$, $z = \sqrt[3]{c}$, các số không âm. Ta dùng đồng nhất thức (kiểm tra bằng khai triển):

Put $x = \sqrt[3]{a}$, $y = \sqrt[3]{b}$, $z = \sqrt[3]{c}$, all non-negative. We use the identity (check by expanding):

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z) \cdot (x^2 + y^2 + z^2 - xy - yz - zx) \quad (2.2)$$

Thừa số thứ nhất không âm; thừa số thứ hai không âm theo (2.1). Vậy $a + b + c - 3\sqrt[3]{abc} \geq 0$.

The first factor is non-negative; the second is non-negative by (2.1). Hence $a + b + c - 3\sqrt[3]{abc} \geq 0$.

Dấu bằng khi $x + y + z = 0$ (suy ra $x = y = z = 0$) hoặc $x = y = z$. Cả hai trường hợp cho $a = b = c$.

Equality needs $x + y + z = 0$ (which forces $x = y = z = 0$) or $x = y = z$. Both cases give $a = b = c$. ■

ĐỊNH LÝ 2.9 (AM–GM n số) / THEOREM 2.9 (n-term AM–GM) — Với n số không âm $a_1, \dots, a_n$: $(a_1 + \dots + a_n)/n \geq (a_1 \cdot a_2 \cdots a_n)^{1/n}$. Dấu bằng khi và chỉ khi $a_1 = \dots = a_n$.
For n non-negative numbers $a_1, \dots, a_n$: $(a_1 + \dots + a_n)/n \geq (a_1 \cdot a_2 \cdots a_n)^{1/n}$, with equality if and only if $a_1 = \dots = a_n$.

Chứng minh. / *Proof.*

Nếu một số bằng 0 thì vế phải bằng 0, bất đẳng thức hiển nhiên, và dấu bằng chỉ xảy ra khi mọi số bằng 0. Xét các số dương. Gọi $P(n)$ là mệnh đề "bất đẳng thức và điều kiện dấu bằng đúng với n số dương". Ta dùng quy nạp Cauchy (quy nạp lên và lùi xuống).

If some number is 0 the right-hand side is 0, the inequality is clear, and equality forces all numbers to be 0. Consider positive numbers. Let $P(n)$ be the statement "the inequality and its

equality condition hold for n positive numbers". We use Cauchy's induction (go up, then step down).

1. $P(2)$ đúng theo Định lý 2.7.

$P(2)$ holds by Theorem 2.7.

2. $P(n) \Rightarrow P(2n)$. Chia $2n$ số thành hai nhóm n số, có trung bình cộng A_1, A_2 và trung bình nhân G_1, G_2 . Theo $P(n)$, $A_1 \geq G_1, A_2 \geq G_2$. Theo $P(2)$: trung bình cộng của $2n$ số bằng $(A_1 + A_2)/2 \geq (G_1 + G_2)/2 \geq \sqrt{(G_1 G_2)}$, mà $\sqrt{(G_1 G_2)}$ chính là trung bình nhân của $2n$ số. Dấu bằng buộc $A_1 = G_1, A_2 = G_2$ và $G_1 = G_2$; theo $P(n)$ mỗi nhóm gồm các số bằng nhau, và hai nhóm có cùng trung bình nhân nên mọi số bằng nhau.

$P(n) \Rightarrow P(2n)$. Split the $2n$ numbers into two groups of n , with arithmetic means A_1, A_2 and geometric means G_1, G_2 . By $P(n)$, $A_1 \geq G_1$ and $A_2 \geq G_2$. By $P(2)$: the arithmetic mean of the $2n$ numbers is $(A_1 + A_2)/2 \geq (G_1 + G_2)/2 \geq \sqrt{(G_1 G_2)}$, and $\sqrt{(G_1 G_2)}$ is exactly the geometric mean of the $2n$ numbers. Equality forces $A_1 = G_1, A_2 = G_2$ and $G_1 = G_2$; by $P(n)$ each group consists of equal numbers, and the two groups share the same geometric mean, so all numbers are equal.

3. $P(n) \Rightarrow P(n-1)$ với $n \geq 3$. Cho $n-1$ số dương $x_1, \dots, x_{n-1}$ có trung bình cộng m . Áp dụng $P(n)$ cho n số $x_1, \dots, x_{n-1}, m$: trung bình cộng của chúng vẫn bằng m , nên $m \geq (x_1 \cdots x_{n-1} \cdot m)^{1/n}$. Lũy thừa n hai vế (cả hai dương): $m^n \geq x_1 \cdots x_{n-1} \cdot m$, tức $m^{n-1} \geq x_1 \cdots x_{n-1}$. Dấu bằng khi đó là dấu bằng của $P(n)$, buộc $x_1 = \dots = x_{n-1} = m$.

$P(n) \Rightarrow P(n-1)$ for $n \geq 3$. Take $n-1$ positive numbers $x_1, \dots, x_{n-1}$ with arithmetic mean m . Apply $P(n)$ to the n numbers $x_1, \dots, x_{n-1}, m$: their arithmetic mean is still m , so $m \geq (x_1 \cdots x_{n-1} \cdot m)^{1/n}$. Raise both (positive) sides to the power n : $m^n \geq x_1 \cdots x_{n-1} \cdot m$, that is $m^{n-1} \geq x_1 \cdots x_{n-1}$. Equality here is equality in $P(n)$, which forces $x_1 = \dots = x_{n-1} = m$.

Từ $P(2)$, bước 2 cho $P(4), P(8), P(16), \dots$, tức $P(2^k)$ với mọi k ; với n bất kỳ chọn $2^k \geq n$ rồi lùi bằng bước 3 từng đơn vị xuống n . Vậy $P(n)$ đúng với mọi $n \geq 2$.

From $P(2)$, step 2 gives $P(4), P(8), P(16), \dots$, that is $P(2^k)$ for every k ; for any n pick $2^k \geq n$ and step down one unit at a time with step 3. Hence $P(n)$ holds for all $n \geq 2$. ■

HỆ QUẢ 2.10 / COROLLARY 2.10 — Nếu $x_1, \dots, x_n > 0$ và $x_1 \cdot x_2 \cdots x_n = 1$ thì $x_1 + \dots + x_n \geq n$, dấu bằng khi và chỉ khi mọi $x_i = 1$.

If $x_1, \dots, x_n > 0$ and $x_1 \cdot x_2 \cdots x_n = 1$ then $x_1 + \dots + x_n \geq n$, with equality if and only if every $x_i = 1$.

Chứng minh. / Proof.

Theo Định lý 2.9: $(x_1 + \dots + x_n)/n \geq 1^{1/n} = 1$, dấu bằng khi các số bằng nhau; khi đó mỗi số bằng 1 vì tích bằng 1.

By Theorem 2.9: $(x_1 + \dots + x_n)/n \geq 1^{1/n} = 1$, with equality when the numbers are equal; then each equals 1 because the product is 1. ■

ĐỊNH NGHĨA 2.11 (Điểm rơi) / DEFINITION 2.11 (Equality point) — Cho biểu thức f cần tìm giá trị nhỏ nhất (lớn nhất) trên một miền. Điểm rơi là bộ giá trị của các biến tại đó giá trị ấy đạt được. Khi dùng AM–GM, điểm rơi phải làm các số trong cùng một trung bình bằng nhau.

Let f be an expression whose minimum (maximum) is sought on a region. The equality point is the set

of values of the variables at which this value is attained. When AM–GM is used, the equality point must make all numbers inside one mean equal.

Quy trình dùng điểm rơi gồm ba việc, theo thứ tự: dự đoán điểm rơi (thường nơi các biến đối xứng, hoặc nơi một biến chạm biên); chọn hệ số tách để các số trong AM–GM bằng nhau tại điểm đó; áp dụng AM–GM rồi kiểm tra điểm rơi có thuộc miền xác định không.

The equality-point procedure has three steps, in this order: guess the equality point (usually where the variables are symmetric, or where one variable meets the boundary); choose the split coefficients so that the numbers inside AM–GM are equal at that point; apply AM–GM and check that the equality point lies in the domain.

PHÂN TÍCH / ANALYSIS — Cần chặn dưới $x + 4/x^2$ với $x > 0$. Tích hai hạng tử x và $4/x^2$ vẫn còn x , nên AM–GM hai số không khử được biến. Muốn tích là hằng số ta cần tổng $x/2 + x/2 + 4/x^2$: tích là $(x/2) \cdot (x/2) \cdot (4/x^2) = 1$. Việc tách x thành hai nửa bằng nhau thể hiện điều ta muốn: ba số bằng nhau tại điểm rơi, tức $x/2 = 4/x^2$, suy ra $x^3 = 8$.

We need a lower bound for $x + 4/x^2$ with $x > 0$. The product of the two terms x and $4/x^2$ still contains x , so two-term AM–GM cannot remove the variable. To make the product a constant we want the sum $x/2 + x/2 + 4/x^2$: its product is $(x/2) \cdot (x/2) \cdot (4/x^2) = 1$. Splitting x into two equal halves expresses what we want: the three numbers are equal at the equality point, $x/2 = 4/x^2$, so $x^3 = 8$.

VÍ DỤ 2.3 (Điểm rơi, tách hạng tử) / EXAMPLE 2.3 (Equality point, splitting) — Tìm giá trị nhỏ nhất của biểu thức $x + 4/x^2$ với $x > 0$.

Find the minimum of $x + 4/x^2$ for $x > 0$.

Lời giải. / Solution.

Viết $x + 4/x^2 = x/2 + x/2 + 4/x^2$ rồi áp dụng Định lý 2.8 cho ba số dương:

Write $x + 4/x^2 = x/2 + x/2 + 4/x^2$ and apply Theorem 2.8 to the three positive numbers:

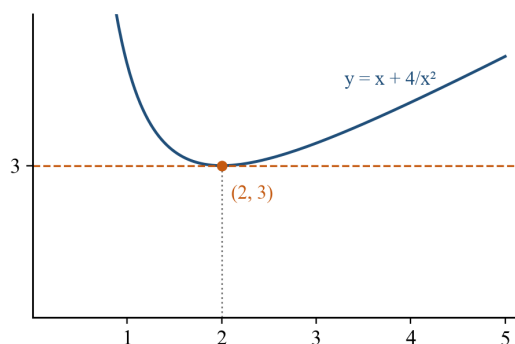
$$x/2 + x/2 + 4/x^2 \geq 3 \cdot \sqrt[3]{(x/2) \cdot (x/2) \cdot (4/x^2)} = 3 \cdot \sqrt[3]{1} = 3$$

Dấu bằng khi $x/2 = 4/x^2$, tức $x^3 = 8$, $x = 2$ (thuộc miền $x > 0$). Kiểm tra: $2 + 4/4 = 3$.

Equality holds when $x/2 = 4/x^2$, that is $x^3 = 8$, $x = 2$ (which lies in $x > 0$). Check: $2 + 4/4 = 3$.

Vậy giá trị nhỏ nhất bằng 3, đạt tại $x = 2$.

Hence the minimum is 3, attained at $x = 2$. ■



Hình 2.1. Đồ thị $y = x + 4/x^2$: cực tiểu 3 tại $x = 2$

Figure 2.1. Graph of $y = x + 4/x^2$: minimum 3 at $x = 2$

VÍ DỤ 2.4 (Nhân ba bất đẳng thức) / EXAMPLE 2.4 (Multiplying three inequalities) —

Chứng minh rằng với mọi $a, b, c > 0$: $(a + b)(b + c)(c + a) \geq 8abc$.

Prove that for all $a, b, c > 0$: $(a + b)(b + c)(c + a) \geq 8abc$.

Lời giải. / Solution.

Theo Định lý 2.7 áp dụng cho từng cặp: $a + b \geq 2\sqrt{ab}$, $b + c \geq 2\sqrt{bc}$, $c + a \geq 2\sqrt{ca}$.

By Theorem 2.7 applied to each pair: $a + b \geq 2\sqrt{ab}$, $b + c \geq 2\sqrt{bc}$, $c + a \geq 2\sqrt{ca}$.

Cả ba vế đều dương nên nhân được theo vế (Tính chất 2.2(iii)):

All three sides are positive, so we may multiply them (Property 2.2(iii)):

$$(a + b)(b + c)(c + a) \geq 8 \cdot \sqrt{ab} \cdot \sqrt{bc} \cdot \sqrt{ca} = 8 \cdot \sqrt{a^2 b^2 c^2} = 8abc$$

Dấu bằng khi $a = b$, $b = c$, $c = a$, tức $a = b = c$.

Equality holds when $a = b$, $b = c$, $c = a$, that is $a = b = c$. ■

NHẬN XÉT / REMARK — Theo Tính chất 2.3(c), $(a + b)(b + c)(c + a) \geq 8abc$ tương đương $p \cdot q - abc \geq 8abc$, tức $(a + b + c)(ab + bc + ca) \geq 9abc$. Chia cho $abc > 0$ ta được $(a + b + c)(1/a + 1/b + 1/c) \geq 9$, bất đẳng thức tổng nghịch đảo cho $n = 3$.

By Property 2.3(c), $(a + b)(b + c)(c + a) \geq 8abc$ is equivalent to $p \cdot q - abc \geq 8abc$, that is $(a + b + c)(ab + bc + ca) \geq 9abc$. Dividing by $abc > 0$ we get $(a + b + c)(1/a + 1/b + 1/c) \geq 9$, the reciprocal-sum inequality for $n = 3$.

PHÂN TÍCH / ANALYSIS — Cần chặn trên x^2y khi biết tổng $x + y = 6$. Tích $x \cdot x \cdot y$ có ba thừa số, nên dùng AM–GM ba số cho ba số mà tổng của chúng là hằng số. Tổng $x + x + y$ không là hằng số, nhưng $x/2 + x/2 + y = x + y = 6$ thì có. Vậy dùng ba số $x/2$, $x/2$, y . Điểm rơi là $x/2 = y$.

We need an upper bound for x^2y given $x + y = 6$. The product $x \cdot x \cdot y$ has three factors, so we use three-term AM–GM on three numbers whose sum is a constant. The sum $x + x + y$ is not constant, but $x/2 + x/2 + y = x + y = 6$ is. So we use the three numbers $x/2$, $x/2$, y . The equality point is $x/2 = y$.

VÍ DỤ 2.5 (Tổng không đổi, chia trọng số) / EXAMPLE 2.5 (Fixed sum, weighting) —

Cho $x, y > 0$ với $x + y = 6$. Tìm giá trị lớn nhất của x^2y .

Let $x, y > 0$ with $x + y = 6$. Find the maximum of x^2y .

Lời giải. / Solution.

Theo Định lý 2.8 cho ba số dương $x/2$, $x/2$, y :

By Theorem 2.8 for the three positive numbers $x/2$, $x/2$, y :

$$(x/2) \cdot (x/2) \cdot y \leq ((x/2 + x/2 + y)/3)^3 = (6/3)^3 = 8$$

Do đó $x^2y = 4 \cdot (x/2) \cdot (x/2) \cdot y \leq 32$.

Hence $x^2y = 4 \cdot (x/2) \cdot (x/2) \cdot y \leq 32$.

Dấu bằng khi $x/2 = y$ và $x + y = 6$, tức $x = 4$, $y = 2$. Kiểm tra: $4^2 \cdot 2 = 32$.

Equality holds when $x/2 = y$ and $x + y = 6$, that is $x = 4$, $y = 2$. Check: $4^2 \cdot 2 = 32$.

Vậy giá trị lớn nhất của x^2y bằng 32, đạt tại $(x, y) = (4, 2)$.

Hence the maximum of x^2y is 32, attained at $(x, y) = (4, 2)$. ■

PHÂN TÍCH / ANALYSIS — Tích $1 \cdot 2 \cdots n$ thuộc về trung bình nhân của n số $1, 2, \dots, n$, còn trung bình cộng của chúng tính được ngay bằng công thức tổng cấp số cộng: $(n+1)/2$. Đề đòi bất đẳng thức chặt, nên cần chỉ ra các số không bằng nhau.

The product $1 \cdot 2 \cdots n$ is the geometric mean (to the power n) of the n numbers $1, 2, \dots, n$, and their arithmetic mean follows at once from the sum of an arithmetic progression: $(n+1)/2$. The statement asks for a strict inequality, so we must point out that the numbers are not all equal.

VÍ DỤ 2.6 (AM–GM cho dãy số nguyên) / EXAMPLE 2.6 (AM–GM on a run of integers) — Chứng minh rằng với mọi số nguyên $n \geq 2$: $n! < ((n+1)/2)^n$.

Prove that for every integer $n \geq 2$: $n! < ((n+1)/2)^n$.

Lời giải. / Solution.

Áp dụng Định lý 2.9 cho n số dương $1, 2, \dots, n$. Trung bình cộng của chúng là $(1 + 2 + \dots + n)/n = (n+1)/2$.

Apply Theorem 2.9 to the n positive numbers $1, 2, \dots, n$. Their arithmetic mean is $(1 + 2 + \dots + n)/n = (n+1)/2$.

$$(n+1)/2 \geq (1 \cdot 2 \cdots n)^{1/n} = (n!)^{1/n}$$

Với $n \geq 2$ các số $1, 2, \dots, n$ không bằng nhau (chẳng hạn $1 \neq 2$) nên dấu bằng không xảy ra, bất đẳng thức là chặt.

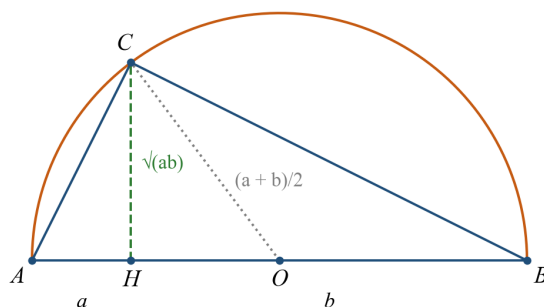
For $n \geq 2$ the numbers $1, 2, \dots, n$ are not all equal (for instance $1 \neq 2$), so equality cannot occur and the inequality is strict.

Lũy thừa n hai vế dương: $n! < ((n+1)/2)^n$.

Raising both positive sides to the power n : $n! < ((n+1)/2)^n$. ■

NHẬN XÉT / REMARK — Hình học của AM–GM hai số: trên đường kính $AB = a + b$ của nửa đường tròn, lấy H sao cho $AH = a$, $HB = b$; đường vuông góc với AB tại H cắt nửa đường tròn ở C . Theo hệ thức lượng trong tam giác vuông ACB , $CH^2 = AH \cdot HB = ab$, nên $CH = \sqrt{ab}$; còn bán kính $OC = (a+b)/2$ không nhỏ hơn đường cao CH . Dấu bằng khi H trùng O .

The geometry of two-term AM–GM: on the diameter $AB = a + b$ of a semicircle take H with $AH = a$, $HB = b$; the perpendicular to AB at H meets the semicircle at C . By the metric relation in the right triangle ACB , $CH^2 = AH \cdot HB = ab$, so $CH = \sqrt{ab}$, while the radius $OC = (a+b)/2$ is at least the altitude CH . Equality when H coincides with O .



Hình 2.2. AM–GM hai số trên nửa đường tròn: $CH = \sqrt{ab} \leq OC = (a + b)/2$

Figure 2.2. Two-term AM–GM on a semicircle: $CH = \sqrt{ab} \leq OC = (a + b)/2$

LỖI HAY GẶP / COMMON MISTAKE — Áp dụng AM–GM mà điểm rơi nằm ngoài miền. Với $x \geq 2$, từ $x + 1/x \geq 2$ không được kết luận giá trị nhỏ nhất là 2: dấu bằng cần $x = 1$, không thuộc miền. Giá trị nhỏ nhất thật là $5/2$, đạt tại $x = 2$. Mọi dấu bằng trong chuỗi phải xảy ra đồng thời tại một điểm của miền.

Applying AM–GM when the equality point lies outside the domain. For $x \geq 2$, from $x + 1/x \geq 2$ one may not conclude that the minimum is 2: equality needs $x = 1$, which is not in the domain. The true minimum is $5/2$, attained at $x = 2$. Every equality in a chain must hold simultaneously at one point of the domain.

LỖI HAY GẶP / COMMON MISTAKE — Dùng AM–GM cho số có thể âm. Với $a, b < 0$ thì $(a + b)/2 \geq \sqrt{ab}$ vô nghĩa. Kiểm tra $a, b \geq 0$ trước khi áp dụng, và với $x + 4/x^2$ chỉ xét $x > 0$.

Using AM–GM on numbers that may be negative. For $a, b < 0$ the statement $(a + b)/2 \geq \sqrt{ab}$ makes no sense. Check $a, b \geq 0$ first, and for $x + 4/x^2$ consider only $x > 0$.

PHẢI THUỘC / MEMORISE — AM–GM: $(a_1 + \dots + a_n)/n \geq (a_1 \cdots a_n)^{1/n}$ với $a_i \geq 0$, dấu bằng khi và chỉ khi mọi a_i bằng nhau. Dạng ba số: $a + b + c \geq 3\sqrt[3]{abc}$.

AM–GM: $(a_1 + \dots + a_n)/n \geq (a_1 \cdots a_n)^{1/n}$ for $a_i \geq 0$, with equality if and only if all a_i are equal. Three-term form: $a + b + c \geq 3\sqrt[3]{abc}$.

2.3. Bất đẳng thức Cauchy–Schwarz — The Cauchy–Schwarz inequality

ĐỊNH LÝ 2.12 (Cauchy–Schwarz (Bunyakovsky)) / THEOREM 2.12 (Cauchy–Schwarz (Bunyakovsky)) — Với mọi số thực $a_1, \dots, a_n$ và $b_1, \dots, b_n$: $(a_1b_1 + \dots + a_nb_n)^2 \leq (a_1^2 + \dots + a_n^2)(b_1^2 + \dots + b_n^2)$. Dấu bằng khi và chỉ khi $a_ib_j = a_jb_i$ với mọi i, j (hai bộ số tỉ lệ với nhau).
For all real $a_1, \dots, a_n$ and $b_1, \dots, b_n$: $(a_1b_1 + \dots + a_nb_n)^2 \leq (a_1^2 + \dots + a_n^2)(b_1^2 + \dots + b_n^2)$. Equality holds if and only if $a_ib_j = a_jb_i$ for all i, j (the two lists are proportional).

Chứng minh. / Proof.

Dùng đồng nhất thức Lagrange, gồm tổng trên mọi cặp chỉ số $i < j$:

We use Lagrange's identity, where the sum runs over all pairs of indices $i < j$:

$$(a_1^2 + \dots + a_n^2)(b_1^2 + \dots + b_n^2) - (a_1b_1 + \dots + a_nb_n)^2 = \sum (a_ib_j - a_jb_i)^2 \quad (2.3)$$

Đồng nhất thức đúng vì khai triển vế trái cho tổng $\sum_{i,j} a_i^2 b_j^2$ trừ đi $\sum_{i,j} a_i b_i a_j b_j$; các số hạng $i = j$ triệt tiêu, mỗi cặp $i < j$ còn $a_i^2 b_j^2 + a_j^2 b_i^2 - 2a_i b_i a_j b_j = (a_i b_j - a_j b_i)^2$.

The identity holds because expanding the left side gives $\sum_{i,j} a_i^2 b_j^2$ minus $\sum_{i,j} a_i b_i a_j b_j$; the terms with $i = j$ cancel, and each pair $i < j$ leaves $a_i^2 b_j^2 + a_j^2 b_i^2 - 2a_i b_i a_j b_j = (a_i b_j - a_j b_i)^2$.

Vế phải là tổng các bình phương nên không âm, từ đó có bất đẳng thức. Nó bằng 0 khi và chỉ khi mọi hiệu $a_i b_j - a_j b_i$ bằng 0.

The right side is a sum of squares and so is non-negative, which gives the inequality. It is 0 if and only if every difference $a_i b_j - a_j b_i$ is 0. ■

NHẬN XÉT / REMARK — Chứng minh thứ hai của Định lý 2.12 bằng tam thức bậc hai.

Xét $f(t) = \sum (a_i t - b_i)^2 = A \cdot t^2 - 2B \cdot t + C$ với $A = \sum a_i^2$, $B = \sum a_i b_i$, $C = \sum b_i^2$. Vì $f(t) \geq 0$ với mọi t , và nếu $A > 0$ thì tam thức bậc hai không có hai nghiệm phân biệt, nên biệt thức rút gọn $B^2 - AC \leq 0$, tức $B^2 \leq AC$. Nếu $A = 0$ thì mọi $a_i = 0$ và hai vế đều bằng 0.

A second proof of Theorem 2.12 through a quadratic trinomial. Consider $f(t) = \sum (a_i t - b_i)^2 = A \cdot t^2 - 2B \cdot t + C$ with $A = \sum a_i^2$, $B = \sum a_i b_i$, $C = \sum b_i^2$. Since $f(t) \geq 0$ for every t , and if $A > 0$ the trinomial cannot have two distinct roots, the reduced discriminant satisfies $B^2 - AC \leq 0$, that is $B^2 \leq AC$. If $A = 0$ then every $a_i = 0$ and both sides are 0.

HỆ QUẢ 2.13 (Dạng Engel (Titu)) / COROLLARY 2.13 (Engel form (Titu's lemma)) —

Với $a_1, \dots, a_n$ thực và $b_1, \dots, b_n > 0$: $a_1^2/b_1 + \dots + a_n^2/b_n \geq (a_1 + \dots + a_n)^2/(b_1 + \dots + b_n)$. Dấu bằng khi và chỉ khi $a_1/b_1 = \dots = a_n/b_n$.

For real $a_1, \dots, a_n$ and $b_1, \dots, b_n > 0$: $a_1^2/b_1 + \dots + a_n^2/b_n \geq (a_1 + \dots + a_n)^2/(b_1 + \dots + b_n)$. Equality holds if and only if $a_1/b_1 = \dots = a_n/b_n$.

Chứng minh. / Proof.

Áp dụng Định lý 2.12 cho hai bộ số $x_i = a_i/\sqrt{b_i}$ và $y_i = \sqrt{b_i}$:

Apply Theorem 2.12 to the two lists $x_i = a_i/\sqrt{b_i}$ and $y_i = \sqrt{b_i}$:

$$(\sum a_i)^2 = (\sum x_i y_i)^2 \leq (\sum x_i^2)(\sum y_i^2) = (\sum a_i^2/b_i) \cdot (\sum b_i)$$

Chia hai vế cho $\sum b_i > 0$. Dấu bằng khi $x_i/y_i = a_i/b_i$ không đổi theo i .

Divide both sides by $\sum b_i > 0$. Equality holds when $x_i/y_i = a_i/b_i$ does not depend on i . ■

HỆ QUẢ 2.14 (Cauchy–Schwarz dạng căn) / COROLLARY 2.14 (Radical form of Cauchy–Schwarz) —

Với $a_1, \dots, a_n \geq 0$ và $b_1, \dots, b_n \geq 0$: $\sqrt{a_1 b_1} + \dots + \sqrt{a_n b_n} \leq \sqrt{(a_1 + \dots + a_n)(b_1 + \dots + b_n)}$. Dấu bằng khi hai bộ tỉ lệ nhau.

For $a_1, \dots, a_n \geq 0$ and $b_1, \dots, b_n \geq 0$: $\sqrt{a_1 b_1} + \dots + \sqrt{a_n b_n} \leq \sqrt{(a_1 + \dots + a_n)(b_1 + \dots + b_n)}$. Equality when the two lists are proportional.

Chứng minh. / Proof.

Áp dụng Định lý 2.12 cho hai bộ $\sqrt{a_i}$ và $\sqrt{b_i}$ (các số thực không âm): $(\sum \sqrt{a_i} \cdot \sqrt{b_i})^2 \leq (\sum a_i)(\sum b_i)$. Lấy căn bậc hai không âm hai vế.

Apply Theorem 2.12 to the lists $\sqrt{a_i}$ and $\sqrt{b_i}$ (non-negative reals): $(\sum \sqrt{a_i} \cdot \sqrt{b_i})^2 \leq (\sum a_i)(\sum b_i)$. Take non-negative square roots of both sides. ■

$$a^2/x + b^2/y + c^2/z \geq (a + b + c)^2/(x + y + z) \quad (2.4)$$

ĐỊNH LÝ 2.15 (Hölder ba bộ ba số) / THEOREM 2.15 (Hölder for three triples) — Với mọi số không âm a_i, x_i, u_i ($i = 1, 2, 3$): $(a_1^3 + a_2^3 + a_3^3)(x_1^3 + x_2^3 + x_3^3)(u_1^3 + u_2^3 + u_3^3) \geq (a_1x_1u_1 + a_2x_2u_2 + a_3x_3u_3)^3$.

For all non-negative a_i, x_i, u_i ($i = 1, 2, 3$): $(a_1^3 + a_2^3 + a_3^3)(x_1^3 + x_2^3 + x_3^3)(u_1^3 + u_2^3 + u_3^3) \geq (a_1x_1u_1 + a_2x_2u_2 + a_3x_3u_3)^3$.

Chứng minh. / Proof.

Đặt $A = \sum a_i^3$, $X = \sum x_i^3$, $U = \sum u_i^3$. Nếu một trong ba số này bằng 0 thì bộ tương ứng toàn số 0 và hai vế đều bằng 0. Xét $A, X, U > 0$. Với mỗi i , theo Định lý 2.8:

Put $A = \sum a_i^3$, $X = \sum x_i^3$, $U = \sum u_i^3$. If one of them is 0 the corresponding triple is all zeros and both sides are 0. Take $A, X, U > 0$. For each i , by Theorem 2.8:

$$a_i^3/A + x_i^3/X + u_i^3/U \geq 3 \cdot a_i x_i u_i / (AXU)^{1/3}$$

Cộng ba bất đẳng thức ($i = 1, 2, 3$): vế trái bằng $1 + 1 + 1 = 3$, nên $3 \geq 3 \cdot \sum a_i x_i u_i / (AXU)^{1/3}$, tức $(AXU)^{1/3} \geq \sum a_i x_i u_i$. Lập phương hai vế không âm.

Add the three inequalities ($i = 1, 2, 3$): the left side is $1 + 1 + 1 = 3$, so $3 \geq 3 \cdot \sum a_i x_i u_i / (AXU)^{1/3}$, that is $(AXU)^{1/3} \geq \sum a_i x_i u_i$. Cube both non-negative sides. ■

NHẬN XÉT / REMARK — Lấy $x_i = u_i = 1$ trong Định lý 2.15 được $9 \cdot \sum a_i^3 \geq (\sum a_i)^3$, tức $a^3 + b^3 + c^3 \geq (a + b + c)^3/9$. Kết quả này cũng suy ra từ Chebyshev; cách này không cần sắp thứ tự.

Taking $x_i = u_i = 1$ in Theorem 2.15 gives $9 \cdot \sum a_i^3 \geq (\sum a_i)^3$, that is $a^3 + b^3 + c^3 \geq (a + b + c)^3/9$. The same result follows from Chebyshev; this route needs no ordering of the numbers.

Dạng Engel là công cụ chính để chặn dưới một tổng phân thức: tử số là bình phương, mẫu số là các số dương. Khi tử không sẵn bình phương, nhân cả tử và mẫu với cùng một số để tạo ra bình phương.

The Engel form is the main tool for bounding a sum of fractions from below: the numerators are squares and the denominators are positive. When a numerator is not already a square, multiply numerator and denominator by the same number to create one.

PHÂN TÍCH / ANALYSIS — Đề cho điều kiện $x^2 + 2y^2 + 3z^2 = 6$ và hỏi giá trị lớn nhất của tổng $x + y + z$, một biểu thức bậc nhất. Cauchy–Schwarz nối một tổng bậc nhất với tổng các bình phương. Ta cần viết $x + y + z = \sum a_i b_i$ sao cho $\sum b_i^2$ chính là $x^2 + 2y^2 + 3z^2$: chọn $b = (x, \sqrt{2} \cdot y, \sqrt{3} \cdot z)$ và $a = (1, 1/\sqrt{2}, 1/\sqrt{3})$.

The statement gives the condition $x^2 + 2y^2 + 3z^2 = 6$ and asks for the maximum of the sum $x + y + z$, a linear expression. Cauchy–Schwarz links a linear sum with a sum of squares. We need $x + y + z = \sum a_i b_i$ with $\sum b_i^2$ equal to $x^2 + 2y^2 + 3z^2$: take $b = (x, \sqrt{2} \cdot y, \sqrt{3} \cdot z)$ and $a = (1, 1/\sqrt{2}, 1/\sqrt{3})$.

VÍ DỤ 2.7 (Cauchy–Schwarz có trọng số) / EXAMPLE 2.7 (Weighted Cauchy–Schwarz)

— Cho x, y, z là các số thực thỏa mãn $x^2 + 2y^2 + 3z^2 = 6$. Tìm giá trị lớn nhất của $x + y + z$.

Let x, y, z be real numbers with $x^2 + 2y^2 + 3z^2 = 6$. Find the maximum of $x + y + z$.

Lời giải. / Solution.

Viết $x + y + z = 1 \cdot x + (1/\sqrt{2}) \cdot (\sqrt{2} \cdot y) + (1/\sqrt{3}) \cdot (\sqrt{3} \cdot z)$ và áp dụng Định lý 2.12:

Write $x + y + z = 1 \cdot x + (1/\sqrt{2}) \cdot (\sqrt{2} \cdot y) + (1/\sqrt{3}) \cdot (\sqrt{3} \cdot z)$ and apply Theorem 2.12:

$$(x + y + z)^2 \leq (1 + 1/2 + 1/3) \cdot (x^2 + 2y^2 + 3z^2) = (11/6) \cdot 6 = 11$$

Suy ra $x + y + z \leq \sqrt{11}$.

Hence $x + y + z \leq \sqrt{11}$.

Dấu bằng khi $(x, \sqrt{2} \cdot y, \sqrt{3} \cdot z)$ tỉ lệ với $(1, 1/\sqrt{2}, 1/\sqrt{3})$, tức $x = k, y = k/2, z = k/3$ với $k > 0$. Thế vào điều kiện: $k^2(1 + 2/4 + 3/9) = (11/6)k^2 = 6$, nên $k = 6/\sqrt{11}$. Khi đó $x + y + z = (11/6) \cdot k = \sqrt{11}$.

Equality holds when $(x, \sqrt{2} \cdot y, \sqrt{3} \cdot z)$ is proportional to $(1, 1/\sqrt{2}, 1/\sqrt{3})$, that is $x = k, y = k/2, z = k/3$ with $k > 0$. Substituting into the condition: $k^2(1 + 2/4 + 3/9) = (11/6)k^2 = 6$, so $k = 6/\sqrt{11}$. Then $x + y + z = (11/6) \cdot k = \sqrt{11}$.

Vậy giá trị lớn nhất bằng $\sqrt{11}$.

Hence the maximum is $\sqrt{11}$. ■

PHÂN TÍCH / ANALYSIS — Mẫu số $a + 2b, b + 2c, c + 2a$ cộng lại cho $3(a + b + c) = 9$, một hằng số, còn tử số đều bằng $1 = 1^2$. Đó là đúng hình dáng của dạng Engel: tử là bình phương, tổng mẫu là hằng số.

The denominators $a + 2b, b + 2c, c + 2a$ add up to $3(a + b + c) = 9$, a constant, and the numerators are all $1 = 1^2$. This is exactly the shape of the Engel form: square numerators and a constant sum of denominators.

VÍ DỤ 2.8 (Dạng Engel với tử bằng 1) / EXAMPLE 2.8 (Engel form with numerator 1)

— Cho $a, b, c > 0$ với $a + b + c = 3$. Chứng minh rằng $1/(a + 2b) + 1/(b + 2c) + 1/(c + 2a) \geq 1$.

Let $a, b, c > 0$ with $a + b + c = 3$. Prove that $1/(a + 2b) + 1/(b + 2c) + 1/(c + 2a) \geq 1$.

Lời giải. / Solution.

Viết mỗi số hạng dưới dạng $1^2/(\text{mẫu})$ và áp dụng Hệ quả 2.13:

Write each term as $1^2/(\text{denominator})$ and apply Corollary 2.13:

$$1/(a + 2b) + 1/(b + 2c) + 1/(c + 2a) \geq (1 + 1 + 1)^2 / [(a + 2b) + (b + 2c) + (c + 2a)] = 9 / (3(a + b + c)) = 9/9 = 1$$

Dấu bằng khi $a + 2b = b + 2c = c + 2a$. Từ hai đẳng thức này: $a + b = 2c$ và $b + c = 2a$. Trừ vế theo vế: $a - c = 2c - 2a$, suy ra $a = c$, rồi $b = 2a - c = a$. Với $a + b + c = 3$ ta được $a = b = c = 1$; kiểm tra: ba phân số bằng $1/3$, tổng bằng 1.

Equality needs $a + 2b = b + 2c = c + 2a$. These give $a + b = 2c$ and $b + c = 2a$. Subtracting: $a - c = 2c - 2a$, so $a = c$, and then $b = 2a - c = a$. With $a + b + c = 3$ we get $a = b = c = 1$; check: three fractions equal to $1/3$, sum 1.

Vậy bất đẳng thức đúng, dấu bằng tại $a = b = c = 1$.

Hence the inequality holds, with equality at $a = b = c = 1$. ■

NHẬN XÉT / REMARK — Cách khác cho Ví dụ 2.8: theo Định lý 2.8, tổng ba số dương không nhỏ hơn $3 \cdot \sqrt[3]{\text{tích}}$. Ở đây tích các nghịch đảo bằng $1/[(a + 2b)(b + 2c)(c + 2a)]$, còn theo AM–GM các mẫu có tích nhỏ hơn hoặc bằng $((9)/3)^3 = 27$, nên tổng $\geq 3 \cdot \sqrt[3]{(1/27)} = 1$. Hai

cách cho cùng dấu bằng $a = b = c = 1$.

Another route for Example 2.8: by Theorem 2.8 the sum of three positive numbers is at least $3 \cdot \sqrt[3]{\text{product}}$. Here the product of the reciprocals is $1/[(a+2b)(b+2c)(c+2a)]$, and by AM–GM the denominators have product at most $(9/3)^3 = 27$, so the sum is at least $3 \cdot \sqrt[3]{1/27} = 1$. Both routes give the same equality case $a = b = c = 1$.

PHÂN TÍCH / ANALYSIS — Tổng $a/b + b/c + c/a$ có mẫu khác nhau và tử không phải bình phương. Viết $a/b = a^2/(ab)$: tử thành bình phương, mẫu là các tích đôi một ab, bc, ca . Tổng mẫu là $ab + bc + ca$, mà tổng tử trước khi bình phương là $a + b + c$, vậy dạng Engel cho $(a + b + c)^2/(ab + bc + ca)$.

The sum $a/b + b/c + c/a$ has different denominators and the numerators are not squares. Write $a/b = a^2/(ab)$: the numerator becomes a square and the denominators are the pairwise products ab, bc, ca . Their sum is $ab + bc + ca$ and the numerators sum to $a + b + c$ before squaring, so the Engel form gives $(a + b + c)^2/(ab + bc + ca)$.

VÍ DỤ 2.9 (Tạo bình phương ở tử) / EXAMPLE 2.9 (Creating squares in the numerators) — Chứng minh rằng với mọi $a, b, c > 0$: $a/b + b/c + c/a \geq (a + b + c)^2/(ab + bc + ca) \geq 3$.

Prove that for all $a, b, c > 0$: $a/b + b/c + c/a \geq (a + b + c)^2/(ab + bc + ca) \geq 3$.

Lời giải. / Solution.

Viết $a/b = a^2/(ab)$, $b/c = b^2/(bc)$, $c/a = c^2/(ca)$ rồi dùng Hệ quả 2.13 với các mẫu dương ab, bc, ca :

Write $a/b = a^2/(ab)$, $b/c = b^2/(bc)$, $c/a = c^2/(ca)$ and use Corollary 2.13 with the positive denominators ab, bc, ca :

$$a/b + b/c + c/a \geq (a + b + c)^2/(ab + bc + ca)$$

Bất đẳng thức thứ hai tương đương $(a + b + c)^2 \geq 3(ab + bc + ca)$ (nhân hai vế với $ab + bc + ca > 0$), tức $a^2 + b^2 + c^2 \geq ab + bc + ca$, đúng theo Bổ đề 2.5(c).

The second inequality is equivalent to $(a + b + c)^2 \geq 3(ab + bc + ca)$ (multiply by $ab + bc + ca > 0$), that is $a^2 + b^2 + c^2 \geq ab + bc + ca$, which holds by Lemma 2.5(c).

Dấu bằng ở cả hai bước khi $a/(ab) = b/(bc) = c/(ca)$, tức $1/b = 1/c = 1/a$, và $a = b = c$. Vậy dấu bằng khi $a = b = c$.

Equality in both steps needs $a/(ab) = b/(bc) = c/(ca)$, that is $1/b = 1/c = 1/a$, together with $a = b = c$. Hence equality holds when $a = b = c$. ■

NHẬN XÉT / REMARK — Hai bộ số trong Định lý 2.12 có thể chọn tùy ý. Chọn sao cho một trong hai tổng bình phương là hằng số (hoặc là điều kiện đề cho) thì vế phải trở thành một số biết trước. Dấu bằng cho ta điểm rơi: hai bộ tỉ lệ nhau.

The two lists in Theorem 2.12 can be chosen freely. Choose them so that one of the two sums of squares is a constant (or the given condition); the right-hand side then becomes a known number. The equality case gives the equality point: the two lists are proportional.

NHẬN XÉT / REMARK — Ý nghĩa hình học của Định lý 2.12 với $n = 2$: $u = (a, b)$ và $v = (c, d)$ có tích vô hướng $u \cdot v = ac + bd = |u| \cdot |v| \cdot \cos \varphi$, nên $(ac + bd)^2 \leq |u|^2 \cdot |v|^2 = (a^2 + b^2)(c^2 +$

d^2) vì $\cos^2 \varphi \leq 1$. Dấu bằng khi $\varphi = 0$ hoặc $\varphi = 180$ độ, tức hai vectơ song song, đúng điều kiện $ad = bc$.

Geometric meaning of Theorem 2.12 for $n = 2$: $u = (a, b)$ and $v = (c, d)$ have dot product $u \cdot v = ac + bd = |u| \cdot |v| \cdot \cos \varphi$, so $(ac + bd)^2 \leq |u|^2 \cdot |v|^2 = (a^2 + b^2)(c^2 + d^2)$ because $\cos^2 \varphi \leq 1$. Equality when $\varphi = 0$ or $\varphi = 180$ degrees, that is when the two vectors are parallel, exactly the condition $ad = bc$.

LỖI HAY GẶP / COMMON MISTAKE — Dùng dạng Engel khi một mẫu có thể âm hoặc bằng 0. Phải ghi rõ $b_i > 0$ trong lời giải.

Using the Engel form when a denominator may be negative or zero. State $b_i > 0$ explicitly in the solution.

LỖI HAY GẶP / COMMON MISTAKE — Viết dấu bằng của Cauchy–Schwarz là $a_i = b_i$. Điều kiện đúng là hai bộ tỉ lệ ($a_i = \lambda \cdot b_i$), và hệ số tỉ lệ λ phải khớp với điều kiện của đề.

Writing the equality case of Cauchy–Schwarz as $a_i = b_i$. The correct condition is that the lists are proportional ($a_i = \lambda \cdot b_i$), and λ must be compatible with the constraint of the problem.

2.4. Bất đẳng thức hoán vị và Chebyshev — The rearrangement and Chebyshev inequalities

ĐỊNH LÝ 2.16 (Bất đẳng thức hoán vị) / THEOREM 2.16 (Rearrangement inequality)

— Cho $a_1 \leq a_2 \leq \dots \leq a_n$ và $b_1 \leq b_2 \leq \dots \leq b_n$. Với mọi hoán vị σ của $\{1, \dots, n\}$:

$$a_1 b_1 + \dots + a_n b_n \geq a_1 b_{\sigma(1)} + \dots + a_n b_{\sigma(n)} \geq a_1 b_n + a_2 b_{n-1} + \dots + a_n b_1.$$

Let $a_1 \leq a_2 \leq \dots \leq a_n$ and $b_1 \leq b_2 \leq \dots \leq b_n$. For every permutation σ of $\{1, \dots, n\}$:

$$a_1 b_1 + \dots + a_n b_n \geq a_1 b_{\sigma(1)} + \dots + a_n b_{\sigma(n)} \geq a_1 b_n + a_2 b_{n-1} + \dots + a_n b_1.$$

Chứng minh. / Proof.

Tổng cùng thứ tự là lớn nhất. Giả sử σ không phải hoán vị đồng nhất. Khi đó tồn tại chỉ số i với $\sigma(i) > \sigma(i+1)$ (nếu $\sigma(1) < \sigma(2) < \dots$ thì σ là đồng nhất). Đổi chỗ hai giá trị $\sigma(i)$ và $\sigma(i+1)$ cho nhau. Tổng thay đổi một lượng:

The similarly ordered sum is the largest. Suppose σ is not the identity. Then some index i has $\sigma(i) > \sigma(i+1)$ (if $\sigma(1) < \sigma(2) < \dots$ then σ is the identity). Swap the two values $\sigma(i)$ and $\sigma(i+1)$. The sum changes by:

$$a_i b_{\sigma(i+1)} + a_{i+1} b_{\sigma(i)} - a_i b_{\sigma(i)} - a_{i+1} b_{\sigma(i+1)} = (a_{i+1} - a_i)(b_{\sigma(i)} - b_{\sigma(i+1)}) \geq 0$$

vì $a_{i+1} \geq a_i$ và $\sigma(i) > \sigma(i+1)$ cho $b_{\sigma(i)} \geq b_{\sigma(i+1)}$. Mỗi lần đổi chỗ như vậy làm số cặp ngược thứ tự giảm đúng 1, nên sau hữu hạn bước ta tới hoán vị đồng nhất, và tổng không giảm ở mỗi bước. Do đó tổng ban đầu không vượt quá tổng cùng thứ tự.

because $a_{i+1} \geq a_i$, and $\sigma(i) > \sigma(i+1)$ gives $b_{\sigma(i)} \geq b_{\sigma(i+1)}$. Each such swap reduces the number of out-of-order pairs by exactly 1, so after finitely many steps we reach the identity, and the sum never decreases along the way. Hence the original sum does not exceed the similarly ordered sum.

Bất đẳng thức bên phải: áp dụng kết quả vừa chứng minh cho bộ a_i và bộ tăng $b'_k = -b_{n+1-k}$. Với hoán vị τ bất kỳ, đặt $\rho(i) = n+1 - \tau(i)$; ta có $\sum a_i b'_i \geq \sum a_i b'_{\tau(i)}$, tức $-\sum a_i b_{n+1-i} \geq -\sum a_i b_{\rho(i)}$, hay $\sum a_i b_{\rho(i)} \geq \sum a_i b_{n+1-i}$. Vì ρ chạy khắp mọi hoán vị khi τ chạy khắp mọi hoán vị, bất đẳng thức bên phải đúng.

The right inequality: apply the result just proved to the list a_i and the increasing list $b'_k = -b_{n+1-k}$. For any permutation τ put $\rho(i) = n + 1 - \tau(i)$; we have $\sum a_i b'_i \geq \sum a_i b'_{\tau(i)}$, that is $-\sum a_i b_{n+1-i} \geq -\sum a_i b_{\rho(i)}$, or $\sum a_i b_{\rho(i)} \geq \sum a_i b_{n+1-i}$. Since ρ runs over all permutations as τ does, the right inequality holds. ■

HỆ QUẢ 2.17 (Bất đẳng thức Chebyshev) / COROLLARY 2.17 (Chebyshev's inequality)

— Cho $a_1 \leq \dots \leq a_n$ và $b_1 \leq \dots \leq b_n$. Khi đó $n \cdot (a_1 b_1 + \dots + a_n b_n) \geq (a_1 + \dots + a_n)(b_1 + \dots + b_n)$. Nếu một bộ tăng và bộ kia giảm thì bất đẳng thức đổi chiều.

Let $a_1 \leq \dots \leq a_n$ and $b_1 \leq \dots \leq b_n$. Then $n \cdot (a_1 b_1 + \dots + a_n b_n) \geq (a_1 + \dots + a_n)(b_1 + \dots + b_n)$. If one list is increasing and the other decreasing, the inequality reverses.

Chứng minh. / Proof.

Với $k = 0, 1, \dots, n-1$, xét tổng dịch vòng $S_k = \sum a_i b_{i+k}$, chỉ số b tính theo modulo n ($b_{n+1} = b_1, \dots$). Mỗi S_k là tổng $a_i b_{\sigma(i)}$ với một hoán vị σ , nên theo Định lý 2.16, $S_k \leq S_0 = \sum a_i b_i$.

For $k = 0, 1, \dots, n-1$ consider the shifted sum $S_k = \sum a_i b_{i+k}$, with indices of b taken modulo n ($b_{n+1} = b_1, \dots$). Each S_k is a sum $a_i b_{\sigma(i)}$ for some permutation σ , so by Theorem 2.16, $S_k \leq S_0 = \sum a_i b_i$.

Cộng n bất đẳng thức đó: $\sum_k S_k \leq n \cdot \sum a_i b_i$. Mặt khác $\sum_k S_k = \sum_i \sum_j a_i b_j = (\sum a_i)(\sum b_j)$, vì khi i cố định, $i+k$ chạy hết các chỉ số khi k chạy từ 0 tới $n-1$.

Add these n inequalities: $\sum_k S_k \leq n \cdot \sum a_i b_i$. On the other hand $\sum_k S_k = \sum_i \sum_j a_i b_j = (\sum a_i)(\sum b_j)$, because for fixed i , the index $i+k$ runs through all indices as k runs from 0 to $n-1$.

Trường hợp một bộ tăng, một bộ giảm: thay b_i bằng $-b_i$ (bộ tăng) rồi áp dụng kết quả trên.

Case of one increasing and one decreasing list: replace b_i by $-b_i$ (an increasing list) and apply the result above. ■

$$n \cdot \sum a_i b_i \geq (\sum a_i)(\sum b_i) \quad (\text{cùng chiều tăng}) \quad (2.5)$$

PHẢI THUỘC / MEMORISE — Tổng nghịch đảo và tích bằng 1: nếu $x_1 \cdots x_n = 1$ và $x_i > 0$ thì $\sum x_i \geq n$; với $x_i > 0$ bất kỳ thì $(\sum x_i)(\sum 1/x_i) \geq n^2$.

Reciprocal sums and unit products: if $x_1 \cdots x_n = 1$ and $x_i > 0$ then $\sum x_i \geq n$; for any $x_i > 0$, $(\sum x_i)(\sum 1/x_i) \geq n^2$.

PHẢI THUỘC / MEMORISE — Cauchy–Schwarz: $(\sum a_i b_i)^2 \leq (\sum a_i^2)(\sum b_i^2)$, dấu bằng khi hai bộ tỉ lệ. Engel: $\sum a_i^2/b_i \geq (\sum a_i)^2/\sum b_i$ với $b_i > 0$.

Cauchy–Schwarz: $(\sum a_i b_i)^2 \leq (\sum a_i^2)(\sum b_i^2)$, with equality when the lists are proportional. Engel: $\sum a_i^2/b_i \geq (\sum a_i)^2/\sum b_i$ for $b_i > 0$.

NHẬN XÉT / REMARK — Hai hệ quả nhanh của hoán vị và Chebyshev. Lấy $b_i = a_i$: $n \cdot \sum a_i^2 \geq (\sum a_i)^2$, tức $AM \leq QM$, chứng minh thứ ba của bất đẳng thức này. Với $a \leq b \leq c$, so sánh tổng cùng thứ tự $a \cdot a + b \cdot b + c \cdot c$ với tổng đã dịch vòng $a \cdot b + b \cdot c + c \cdot a$: $a^2 + b^2 + c^2 \geq ab + bc + ca$, trùng Bổ đề 2.5(c).

Two quick consequences of rearrangement and Chebyshev. Take $b_i = a_i$: $n \cdot \sum a_i^2 \geq (\sum a_i)^2$, that is $AM \leq QM$, a third proof of this inequality. For $a \leq b \leq c$, compare the similarly ordered sum $a \cdot a + b \cdot b + c \cdot c$ with the shifted sum $a \cdot b + b \cdot c + c \cdot a$: $a^2 + b^2 + c^2 \geq ab + bc + ca$, the same as Lemma 2.5(c).

LỖI HAY GẶP / COMMON MISTAKE — Dùng Chebyshev cho hai dãy ngược chiều. Với $(a) = (1, 2, 3)$ và $(b) = (3, 2, 1)$: $n \cdot \sum a_i b_i = 3 \cdot 10 = 30$ còn $(\sum a_i)(\sum b_i) = 36$, nên bất đẳng thức " $\geq$ " SAI; đúng là chiều ngược lại.

Using Chebyshev for two lists in opposite directions. For $(a) = (1, 2, 3)$ and $(b) = (3, 2, 1)$: $n \cdot \sum a_i b_i = 3 \cdot 10 = 30$ while $(\sum a_i)(\sum b_i) = 36$, so the inequality " $\geq$ " FAILS; the reverse direction is the correct one.

LỖI HAY GẶP / COMMON MISTAKE — Dùng điều kiện "tích bằng 1" khi các số có thể âm. Với $x_1 = x_2 = -1$ thì $x_1 x_2 = 1$ nhưng $x_1 + x_2 = -2 < 2$. Hệ quả 2.10 đòi mọi số dương.

Using the condition "product equals 1" when the numbers may be negative. For $x_1 = x_2 = -1$ we have $x_1 x_2 = 1$ but $x_1 + x_2 = -2 < 2$. Corollary 2.10 requires every number positive.

HỆ QUẢ 2.18 (Tổng tỉ số qua hoán vị) / COROLLARY 2.18 (Sum of ratios under a permutation) — Với $a_1, \dots, a_n > 0$ và mọi hoán vị σ của $\{1, \dots, n\}$: $a_1/a_{\sigma(1)} + \dots + a_n/a_{\sigma(n)} \geq n$. Dấu bằng khi và chỉ khi $a_i = a_{\sigma(i)}$ với mọi i .

For $a_1, \dots, a_n > 0$ and every permutation σ of $\{1, \dots, n\}$: $a_1/a_{\sigma(1)} + \dots + a_n/a_{\sigma(n)} \geq n$. Equality holds if and only if $a_i = a_{\sigma(i)}$ for every i .

Chứng minh. / Proof.

Mỗi chỉ số xuất hiện đúng một lần ở tử và đúng một lần ở mẫu, nên tích n tỉ số bằng $(a_1 \cdots a_n)/(a_{\sigma(1)} \cdots a_{\sigma(n)}) = 1$. Áp dụng Hệ quả 2.10 cho n số dương này.

Each index appears exactly once in the numerators and once in the denominators, so the product of the n ratios is $(a_1 \cdots a_n)/(a_{\sigma(1)} \cdots a_{\sigma(n)}) = 1$. Apply Corollary 2.10 to these n positive numbers. ■

NHẬN XÉT / REMARK — Với $n = 3$ và σ là hoán vị vòng ta được $a/b + b/c + c/a \geq 3$, bất đẳng thức đã gặp ở Ví dụ 2.9 (bước thứ hai). Cách chứng minh này không cần bình phương nào.

For $n = 3$ and σ the cyclic permutation we get $a/b + b/c + c/a \geq 3$, the inequality met in Example 2.9 (its second step). This proof needs no squares at all.

PHẢI THUỘC / MEMORISE — Hai dãy cùng chiều: tổng tích cùng thứ tự là lớn nhất, tổng tích ngược thứ tự là bé nhất. Chebyshev: $n \cdot \sum a_i b_i \geq (\sum a_i)(\sum b_i)$ khi cả hai dãy cùng tăng.

Two lists in the same direction: the similarly ordered sum of products is the largest and the oppositely ordered one the smallest. Chebyshev: $n \cdot \sum a_i b_i \geq (\sum a_i)(\sum b_i)$ when both lists are increasing.

PHÂN TÍCH / ANALYSIS — Vế trái $a^3 + b^3 + c^3$ gồm $a \cdot a^2, b \cdot b^2, c \cdot c^2$, còn vế phải $a^2 b + b^2 c + c^2 a$ gồm $a^2 \cdot b, b^2 \cdot c, c^2 \cdot a$: cùng các thừa số a^2, b^2, c^2 nhưng thừa số còn lại bị hoán vị vòng. Bộ (a, b, c) và bộ (a^2, b^2, c^2) sắp thứ tự giống nhau (với $a, b, c > 0$), nên tổng cùng thứ tự không bé hơn tổng đã hoán vị.

The left side $a^3 + b^3 + c^3$ consists of $a \cdot a^2, b \cdot b^2, c \cdot c^2$, and the right side $a^2 b + b^2 c + c^2 a$ of $a^2 \cdot b, b^2 \cdot c, c^2 \cdot a$: the same factors a^2, b^2, c^2 but the other factor is cyclically permuted. The list (a, b, c) and the list (a^2, b^2, c^2) are ordered alike (for $a, b, c > 0$), so the similarly ordered sum is at least the permuted sum.

VÍ DỤ 2.10 (Sắp xếp lại) / EXAMPLE 2.10 (Rearrangement) — Chứng minh rằng với mọi $a, b, c > 0$: $a^3 + b^3 + c^3 \geq a^2 b + b^2 c + c^2 a$. Tìm các trường hợp dấu bằng.

Prove that for all $a, b, c > 0$: $a^3 + b^3 + c^3 \geq a^2 b + b^2 c + c^2 a$. Find the equality cases.

Lời giải. / Solution.

Gọi $u_1 \leq u_2 \leq u_3$ là ba số a, b, c sắp theo thứ tự tăng. Vì các số dương nên $u_1^2 \leq u_2^2 \leq u_3^2$: hai bộ (u_1^2, u_2^2, u_3^2) và (u_1, u_2, u_3) được sắp cùng thứ tự.

Let $u_1 \leq u_2 \leq u_3$ be the numbers a, b, c in increasing order. Since they are positive, $u_1^2 \leq u_2^2 \leq u_3^2$: the lists (u_1^2, u_2^2, u_3^2) and (u_1, u_2, u_3) are ordered alike.

Trong tổng $a^2b + b^2c + c^2a$, mỗi bình phương u_j^2 được nhân với đúng một trong ba số u_1, u_2, u_3 (số đứng sau nó theo vòng a, b, c), và ba thừa số này đôi một khác vị trí, nên tổng có dạng $\sum u_j^2 \cdot u_{\sigma(j)}$ với σ là một hoán vị.

In the sum $a^2b + b^2c + c^2a$, each square u_j^2 is multiplied by exactly one of u_1, u_2, u_3 (the number following it in the cycle a, b, c), and these three factors occupy different positions, so the sum has the form $\sum u_j^2 \cdot u_{\sigma(j)}$ for some permutation σ .

Theo Định lý 2.16, tổng đó không vượt quá tổng cùng thứ tự $u_1^2 \cdot u_1 + u_2^2 \cdot u_2 + u_3^2 \cdot u_3 = a^3 + b^3 + c^3$. Đây là bất đẳng thức cần chứng minh.

By Theorem 2.16, that sum does not exceed the similarly ordered sum $u_1^2 \cdot u_1 + u_2^2 \cdot u_2 + u_3^2 \cdot u_3 = a^3 + b^3 + c^3$. This is the required inequality.

Dấu bằng: theo Định lý 2.8 cho ba số dương, $a^3 + a^3 + b^3 \geq 3a^2b$, dấu bằng khi $a = b$. Viết hai bất đẳng thức tương tự cho (b, c) và (c, a) rồi cộng lại: $3(a^3 + b^3 + c^3) \geq 3(a^2b + b^2c + c^2a)$. Dấu bằng toàn bộ khi $a = b, b = c, c = a$.

Equality: by Theorem 2.8 for three positive numbers, $a^3 + a^3 + b^3 \geq 3a^2b$, with equality when $a = b$. Write the two similar inequalities for (b, c) and (c, a) and add: $3(a^3 + b^3 + c^3) \geq 3(a^2b + b^2c + c^2a)$. Equality throughout needs $a = b, b = c, c = a$.

Vậy bất đẳng thức đúng, dấu bằng khi và chỉ khi $a = b = c$.

Hence the inequality holds, with equality if and only if $a = b = c$. ■

NHẬN XÉT / REMARK — Bất đẳng thức hoán vị cho biết hai việc cùng lúc: tổng lớn nhất khi ghép lớn với lớn, bé nhất khi ghép lớn với bé. Vì vậy nó dùng được cho cả chặn trên lẫn chặn dưới. Ví dụ, nếu $a \leq b \leq c$ thì $a \cdot c + b \cdot b + c \cdot a$ nhỏ hơn hoặc bằng $a^2 + b^2 + c^2$.

The rearrangement inequality says two things at once: the sum is largest when large pairs with large, and smallest when large pairs with small. It therefore gives both upper and lower bounds. For example, if $a \leq b \leq c$ then $a \cdot c + b \cdot b + c \cdot a$ is at most $a^2 + b^2 + c^2$.

LỖI HAY GẶP / COMMON MISTAKE — Dùng hoán vị mà không kiểm tra thứ tự của hai bộ. Với a, b, c âm, bộ (a, b, c) và (a^2, b^2, c^2) không cùng thứ tự, kết luận có thể sai. Phải ghi rõ điều kiện dương hoặc sắp xếp lại trước.

Using rearrangement without checking the order of the two lists. For negative a, b, c the lists (a, b, c) and (a^2, b^2, c^2) are not ordered alike and the conclusion may fail. State the positivity condition or sort first.

LỖI HAY GẶP / COMMON MISTAKE — Giả sử $a \geq b \geq c$ cho biểu thức chỉ đối xứng vòng quanh. Với $a^2b + b^2c + c^2a$, bộ $(3, 2, 1)$ cho $18 + 4 + 3 = 25$ còn bộ $(1, 2, 3)$ cho $2 + 12 + 9 = 23$: thứ tự quyết định giá trị. Chỉ được sắp thứ tự khi biểu thức đối xứng theo mọi hoán vị; còn lại chỉ được quay vòng.

Assuming $a \geq b \geq c$ for an expression that is only cyclic. For $a^2b + b^2c + c^2a$ the triple $(3, 2, 1)$ gives

$18 + 4 + 3 = 25$ while $(1, 2, 3)$ gives $2 + 12 + 9 = 23$: the order decides the value. Sorting is allowed only for an expression symmetric under every permutation; otherwise one may only rotate.

2.5. Chuỗi trung bình và bất đẳng thức Bernoulli — The chain of means and Bernoulli's inequality

ĐỊNH LÝ 2.19 (Chuỗi HM–GM–AM–QM) / THEOREM 2.19 (HM–GM–AM–QM chain) — Với n số dương $x_1, \dots, x_n$, gọi $HM = n/(1/x_1 + \dots + 1/x_n)$ (trung bình điều hòa), $GM = (x_1 \cdots x_n)^{1/n}$, $AM = (x_1 + \dots + x_n)/n$, $QM = \sqrt{(x_1^2 + \dots + x_n^2)/n}$ (trung bình bình phương). Khi đó $HM \leq GM \leq AM \leq QM$, và dấu bằng ở bất kỳ chỗ nào xảy ra khi và chỉ khi mọi x_i bằng nhau.

For n positive numbers $x_1, \dots, x_n$, let $HM = n/(1/x_1 + \dots + 1/x_n)$ (harmonic mean), $GM = (x_1 \cdots x_n)^{1/n}$, $AM = (x_1 + \dots + x_n)/n$, $QM = \sqrt{(x_1^2 + \dots + x_n^2)/n}$ (quadratic mean). Then $HM \leq GM \leq AM \leq QM$, and equality anywhere in the chain holds if and only if all x_i are equal.

Chứng minh. / Proof.

$GM \leq AM$ chính là Định lý 2.9.

$GM \leq AM$ is Theorem 2.9 itself.

$HM \leq GM$: áp dụng Định lý 2.9 cho n số dương $1/x_1, \dots, 1/x_n$: $(1/x_1 + \dots + 1/x_n)/n \geq (1/(x_1 \cdots x_n))^{1/n} = 1/GM$. Lấy nghịch đảo hai vế dương: $n/(1/x_1 + \dots + 1/x_n) \leq GM$.

$HM \leq GM$: apply Theorem 2.9 to the n positive numbers $1/x_1, \dots, 1/x_n$: $(1/x_1 + \dots + 1/x_n)/n \geq (1/(x_1 \cdots x_n))^{1/n} = 1/GM$. Taking reciprocals of the positive sides: $n/(1/x_1 + \dots + 1/x_n) \leq GM$.

$AM \leq QM$: áp dụng Định lý 2.12 cho bộ $(1, \dots, 1)$ và $(x_1, \dots, x_n)$: $(x_1 + \dots + x_n)^2 \leq n \cdot (x_1^2 + \dots + x_n^2)$. Chia cho n^2 rồi lấy căn dương hai vế.

$AM \leq QM$: apply Theorem 2.12 to the lists $(1, \dots, 1)$ and $(x_1, \dots, x_n)$: $(x_1 + \dots + x_n)^2 \leq n \cdot (x_1^2 + \dots + x_n^2)$. Divide by n^2 and take positive square roots.

Dấu bằng: mỗi bước có dấu bằng khi các số bằng nhau (AM–GM) hoặc khi (x_i) tỉ lệ với $(1, \dots, 1)$ (Cauchy–Schwarz), tức cũng là khi các số bằng nhau.

Equality: each step has equality when the numbers are equal (AM–GM) or when (x_i) is proportional to $(1, \dots, 1)$ (Cauchy–Schwarz), which again means the numbers are equal. ■

$$2ab/(a+b) \leq \sqrt{ab} \leq (a+b)/2 \leq \sqrt{(a^2+b^2)/2} \quad (a, b > 0) \quad (2.6)$$

PHẢI THUỘC / MEMORISE — Với $a, b > 0$: $2ab/(a+b) \leq \sqrt{ab} \leq (a+b)/2 \leq \sqrt{(a^2+b^2)/2}$. Hệ quả hay dùng: $(x+y+z)^2 \leq 3(x^2+y^2+z^2)$.

For $a, b > 0$: $2ab/(a+b) \leq \sqrt{ab} \leq (a+b)/2 \leq \sqrt{(a^2+b^2)/2}$. A frequent consequence: $(x+y+z)^2 \leq 3(x^2+y^2+z^2)$.

NHẬN XÉT / REMARK — Từ $AM \leq QM$ cho hai số: $(\sqrt{x} + \sqrt{y})/2 \leq \sqrt{(x+y)/2}$, tức $\sqrt{x} + \sqrt{y} \leq \sqrt{2(x+y)}$ với $x, y \geq 0$. Đây là cách nhanh để chặn tổng hai căn bằng tổng bên trong, dấu bằng khi $x = y$.

From $AM \leq QM$ for two numbers: $(\sqrt{x} + \sqrt{y})/2 \leq \sqrt{(x+y)/2}$, that is $\sqrt{x} + \sqrt{y} \leq \sqrt{2(x+y)}$ for $x, y \geq 0$. This is a quick way to bound a sum of two roots by the sum inside, with equality when $x = y$.

ĐỊNH LÝ 2.20 (Bất đẳng thức Bernoulli) / THEOREM 2.20 (Bernoulli's inequality) — Với mọi số thực $x \geq -1$ và số nguyên dương n : $(1+x)^n \geq 1+nx$. Dấu bằng khi và chỉ khi $x = 0$ hoặc $n = 1$.
For every real $x \geq -1$ and positive integer n : $(1+x)^n \geq 1+nx$. Equality holds if and only if $x = 0$ or $n = 1$.

Chứng minh. / Proof.

Nếu $x = 0$ hoặc $n = 1$ thì hai vế bằng nhau. Xét $x \geq -1$, $x \neq 0$ và $n \geq 2$, ta chứng minh $(1+x)^n > 1+nx$.

If $x = 0$ or $n = 1$ both sides are equal. Take $x \geq -1$, $x \neq 0$ and $n \geq 2$; we prove $(1+x)^n > 1+nx$.

Với $x = -1$: vế trái bằng 0, vế phải bằng $1-n < 0$, đúng. Với $x > -1$, $x \neq 0$, quy nạp theo n . Cơ sở $n = 2$: $(1+x)^2 = 1+2x+x^2 > 1+2x$ vì $x \neq 0$. Bước quy nạp: giả sử $(1+x)^n > 1+nx$. Vì $1+x > 0$, nhân hai vế:

For $x = -1$: the left side is 0 and the right side is $1-n < 0$, true. For $x > -1$, $x \neq 0$, use induction on n . Base $n = 2$: $(1+x)^2 = 1+2x+x^2 > 1+2x$ because $x \neq 0$. Inductive step: assume $(1+x)^n > 1+nx$. Since $1+x > 0$, multiply both sides:

$$(1+x)^{n+1} > (1+nx)(1+x) = 1 + (n+1)x + nx^2 \geq 1 + (n+1)x$$

Vậy bất đẳng thức đúng với $n+1$.

So the inequality holds for $n+1$. ■

$$(1+x)^n \geq 1+nx \quad (x \geq -1, n \in \mathbb{Z}^+) \quad (2.7)$$

HỆ QUẢ 2.21 (Bất đẳng thức Weierstrass) / COROLLARY 2.21 (Weierstrass product inequality) — Nếu $x_1, \dots, x_n \geq -1$ cùng dấu (tất cả không âm, hoặc tất cả không dương) thì $(1+x_1)(1+x_2)\dots(1+x_n) \geq 1+x_1+x_2+\dots+x_n$.
If $x_1, \dots, x_n \geq -1$ all have the same sign (all non-negative, or all non-positive) then $(1+x_1)(1+x_2)\dots(1+x_n) \geq 1+x_1+x_2+\dots+x_n$.

Chứng minh. / Proof.

Quy nạp theo n . Với $n = 1$ hai vế bằng nhau. Giả sử đúng với n số và đặt $S = x_1 + \dots + x_n$. Thêm số x_{n+1} cùng dấu với các số trước, $1+x_{n+1} \geq 0$. Nhân bất đẳng thức $(1+x_1)\dots(1+x_n) \geq 1+S$ với $1+x_{n+1} \geq 0$:

Induction on n . For $n = 1$ both sides are equal. Assume the claim for n numbers and put $S = x_1 + \dots + x_n$. Add a number x_{n+1} of the same sign as the earlier ones, so $1+x_{n+1} \geq 0$. Multiply the inequality $(1+x_1)\dots(1+x_n) \geq 1+S$ by $1+x_{n+1} \geq 0$:

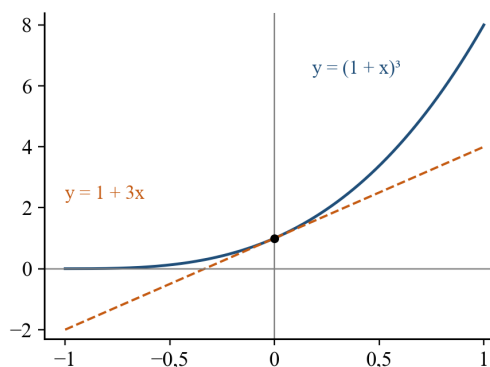
$$(1+x_1)\dots(1+x_{n+1}) \geq (1+S)(1+x_{n+1}) = 1+S+x_{n+1}+S \cdot x_{n+1} \geq 1+S+x_{n+1}$$

Bước cuối đúng vì S và x_{n+1} cùng dấu nên $S \cdot x_{n+1} \geq 0$.

The last step holds because S and x_{n+1} have the same sign, so $S \cdot x_{n+1} \geq 0$. ■

NHẬN XÉT / REMARK — Khi $x_1 = \dots = x_n = x$ ta được lại Định lý 2.20. Điều kiện "cùng dấu" không thể bỏ: với $x_1 = 1$, $x_2 = -1/2$ thì $(1+1)(1-1/2) = 1$, còn $1+x_1+x_2 = 3/2 > 1$.

When $x_1 = \dots = x_n = x$ we recover Theorem 2.20. The condition "same sign" cannot be dropped: for $x_1 = 1, x_2 = -1/2$ we get $(1+1)(1-1/2) = 1$ while $1 + x_1 + x_2 = 3/2 > 1$.



Hình 2.3. Đường $y = (1+x)^3$ nằm trên tiếp tuyến $y = 1+3x$ tại $x=0$ với $x \geq -1$
Figure 2.3. The curve $y = (1+x)^3$ lies above the tangent $y = 1+3x$ at $x=0$ for $x \geq -1$

PHÂN TÍCH / ANALYSIS — Số $1,01^{100} = (1 + 1/100)^{100}$ có dạng $(1+x)^n$ với $x = 1/100$ và $n = 100$, và $nx = 1$. Bernoulli cho ngay $1 + nx = 2$, nên ta suy ra cận dưới 2. Chỉ còn việc chọn bất đẳng thức chặt vì $x \neq 0$ và $n \geq 2$.

The number $1.01^{100} = (1 + 1/100)^{100}$ has the form $(1+x)^n$ with $x = 1/100$ and $n = 100$, and $nx = 1$. Bernoulli gives $1 + nx = 2$ at once, hence a lower bound of 2. What remains is to note that the inequality is strict because $x \neq 0$ and $n \geq 2$.

VÍ DỤ 2.11 (Bernoulli với số cụ thể) / EXAMPLE 2.11 (Bernoulli with concrete numbers) — Không dùng máy tính, chứng minh rằng $1,01^{100} > 2$.

Without a calculator, prove that $1.01^{100} > 2$.

Lời giải. / Solution.

Đặt $x = 1/100, n = 100$. Vì $x > -1, x \neq 0$ và $n \geq 2$, Định lý 2.20 cho bất đẳng thức chặt:
Put $x = 1/100, n = 100$. Since $x > -1, x \neq 0$ and $n \geq 2$, Theorem 2.20 gives a strict inequality:

$$(1 + 1/100)^{100} > 1 + 100 \cdot (1/100) = 2$$

Vậy $1,01^{100} > 2$.

Hence $1.01^{100} > 2$. ■

NHẬN XÉT / REMARK — Cận 2 khá thô: $1,01^{100}$ thực tế xấp xỉ 2,7. Để lấy cận tốt hơn, dùng khai triển nhị thức, giữ thêm số hạng bậc hai: $(1+x)^n \geq 1 + nx + C(n, 2)x^2$ với $x \geq 0$ ($C(n, k)$ là số tổ hợp chập k của n , SGK viết C_n^k). Với $x = 1/100, n = 100$ cận này cho $1 + 1 + 0,495$.

The bound 2 is crude: 1.01^{100} is in fact about 2.7. For a better bound use the binomial expansion and keep the quadratic term: $(1+x)^n \geq 1 + nx + C(n, 2)x^2$ for $x \geq 0$ ($C(n, k)$ is the number of k -element subsets of an n -element set; the textbook writes C_n^k). With $x = 1/100, n = 100$ this bound gives $1 + 1 + 0.495$.

LỖI HAY GẶP / COMMON MISTAKE — Dùng Bernoulli khi $x < -1$. Với $x = -3$ và $n = 5$ thì $(1+x)^5 = (-2)^5 = -32$, nhỏ hơn $1 + nx = -14$, nên bất đẳng thức SAI.

Using Bernoulli when $x < -1$. For $x = -3$ and $n = 5$ we get $(1 + x)^5 = (-2)^5 = -32$, which is smaller than $1 + nx = -14$, so the inequality FAILS.

2.6. Trị tuyệt đối, bất đẳng thức tam giác và dạng căn Minkowski — Absolute values, the triangle inequality and Minkowski's form

ĐỊNH LÝ 2.22 (Bất đẳng thức tam giác) / THEOREM 2.22 (Triangle inequality) — Với mọi số thực a, b : $|a + b| \leq |a| + |b|$, dấu bằng khi và chỉ khi $ab \geq 0$. Hệ quả: $||a| - |b|| \leq |a - b| \leq |a| + |b|$.

For all real a, b : $|a + b| \leq |a| + |b|$, with equality if and only if $ab \geq 0$. Consequence: $||a| - |b|| \leq |a - b| \leq |a| + |b|$.

Chứng minh. / Proof.

Cả hai vế không âm nên so sánh bình phương của chúng (Tính chất 2.2(v)): $(|a| + |b|)^2 - (a + b)^2 = 2|ab| - 2ab \geq 0$, vì $|ab| \geq ab$. Dấu bằng khi $|ab| = ab$, tức $ab \geq 0$.

Both sides are non-negative, so compare their squares (Property 2.2(v)): $(|a| + |b|)^2 - (a + b)^2 = 2|ab| - 2ab \geq 0$, because $|ab| \geq ab$. Equality when $|ab| = ab$, that is $ab \geq 0$.

Hệ quả: $a = (a - b) + b$ nên $|a| \leq |a - b| + |b|$, tức $|a| - |b| \leq |a - b|$. Đổi vai trò a, b : $|b| - |a| \leq |a - b|$. Hai điều này cho $||a| - |b|| \leq |a - b|$. Còn $|a - b| = |a + (-b)| \leq |a| + |b|$.

Consequence: $a = (a - b) + b$ gives $|a| \leq |a - b| + |b|$, that is $|a| - |b| \leq |a - b|$. Swapping the roles of a and b : $|b| - |a| \leq |a - b|$. Together these give $||a| - |b|| \leq |a - b|$. Also $|a - b| = |a + (-b)| \leq |a| + |b|$. ■

TÍNH CHẤT 2.23 (Trị tuyệt đối và khoảng) / PROPERTY 2.23 (Absolute value and intervals) — Với $r \geq 0$: $|x| \leq r$ khi và chỉ khi $-r \leq x \leq r$; $|x| \geq r$ khi và chỉ khi $x \geq r$ hoặc $x \leq -r$.
For $r \geq 0$: $|x| \leq r$ if and only if $-r \leq x \leq r$; $|x| \geq r$ if and only if $x \geq r$ or $x \leq -r$.

Chứng minh. / Proof.

$|x|$ bằng số lớn hơn trong hai số x và $-x$. Vậy $|x| \leq r$ khi và chỉ khi $x \leq r$ và $-x \leq r$, tức $-r \leq x \leq r$. Khẳng định thứ hai là phủ định của khẳng định " $|x| < r$ ", tức $-r < x < r$, nên đúng khi $x \leq -r$ hoặc $x \geq r$.

$|x|$ equals the larger of the two numbers x and $-x$. So $|x| \leq r$ if and only if $x \leq r$ and $-x \leq r$, that is $-r \leq x \leq r$. The second claim is the negation of " $|x| < r$ ", that is $-r < x < r$, so it holds exactly when $x \leq -r$ or $x \geq r$. ■

PHẢI THUỘC / MEMORISE — Bất đẳng thức tam giác: $|a + b| \leq |a| + |b|$, dấu bằng khi $ab \geq 0$. Với $r \geq 0$: $|x| \leq r \Leftrightarrow -r \leq x \leq r$.

Triangle inequality: $|a + b| \leq |a| + |b|$, with equality when $ab \geq 0$. For $r \geq 0$: $|x| \leq r \Leftrightarrow -r \leq x \leq r$.

ĐỊNH LÝ 2.24 (Dạng căn Minkowski) / THEOREM 2.24 (Minkowski's form) — Với mọi số thực a, b, c, d : $\sqrt{a^2 + b^2} + \sqrt{c^2 + d^2} \geq \sqrt{(a + c)^2 + (b + d)^2}$. Dấu bằng khi và chỉ khi $ad = bc$ và $ac + bd \geq 0$.

For all real a, b, c, d : $\sqrt{a^2 + b^2} + \sqrt{c^2 + d^2} \geq \sqrt{(a + c)^2 + (b + d)^2}$. Equality holds if and only if $ad = bc$ and $ac + bd \geq 0$.

Chứng minh. / Proof.

Cả hai vế không âm nên so sánh bình phương. Vế trái bình phương bằng $a^2 + b^2 + c^2 + d^2 + 2\sqrt{((a^2 + b^2)(c^2 + d^2))}$; vế phải bình phương bằng $a^2 + b^2 + c^2 + d^2 + 2(ac + bd)$. Cần chứng minh $\sqrt{((a^2 + b^2)(c^2 + d^2))} \geq ac + bd$.

Both sides are non-negative, so compare squares. The left side squared is $a^2 + b^2 + c^2 + d^2 + 2\sqrt{((a^2 + b^2)(c^2 + d^2))}$; the right side squared is $a^2 + b^2 + c^2 + d^2 + 2(ac + bd)$. We must show $\sqrt{((a^2 + b^2)(c^2 + d^2))} \geq ac + bd$.

Theo (2.3) với $n = 2$: $(a^2 + b^2)(c^2 + d^2) - (ac + bd)^2 = (ad - bc)^2 \geq 0$. Vậy $\sqrt{((a^2 + b^2)(c^2 + d^2))} \geq |ac + bd| \geq ac + bd$.

By (2.3) with $n = 2$: $(a^2 + b^2)(c^2 + d^2) - (ac + bd)^2 = (ad - bc)^2 \geq 0$. Hence $\sqrt{((a^2 + b^2)(c^2 + d^2))} \geq |ac + bd| \geq ac + bd$.

Dấu bằng khi $(ad - bc)^2 = 0$ và $|ac + bd| = ac + bd$, tức $ad = bc$ và $ac + bd \geq 0$.

Equality holds when $(ad - bc)^2 = 0$ and $|ac + bd| = ac + bd$, that is $ad = bc$ and $ac + bd \geq 0$. ■

$$\sqrt{a^2 + b^2} + \sqrt{c^2 + d^2} \geq \sqrt{(a + c)^2 + (b + d)^2} \quad (2.8)$$

Ý nghĩa hình học: $\sqrt{a^2 + b^2}$ là độ dài vector (a, b) , nên Định lý 2.24 nói rằng độ dài tổng hai vector không vượt quá tổng các độ dài. Dấu bằng khi hai vector cùng hướng. Dạng này dùng cho các biểu thức hai căn mà bên trong là tổng hai bình phương.

Geometric meaning: $\sqrt{a^2 + b^2}$ is the length of the vector (a, b) , so Theorem 2.24 says that the length of a sum of two vectors does not exceed the sum of the lengths. Equality holds when the two vectors point the same way. It applies to expressions with two square roots whose radicands are sums of two squares.

PHÂN TÍCH / ANALYSIS — Hai căn có dạng $\sqrt{x^2 + 2^2}$ và $\sqrt{(6 - x)^2 + 3^2}$: bên trong là tổng hai bình phương, trong đó phần chứa x là x và $6 - x$ có tổng bằng 6, không phụ thuộc x . Đặt $(a, b) = (x, 2)$ và $(c, d) = (6 - x, 3)$ thì $a + c = 6$ không đổi. Về hình học, tổng là $MP + PN$ với $M(0, 2)$, $N(6, -3)$, $P(x, 0)$ trên trục hoành, và đường gấp khúc ngắn nhất khi M, P, N thẳng hàng.

The two roots have the form $\sqrt{x^2 + 2^2}$ and $\sqrt{(6 - x)^2 + 3^2}$: inside are sums of two squares, and the x -dependent parts x and $6 - x$ add up to 6, independent of x . Put $(a, b) = (x, 2)$ and $(c, d) = (6 - x, 3)$, so $a + c = 6$ is constant. Geometrically the sum is $MP + PN$ with $M(0, 2)$, $N(6, -3)$, $P(x, 0)$ on the horizontal axis, and the broken line is shortest when M, P, N are collinear.

VÍ DỤ 2.12 (Dạng căn và hình học) / EXAMPLE 2.12 (Radical form and geometry) —

Tìm giá trị nhỏ nhất của $F(x) = \sqrt{x^2 + 4} + \sqrt{(6 - x)^2 + 9}$ trên $\mathbb{R}$.

Find the minimum of $F(x) = \sqrt{x^2 + 4} + \sqrt{(6 - x)^2 + 9}$ over $\mathbb{R}$.

Lời giải. / Solution.

Đặt $a = x$, $b = 2$, $c = 6 - x$, $d = 3$. Theo Định lý 2.24:

Put $a = x$, $b = 2$, $c = 6 - x$, $d = 3$. By Theorem 2.24:

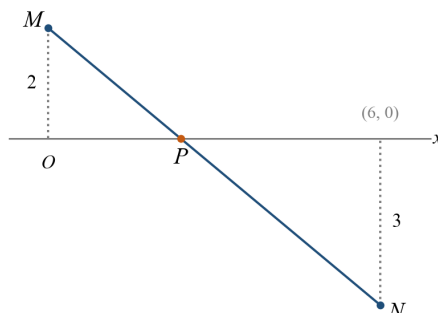
$$F(x) \geq \sqrt{(x + 6 - x)^2 + (2 + 3)^2} = \sqrt{36 + 25} = \sqrt{61}$$

Dấu bằng khi $ad = bc$, tức $3x = 2(6 - x)$, $x = 12/5$; và $ac + bd = x(6 - x) + 6 = (12/5) \cdot (18/5) + 6 > 0$. Hai điều kiện đều thỏa mãn.

Equality holds when $ad = bc$, that is $3x = 2(6 - x)$, $x = 12/5$; and $ac + bd = x(6 - x) + 6 = (12/5) \cdot (18/5) + 6 > 0$. Both conditions are met.

Vậy giá trị nhỏ nhất bằng $\sqrt{61}$, đạt tại $x = 12/5$.

Hence the minimum is $\sqrt{61}$, attained at $x = 12/5$. ■



Hình 2.4. Tổng $MP + PN$ nhỏ nhất bằng $MN = \sqrt{61}$ khi P có hoành độ $12/5$

Figure 2.4. The sum $MP + PN$ is smallest, equal to $MN = \sqrt{61}$, when P has abscissa $12/5$

NHẬN XÉT / REMARK — Bất đẳng thức tam giác cho nhiều số: $|a_1| + \dots + |a_n| \geq |a_1 + \dots + a_n|$, chứng minh bằng quy nạp theo n từ trường hợp hai số. Một cách dùng: với x thực, $|x - 1| + |x - 7| = |x - 1| + |7 - x| \geq |(x - 1) + (7 - x)| = 6$, dấu bằng khi $(x - 1)(7 - x) \geq 0$, tức $1 \leq x \leq 7$.

The triangle inequality for many numbers: $|a_1| + \dots + |a_n| \geq |a_1 + \dots + a_n|$, proved by induction on n from the two-number case. One use: for real x , $|x - 1| + |x - 7| = |x - 1| + |7 - x| \geq |(x - 1) + (7 - x)| = 6$, with equality when $(x - 1)(7 - x) \geq 0$, that is $1 \leq x \leq 7$.

LỖI HAY GẶP / COMMON MISTAKE — Cho rằng dấu bằng của Minkowski chỉ cần $ad = bc$. Với $(a, b) = (1, 0)$ và $(c, d) = (-1, 0)$ ta có $ad = bc = 0$, nhưng vế trái bằng $1 + 1 = 2$ còn vế phải $\sqrt{((1 - 1)^2 + 0)} = 0$. Hai vectơ phải cùng hướng, tức cần thêm $ac + bd \geq 0$.

Believing that the equality case of Minkowski needs only $ad = bc$. For $(a, b) = (1, 0)$ and $(c, d) = (-1, 0)$ we have $ad = bc = 0$, yet the left side is $1 + 1 = 2$ while the right side is $\sqrt{((1 - 1)^2 + 0)} = 0$. The two vectors must point the same way, so $ac + bd \geq 0$ is also needed.

LỖI HAY GẶP / COMMON MISTAKE — Bỏ dấu giá trị tuyệt đối bằng cách bình phương mà quên rằng $|a| \geq a$ chứ không bằng a . Từ $|a| \geq |b|$ chỉ suy ra $a^2 \geq b^2$, còn muốn suy ra $a \geq b$ thì cần thêm $a, b \geq 0$.

Dropping an absolute value by squaring while forgetting that $|a| \geq a$, not $|a| = a$. From $|a| \geq |b|$ one gets only $a^2 \geq b^2$; to get $a \geq b$ one also needs $a, b \geq 0$.

2.7. Bất đẳng thức Nesbitt và bài toán cực trị có điều kiện — Nesbitt's inequality and constrained extremum problems

ĐỊNH LÝ 2.25 (Bất đẳng thức Nesbitt) / THEOREM 2.25 (Nesbitt's inequality) — Với mọi $a, b, c > 0$: $a/(b + c) + b/(c + a) + c/(a + b) \geq 3/2$. Dấu bằng khi và chỉ khi $a = b = c$.
For all $a, b, c > 0$: $a/(b + c) + b/(c + a) + c/(a + b) \geq 3/2$, with equality if and only if $a = b = c$.

Chứng minh. / Proof.

Viết $a/(b+c) = a^2/(a(b+c))$ và áp dụng Hệ quả 2.13 với các mẫu dương $a(b+c)$, $b(c+a)$, $c(a+b)$:

Write $a/(b+c) = a^2/(a(b+c))$ and apply Corollary 2.13 with the positive denominators $a(b+c)$, $b(c+a)$, $c(a+b)$:

$$\Sigma a/(b+c) \geq (a+b+c)^2/(2(ab+bc+ca))$$

Theo Bỏ đề 2.5(c), $(a+b+c)^2 \geq 3(ab+bc+ca)$, nên vế phải không nhỏ hơn $3/2$.

By Lemma 2.5(c), $(a+b+c)^2 \geq 3(ab+bc+ca)$, so the right side is at least $3/2$.

Dấu bằng cần $a=b=c$ (từ bước cuối); khi $a=b=c$, mỗi phân số bằng $1/2$ và tổng bằng $3/2$.

Equality needs $a=b=c$ (from the last step); when $a=b=c$ each fraction equals $1/2$ and the sum is $3/2$. ■

$$a/(b+c) + b/(c+a) + c/(a+b) \geq 3/2 \quad (a, b, c > 0) \quad (2.9)$$

NHẬN XÉT / REMARK — Giá trị $3/2$ của Nesbitt chỉ đạt khi $a=b=c$. Khi một biến tiến tới 0 thì tổng lớn hơn: $(a, b, c) = (1, 1, 0)$ cho $1+1+0=2 > 3/2$, nên cận $3/2$ là chặt nhưng chỉ đạt ở tâm.

The value $3/2$ in Nesbitt is attained only at $a=b=c$. When one variable tends to 0 the sum is larger: $(a, b, c) = (1, 1, 0)$ gives $1+1+0=2 > 3/2$, so the bound $3/2$ is sharp but attained only at the centre.

HỆ QUẢ 2.26 (Nesbitt bốn biến) / COROLLARY 2.26 (Four-variable Nesbitt) — Với $a, b, c, d > 0$: $a/(b+c) + b/(c+d) + c/(d+a) + d/(a+b) \geq 2$. Dấu bằng khi và chỉ khi $a=c$ và $b=d$.

For $a, b, c, d > 0$: $a/(b+c) + b/(c+d) + c/(d+a) + d/(a+b) \geq 2$. Equality holds if and only if $a=c$ and $b=d$.

Chứng minh. / Proof.

Viết $a/(b+c) = a^2/(a(b+c))$ và tương tự, rồi dùng Hệ quả 2.13 với bốn mẫu dương. Tổng mẫu bằng $ab+ac+bc+bd+cd+ca+da+db = ab+2ac+bc+2bd+cd+da$. Vậy tổng cần chứng minh không nhỏ hơn

Write $a/(b+c) = a^2/(a(b+c))$ and similarly, then use Corollary 2.13 with the four positive denominators. The sum of the denominators is $ab+ac+bc+bd+cd+ca+da+db = ab+2ac+bc+2bd+cd+da$. So the sum is at least

$$(a+b+c+d)^2/(ab+bc+cd+da+2ac+2bd)$$

Hiệu $(a+b+c+d)^2 - 2(ab+bc+cd+da+2ac+2bd) = a^2+b^2+c^2+d^2-2ac-2bd = (a-c)^2 + (b-d)^2 \geq 0$, nên phân số trên không nhỏ hơn 2.

The difference $(a+b+c+d)^2 - 2(ab+bc+cd+da+2ac+2bd) = a^2+b^2+c^2+d^2-2ac-2bd = (a-c)^2 + (b-d)^2 \geq 0$, so the fraction above is at least 2.

Dấu bằng cần $a=c$, $b=d$ (từ bước cuối). Khi $a=c$ và $b=d$, bốn số hạng là $a/(b+a)$, $b/(a+b)$, $a/(b+a)$, $b/(a+b)$, tổng bằng $2(a+b)/(a+b) = 2$.

Equality needs $a = c$ and $b = d$ (from the last step). When $a = c$ and $b = d$ the four terms are $a/(b + a)$, $b/(a + b)$, $a/(b + a)$, $b/(a + b)$, summing to $2(a + b)/(a + b) = 2$. ■

ĐỊNH NGHĨA 2.27 (Giá trị nhỏ nhất) / DEFINITION 2.27 (Minimum value) — Hàm f có giá trị nhỏ nhất m trên tập M nếu (1) $f(x) \geq m$ với mọi $x \in M$ và (2) tồn tại $x_0 \in M$ để $f(x_0) = m$. Giá trị lớn nhất định nghĩa tương tự với chiều ngược lại.

A function f has minimum value m on a set M if (1) $f(x) \geq m$ for all $x \in M$ and (2) there is $x_0 \in M$ with $f(x_0) = m$. The maximum is defined similarly with the reverse direction.

Lời giải bài cực trị có hai nửa không thể thiếu: chặn (điều kiện (1)) và đạt được (điều kiện (2)). Bỏ nửa thứ hai là lỗi phổ biến nhất, như ví dụ sau cho thấy khi điều kiện đề cản điểm rơi quen thuộc.

A solution to an extremum problem has two indispensable halves: the bound (condition (1)) and attainment (condition (2)). Dropping the second half is the most common error, as the next example shows when the constraint of the problem blocks the familiar equality point.

PHÂN TÍCH / ANALYSIS — Không có ràng buộc, $a + 1/a \geq 2$ (tại $a = 1$) và $b + 4/b \geq 4$ (tại $b = 2$), nên giá trị nhỏ nhất là 6 tại $(a, b) = (1, 2)$. Nhưng khi đó $a + b = 3 > 2$, vi phạm điều kiện. Điểm rơi quen thuộc nằm ngoài miền, nên cực tiểu phải ở biên $a + b = 2$. Muốn xử lý, đặt $t = a + b$ và dùng dạng Engel để gom $1/a + 4/b$ thành một hàm của t .

Without the constraint, $a + 1/a \geq 2$ (at $a = 1$) and $b + 4/b \geq 4$ (at $b = 2$), so the minimum would be 6 at $(a, b) = (1, 2)$. But then $a + b = 3 > 2$, violating the condition. The familiar equality point lies outside the domain, so the minimum must be on the boundary $a + b = 2$. To handle it, put $t = a + b$ and use the Engel form to collect $1/a + 4/b$ into a function of t .

VÍ DỤ 2.13 (Điểm rơi bị ràng buộc chặn) / EXAMPLE 2.13 (Equality point blocked by a constraint) — Cho $a, b > 0$ thỏa mãn $a + b \leq 2$. Tìm giá trị nhỏ nhất của $P = a + b + 1/a + 4/b$.

Let $a, b > 0$ with $a + b \leq 2$. Find the minimum of $P = a + b + 1/a + 4/b$.

Lời giải. / Solution.

Đặt $t = a + b$, $0 < t \leq 2$. Theo Hệ quả 2.13: $1/a + 4/b = 1^2/a + 2^2/b \geq (1 + 2)^2/(a + b) = 9/t$. Vậy $P \geq t + 9/t$.

Put $t = a + b$, $0 < t \leq 2$. By Corollary 2.13: $1/a + 4/b = 1^2/a + 2^2/b \geq (1 + 2)^2/(a + b) = 9/t$. Hence $P \geq t + 9/t$.

Ta chứng minh $t + 9/t \geq 13/2$ với $0 < t \leq 2$:

We show that $t + 9/t \geq 13/2$ for $0 < t \leq 2$:

$$t + 9/t - 13/2 = (2t^2 - 13t + 18)/(2t) = (2t - 9)(t - 2)/(2t) \geq 0$$

vì $t > 0$, $2t - 9 < 0$ và $t - 2 \leq 0$ nên tích $(2t - 9)(t - 2)$ không âm.

because $t > 0$, $2t - 9 < 0$ and $t - 2 \leq 0$, so the product $(2t - 9)(t - 2)$ is non-negative.

Vậy $P \geq 13/2$. Dấu bằng cần $t = 2$ và, theo dạng Engel, $1/a : 2/b$ bằng nhau, tức $b = 2a$. Từ $a + b = 2$ ta được $a = 2/3$, $b = 4/3$ (thuộc miền).

Hence $P \geq 13/2$. Equality needs $t = 2$ and, in the Engel form, $1/a = 2/b$, that is $b = 2a$. From $a + b = 2$ we get $a = 2/3$, $b = 4/3$ (inside the domain).

Kiểm tra: $P = 2 + 3/2 + 3 = 13/2$. Vậy giá trị nhỏ nhất bằng $13/2$, đạt tại $(a, b) = (2/3, 4/3)$.

Check: $P = 2 + 3/2 + 3 = 13/2$. Hence the minimum is $13/2$, attained at $(a, b) = (2/3, 4/3)$. ■

PHÂN TÍCH / ANALYSIS — Biểu thức $a^2b + b^2c + c^2a + abc$ chỉ bất biến khi hoán vị vòng, không đối xứng, nên không thể giả sử $a \geq b \geq c$. Nhưng ta luôn có thể quay vòng để một số nằm giữa hai số kia đứng ở vị trí b . Khi đó $(a - b)(b - c) \geq 0$, và hiệu giữa $b(a + c)^2$ với biểu thức đã cho đúng bằng $c(a - b)(b - c)$, kiểm tra bằng khai triển. Sau đó $b(a + c)^2 = 4 \cdot b \cdot ((a + c)/2)^2$ được chặn bằng AM–GM ba số vì $b + (a + c)/2 + (a + c)/2 = 3$.

The expression $a^2b + b^2c + c^2a + abc$ is invariant only under cyclic permutation, not symmetric, so we cannot assume $a \geq b \geq c$. But we can always rotate so that a number lying between the other two sits in position b . Then $(a - b)(b - c) \geq 0$, and the difference between $b(a + c)^2$ and the given expression is exactly $c(a - b)(b - c)$, as expansion confirms. Then $b(a + c)^2 = 4 \cdot b \cdot ((a + c)/2)^2$ is bounded by three-term AM–GM because $b + (a + c)/2 + (a + c)/2 = 3$.

VÍ DỤ 2.14 (Quay vòng và so sánh với $b(a + c)^2$) / EXAMPLE 2.14 (Rotation and comparison with $b(a + c)^2$) — Cho $a, b, c \geq 0$ với $a + b + c = 3$. Chứng minh rằng $a^2b + b^2c + c^2a + abc \leq 4$, và tìm mọi trường hợp dấu bằng.

Let $a, b, c \geq 0$ with $a + b + c = 3$. Prove that $a^2b + b^2c + c^2a + abc \leq 4$, and find all equality cases.

Lời giải. / Solution.

Gọi $E(a, b, c) = a^2b + b^2c + c^2a + abc$. Quay vòng (a, b, c) thành (b, c, a) không đổi E . Trong ba số luôn có một số nằm giữa hai số còn lại (không lớn nhất, không nhỏ nhất); quay vòng sao cho số đó là b . Khi đó $(a - b)(b - c) \geq 0$.

Let $E(a, b, c) = a^2b + b^2c + c^2a + abc$. Rotating (a, b, c) to (b, c, a) leaves E unchanged. Among the three numbers one lies between the other two (neither the largest nor the smallest); rotate so that this number is b . Then $(a - b)(b - c) \geq 0$.

Khai triển:

Expand:

$$b(a + c)^2 - E = (a^2b + 2abc + bc^2) - (a^2b + b^2c + c^2a + abc) = abc + bc^2 - b^2c - c^2a = c(a - b)(b - c) \geq 0$$

Do đó $E \leq b(a + c)^2 = 4 \cdot b \cdot ((a + c)/2) \cdot ((a + c)/2)$. Theo Định lý 2.8 cho ba số không âm $b, (a + c)/2, (a + c)/2$ có tổng bằng 3:

So $E \leq b(a + c)^2 = 4 \cdot b \cdot ((a + c)/2) \cdot ((a + c)/2)$. By Theorem 2.8 for the three non-negative numbers $b, (a + c)/2, (a + c)/2$, whose sum is 3:

$$b \cdot ((a + c)/2) \cdot ((a + c)/2) \leq ((b + (a + c)/2 + (a + c)/2)/3)^3 = 1$$

Suy ra $E \leq 4$.

Hence $E \leq 4$.

Dấu bằng cần $c(a - b)(b - c) = 0$ và $b = (a + c)/2 = 1$, tức $b = 1, a + c = 2$ và $c = 0$ hoặc $a = 1$ hoặc $c = 1$. Ba khả năng cho $(a, b, c) = (2, 1, 0)$ hoặc $(1, 1, 1)$. Trả lại phép quay vòng, các trường hợp dấu bằng của đề là $(1, 1, 1), (2, 1, 0), (0, 2, 1), (1, 0, 2)$.

Equality needs $c(a - b)(b - c) = 0$ and $b = (a + c)/2 = 1$, that is $b = 1$, $a + c = 2$ and $c = 0$ or $a = 1$ or $c = 1$. These give $(a, b, c) = (2, 1, 0)$ or $(1, 1, 1)$. Undoing the rotation, the equality cases of the problem are $(1, 1, 1)$, $(2, 1, 0)$, $(0, 2, 1)$, $(1, 0, 2)$.

Kiểm tra: $E(2, 1, 0) = 4 \cdot 1 = 4$. Vậy giá trị lớn nhất của E bằng 4.

Check: $E(2, 1, 0) = 4 \cdot 1 = 4$. Hence the maximum of E is 4. ■

NHẬN XÉT / REMARK — Điều kiện $a, b, c \geq 0$ (cho phép bằng 0) là cần thiết: dấu bằng thứ hai $(2, 1, 0)$ có một biến bằng 0. Nếu đề đòi $a, b, c > 0$ thì giá trị 4 không còn đạt được trừ tại $(1, 1, 1)$, nhưng 4 vẫn là cận trên nhỏ nhất.

The condition $a, b, c \geq 0$ (zero allowed) matters: the second equality case $(2, 1, 0)$ has a variable equal to 0. If the problem demanded $a, b, c > 0$, the value 4 would be attained only at $(1, 1, 1)$, while 4 would still be the least upper bound.

NHẬN XÉT / REMARK — Tổng quát hóa Ví dụ 2.13: với $a, b > 0$ và $a + b \leq s$, giá trị nhỏ nhất của $a + b + 1/a + 4/b$ là 6 nếu $s \geq 3$ (đạt tại $(1, 2)$, nằm trong miền), và là $s + 9/s$ nếu $0 < s < 3$ (đạt tại $a = s/3$, $b = 2s/3$, trên biên). Ngưỡng $s = 3$ chính là tổng của điểm rơi không ràng buộc.

A generalisation of Example 2.13: for $a, b > 0$ with $a + b \leq s$, the minimum of $a + b + 1/a + 4/b$ is 6 if $s \geq 3$ (attained at $(1, 2)$, inside the domain), and $s + 9/s$ if $0 < s < 3$ (attained at $a = s/3$, $b = 2s/3$, on the boundary). The threshold $s = 3$ is exactly the sum of the unconstrained equality point.

NHẬN XÉT / REMARK — Tổng quát hóa Ví dụ 2.7: nếu $w_1x_1^2 + \dots + w_nx_n^2 = c$ với $w_i > 0$, $c > 0$ thì $x_1 + \dots + x_n \leq \sqrt[n]{c \cdot (1/w_1 + \dots + 1/w_n)}$. Với $(w) = (1, 2, 3)$ và $c = 6$ ta được $\sqrt[6]{6 \cdot 11/6} = \sqrt[6]{11}$.

A generalisation of Example 2.7: if $w_1x_1^2 + \dots + w_nx_n^2 = c$ with $w_i > 0$, $c > 0$ then $x_1 + \dots + x_n \leq \sqrt[n]{c \cdot (1/w_1 + \dots + 1/w_n)}$. With $(w) = (1, 2, 3)$ and $c = 6$ we get $\sqrt[6]{6 \cdot 11/6} = \sqrt[6]{11}$.

LỖI HAY GẶP / COMMON MISTAKE — Chứng minh $f \geq m$ rồi kết luận giá trị nhỏ nhất là m mà không nêu điểm đạt. Thiếu điều kiện (2) của Định nghĩa 2.27 thì m chỉ là một cận dưới, chưa chắc là giá trị nhỏ nhất.

Proving $f \geq m$ and then declaring the minimum to be m without exhibiting a point where it is attained. Without condition (2) of Definition 2.27, m is only a lower bound, not necessarily the minimum.

LỖI HAY GẶP / COMMON MISTAKE — Chia hai vế cho một biểu thức chưa biết dấu. Từ $x^2 \geq xy$ không suy ra $x \geq y$: $x = -3$, $y = 1$ cho $9 \geq -3$ nhưng $-3 < 1$. Phải xét riêng $x > 0$ và $x < 0$, hoặc chuyển vế rồi phân tích $x(x - y) \geq 0$.

Dividing both sides by an expression of unknown sign. From $x^2 \geq xy$ one cannot deduce $x \geq y$: $x = -3$, $y = 1$ gives $9 \geq -3$ but $-3 < 1$. Treat $x > 0$ and $x < 0$ separately, or move everything to one side and factor $x(x - y) \geq 0$.

LỖI HAY GẶP / COMMON MISTAKE — Nhân hai bất đẳng thức cùng chiều khi có số âm. Từ $a > b$ và $c > d$ không suy ra $ac > bd$: $a = 1$, $b = -5$, $c = 2$, $d = -3$ cho $ac = 2 < 15 = bd$. Tính chất 2.2(iii) đòi mọi số không âm.

Multiplying same-direction inequalities when negative numbers are present. From $a > b$ and $c > d$ one cannot deduce $ac > bd$: $a = 1$, $b = -5$, $c = 2$, $d = -3$ gives $ac = 2 < 15 = bd$. Property 2.2(iii) requires all numbers non-negative.

LỖI HAY GẶP / COMMON MISTAKE — Xử lý biểu thức có hai biến bằng cách tối ưu từng biến riêng rồi ghép lại, trong khi ràng buộc nối các biến với nhau. Với $a + b \leq 2$ và $P = a$

+ b + 1/a + 4/b, tối ưu riêng cho a = 1, b = 2, tức P = 6, nhưng điểm này vi phạm a + b ≤ 2 và cận 6 không đạt được; giá trị nhỏ nhất thật là 13/2.

Optimising each variable separately and then combining, while a constraint links the variables. With a + b ≤ 2 and P = a + b + 1/a + 4/b, separate optimisation gives a = 1, b = 2, that is P = 6, but this point violates a + b ≤ 2 and the bound 6 is not attained; the true minimum is 13/2.

PHẢI THUỘC / MEMORISE — Một bài cực trị chỉ hoàn thành khi có đủ: (1) chứng minh bất đẳng thức; (2) chỉ ra bộ giá trị biến làm dấu bằng xảy ra và thuộc miền xác định; (3) kết luận bằng một câu "Vậy giá trị nhỏ nhất bằng ...".

An extremum problem is finished only when you have: (1) proved the inequality; (2) exhibited values of the variables for which equality holds and which lie in the domain; (3) concluded with a sentence "Hence the minimum is ...".

2.8. Kỹ thuật tách – ghép và các bổ đề nhỏ — *Splitting, pairing and small lemmas*

Nhiều bài khó thực ra là tổng của vài bất đẳng thức nhỏ, mỗi bất đẳng thức chỉ cần một dòng. Các bổ đề sau xuất hiện lặp lại ở dạng phân thức, bậc ba và tổng nghịch đảo.

Many hard problems are really a sum of a few small inequalities, each needing one line. The lemmas that follow recur in fractional, cubic and reciprocal-sum form.

BỔ ĐỀ 2.28 (Bốn bổ đề tách – ghép) / LEMMA 2.28 (Four splitting lemmas) — Với x, y > 0:

- (a) $x^2/y \geq 2x - y$, dấu bằng khi x = y;
- (b) $1/x + 1/y \geq 4/(x + y)$, dấu bằng khi x = y;
- (c) $x^3 + y^3 \geq xy(x + y)$, dấu bằng khi x = y;
- (d) $x/y + y/x \geq 2$, dấu bằng khi x = y.

For x, y > 0:

- (a) $x^2/y \geq 2x - y$, with equality when x = y;
- (b) $1/x + 1/y \geq 4/(x + y)$, with equality when x = y;
- (c) $x^3 + y^3 \geq xy(x + y)$, with equality when x = y;
- (d) $x/y + y/x \geq 2$, with equality when x = y.

Chứng minh. / *Proof.*

- (a) $x^2/y - (2x - y) = (x^2 - 2xy + y^2)/y = (x - y)^2/y \geq 0$ vì y > 0.
- (a) $x^2/y - (2x - y) = (x^2 - 2xy + y^2)/y = (x - y)^2/y \geq 0$ because y > 0.
- (b) $1/x + 1/y - 4/(x + y) = [(x + y)^2 - 4xy]/(xy(x + y)) = (x - y)^2/(xy(x + y)) \geq 0$.
- (b) $1/x + 1/y - 4/(x + y) = [(x + y)^2 - 4xy]/(xy(x + y)) = (x - y)^2/(xy(x + y)) \geq 0$.
- (c) $x^3 + y^3 - xy(x + y) = x^3 - x^2y - xy^2 + y^3 = (x + y)(x - y)^2 \geq 0$.
- (c) $x^3 + y^3 - xy(x + y) = x^3 - x^2y - xy^2 + y^3 = (x + y)(x - y)^2 \geq 0$.
- (d) $x/y + y/x - 2 = (x - y)^2/(xy) \geq 0$.
- (d) $x/y + y/x - 2 = (x - y)^2/(xy) \geq 0$. ■

BỔ ĐỀ 2.29 (Tách – ghép bậc n + 1) / LEMMA 2.29 (Splitting of degree n + 1) — Với x, y ≥ 0 và n ∈ ℤ⁺: $x^{n+1} + y^{n+1} \geq x^n y + xy^n$. Dấu bằng khi và chỉ khi x = y.

For x, y ≥ 0 and n ∈ ℤ⁺: $x^{n+1} + y^{n+1} \geq x^n y + xy^n$. Equality holds if and only if x = y.

Chứng minh. / Proof.

Hiệu hai vế bằng $(x^n - y^n)(x - y)$. Theo Tính chất 2.2(v), $x^n - y^n$ cùng dấu với $x - y$ khi $x, y \geq 0$, nên tích không âm; nó bằng 0 chỉ khi $x = y$.

The difference of the two sides equals $(x^n - y^n)(x - y)$. By Property 2.2(v), $x^n - y^n$ has the same sign as $x - y$ for $x, y \geq 0$, so the product is non-negative; it is 0 only when $x = y$. ■

NHẬN XÉT / REMARK — Với $n = 2$ ta được $x^3 + y^3 \geq x^2y + xy^2$, trùng Bổ đề 2.28(c). Với $n = 4$: $x^5 + y^5 \geq x^4y + xy^4$. Cộng vòng cho ba cặp: $2(a^{n+1} + b^{n+1} + c^{n+1}) \geq ab(a^{n-1} + b^{n-1}) + bc(b^{n-1} + c^{n-1}) + ca(c^{n-1} + a^{n-1})$.

For $n = 2$ we get $x^3 + y^3 \geq x^2y + xy^2$, the same as Lemma 2.28(c). For $n = 4$: $x^5 + y^5 \geq x^4y + xy^4$. Adding cyclically over three pairs: $2(a^{n+1} + b^{n+1} + c^{n+1}) \geq ab(a^{n-1} + b^{n-1}) + bc(b^{n-1} + c^{n-1}) + ca(c^{n-1} + a^{n-1})$.

HỆ QUẢ 2.30 (Tổng nghịch đảo) / COROLLARY 2.30 (Sum of reciprocals) — Với n số dương $x_1, \dots, x_n$: $(x_1 + \dots + x_n)(1/x_1 + \dots + 1/x_n) \geq n^2$. Dấu bằng khi và chỉ khi mọi x_i bằng nhau.

For n positive numbers $x_1, \dots, x_n$: $(x_1 + \dots + x_n)(1/x_1 + \dots + 1/x_n) \geq n^2$. Equality holds if and only if all x_i are equal.

Chứng minh. / Proof.

Áp dụng Định lý 2.12 cho hai bộ $\sqrt{x_i}$ và $1/\sqrt{x_i}$: tích từng cặp bằng 1, nên $(\sum 1)^2 = n^2 \leq (\sum x_i)(\sum 1/x_i)$. Dấu bằng khi hai bộ tỉ lệ, tức $\sqrt{x_i} = \lambda/\sqrt{x_i}$, $x_i = \lambda$ không đổi.

Apply Theorem 2.12 to the lists $\sqrt{x_i}$ and $1/\sqrt{x_i}$: each pair multiplies to 1, so $(\sum 1)^2 = n^2 \leq (\sum x_i)(\sum 1/x_i)$. Equality when the lists are proportional, that is $\sqrt{x_i} = \lambda/\sqrt{x_i}$, $x_i = \lambda$ constant. ■

NHẬN XÉT / REMARK — Với $n = 3$, Hệ quả 2.30 cho $(a + b + c)(1/a + 1/b + 1/c) \geq 9$, tức $1/a + 1/b + 1/c \geq 9/(a + b + c)$. Dạng này quen dùng khi biết tổng $a + b + c$.

For $n = 3$, Corollary 2.30 gives $(a + b + c)(1/a + 1/b + 1/c) \geq 9$, that is $1/a + 1/b + 1/c \geq 9/(a + b + c)$. This form is used when the sum $a + b + c$ is known.

HỆ QUẢ 2.31 (AM–GM có trọng số nguyên) / COROLLARY 2.31 (AM–GM with integer weights) — Với $x_1, \dots, x_k > 0$ và các số nguyên dương $p_1, \dots, p_k$, đặt $N = p_1 + \dots + p_k$. Khi đó $(p_1x_1 + \dots + p_kx_k)/N \geq (x_1^{p_1} \cdots x_k^{p_k})^{1/N}$, dấu bằng khi và chỉ khi $x_1 = \dots = x_k$.

For $x_1, \dots, x_k > 0$ and positive integers $p_1, \dots, p_k$, put $N = p_1 + \dots + p_k$. Then $(p_1x_1 + \dots + p_kx_k)/N \geq (x_1^{p_1} \cdots x_k^{p_k})^{1/N}$, with equality if and only if $x_1 = \dots = x_k$.

Chứng minh. / Proof.

Áp dụng Định lý 2.9 cho N số dương gồm p_1 số bằng x_1 , p_2 số bằng x_2 , ..., p_k số bằng x_k . Trung bình cộng là $(p_1x_1 + \dots + p_kx_k)/N$, trung bình nhân là $(x_1^{p_1} \cdots x_k^{p_k})^{1/N}$. Dấu bằng khi N số bằng nhau, tức $x_1 = \dots = x_k$.

Apply Theorem 2.9 to the N positive numbers consisting of p_1 copies of x_1 , p_2 copies of x_2 , ..., p_k copies of x_k . The arithmetic mean is $(p_1x_1 + \dots + p_kx_k)/N$ and the geometric mean is $(x_1^{p_1} \cdots x_k^{p_k})^{1/N}$. Equality when all N numbers are equal, that is $x_1 = \dots = x_k$. ■

NHẬN XÉT / REMARK — Cộng vòng Bỏ đề 2.28(a) cho các cặp (a, b) , (b, c) , (c, a) ta được $a^2/b + b^2/c + c^2/a \geq (2a - b) + (2b - c) + (2c - a) = a + b + c$, kết quả trùng với dạng Engel nhưng chỉ cần một dòng.

Adding Lemma 2.28(a) cyclically for the pairs (a, b) , (b, c) , (c, a) gives $a^2/b + b^2/c + c^2/a \geq (2a - b) + (2b - c) + (2c - a) = a + b + c$, the same as the Engel form but in a single line.

NHẬN XÉT / REMARK — Cộng Bỏ đề 2.28(c) cho ba cặp được $2(a^3 + b^3 + c^3) \geq ab(a + b) + bc(b + c) + ca(c + a)$. Về phải còn viết được bằng $(a + b + c)(ab + bc + ca) - 3abc$, nên bất đẳng thức này nổi bậc ba với các tổng đối xứng sơ cấp.

Adding Lemma 2.28(c) over three pairs gives $2(a^3 + b^3 + c^3) \geq ab(a + b) + bc(b + c) + ca(c + a)$. The right side equals $(a + b + c)(ab + bc + ca) - 3abc$, so this inequality links cubes with the elementary symmetric sums.

NHẬN XÉT / REMARK — Hệ quả 2.31 giải thích cách chọn hệ số ở Ví dụ 2.5: để chặn x^2y ta dùng hai bản sao của x và một bản sao của y , nên $N = 3$ và điểm rơi là các số tách ra bằng nhau. Cùng cách ấy, a^2b^3 với $2a + 3b$ cố định dùng hai bản sao của a và ba bản sao của b ($N = 5$).

Corollary 2.31 explains the choice of coefficients in Example 2.5: to bound x^2y we use two copies of x and one copy of y , so $N = 3$ and the equality point is where the split numbers are equal. By the same device, a^2b^3 with $2a + 3b$ fixed uses two copies of a and three copies of b ($N = 5$).

LỖI HAY GẶP / COMMON MISTAKE — Cộng bất đẳng thức cùng chiều rồi trừ. Có thể cộng hai bất đẳng thức cùng chiều, nhưng không được trừ chúng: từ $a \geq b$ và $c \geq d$ không suy ra $a - c \geq b - d$ (chẳng hạn $3 \geq 1$ và $5 \geq 0$ cho $3 - 5 = -2 < 1 - 0 = 1$). Muốn trừ, chuyển về dạng hiệu trước.

Adding same-direction inequalities and then subtracting. Two inequalities in the same direction can be added but not subtracted: from $a \geq b$ and $c \geq d$ one cannot deduce $a - c \geq b - d$ (for instance $3 \geq 1$ and $5 \geq 0$ give $3 - 5 = -2 < 1 - 0 = 1$). To subtract, rewrite in difference form first.

PHẢI THUỘC / MEMORISE — $x^2/y \geq 2x - y$; $1/x + 1/y \geq 4/(x + y)$; $x^3 + y^3 \geq xy(x + y)$; $(\sum x_i)(\sum 1/x_i) \geq n^2$. Cả bốn đều chứng minh trong một dòng từ $(x - y)^2 \geq 0$ hoặc Cauchy–Schwarz.

$x^2/y \geq 2x - y$; $1/x + 1/y \geq 4/(x + y)$; $x^3 + y^3 \geq xy(x + y)$; $(\sum x_i)(\sum 1/x_i) \geq n^2$. All four follow in one line from $(x - y)^2 \geq 0$ or Cauchy–Schwarz.

2.9. Bảng chiến lược chọn công cụ — Strategy table: choosing the tool

Dấu hiệu trong đề <i>Sign in the problem</i>	Công cụ nên thử <i>Tool to try</i>	Ví dụ <i>Example</i>
Hiệu hai vế gom được thành tổng các bình phương <i>The difference of the sides groups into a sum of squares</i>	Biến đổi tương đương, Bỏ đề 2.5 <i>Equivalent transformation, Lemma 2.5</i>	Ví dụ 2.1, 2.2 <i>Example 2.1, 2.2</i>

Dấu hiệu trong đề <i>Sign in the problem</i>	Công cụ nên thử <i>Tool to try</i>	Ví dụ <i>Example</i>
Tích hoặc tổng cố định, cần cực trị, hạng tử dương <i>Fixed product or sum, extremum wanted, positive terms</i>	AM–GM với điểm rơi, tách hạng tử <i>AM–GM with equality point, splitting</i>	Ví dụ 2.3, 2.5 <i>Example 2.3, 2.5</i>
Phân thức x^2/y , tổng nghịch đảo, $x^3 + y^3$, tích các tổng $a + b$, $b + c$, $c + a$ <i>Fractions x^2/y, sums of reciprocals, $x^3 + y^3$, products of sums $a + b$, $b + c$, $c + a$</i>	Bổ đề tách – ghép, AM–GM từng cặp <i>Splitting lemmas, AM–GM on each pair</i>	Bổ đề 2.28, Ví dụ 2.4 <i>Lemma 2.28, Example 2.4</i>
Biểu thức bậc nhất bị chặn bởi tổng bình phương <i>A linear expression bounded by a sum of squares</i>	Cauchy–Schwarz có trọng số <i>Weighted Cauchy–Schwarz</i>	Ví dụ 2.7 <i>Example 2.7</i>
Tổng phân thức, tổng mẫu hoặc tổng tử biết trước <i>A sum of fractions with known sum of denominators or numerators</i>	Dạng Engel (Titu), Nesbitt <i>Engel form (Titu), Nesbitt</i>	Ví dụ 2.8, 2.9 <i>Example 2.8, 2.9</i>
Hai vế có cùng thừa số, chỉ khác hoán vị vòng <i>Both sides share factors and differ by a cyclic shift</i>	Bất đẳng thức hoán vị, Chebyshev <i>Rearrangement, Chebyshev</i>	Ví dụ 2.10 <i>Example 2.10</i>
Lũy thừa $(1 + x)^n$ so với $1 + nx$ <i>A power $(1 + x)^n$ against $1 + nx$</i>	Bernoulli	Ví dụ 2.11 <i>Example 2.11</i>
Tổng hai căn $\sqrt{p^2 + q^2}$ với phần chứa biến có tổng không đổi <i>A sum of two roots $\sqrt{p^2 + q^2}$ whose variable parts have constant sum</i>	Minkowski, hình học <i>Minkowski, geometry</i>	Ví dụ 2.12 <i>Example 2.12</i>
Có điều kiện dạng " $\leq$ " chặn điểm rơi quen thuộc <i>A condition of the form "$\leq$" blocking the familiar equality point</i>	Đặt $t =$ tổng, khảo sát theo t <i>Put $t =$ the sum and study in t</i>	Ví dụ 2.13 <i>Example 2.13</i>
Biểu thức chỉ bất biến theo hoán vị vòng <i>An expression invariant only under cyclic permutation</i>	Quay vòng để một biến nằm giữa <i>Rotate so that one variable lies in the middle</i>	Ví dụ 2.14 <i>Example 2.14</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Bất đẳng thức	Inequality	Quan hệ $\geq, >, \leq$ hoặc $<$ giữa hai biểu thức <i>A relation $\geq, >, \leq$ or $<$ between two expressions</i>
Dấu bằng	Equality case	Giá trị biến làm hai vế bằng nhau <i>Values of the variables making both sides equal</i>
Điểm rơi	Equality point	Điểm tại đó AM–GM thành đẳng thức <i>The point at which AM–GM becomes an equality</i>
Biến đổi tương đương	Equivalent transformation	Biến đổi hai chiều, không đổi tập nghiệm <i>A two-way step that keeps the solution set</i>
Trung bình cộng	Arithmetic mean	$(a_1 + \dots + a_n)/n$
Trung bình nhân	Geometric mean	$(a_1 \cdots a_n)^{1/n}$, các số không âm <i>$(a_1 \cdots a_n)^{1/n}$, numbers non-negative</i>
Trung bình điều hòa	Harmonic mean	$n/(1/x_1 + \dots + 1/x_n)$, các số dương <i>$n/(1/x_1 + \dots + 1/x_n)$, numbers positive</i>
Trung bình bình phương	Quadratic mean	$\sqrt{((x_1^2 + \dots + x_n^2)/n)}$
Quy nạp Cauchy	Cauchy induction	Quy nạp lên 2^k rồi lùi từng bước <i>Induction up to 2^k, then stepping down</i>
Đồng nhất thức Lagrange	Lagrange's identity	Biểu diễn hiệu hai vế Cauchy–Schwarz bằng tổng bình phương <i>Writes the Cauchy–Schwarz gap as a sum of squares</i>
Dạng Engel	Engel form	$\sum a_i^2/b_i \geq (\sum a_i)^2/\sum b_i$
Hai bộ tỉ lệ	Proportional lists	Điều kiện dấu bằng của Cauchy–Schwarz <i>Equality condition of Cauchy–Schwarz</i>
Cùng thứ tự	Similarly ordered	Hai dãy cùng tăng <i>Both lists increasing</i>
Hoán vị	Permutation	Cách sắp xếp lại n phần tử <i>A rearrangement of n elements</i>
Dịch vòng	Cyclic shift	Hoán vị (a, b, c) thành (b, c, a) <i>Permuting (a, b, c) to (b, c, a)</i>
Giá trị tuyệt đối	Absolute value	Bằng x nếu $x \geq 0$, bằng $-x$ nếu $x < 0$ <i>Equals x if $x \geq 0$, equals $-x$ if $x < 0$</i>
Bất đẳng thức tam giác	Triangle inequality	Trị tuyệt đối của tổng không vượt tổng các trị tuyệt đối <i>The absolute value of a sum is at most the sum of the absolute values</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Giá trị nhỏ nhất	Minimum value	Cận dưới đạt được tại một điểm của miền <i>A lower bound attained at a point of the domain</i>
Cận dưới	Lower bound	Số không vượt quá mọi giá trị của hàm <i>A number not exceeding any value of the function</i>
Ràng buộc	Constraint	Điều kiện cho trước giữa các biến <i>A given condition linking the variables</i>
Tách hạng tử	Term splitting	Viết một hạng tử thành tổng để dùng AM–GM <i>Writing a term as a sum so that AM–GM applies</i>
Phản ví dụ	Counterexample	Bộ giá trị làm một khẳng định sai <i>Values that make a claim false</i>
Tam thức bậc hai	Quadratic trinomial	$ax^2 + bx + c$ với $a \neq 0$ <i>$ax^2 + bx + c$ with $a \neq 0$</i>
Biệt thức	Discriminant	$\Delta = b^2 - 4ac$, quyết định dấu tam thức <i>$\Delta = b^2 - 4ac$, decides the sign of the trinomial</i>
Trung bình có trọng số	Weighted mean	$(p_1x_1 + \dots + p_kx_k)/N$ với $N = \sum p_i$ <i>$(p_1x_1 + \dots + p_kx_k)/N$ with $N = \sum p_i$</i>

2.10. Bài tự luyện — Practice problems

Mức 1 — Học sinh giỏi cấp tỉnh — Level 1 — Provincial olympiad

Bài 2.1 / Problem 2.1 — Chứng minh rằng với mọi số thực a, b, c, d : $a^2 + b^2 + c^2 + d^2 \geq (a + b)(c + d)$. Tìm các trường hợp dấu bằng.

Prove that for all real a, b, c, d : $a^2 + b^2 + c^2 + d^2 \geq (a + b)(c + d)$. Find the equality cases.

Bài 2.2 / Problem 2.2 — Tìm giá trị nhỏ nhất của biểu thức $9x + 1/(x - 1)$ với $x > 1$.

Find the minimum of the expression $9x + 1/(x - 1)$ for $x > 1$.

Bài 2.3 / Problem 2.3 — Chứng minh rằng với mọi $a, b, c > 0$: $(a + b + c)(1/a + 1/b + 1/c) \geq 9$. Suy ra: nếu $a + b + c = 1$ thì $1/a + 1/b + 1/c \geq 9$.

Prove that for all $a, b, c > 0$: $(a + b + c)(1/a + 1/b + 1/c) \geq 9$. Deduce: if $a + b + c = 1$ then $1/a + 1/b + 1/c \geq 9$.

Bài 2.4 / Problem 2.4 — Tìm giá trị nhỏ nhất của $f(x) = |x - 1| + |x - 3| + |x - 7|$ trên $\mathbb{R}$.

Find the minimum of $f(x) = |x - 1| + |x - 3| + |x - 7|$ over $\mathbb{R}$.

Mức 2 — Học sinh giỏi quốc gia — Level 2 — National olympiad

Bài 2.5 / Problem 2.5 — Cho $a, b > 0$ thỏa mãn $2a + 3b = 12$. Tìm giá trị lớn nhất của a^2b^3 .

Let $a, b > 0$ satisfy $2a + 3b = 12$. Find the maximum of a^2b^3 .

Bài 2.6 / Problem 2.6 — Cho x, y, z là các số thực thỏa mãn $x + 2y - 2z = 9$. Tìm giá trị nhỏ nhất của $x^2 + y^2 + z^2$ và các giá trị x, y, z tại đó.

Let x, y, z be real numbers with $x + 2y - 2z = 9$. Find the minimum of $x^2 + y^2 + z^2$ and the values of x, y, z where it is attained.

Bài 2.7 / Problem 2.7 — Cho $a, b, c > 0$ với $a + b + c = 1$. Tìm giá trị nhỏ nhất của $a^2/(a + b) + b^2/(b + c) + c^2/(c + a)$.

Let $a, b, c > 0$ with $a + b + c = 1$. Find the minimum of $a^2/(a + b) + b^2/(b + c) + c^2/(c + a)$.

Bài 2.8 / Problem 2.8 — Chứng minh rằng với mọi $a, b, c > 0$: $a^3 + b^3 + c^3 \geq (a + b + c)(a^2 + b^2 + c^2)/3 \geq (a + b + c)^3/9$.

Prove that for all $a, b, c > 0$: $a^3 + b^3 + c^3 \geq (a + b + c)(a^2 + b^2 + c^2)/3 \geq (a + b + c)^3/9$.

Mức 3 — Olympic quốc tế — Level 3 — International olympiad

Bài 2.9 / Problem 2.9 — Chứng minh rằng với mọi $a, b, c > 0$: $a^3/(a + 2b) + b^3/(b + 2c) + c^3/(c + 2a) \geq (a^2 + b^2 + c^2)^2/(a + b + c)^2 \geq (a^2 + b^2 + c^2)/3$.

Prove that for all $a, b, c > 0$: $a^3/(a + 2b) + b^3/(b + 2c) + c^3/(c + 2a) \geq (a^2 + b^2 + c^2)^2/(a + b + c)^2 \geq (a^2 + b^2 + c^2)/3$.

Bài 2.10 / Problem 2.10 — Chứng minh rằng với mọi số nguyên $n \geq 2$: $1 \cdot 3 \cdot 5 \cdots (2n - 1) < n^n$.

Prove that for every integer $n \geq 2$: $1 \cdot 3 \cdot 5 \cdots (2n - 1) < n^n$.

Bài 2.11 / Problem 2.11 — Tìm giá trị nhỏ nhất của $F(x) = \sqrt{x^2 - 2x + 5} + \sqrt{x^2 - 10x + 34}$ trên $\mathbb{R}$.

Find the minimum of $F(x) = \sqrt{x^2 - 2x + 5} + \sqrt{x^2 - 10x + 34}$ over $\mathbb{R}$.

Bài 2.12 / Problem 2.12 — Chứng minh rằng với mọi $a, b, c > 0$: $a/b + b/c + c/a \geq (a + b + c)/\sqrt[3]{abc}$. Tìm các trường hợp dấu bằng.

Prove that for all $a, b, c > 0$: $a/b + b/c + c/a \geq (a + b + c)/\sqrt[3]{abc}$. Find the equality cases.

2.11. Lời giải bài tự luyện — Solutions to practice problems

Bài 2.1 — Problem 2.1

Khai triển $(a + b)(c + d) = ac + ad + bc + bd$. Ta có đồng nhất thức (kiểm tra bằng khai triển bốn bình phương ở vế phải):

Expand $(a + b)(c + d) = ac + ad + bc + bd$. We have the identity (check by expanding the four squares on the right):

$$a^2 + b^2 + c^2 + d^2 - (a + b)(c + d) = (1/2) \cdot [(a - c)^2 + (a - d)^2 + (b - c)^2 + (b - d)^2]$$

Vế phải là tổng bình phương, không âm, nên bất đẳng thức đúng.

The right side is a sum of squares, so it is non-negative and the inequality holds.

Dấu bằng khi $a = c, a = d, b = c, b = d$, tức $a = b = c = d$. Vậy dấu bằng khi và chỉ khi bốn số bằng nhau.

Equality holds when $a = c, a = d, b = c, b = d$, that is $a = b = c = d$. Hence equality holds if and only if the four numbers are equal. ■

Bài 2.2 — Problem 2.2

Điều kiện $x > 1$ cho $x - 1 > 0$. Viết $9x + 1/(x - 1) = 9(x - 1) + 1/(x - 1) + 9$. Theo AM–GM hai số dương:

The condition $x > 1$ gives $x - 1 > 0$. Write $9x + 1/(x - 1) = 9(x - 1) + 1/(x - 1) + 9$. By two-term AM–GM on positive numbers:

$$9(x - 1) + 1/(x - 1) \geq 2 \cdot \sqrt{(9(x - 1)) \cdot 1/(x - 1)} = 6$$

Do đó biểu thức không nhỏ hơn $6 + 9 = 15$. Dấu bằng khi $9(x - 1) = 1/(x - 1)$, tức $(x - 1)^2 = 1/9$, $x - 1 = 1/3$ (lấy nghiệm dương), $x = 4/3 > 1$.

So the expression is at least $6 + 9 = 15$. Equality holds when $9(x - 1) = 1/(x - 1)$, that is $(x - 1)^2 = 1/9$, $x - 1 = 1/3$ (the positive root), $x = 4/3 > 1$.

Kiểm tra: $9 \cdot (4/3) + 1/(1/3) = 12 + 3 = 15$. Vậy giá trị nhỏ nhất bằng 15, đạt tại $x = 4/3$.

Check: $9 \cdot (4/3) + 1/(1/3) = 12 + 3 = 15$. Hence the minimum is 15, attained at $x = 4/3$. ■

Bài 2.3 — Problem 2.3

Khai triển tích:

Expand the product:

$$(a + b + c)(1/a + 1/b + 1/c) = 3 + (a/b + b/a) + (b/c + c/b) + (c/a + a/c)$$

Với $x, y > 0$, theo AM–GM hai số, $x/y + y/x \geq 2\sqrt{(1)} = 2$. Áp dụng cho ba cặp: tổng ba ngoặc không nhỏ hơn 6. Vậy tích không nhỏ hơn $3 + 6 = 9$, dấu bằng khi $a = b = c$.

For $x, y > 0$, two-term AM–GM gives $x/y + y/x \geq 2\sqrt{(1)} = 2$. Applied to the three pairs, the sum of the three brackets is at least 6. So the product is at least $3 + 6 = 9$, with equality when $a = b = c$.

Nếu $a + b + c = 1$ thì tích bằng $1/a + 1/b + 1/c$, nên $1/a + 1/b + 1/c \geq 9$, dấu bằng tại $a = b = c = 1/3$.

If $a + b + c = 1$ the product equals $1/a + 1/b + 1/c$, so $1/a + 1/b + 1/c \geq 9$, with equality at $a = b = c = 1/3$. ■

Bài 2.4 — Problem 2.4

Theo bất đẳng thức tam giác, $|x - 1| + |x - 7| = |x - 1| + |7 - x| \geq |(x - 1) + (7 - x)| = 6$, dấu bằng khi $1 \leq x \leq 7$.

By the triangle inequality, $|x - 1| + |x - 7| = |x - 1| + |7 - x| \geq |(x - 1) + (7 - x)| = 6$, with equality when $1 \leq x \leq 7$.

Mặt khác $|x - 3| \geq 0$, dấu bằng khi $x = 3$. Cộng hai bất đẳng thức: $f(x) \geq 6 + 0 = 6$.

Also $|x - 3| \geq 0$, with equality when $x = 3$. Adding the two inequalities: $f(x) \geq 6 + 0 = 6$.

Tại $x = 3$ (thuộc đoạn $[1, 7]$) cả hai dấu bằng cùng xảy ra: $f(3) = 2 + 0 + 4 = 6$. Vậy giá trị nhỏ nhất bằng 6, đạt tại $x = 3$.

At $x = 3$ (which lies in $[1, 7]$) both equalities hold at once: $f(3) = 2 + 0 + 4 = 6$. Hence the minimum is 6, attained at $x = 3$. ■

Bài 2.5 — Problem 2.5

Áp dụng AM–GM cho năm số dương a, a, b, b, b (hai số a và ba số b); tổng của chúng là $2a + 3b = 12$:

Apply AM–GM to the five positive numbers a, a, b, b, b (two copies of a and three of b); their sum is $2a + 3b = 12$:

$$a \cdot a \cdot b \cdot b \cdot b \leq ((a + a + b + b + b)/5)^5 = (12/5)^5$$

Dấu bằng khi $a = b$; cùng $2a + 3b = 12$ cho $a = b = 12/5$ (dương).

Equality holds when $a = b$; with $2a + 3b = 12$ this gives $a = b = 12/5$ (positive).

Vậy giá trị lớn nhất của a^2b^3 bằng $(12/5)^5 = 248832/3125$, đạt tại $a = b = 12/5$.

Hence the maximum of a^2b^3 is $(12/5)^5 = 248832/3125$, attained at $a = b = 12/5$. ■

Bài 2.6 — Problem 2.6

Áp dụng Cauchy–Schwarz cho bộ $(1, 2, -2)$ và (x, y, z) :

Apply Cauchy–Schwarz to the lists $(1, 2, -2)$ and (x, y, z) :

$$81 = (x + 2y - 2z)^2 \leq (1^2 + 2^2 + (-2)^2)(x^2 + y^2 + z^2) = 9(x^2 + y^2 + z^2)$$

Suy ra $x^2 + y^2 + z^2 \geq 9$. Dấu bằng khi $(x, y, z) = k(1, 2, -2)$; thế vào điều kiện: $k + 4k + 4k = 9k = 9$, nên $k = 1$.

Hence $x^2 + y^2 + z^2 \geq 9$. Equality holds when $(x, y, z) = k(1, 2, -2)$; substituting into the condition: $k + 4k + 4k = 9k = 9$, so $k = 1$.

Vậy giá trị nhỏ nhất bằng 9, đạt tại $(x, y, z) = (1, 2, -2)$.

Hence the minimum is 9, attained at $(x, y, z) = (1, 2, -2)$. ■

Bài 2.7 — Problem 2.7

Các mẫu $a + b, b + c, c + a$ đều dương. Theo dạng Engel:

The denominators $a + b, b + c, c + a$ are all positive. By the Engel form:

$$\begin{aligned} a^2/(a + b) + b^2/(b + c) + c^2/(c + a) &\geq (a + b + c)^2/[(a + b) + (b + c) + (c + a)] \\ &= 1/(2(a + b + c)) = 1/2 \end{aligned}$$

Tại $a = b = c = 1/3$: mỗi số hạng bằng $(1/9)/(2/3) = 1/6$, tổng bằng $1/2$, nên cận $1/2$ đạt được.

At $a = b = c = 1/3$: each term equals $(1/9)/(2/3) = 1/6$ and the sum is $1/2$, so the bound $1/2$ is attained.

Vậy giá trị nhỏ nhất bằng $1/2$.

Hence the minimum is $1/2$. ■

Bài 2.8 — Problem 2.8

Bất đẳng thức thứ nhất: không mất tổng quát $a \leq b \leq c$. Khi đó $a^2 \leq b^2 \leq c^2$ (các số dương), hai bộ (a, b, c) và (a^2, b^2, c^2) cùng thứ tự. Theo Chebyshev:

First inequality: WLOG $a \leq b \leq c$. Then $a^2 \leq b^2 \leq c^2$ (the numbers are positive), so the lists (a, b, c) and (a^2, b^2, c^2) are ordered alike. By Chebyshev:

$$3(a^3 + b^3 + c^3) \geq (a + b + c)(a^2 + b^2 + c^2)$$

Chia hai vế cho 3 được bất đẳng thức thứ nhất.

Dividing both sides by 3 gives the first inequality.

Bất đẳng thức thứ hai: theo chuỗi QM–AM (hay Cauchy–Schwarz cho bộ $(1, 1, 1)$ và (a, b, c)), $3(a^2 + b^2 + c^2) \geq (a + b + c)^2$. Nhân hai vế với $(a + b + c)/9 > 0$:

Second inequality: by QM–AM (or Cauchy–Schwarz for the lists $(1, 1, 1)$ and (a, b, c)), $3(a^2 + b^2 + c^2) \geq (a + b + c)^2$. Multiply both sides by $(a + b + c)/9 > 0$:

$$(a + b + c)(a^2 + b^2 + c^2)/3 \geq (a + b + c)^3/9$$

Dấu bằng cả hai bước khi $a = b = c$.

Equality in both steps holds when $a = b = c$. ■

Bài 2.9 — Problem 2.9

Viết $a^3/(a + 2b) = (a^2)^2/(a^2 + 2ab)$ và tương tự. Các mẫu $a^2 + 2ab$, $b^2 + 2bc$, $c^2 + 2ca$ đều dương, tổng của chúng là $a^2 + b^2 + c^2 + 2(ab + bc + ca) = (a + b + c)^2$. Theo dạng Engel với tử a^2 , b^2 , c^2 :

Write $a^3/(a + 2b) = (a^2)^2/(a^2 + 2ab)$ and similarly. The denominators $a^2 + 2ab$, $b^2 + 2bc$, $c^2 + 2ca$ are positive and sum to $a^2 + b^2 + c^2 + 2(ab + bc + ca) = (a + b + c)^2$. By the Engel form with numerators a^2 , b^2 , c^2 :

$$a^3/(a + 2b) + b^3/(b + 2c) + c^3/(c + 2a) \geq (a^2 + b^2 + c^2)^2/(a + b + c)^2$$

Bất đẳng thức thứ hai: chia hai vế cho $a^2 + b^2 + c^2 > 0$, cần $(a^2 + b^2 + c^2)/(a + b + c)^2 \geq 1/3$, tức $3(a^2 + b^2 + c^2) \geq (a + b + c)^2$. Bất đẳng thức này tương đương $a^2 + b^2 + c^2 \geq ab + bc + ca$, đúng vì hiệu bằng $(1/2) \cdot [(a - b)^2 + (b - c)^2 + (c - a)^2]$.

Second inequality: divide by $a^2 + b^2 + c^2 > 0$; we need $(a^2 + b^2 + c^2)/(a + b + c)^2 \geq 1/3$, that is $3(a^2 + b^2 + c^2) \geq (a + b + c)^2$. This is equivalent to $a^2 + b^2 + c^2 \geq ab + bc + ca$, true because the difference is $(1/2) \cdot [(a - b)^2 + (b - c)^2 + (c - a)^2]$.

Tại $a = b = c = 1$: vế trái bằng $3 \cdot (1/3) = 1$, vế giữa bằng $9/9 = 1$, vế phải bằng $3/3 = 1$, nên dấu bằng xảy ra khi $a = b = c$.

At $a = b = c = 1$: the left side is $3 \cdot (1/3) = 1$, the middle is $9/9 = 1$, the right is $3/3 = 1$, so equality holds when $a = b = c$. ■

Bài 2.10 — Problem 2.10

Xét n số dương lẻ $1, 3, 5, \dots, 2n - 1$. Tổng của chúng là n^2 (cấp số cộng n số hạng, công sai 2: tổng bằng $n \cdot (1 + (2n - 1))/2 = n^2$), nên trung bình cộng bằng n .

Consider the n positive odd numbers $1, 3, 5, \dots, 2n - 1$. Their sum is n^2 (an arithmetic progression with n terms and common difference 2: the sum is $n \cdot (1 + (2n - 1))/2 = n^2$), so the arithmetic mean is n .

Theo AM–GM cho n số: $(1 \cdot 3 \cdots (2n - 1))^{1/n} \leq n$.

By AM–GM for n numbers: $(1 \cdot 3 \cdots (2n - 1))^{1/n} \leq n$.

Với $n \geq 2$ các số 1 và 3 khác nhau nên các số không đều bằng nhau, dấu bằng không xảy ra: $(1 \cdot 3 \cdots (2n-1))^{1/n} < n$.

For $n \geq 2$ the numbers 1 and 3 differ, so the numbers are not all equal and equality cannot occur: $(1 \cdot 3 \cdots (2n-1))^{1/n} < n$.

Lũy thừa n hai vế dương: $1 \cdot 3 \cdot 5 \cdots (2n-1) < n^n$. Kiểm tra $n = 2$: $1 \cdot 3 = 3 < 4$.

Raising both positive sides to the power n : $1 \cdot 3 \cdot 5 \cdots (2n-1) < n^n$. Check $n = 2$: $1 \cdot 3 = 3 < 4$. ■

Bài 2.11 — Problem 2.11

Hoàn thành bình phương: $x^2 - 2x + 5 = (x-1)^2 + 2^2$ và $x^2 - 10x + 34 = (x-5)^2 + 3^2$. Đặt $a = x-1$, $b = 2$, $c = 5-x$, $d = 3$ (chú ý $(5-x)^2 = (x-5)^2$).

Complete the squares: $x^2 - 2x + 5 = (x-1)^2 + 2^2$ and $x^2 - 10x + 34 = (x-5)^2 + 3^2$. Put $a = x-1$, $b = 2$, $c = 5-x$, $d = 3$ (note $(5-x)^2 = (x-5)^2$).

Theo bất đẳng thức Minkowski:

By Minkowski's inequality:

$$F(x) \geq \sqrt{(a+c)^2 + (b+d)^2} = \sqrt{4^2 + 5^2} = \sqrt{41}$$

Dấu bằng khi $ad = bc$, tức $3(x-1) = 2(5-x)$, $5x = 13$, $x = 13/5$; và $ac + bd = (x-1)(5-x) + 6 = (8/5)(12/5) + 6 > 0$. Cả hai điều kiện thỏa mãn.

Equality holds when $ad = bc$, that is $3(x-1) = 2(5-x)$, $5x = 13$, $x = 13/5$; and $ac + bd = (x-1)(5-x) + 6 = (8/5)(12/5) + 6 > 0$. Both conditions are met.

Vậy giá trị nhỏ nhất bằng $\sqrt{41}$, đạt tại $x = 13/5$.

Hence the minimum is $\sqrt{41}$, attained at $x = 13/5$. ■

Bài 2.12 — Problem 2.12

Đặt $t = \sqrt[3]{abc} > 0$. Theo AM–GM ba số dương a/b , a/b , b/c :

Put $t = \sqrt[3]{abc} > 0$. By three-term AM–GM on the positive numbers a/b , a/b , b/c :

$$a/b + a/b + b/c \geq 3 \cdot \sqrt[3]{(a/b) \cdot (a/b) \cdot (b/c)} = 3 \cdot \sqrt[3]{a^2/(bc)} = 3 \cdot \sqrt[3]{a^3/(abc)} = 3a/t$$

Tương tự, với bộ $(b/c, b/c, c/a)$ và $(c/a, c/a, a/b)$:

Similarly, for the triples $(b/c, b/c, c/a)$ and $(c/a, c/a, a/b)$:

$$b/c + b/c + c/a \geq 3b/t, \quad c/a + c/a + a/b \geq 3c/t$$

Cộng ba bất đẳng thức: vế trái là $3(a/b + b/c + c/a)$ vì mỗi phân số xuất hiện đúng ba lần; vế phải là $3(a + b + c)/t$. Chia cho 3 được điều phải chứng minh.

Add the three inequalities: the left side is $3(a/b + b/c + c/a)$ because each fraction appears exactly three times; the right side is $3(a + b + c)/t$. Divide by 3 to finish.

Dấu bằng khi $a/b = b/c = c/a$. Tích ba tỉ số này bằng 1 nên mỗi tỉ số bằng 1, tức $a = b = c$; ngược lại $a = b = c$ cho hai vế cùng bằng 3. Vậy dấu bằng khi và chỉ khi $a = b = c$.

Equality holds when $a/b = b/c = c/a$. The product of these three ratios is 1, so each equals 1, that is $a = b = c$; conversely $a = b = c$ makes both sides equal 3. Hence equality holds if and only if $a = b = c$. ■

Chương 3. Kỹ thuật chứng minh bất đẳng thức nâng cao — Chapter 3. Advanced techniques for inequalities

Mục tiêu chương — Chapter objectives

- Đưa bất đẳng thức có điều kiện về dạng thuần nhất, và ngược lại dùng điều kiện để hạ bậc.
Turn a constrained inequality into a homogeneous one, and use the constraint to lower the degree.
- Chứng minh và vận dụng bất đẳng thức Schur, phương pháp SOS với tiêu chuẩn S_a , S_b , S_c .
Prove and apply Schur's inequality and the SOS method with the criteria on S_a , S_b , S_c .
- Dùng đánh giá tiếp tuyến, dồn biến về hai biến bằng nhau và đổi biến p , q , r .
Use tangent-line estimates, mixing variables to two equal ones, and the p , q , r substitution.
- Đổi biến Ravi cho cạnh tam giác; dùng hàm lồi và bất đẳng thức Jensen rời rạc mà không cần đạo hàm.
Apply the Ravi substitution to triangle sides; use convex functions and discrete Jensen without derivatives.
- Chọn kỹ thuật theo dấu hiệu của đề và trình bày lời giải đủ điểm.
Choose a technique from the shape of the problem and write a solution that earns full marks.

3.1. Thuần nhất hóa và chuẩn hóa — Homogenisation and normalisation

Nhiều đề cho điều kiện như $abc = 1$, $a + b + c = 3$ hay $ab + bc + ca = 3$. Điều kiện làm các số hạng có bậc khác nhau và che mất cấu trúc của bất đẳng thức. Có hai thao tác ngược chiều nhau: thuần nhất hóa dùng điều kiện để cho mọi số hạng cùng bậc, còn chuẩn hóa dùng tính thuần nhất để thêm một điều kiện gọn vào đề.

Many problems come with a condition such as $abc = 1$, $a + b + c = 3$ or $ab + bc + ca = 3$. The condition gives the terms different degrees and hides the structure of the inequality. Two opposite moves are available: homogenisation uses the condition to give every term the same degree, while normalisation uses homogeneity to add a convenient condition to the problem.

ĐỊNH NGHĨA 3.1 (Đa thức thuần nhất) / DEFINITION 3.1 (Homogeneous polynomial)

— Đa thức $P(a, b, c)$ gọi là thuần nhất bậc k nếu $P(ta, tb, tc) = t^k \cdot P(a, b, c)$ với mọi số thực t . Bất đẳng thức $P(a, b, c) \geq 0$ (hoặc $F \geq G$ với F, G thuần nhất cùng bậc) gọi là thuần nhất. Thương của hai đa thức thuần nhất bậc m và n là hàm thuần nhất bậc $m - n$.

A polynomial $P(a, b, c)$ is homogeneous of degree k if $P(ta, tb, tc) = t^k \cdot P(a, b, c)$ for every real t . An inequality $P(a, b, c) \geq 0$ (or $F \geq G$ with F, G homogeneous of the same degree) is called homogeneous. A quotient of homogeneous polynomials of degrees m and n is homogeneous of degree $m - n$.

TÍNH CHẤT 3.2 (Chuẩn hóa) / PROPERTY 3.2 (Normalisation) — Cho $F(a, b, c)$ thuần nhất (bậc nào cũng được), D là tập các bộ số dương, và $h(a, b, c) > 0$ là hàm thuần nhất bậc $d > 0$ trên D (ví dụ $h = a + b + c$, $h = abc$ với $d = 3$, $h = ab + bc + ca$ với $d = 2$). Nếu $F \geq 0$ đúng với mọi bộ trong D có $h = 1$ thì $F \geq 0$ đúng với mọi bộ trong D . Ta gọi đây là chuẩn hóa.

Let $F(a, b, c)$ be homogeneous (of any degree), D a set of positive triples, and $h(a, b, c) > 0$ a homogeneous function of degree $d > 0$ on D (for example $h = a + b + c$, $h = abc$ with $d = 3$, $h = ab +$

$bc + ca$ with $d = 2$). If $F \geq 0$ holds for every triple in D with $h = 1$, then $F \geq 0$ holds for every triple in D . This is called normalisation.

Chứng minh. / Proof.

Lấy (a, b, c) bất kỳ trong D và đặt $s = h(a, b, c)^{1/d} > 0$. Bộ $(a/s, b/s, c/s)$ có $h = s^{-d} \cdot h(a, b, c) = 1$. Giả thiết cho $F(a/s, b/s, c/s) \geq 0$.

Take any (a, b, c) in D and put $s = h(a, b, c)^{1/d} > 0$. The triple $(a/s, b/s, c/s)$ has $h = s^{-d} \cdot h(a, b, c) = 1$. The hypothesis gives $F(a/s, b/s, c/s) \geq 0$.

Vì F thuần nhất bậc k nên $F(a, b, c) = s^k \cdot F(a/s, b/s, c/s) \geq 0$, do $s^k > 0$.

Since F is homogeneous of degree k , $F(a, b, c) = s^k \cdot F(a/s, b/s, c/s) \geq 0$, because $s^k > 0$. ■

Hai cách dùng. Đề thuần nhất: tự chọn điều kiện cho dễ tính, chẳng hạn $a + b + c = 3$ hoặc $abc = 1$. Đề có điều kiện: nhân hoặc chia từng số hạng cho lũy thừa của biểu thức điều kiện để mọi số hạng cùng bậc, rồi chứng minh bằng các bất đẳng thức thuần nhất quen thuộc. Khi bậc của điều kiện không chia hết bậc của số hạng, ta lũy thừa cả hai vế (vế dương) để tránh căn.

There are two uses. For a homogeneous problem, choose a convenient condition yourself, such as $a + b + c = 3$ or $abc = 1$. For a constrained problem, multiply or divide each term by a power of the constraint expression so that all terms have the same degree, then prove the result with familiar homogeneous inequalities. When the degree of the constraint does not divide the degree of a term, raise both (positive) sides to a power to avoid roots.

PHÂN TÍCH / ANALYSIS — Điều kiện $ab + bc + ca = 3$ có bậc 2, vế trái $(a + b)(b + c)(c + a)$ có bậc 3. Đưa 8 về bậc 3 cần $(q/3)^{3/2}$, có căn. Thay vì thế, tách bất đẳng thức làm hai bước: bậc 3 so với tích $p \cdot q$, rồi dùng $p \geq 3$ suy ra từ $p^2 \geq 3q = 9$.

The condition $ab + bc + ca = 3$ has degree 2, the left side $(a + b)(b + c)(c + a)$ has degree 3. Writing 8 in degree 3 needs $(q/3)^{3/2}$, a root. Instead split the proof in two: degree 3 against the product $p \cdot q$, then use $p \geq 3$, which follows from $p^2 \geq 3q = 9$.

VÍ DỤ 3.1 (Chuẩn hóa điều kiện) / EXAMPLE 3.1 (Using a normalising condition) —

Cho $a, b, c > 0$ thỏa $ab + bc + ca = 3$. Chứng minh $(a + b)(b + c)(c + a) \geq 8$.

Let $a, b, c > 0$ with $ab + bc + ca = 3$. Prove that $(a + b)(b + c)(c + a) \geq 8$.

Lời giải. / Solution.

Đặt $p = a + b + c$, $q = ab + bc + ca = 3$, $r = abc$. Khai triển trực tiếp:

Put $p = a + b + c$, $q = ab + bc + ca = 3$, $r = abc$. Direct expansion gives:

$$(a + b)(b + c)(c + a) = a^2b + a^2c + b^2a + b^2c + c^2a + c^2b + 2abc = pq - r$$

Hiệu $pq - 9r = a(b - c)^2 + b(c - a)^2 + c(a - b)^2 \geq 0$, nên $r \leq pq/9$.

The difference $pq - 9r = a(b - c)^2 + b(c - a)^2 + c(a - b)^2 \geq 0$, so $r \leq pq/9$.

Do đó $(a + b)(b + c)(c + a) = pq - r \geq (8/9) \cdot pq$.

Hence $(a + b)(b + c)(c + a) = pq - r \geq (8/9) \cdot pq$.

Từ $p^2 - 3q = ((a - b)^2 + (b - c)^2 + (c - a)^2)/2 \geq 0$ ta có $p^2 \geq 9$, tức $p \geq 3$ vì $p > 0$. Vậy $(a + b)(b + c)(c + a) \geq (8/9) \cdot 3 \cdot 3 = 8$.

From $p^2 - 3q = ((a - b)^2 + (b - c)^2 + (c - a)^2)/2 \geq 0$ we get $p^2 \geq 9$, that is $p \geq 3$ since $p > 0$. Hence $(a + b)(b + c)(c + a) \geq (8/9) \cdot 3 \cdot 3 = 8$.

Dấu bằng xảy ra khi $a = b = c = 1$.

Equality holds when $a = b = c = 1$. ■

PHÂN TÍCH / ANALYSIS — Vế trái $a + b + c$ có bậc 1, vế phải $ab + bc + ca$ có bậc 2, điều kiện $a^2 + b^2 + c^2 = 3$ có bậc 2. Nhân vế trái với căn của $(a^2 + b^2 + c^2)/3$ (bằng 1) thì hai vế cùng bậc 2. Cả hai vế dương, bình phương lên để hết căn.

The left side $a + b + c$ has degree 1, the right side $ab + bc + ca$ has degree 2, the condition $a^2 + b^2 + c^2 = 3$ has degree 2. Multiplying the left side by the square root of $(a^2 + b^2 + c^2)/3$ (which equals 1) gives degree 2 on both sides. Both sides are positive, so square to remove the root.

VÍ DỤ 3.2 (Thuần nhất hóa bằng căn) / EXAMPLE 3.2 (Homogenising with a root) —

Cho $a, b, c > 0$ thỏa $a^2 + b^2 + c^2 = 3$. Chứng minh $a + b + c \geq ab + bc + ca$.

Let $a, b, c > 0$ with $a^2 + b^2 + c^2 = 3$. Prove that $a + b + c \geq ab + bc + ca$.

Lời giải. / Solution.

Đặt $P = a^2 + b^2 + c^2 (= 3)$, $p = a + b + c$, $q = ab + bc + ca$. Bất đẳng thức cần chứng minh tương đương $p \cdot \sqrt{P/3} \geq q$, tức (vì hai vế dương) $p^2 \cdot P \geq 3q^2$.

Put $P = a^2 + b^2 + c^2 (= 3)$, $p = a + b + c$, $q = ab + bc + ca$. The claim is equivalent to $p \cdot \sqrt{P/3} \geq q$, that is (both sides positive) $p^2 \cdot P \geq 3q^2$.

Vì $p^2 = P + 2q$ nên $p^2 \cdot P - 3q^2 = (P + 2q)P - 3q^2 = P^2 + 2qP - 3q^2 = (P - q)(P + 3q)$.

Since $p^2 = P + 2q$ we get $p^2 \cdot P - 3q^2 = (P + 2q)P - 3q^2 = P^2 + 2qP - 3q^2 = (P - q)(P + 3q)$.

Mà $P - q = ((a - b)^2 + (b - c)^2 + (c - a)^2)/2 \geq 0$ và $P + 3q > 0$, nên tích không âm.

Now $P - q = ((a - b)^2 + (b - c)^2 + (c - a)^2)/2 \geq 0$ and $P + 3q > 0$, so the product is non-negative.

Với $P = 3$ điều đó cho $p \geq q$. Dấu bằng khi $a = b = c = 1$.

With $P = 3$ this gives $p \geq q$. Equality holds when $a = b = c = 1$. ■

NHẬN XÉT / REMARK — Chuẩn hóa chỉ đúng khi bất đẳng thức thuần nhất. Đề nào có hằng số tự do (ví dụ $a^2 + b^2 + c^2 + 1 \geq 2(ab + bc + ca)$) thì không được tự đặt $a + b + c = 3$.

Normalisation is valid only when the inequality is homogeneous. If the problem has a free constant (for example $a^2 + b^2 + c^2 + 1 \geq 2(ab + bc + ca)$), you may not set $a + b + c = 3$.

LỖI HAY GẶP / COMMON MISTAKE — Đặt $a + b + c = 3$ cho một bất đẳng thức không thuần nhất, hoặc sau khi chuẩn hóa quên rằng điều kiện miền ($a, b, c > 0$) vẫn phải giữ cho mọi bộ số.

Setting $a + b + c = 3$ for an inequality that is not homogeneous, or forgetting after normalising that the domain condition ($a, b, c > 0$) must hold for every triple.

3.2. Bất đẳng thức Schur — Schur's inequality

Ký hiệu $p = a + b + c$, $q = ab + bc + ca$, $r = abc$. Ký hiệu $\Sigma_{\text{sym}} a^2b$ nghĩa là tổng sáu số hạng $a^2b + a^2c + b^2a + b^2c + c^2a + c^2b$. Bất đẳng thức Schur bậc ba có hai dạng dấu bằng: $a = b = c$ và $(a, a, 0)$.

Write $p = a + b + c$, $q = ab + bc + ca$, $r = abc$. The symbol $\Sigma_{\text{sym}} a^2b$ means the sum of six terms $a^2b + a^2c + b^2a + b^2c + c^2a + c^2b$. Schur's inequality of degree three has two kinds of equality case: $a = b = c$ and $(a, a, 0)$.

ĐỊNH LÝ 3.3 (Bất đẳng thức Schur) / THEOREM 3.3 (Schur's inequality) — Với mọi $a, b, c \geq 0$: $a(a-b)(a-c) + b(b-a)(b-c) + c(c-a)(c-b) \geq 0$. Dấu bằng xảy ra khi và chỉ khi $a = b = c$, hoặc hai trong ba số bằng nhau và số còn lại bằng 0.

For all $a, b, c \geq 0$: $a(a-b)(a-c) + b(b-a)(b-c) + c(c-a)(c-b) \geq 0$. Equality holds if and only if $a = b = c$, or two of the numbers are equal and the third is 0.

Chứng minh. / Proof.

Về trái đối xứng nên giả sử $a \geq b \geq c \geq 0$. Gộp hai số hạng đầu: $a(a-b)(a-c) + b(b-a)(b-c) = (a-b)[a(a-c) - b(b-c)]$. Vì $a(a-c) - b(b-c) = (a-b)(a+b-c)$ nên tổng hai số hạng đầu bằng $(a-b)^2(a+b-c)$.

The left side is symmetric, so assume $a \geq b \geq c \geq 0$. Combine the first two terms: $a(a-b)(a-c) + b(b-a)(b-c) = (a-b)[a(a-c) - b(b-c)]$. Since $a(a-c) - b(b-c) = (a-b)(a+b-c)$, the first two terms add up to $(a-b)^2(a+b-c)$.

Do $b \geq c$ nên $a+b-c \geq a \geq 0$, suy ra $(a-b)^2(a+b-c) \geq 0$. Số hạng thứ ba $c(c-a)(c-b) = c(a-c)(b-c) \geq 0$ vì $c \geq 0$, $a \geq c$, $b \geq c$. Vậy tổng không âm.

Because $b \geq c$ we have $a+b-c \geq a \geq 0$, so $(a-b)^2(a+b-c) \geq 0$. The third term $c(c-a)(c-b) = c(a-c)(b-c) \geq 0$ since $c \geq 0$, $a \geq c$, $b \geq c$. Hence the sum is non-negative.

Dấu bằng cần $(a-b)^2(a+b-c) = 0$ và $c(a-c)(b-c) = 0$. Từ yếu tố thứ nhất: $a = b$, hoặc $a+b=c$; trường hợp sau cùng với $c \leq b \leq a$ ép $a = 0$, nên cả ba số bằng 0. Với $a = b$, yếu tố thứ hai thành $c(a-c)^2 = 0$, tức $c = 0$ hoặc $c = a$. Đó là hai dạng đã nêu.

Equality needs $(a-b)^2(a+b-c) = 0$ and $c(a-c)(b-c) = 0$. From the first factor: $a = b$, or $a+b=c$; in the latter case $c \leq b \leq a$ forces $a = 0$, so all three numbers are 0. With $a = b$ the second factor becomes $c(a-c)^2 = 0$, so $c = 0$ or $c = a$. These are the two stated forms. ■

Khai triển và dùng các biểu thức p, q, r , vế trái của bất đẳng thức Schur bằng $a^3 + b^3 + c^3 - \Sigma_{\text{sym}} a^2b + 3abc$, và bằng:

Expanded and written with p, q, r , the left side of Schur's inequality equals $a^3 + b^3 + c^3 - \Sigma_{\text{sym}} a^2b + 3abc$, and also:

$$a(a-b)(a-c) + b(b-a)(b-c) + c(c-a)(c-b) = p^3 - 4pq + 9r \quad (3.1)$$

HỆ QUẢ 3.4 / COROLLARY 3.4 — Với $a, b, c \geq 0$ ta có ba dạng tương đương của bất đẳng thức Schur: (1) $p^3 - 4pq + 9r \geq 0$; (2) $r \geq p(4q - p^2)/9$; (3) nếu $p > 0$ thì $a^2 + b^2 + c^2 + 9abc/p \geq 2(ab + bc + ca)$.

For $a, b, c \geq 0$ there are three equivalent forms of Schur's inequality: (1) $p^3 - 4pq + 9r \geq 0$; (2) $r \geq p(4q - p^2)/9$; (3) if $p > 0$ then $a^2 + b^2 + c^2 + 9abc/p \geq 2(ab + bc + ca)$.

Chứng minh. / Proof.

Dạng (1) là (3.1). Dạng (2) là (1) chuyển vế rồi chia cho 9. Với dạng (3): chia (1) cho $p > 0$ được $p^2 - 4q + 9r/p \geq 0$; thay $p^2 = a^2 + b^2 + c^2 + 2q$ ta được $a^2 + b^2 + c^2 - 2q + 9r/p \geq 0$, đúng là dạng (3).

Form (1) is (3.1). Form (2) is (1) rearranged and divided by 9. For form (3): dividing (1) by $p > 0$ gives $p^2 - 4q + 9r/p \geq 0$; substituting $p^2 = a^2 + b^2 + c^2 + 2q$ gives $a^2 + b^2 + c^2 - 2q + 9r/p \geq 0$, which is form (3). ■

PHÂN TÍCH / ANALYSIS — Điều kiện $a + b + c = 3$ cho $p = 3$ nên $a^2 + b^2 + c^2 = 9 - 2q$. Bất đẳng thức cần chứng minh chỉ còn q và r . Dạng (2) của hệ quả 3.4 cho cận dưới của r theo q , đúng chiều cần dùng.

The condition $a + b + c = 3$ gives $p = 3$, so $a^2 + b^2 + c^2 = 9 - 2q$. The claim then involves only q and r . Form (2) of corollary 3.4 gives a lower bound for r in terms of q , which is the direction we need.

VÍ DỤ 3.3 (Schur với điều kiện tổng) / EXAMPLE 3.3 (Schur with a sum condition) —

Cho $a, b, c \geq 0$ thỏa $a + b + c = 3$. Chứng minh $a^2 + b^2 + c^2 + abc \geq 4$.

Let $a, b, c \geq 0$ with $a + b + c = 3$. Prove that $a^2 + b^2 + c^2 + abc \geq 4$.

Lời giải. / Solution.

Với $p = 3$ ta có $a^2 + b^2 + c^2 = 9 - 2q$, và dạng (2) của hệ quả 3.4 cho $r \geq 3(4q - 9)/9 = (4q - 9)/3$.

With $p = 3$ we have $a^2 + b^2 + c^2 = 9 - 2q$, and form (2) of corollary 3.4 gives $r \geq 3(4q - 9)/9 = (4q - 9)/3$.

$$a^2 + b^2 + c^2 + abc = 9 - 2q + r \geq 9 - 2q + (4q - 9)/3 = 6 - 2q/3$$

Từ $p^2 \geq 3q$ ta có $q \leq 3$, nên $6 - 2q/3 \geq 6 - 2 = 4$.

From $p^2 \geq 3q$ we get $q \leq 3$, so $6 - 2q/3 \geq 6 - 2 = 4$.

Dấu bằng xảy ra khi $q = 3$, tức $a = b = c = 1$.

Equality holds when $q = 3$, that is $a = b = c = 1$. ■

VÍ DỤ 3.4 (Nesbitt mạnh hơn) / EXAMPLE 3.4 (A stronger Nesbitt) — Cho $a, b, c \geq 0$, trong đó không có hai số nào cùng bằng 0. Chứng minh $a/(b + c) + b/(c + a) + c/(a + b) + 4abc/((a + b)(b + c)(c + a)) \geq 2$.

Let $a, b, c \geq 0$ with no two of them equal to 0. Prove that $a/(b + c) + b/(c + a) + c/(a + b) + 4abc/((a + b)(b + c)(c + a)) \geq 2$.

Lời giải. / Solution.

Quy đồng với mẫu chung $(a + b)(b + c)(c + a) > 0$. Tử số của $a/(b + c) + b/(c + a) + c/(a + b)$ là:

Use the common denominator $(a + b)(b + c)(c + a) > 0$. The numerator of $a/(b + c) + b/(c + a) + c/(a + b)$ is:

$$a(a + b)(a + c) + b(b + a)(b + c) + c(c + a)(c + b) = a^3 + b^3 + c^3 + \Sigma_{\text{sym}} a^2b + 3abc$$

Còn $2(a+b)(b+c)(c+a) = 2\sum_{\text{sym}} a^2b + 4abc$. Hiệu của vế trái và vế phải khi nhân với mẫu chung là:

Also $2(a+b)(b+c)(c+a) = 2\sum_{\text{sym}} a^2b + 4abc$. The difference between the two sides, after multiplying by the common denominator, is:

$$(a^3 + b^3 + c^3 + \sum_{\text{sym}} a^2b + 3abc + 4abc) - (2\sum_{\text{sym}} a^2b + 4abc) = a^3 + b^3 + c^3 - \sum_{\text{sym}} a^2b + 3abc$$

Đó chính là vế trái bất đẳng thức Schur, không âm theo định lý 3.3. Dấu bằng khi $a = b = c$ hoặc $(a, a, 0)$ và các hoán vị.

That is exactly the left side of Schur's inequality, non-negative by theorem 3.3. Equality holds when $a = b = c$, or at $(a, a, 0)$ and its permutations. ■

NHẬN XÉT / REMARK — Ví dụ 3.4 làm mạnh bất đẳng thức Nesbitt: số hạng $4abc/((a+b)(b+c)(c+a))$ bằng $1/2$ tại $a = b = c$ và bằng 0 tại $(a, a, 0)$, nên tổng ba phân thức nhận giá trị $3/2$ tại tâm và 2 tại biên. Cả hai điểm đều là dấu bằng của Schur.

Example 3.4 strengthens Nesbitt's inequality: the term $4abc/((a+b)(b+c)(c+a))$ is $1/2$ at $a = b = c$ and 0 at $(a, a, 0)$, so the sum of the three fractions is $3/2$ at the centre and 2 on the boundary. Both points are equality cases of Schur.

PHẢI THUỘC / MEMORISE — Schur: $p^3 - 4pq + 9r \geq 0$ với $a, b, c \geq 0$. Dấu bằng tại $(1, 1, 1)$ và $(1, 1, 0)$. Khi đề có hai dạng dấu bằng này cùng lúc, hãy nghĩ tới Schur.

Schur: $p^3 - 4pq + 9r \geq 0$ for $a, b, c \geq 0$. Equality at $(1, 1, 1)$ and $(1, 1, 0)$. When a problem has both these equality cases at once, think of Schur.

3.3. Phương pháp SOS (tổng các bình phương) — The SOS method (sums of squares)

Nếu $F(a, b, c)$ đối xứng và $F(a, a, a) = 0$ thì thường viết được F thành tổng có hệ số là các biểu thức S_a, S_b, S_c nhân với bình phương hiệu hai biến. Các hệ số này không cần dương hết; định lý 3.5 cho biết khi nào vẫn kết luận được $F \geq 0$.

If $F(a, b, c)$ is symmetric and $F(a, a, a) = 0$, one can usually write F as a sum of squared differences multiplied by coefficients S_a, S_b, S_c . The coefficients need not all be positive; theorem 3.5 says when $F \geq 0$ can still be concluded.

$$F(a, b, c) = S_a(b-c)^2 + S_b(c-a)^2 + S_c(a-b)^2 \quad (3.2)$$

ĐỊNH LÝ 3.5 (Tiêu chuẩn SOS) / THEOREM 3.5 (SOS criteria) — Cho F có dạng (3.2) và giả sử $a \geq b \geq c \geq 0$. Khi đó $F \geq 0$ nếu một trong các điều kiện sau đúng: (i) $S_a \geq 0, S_b \geq 0, S_c \geq 0$; (ii) $S_b \geq 0, S_a + S_b \geq 0, S_c + S_b \geq 0$; (iii) $b > 0, S_b \geq 0, S_c \geq 0$ và $a^2S_b + b^2S_a \geq 0$.

Let F have the form (3.2) and suppose $a \geq b \geq c \geq 0$. Then $F \geq 0$ if one of the following holds: (i) $S_a \geq 0, S_b \geq 0, S_c \geq 0$; (ii) $S_b \geq 0, S_a + S_b \geq 0, S_c + S_b \geq 0$; (iii) $b > 0, S_b \geq 0, S_c \geq 0$ and $a^2S_b + b^2S_a \geq 0$.

Chứng minh. / Proof.

(i) hiển nhiên: ba số hạng đều không âm.

(i) is immediate: all three terms are non-negative.

(ii) Vì $a - c = (a - b) + (b - c)$ với hai số hạng không âm, nên $(a - c)^2 = (a - b)^2 + (b - c)^2 + 2(a - b)(b - c) \geq (a - b)^2 + (b - c)^2$. Nhân với $S_b \geq 0$ rồi cộng vào (3.2):

(ii) Since $a - c = (a - b) + (b - c)$ with both terms non-negative, $(a - c)^2 = (a - b)^2 + (b - c)^2 + 2(a - b)(b - c) \geq (a - b)^2 + (b - c)^2$. Multiply by $S_b \geq 0$ and add into (3.2):

$$F \geq (S_c + S_b)(a - b)^2 + (S_a + S_b)(b - c)^2 \geq 0$$

(iii) Ta có $(a - c)b - a(b - c) = c(a - b) \geq 0$, nên $(a - c)b \geq a(b - c) \geq 0$. Bình phương: $b^2(a - c)^2 \geq a^2(b - c)^2$. Nhân với $S_b/b^2 \geq 0$:

(iii) We have $(a - c)b - a(b - c) = c(a - b) \geq 0$, so $(a - c)b \geq a(b - c) \geq 0$. Squaring: $b^2(a - c)^2 \geq a^2(b - c)^2$. Multiply by $S_b/b^2 \geq 0$:

$$F \geq S_c(a - b)^2 + (b - c)^2 \cdot (b^2 S_a + a^2 S_b)/b^2 \geq 0$$

■

Cách tìm S_a, S_b, S_c : viết hiệu hai vế thành tổng của các biểu thức dạng $(x - y)^2$ nhân hệ số, thường qua các đẳng thức $a^3 + b^3 - ab(a + b) = (a + b)(a - b)^2$, $a^2 + b^2 - 2ab = (a - b)^2$, $1/a - 1/b = (b - a)/(ab)$. Tiêu chuẩn chỉ cần thứ tự $a \geq b \geq c$ nên bất đẳng thức phải đối xứng (hoặc ta xét đủ thứ tự).

To find S_a, S_b, S_c , rewrite the difference of the two sides as a sum of terms $(x - y)^2$ times coefficients, usually via the identities $a^3 + b^3 - ab(a + b) = (a + b)(a - b)^2$, $a^2 + b^2 - 2ab = (a - b)^2$, $1/a - 1/b = (b - a)/(ab)$. The criterion needs the ordering $a \geq b \geq c$, so the inequality must be symmetric (or all orderings must be treated).

VÍ DỤ 3.5 (SOS với mọi hệ số dương) / EXAMPLE 3.5 (SOS with all coefficients positive)

— Chứng minh với $a, b, c > 0$: $(a^2 + b^2)/(a + b) + (b^2 + c^2)/(b + c) + (c^2 + a^2)/(c + a) \geq a + b + c$.

Prove that for $a, b, c > 0$: $(a^2 + b^2)/(a + b) + (b^2 + c^2)/(b + c) + (c^2 + a^2)/(c + a) \geq a + b + c$.

Lời giải. / Solution.

Với mỗi cặp: $(a^2 + b^2)/(a + b) - (a + b)/2 = (2a^2 + 2b^2 - (a + b)^2)/(2(a + b)) = (a - b)^2/(2(a + b))$.

For each pair: $(a^2 + b^2)/(a + b) - (a + b)/2 = (2a^2 + 2b^2 - (a + b)^2)/(2(a + b)) = (a - b)^2/(2(a + b))$.

Cộng ba đẳng thức, vì tổng $(a + b)/2 + (b + c)/2 + (c + a)/2 = a + b + c$:

Adding the three identities, since $(a + b)/2 + (b + c)/2 + (c + a)/2 = a + b + c$:

$$VT - (a + b + c) = (a - b)^2/(2(a + b)) + (b - c)^2/(2(b + c)) + (c - a)^2/(2(c + a)) \geq 0$$

Đây là dạng (3.2) với $S_c = 1/(2(a + b)) > 0$ và các hệ số còn lại tương tự, tiêu chuẩn (i). Dấu bằng khi $a = b = c$.

This is form (3.2) with $S_c = 1/(2(a + b)) > 0$ and the other coefficients similar, criterion (i). Equality holds when $a = b = c$. ■

PHÂN TÍCH / ANALYSIS — Đây là bất đẳng thức Schur bậc 4 (tham số $t = 2$). Viết hiệu thành dạng (3.2): $a^2(a - b)(a - c)$ cộng hoán vị sẽ cho $S_a = (b^2 + c^2 - a^2)/2$, có thể âm khi a lớn nhất. Hai hệ số kia dương khi $a \geq b \geq c$, nên thử tiêu chuẩn (iii).

This is Schur's inequality of degree 4 (parameter $t = 2$). Writing the difference in the form (3.2): $a^2(a - b)(a - c)$ plus its permutations gives $S_a = (b^2 + c^2 - a^2)/2$, which can be negative when a is largest. The other two coefficients are positive when $a \geq b \geq c$, so try criterion (iii).

VÍ DỤ 3.6 (SOS và Schur bậc 4) / EXAMPLE 3.6 (SOS and degree-4 Schur) — Chứng minh với $a, b, c \geq 0$: $a^4 + b^4 + c^4 + abc(a + b + c) \geq a^3b + ab^3 + b^3c + bc^3 + c^3a + ca^3$.

Prove that for $a, b, c \geq 0$: $a^4 + b^4 + c^4 + abc(a + b + c) \geq a^3b + ab^3 + b^3c + bc^3 + c^3a + ca^3$.

Lời giải. / Solution.

Khai triển cho thấy hiệu hai vế bằng $F = a^2(a - b)(a - c) + b^2(b - a)(b - c) + c^2(c - a)(c - b)$. Khai triển nữa cho:

Expanding shows that the difference of the two sides is $F = a^2(a - b)(a - c) + b^2(b - a)(b - c) + c^2(c - a)(c - b)$. A further expansion gives:

$$2F = (b - c)^2(b^2 + c^2 - a^2) + (c - a)^2(c^2 + a^2 - b^2) + (a - b)^2(a^2 + b^2 - c^2)$$

Giả sử $a \geq b \geq c \geq 0$. Nếu $b = 0$ thì $c = 0$ và $F = a^4 \geq 0$. Với $b > 0$: $S_c = (a^2 + b^2 - c^2)/2 \geq 0$ và $S_b = (c^2 + a^2 - b^2)/2 \geq 0$.

Assume $a \geq b \geq c \geq 0$. If $b = 0$ then $c = 0$ and $F = a^4 \geq 0$. For $b > 0$: $S_c = (a^2 + b^2 - c^2)/2 \geq 0$ and $S_b = (c^2 + a^2 - b^2)/2 \geq 0$.

Còn $S_a = (b^2 + c^2 - a^2)/2$ có thể âm; ta kiểm tra:

$S_a = (b^2 + c^2 - a^2)/2$ may be negative; we check:

$$2(a^2S_b + b^2S_a) = a^2(c^2 + a^2 - b^2) + b^2(b^2 + c^2 - a^2) = (a^2 - b^2)^2 + c^2(a^2 + b^2) \geq 0$$

Tiêu chuẩn (iii) cho $F \geq 0$. Dấu bằng khi $a = b = c$ hoặc $(a, a, 0)$.

Criterion (iii) gives $F \geq 0$. Equality holds when $a = b = c$ or at $(a, a, 0)$. ■

NHẬN XÉT / REMARK — Mỗi bất đẳng thức dạng (3.2) có nhiều cách chọn S_a, S_b, S_c , vì $(a - b)^2 + (b - c)^2 + (c - a)^2$ có thể chuyển vế qua lại. Khi một cách chọn không thỏa tiêu chuẩn, thử cách khác trước khi bỏ SOS.

A given inequality of the form (3.2) allows many choices of S_a, S_b, S_c , because terms can be traded between the three squared differences. When one choice fails the criteria, try another before abandoning SOS.

LỖI HAY GẶP / COMMON MISTAKE — Áp tiêu chuẩn (ii) hoặc (iii) mà không nêu giả thiết $a \geq b \geq c$, hoặc dùng cho bất đẳng thức không đối xứng nên không có quyền sắp thứ tự.

Applying criterion (ii) or (iii) without stating the assumption $a \geq b \geq c$, or using it on a non-symmetric inequality where the ordering cannot be assumed.

3.4. Phương pháp tiếp tuyến — The tangent-line method

Khi bất đẳng thức có dạng tổng $g(a) + g(b) + g(c)$ với điều kiện $a + b + c$ cố định, ta tìm một hàm bậc nhất $\alpha x + \beta$ nằm dưới (hoặc trên) g trên cả miền của biến, chạm g tại điểm

xảy ra dấu bằng. Cộng ba đánh giá một biến lại thì điều kiện tổng làm phần còn lại thành hằng số.

When the inequality has the form $g(a) + g(b) + g(c)$ with $a + b + c$ fixed, look for a linear function $\alpha x + \beta$ lying below (or above) g on the whole range of the variable and touching g at the equality point. Adding the three one-variable estimates, the sum condition turns the right side into a constant.

ĐỊNH LÝ 3.6 (Đánh giá tiếp tuyến) / THEOREM 3.6 (Tangent-line estimate) — Cho hàm g xác định trên tập I , điểm $m \in I$ và các số α, β sao cho $g(x) \geq \alpha x + \beta$ với mọi $x \in I$, và $g(m) = \alpha m + \beta$. Khi đó với $x_1, \dots, x_n \in I$ có $x_1 + \dots + x_n = nm$ ta có $g(x_1) + \dots + g(x_n) \geq n \cdot g(m)$. Dấu bằng xảy ra khi $x_1 = \dots = x_n = m$.

Let g be defined on a set I , let $m \in I$ and let α, β be numbers such that $g(x) \geq \alpha x + \beta$ for all $x \in I$, and $g(m) = \alpha m + \beta$. Then for $x_1, \dots, x_n \in I$ with $x_1 + \dots + x_n = nm$ we have $g(x_1) + \dots + g(x_n) \geq n \cdot g(m)$. Equality holds when $x_1 = \dots = x_n = m$.

Chứng minh. / Proof.

Cộng n bất đẳng thức $g(x_i) \geq \alpha x_i + \beta$:

Add the n inequalities $g(x_i) \geq \alpha x_i + \beta$:

$$g(x_1) + \dots + g(x_n) \geq \alpha(x_1 + \dots + x_n) + n\beta = \alpha nm + n\beta = n(\alpha m + \beta) = n \cdot g(m)$$

Khi mọi $x_i = m$ thì mỗi đánh giá là đẳng thức.

When every $x_i = m$ each estimate is an equality. ■

Tìm hệ số góc α không cần đạo hàm. Viết $g(x) - g(m) = (x - m) \cdot h(x)$ bằng biến đổi đại số (rút gọn thừa số $x - m$); khi đó $\alpha = h(m)$. Sau đó kiểm tra $g(x) - \alpha x - \beta$ có nhân tử $(x - m)^2$ và phần còn lại không âm trên I . Nếu phần còn lại đổi dấu trong I thì tiếp tuyến không dùng được trên cả miền.

Finding the slope α needs no derivative. Write $g(x) - g(m) = (x - m) \cdot h(x)$ by algebra (cancelling the factor $x - m$); then $\alpha = h(m)$. Next check that $g(x) - \alpha x - \beta$ has the factor $(x - m)^2$ and that the rest is non-negative on I . If the rest changes sign inside I , the tangent line cannot be used on the whole range.

PHÂN TÍCH / ANALYSIS — Điểm rơi là $a = b = c = 1$ vì tổng bằng 3. Với $g(x) = 1/(x^2 + 1)$: $g(x) - g(1) = 1/(x^2 + 1) - 1/2 = (1 - x)(1 + x)/(2(x^2 + 1)) = (x - 1) \cdot [-(1 + x)/(2(x^2 + 1))]$. Vậy $h(x) = -(1 + x)/(2(x^2 + 1))$ và $\alpha = h(1) = -1/2$. Tiếp tuyến: $g(x) \geq 1/2 - (x - 1)/2 = (2 - x)/2$.

The equality point is $a = b = c = 1$ because the sum is 3. With $g(x) = 1/(x^2 + 1)$: $g(x) - g(1) = 1/(x^2 + 1) - 1/2 = (1 - x)(1 + x)/(2(x^2 + 1)) = (x - 1) \cdot [-(1 + x)/(2(x^2 + 1))]$. So $h(x) = -(1 + x)/(2(x^2 + 1))$ and $\alpha = h(1) = -1/2$. The tangent line: $g(x) \geq 1/2 - (x - 1)/2 = (2 - x)/2$.

VÍ DỤ 3.7 (Tiếp tuyến cơ bản) / EXAMPLE 3.7 (A basic tangent line) — Cho $a, b, c \geq 0$ thỏa $a + b + c = 3$. Chứng minh $1/(a^2 + 1) + 1/(b^2 + 1) + 1/(c^2 + 1) \geq 3/2$.

Let $a, b, c \geq 0$ with $a + b + c = 3$. Prove that $1/(a^2 + 1) + 1/(b^2 + 1) + 1/(c^2 + 1) \geq 3/2$.

Lời giải. / Solution.

Với mọi $x \geq 0$:

For every $x \geq 0$:

$$1/(x^2 + 1) - (2 - x)/2 = (x^3 - 2x^2 + x)/(2(x^2 + 1)) = x(x - 1)^2/(2(x^2 + 1)) \geq 0$$

Vậy $1/(x^2 + 1) \geq (2 - x)/2$ với $x \geq 0$, dấu bằng khi $x = 0$ hoặc $x = 1$.

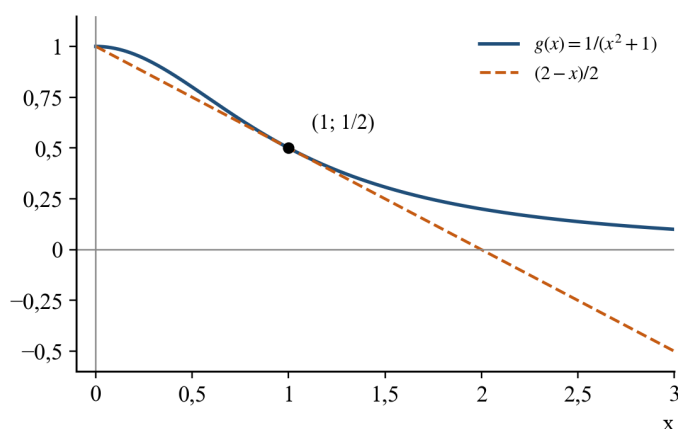
Hence $1/(x^2 + 1) \geq (2 - x)/2$ for $x \geq 0$, with equality at $x = 0$ or $x = 1$.

Áp dụng cho a, b, c rồi cộng: tổng $\geq (6 - (a + b + c))/2 = 3/2$.

Apply it to a, b, c and add: the sum is at least $(6 - (a + b + c))/2 = 3/2$.

Dấu bằng cần cả ba biến thuộc $\{0, 1\}$ và tổng bằng 3, nên chỉ có $a = b = c = 1$.

Equality needs all three variables in $\{0, 1\}$ with sum 3, so only $a = b = c = 1$. ■



Hình 3.1. Đồ thị $g(x) = 1/(x^2 + 1)$ và tiếp tuyến $y = (2 - x)/2$ tại $x = 1$; với $x \geq 0$ đồ thị nằm trên tiếp tuyến.

Figure 3.1. Graph of $g(x) = 1/(x^2 + 1)$ and its tangent line $y = (2 - x)/2$ at $x = 1$; for $x \geq 0$ the graph lies above the line.

PHÂN TÍCH / ANALYSIS — Điểm rơi $x = y = z = 1/3$. Với $g(x) = x/(1 + x^2)$, $g(1/3) = 3/10$. Rút gọn $g(x) - g(1/3) = (10x - 3 - 3x^2)/(10(1 + x^2)) = -(3x - 1)(x - 3)/(10(1 + x^2)) = (x - 1/3) \cdot 3(3 - x)/(10(1 + x^2))$. Vậy $h(x) = 3(3 - x)/(10(1 + x^2))$ và $\alpha = h(1/3) = 18/25$. Chiều bất đẳng thức là $\leq$ nên cần $g(x) \leq \alpha x + \beta$.

The equality point is $x = y = z = 1/3$. With $g(x) = x/(1 + x^2)$, $g(1/3) = 3/10$. Simplify $g(x) - g(1/3) = (10x - 3 - 3x^2)/(10(1 + x^2)) = -(3x - 1)(x - 3)/(10(1 + x^2)) = (x - 1/3) \cdot 3(3 - x)/(10(1 + x^2))$. So $h(x) = 3(3 - x)/(10(1 + x^2))$ and $\alpha = h(1/3) = 18/25$. The inequality points downward ($\leq$), so we need $g(x) \leq \alpha x + \beta$.

VÍ DỤ 3.8 (Tiếp tuyến cho bất đẳng thức $\leq$) / EXAMPLE 3.8 (Tangent line for a $\leq$ inequality) — Cho $x, y, z > 0$ thỏa $x + y + z = 1$. Chứng minh $x/(1 + x^2) + y/(1 + y^2) + z/(1 + z^2) \leq 9/10$.

Let $x, y, z > 0$ with $x + y + z = 1$. Prove that $x/(1 + x^2) + y/(1 + y^2) + z/(1 + z^2) \leq 9/10$.

Lời giải. / Solution.

Tiếp tuyến tại $x = 1/3$ là $y = (18/25)x + 3/50$ (vì $3/10 - (18/25)(1/3) = 3/10 - 6/25 = 3/50$). Với mọi $x > -3/4$:

The tangent at $x = 1/3$ is $y = (18/25)x + 3/50$ (because $3/10 - (18/25)(1/3) = 3/10 - 6/25 = 3/50$). For every $x > -3/4$:

$$(18/25)x + 3/50 - x/(1 + x^2) = (3x - 1)^2(4x + 3)/(50(1 + x^2)) \geq 0$$

Do đó $x/(1 + x^2) \leq (18/25)x + 3/50$ với mọi $x > 0$. Cộng ba bất đẳng thức:

Hence $x/(1 + x^2) \leq (18/25)x + 3/50$ for all $x > 0$. Adding the three inequalities:

$$\Sigma x/(1 + x^2) \leq (18/25)(x + y + z) + 9/50 = 36/50 + 9/50 = 9/10$$

Dấu bằng khi $x = y = z = 1/3$.

Equality holds when $x = y = z = 1/3$. ■

NHẬN XÉT / REMARK — Tiếp tuyến có thể thất bại. Với $a + b + c = 3$, $a, b, c \geq 0$, bất đẳng thức $1/(a^2 + 2) + 1/(b^2 + 2) + 1/(c^2 + 2) \geq 1$ sai: tại $(0; 3/2; 3/2)$ tổng bằng $1/2 + 2 \cdot (4/17) = 33/34 < 1$. Tiếp tuyến tại 1 là $(5 - 2x)/9$ và hiệu bằng $(x - 1)^2(2x - 1)/(9(x^2 + 2))$, âm khi $x < 1/2$. Hiệu đổi dấu trong miền là tín hiệu bất đẳng thức gốc có thể sai hoặc cần một kỹ thuật khác.

The tangent line can fail. With $a + b + c = 3$, $a, b, c \geq 0$, the inequality $1/(a^2 + 2) + 1/(b^2 + 2) + 1/(c^2 + 2) \geq 1$ is false: at $(0, 3/2, 3/2)$ the sum is $1/2 + 2 \cdot (4/17) = 33/34 < 1$. The tangent at 1 is $(5 - 2x)/9$ and the difference equals $(x - 1)^2(2x - 1)/(9(x^2 + 2))$, negative for $x < 1/2$. A difference that changes sign inside the range signals that the original inequality may be false or needs another technique.

LỖI HAY GẶP / COMMON MISTAKE — Chỉ kiểm tra tiếp tuyến tại vài điểm gần điểm rơi mà không chứng minh nó đúng trên toàn miền. Phải có đẳng thức đại số cho $g(x) - \alpha x - \beta$.

Checking the tangent line at a few points near the equality point without proving it on the whole range. An algebraic identity for $g(x) - \alpha x - \beta$ is required.

3.5. Đồn biến về hai biến bằng nhau — Mixing variables

Nhiều bất đẳng thức đối xứng ba biến có giá trị nhỏ nhất (hoặc lớn nhất) khi hai biến bằng nhau. Ta cố định một biến, thay hai biến còn lại bằng trung bình cộng của chúng, chứng minh giá trị của biểu thức không giảm (hoặc không tăng), rồi giải bất đẳng thức một biến còn lại.

Many symmetric inequalities in three variables attain their minimum (or maximum) when two variables are equal. Fix one variable, replace the other two by their arithmetic mean, show the value of the expression does not decrease (or increase), and then solve the remaining one-variable inequality.

BỔ ĐỀ 3.7 (Bổ đề đồn biến) / LEMMA 3.7 (Mixing lemma) — Với mọi số thực a, b đặt $s = a + b$. Khi đó $ab = s^2/4 - (a - b)^2/4 \leq s^2/4$, và $a^2 + b^2 = s^2/2 + (a - b)^2/2 \geq s^2/2$. Tích ab lớn nhất, và $a^2 + b^2$ nhỏ nhất, khi $a = b$.

For real numbers a, b put $s = a + b$. Then $ab = s^2/4 - (a - b)^2/4 \leq s^2/4$ and $a^2 + b^2 = s^2/2 + (a - b)^2/2 \geq s^2/2$. With s fixed, the product ab is largest, and $a^2 + b^2$ smallest, when $a = b$.

Chứng minh. / Proof.

Khai triển: $s^2/4 - (a - b)^2/4 = ((a + b)^2 - (a - b)^2)/4 = ab$. Tương tự $(a + b)^2/2 + (a - b)^2/2 = a^2 + b^2$.

Expanding: $s^2/4 - (a - b)^2/4 = ((a + b)^2 - (a - b)^2)/4 = ab$. Similarly $(a + b)^2/2 + (a - b)^2/2 = a^2 + b^2$. ■

Quy trình: (1) chọn biến cố định, thường là biến nhỏ nhất c (khi tổng bằng 3 thì $c \leq 1$); (2) viết biểu thức dưới dạng $A(c) \cdot ab + B(c) \cdot (a + b) + C(c)$, với $a + b = s$ cố định; (3) nếu $A(c) \geq 0$ thì tăng ab lên $s^2/4$ làm biểu thức không giảm; (4) giải bất đẳng thức một biến, thường có nhân tử $(c - 1)^2$.

Procedure: (1) choose the fixed variable, usually the smallest c (when the sum is 3, $c \leq 1$); (2) write the expression as $A(c) \cdot ab + B(c) \cdot (a + b) + C(c)$ with $a + b = s$ fixed; (3) if $A(c) \geq 0$, raising ab to $s^2/4$ does not decrease the expression; (4) solve the one-variable inequality, which usually has a factor $(c - 1)^2$.

PHÂN TÍCH / ANALYSIS — Biểu thức $2(ab + bc + ca) - abc$, với c cố định và $a + b = 3 - c$ không đổi, chỉ phụ thuộc vào tích ab : nó bằng $(2 - c)ab + 2c(3 - c)$. Hệ số của ab là $2 - c > 0$ khi $c \leq 1$. Vậy giá trị lớn nhất đạt khi ab lớn nhất, tức $a = b$.

With c fixed and $a + b = 3 - c$ constant, the expression $2(ab + bc + ca) - abc$ depends on ab only: it equals $(2 - c)ab + 2c(3 - c)$. The coefficient of ab is $2 - c > 0$ when $c \leq 1$. So the maximum occurs when ab is largest, that is $a = b$.

VÍ DỤ 3.9 (Đồn biến bằng hệ số của ab) / EXAMPLE 3.9 (Mixing through the coefficient of ab) — Cho $a, b, c \geq 0$ thỏa $a + b + c = 3$. Chứng minh $2(ab + bc + ca) - abc \leq 5$.

Let $a, b, c \geq 0$ with $a + b + c = 3$. Prove that $2(ab + bc + ca) - abc \leq 5$.

Lời giải. / Solution.

Giả sử $c = \min\{a, b, c\}$. Vì $3c \leq a + b + c = 3$ nên $0 \leq c \leq 1$. Đặt $F = 2(ab + bc + ca) - abc$. Do $a + b = 3 - c$:

Assume $c = \min\{a, b, c\}$. Since $3c \leq a + b + c = 3$ we have $0 \leq c \leq 1$. Put $F = 2(ab + bc + ca) - abc$. As $a + b = 3 - c$:

$$F = (2 - c)ab + 2c(3 - c)$$

Vì $2 - c > 0$ và $ab \leq ((a + b)/2)^2 = (3 - c)^2/4$ (bổ đề 3.7):

Since $2 - c > 0$ and $ab \leq ((a + b)/2)^2 = (3 - c)^2/4$ (lemma 3.7):

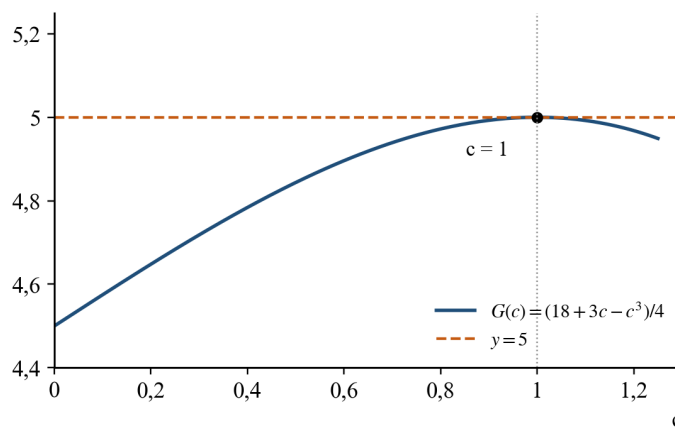
$$F \leq (2 - c)(3 - c)^2/4 + 2c(3 - c) = (18 + 3c - c^3)/4$$

Cuối cùng $5 - (18 + 3c - c^3)/4 = (c^3 - 3c + 2)/4 = (c - 1)^2(c + 2)/4 \geq 0$.

Finally $5 - (18 + 3c - c^3)/4 = (c^3 - 3c + 2)/4 = (c - 1)^2(c + 2)/4 \geq 0$.

Vậy $F \leq 5$. Dấu bằng cần $a = b$ và $c = 1$, tức $a = b = c = 1$.

Hence $F \leq 5$. Equality needs $a = b$ and $c = 1$, that is $a = b = c = 1$. ■



Hình 3.2. Sau khi dồn hai biến nhỏ về nhau, F không vượt quá $G(c) = (18 + 3c - c^3)/4$, và $G(c) \leq 5$ với dấu bằng tại $c = 1$.

Figure 3.2. After merging the two other variables, F does not exceed $G(c) = (18 + 3c - c^3)/4$, and $G(c) \leq 5$ with equality at $c = 1$.

NHẬN XÉT / REMARK — Dồn biến cần chọn đúng biến cố định. Ở ví dụ 3.9 phải lấy c nhỏ nhất để $2 - c > 0$; nếu lấy c lớn nhất thì $2 - c$ có thể âm và chiều đánh giá $ab \leq s^2/4$ bị đảo. Biểu thức với tích ab có hệ số âm cần dồn theo hướng ngược lại (giảm ab).

Mixing needs the right choice of the fixed variable. In example 3.9 c must be the smallest so that $2 - c > 0$; with c the largest, $2 - c$ may be negative and the estimate $ab \leq s^2/4$ goes the wrong way. When the coefficient of ab is negative, mix in the opposite direction (decrease ab).

LỖI HAY GẶP / COMMON MISTAKE — Thay a, b bằng trung bình cộng mà không chứng minh biểu thức không giảm, rồi khẳng định dấu bằng ở $a = b$. Khẳng định đó chưa được chứng minh.

Replacing a, b by their mean without proving that the expression does not decrease, then asserting that equality occurs at $a = b$. That statement is unproved.

3.6. Đổi biến p, q, r — The p, q, r substitution

Với bất đẳng thức đối xứng ba biến, đặt $p = a + b + c$, $q = ab + bc + ca$, $r = abc$. Mọi đa thức đối xứng của a, b, c đều là đa thức của p, q, r . Khi p cố định, biểu thức thường chỉ còn q, r và ta dùng các ràng buộc giữa p, q, r (bảo đảm bởi Schur và AM–GM) để kết luận.

For a symmetric inequality in three variables put $p = a + b + c$, $q = ab + bc + ca$, $r = abc$. Every symmetric polynomial in a, b, c is a polynomial in p, q, r . With p fixed the expression often involves only q and r , and the constraints linking p, q, r (guaranteed by Schur and AM–GM) finish the proof.

TÍNH CHẤT 3.8 / PROPERTY 3.8 — Các đẳng thức sau đúng với mọi số thực a, b, c : $a^2 + b^2 + c^2 = p^2 - 2q$; $a^3 + b^3 + c^3 = p^3 - 3pq + 3r$; $a^2b^2 + b^2c^2 + c^2a^2 = q^2 - 2pr$; $\Sigma_{\text{sym}} a^2b = pq - 3r$; $(a + b)(b + c)(c + a) = pq - r$.

The following identities hold for all real a, b, c : $a^2 + b^2 + c^2 = p^2 - 2q$; $a^3 + b^3 + c^3 = p^3 - 3pq + 3r$; $a^2b^2 + b^2c^2 + c^2a^2 = q^2 - 2pr$; $\Sigma_{\text{sym}} a^2b = pq - 3r$; $(a + b)(b + c)(c + a) = pq - r$.

Chứng minh. / Proof.

Bình phương p : $p^2 = a^2 + b^2 + c^2 + 2q$. Nhân p với q : $pq = \sum_{\text{sym}} a^2b + 3abc$, nên $\sum_{\text{sym}} a^2b = pq - 3r$.

Squaring p : $p^2 = a^2 + b^2 + c^2 + 2q$. Multiplying p by q : $pq = \sum_{\text{sym}} a^2b + 3abc$, so $\sum_{\text{sym}} a^2b = pq - 3r$.

Lập phương p : $p^3 = a^3 + b^3 + c^3 + 3\sum_{\text{sym}} a^2b + 6abc$. Thay $\sum_{\text{sym}} a^2b = pq - 3r$ được $a^3 + b^3 + c^3 = p^3 - 3(pq - 3r) - 6r = p^3 - 3pq + 3r$.

Cubing p : $p^3 = a^3 + b^3 + c^3 + 3\sum_{\text{sym}} a^2b + 6abc$. Substituting $\sum_{\text{sym}} a^2b = pq - 3r$ gives $a^3 + b^3 + c^3 = p^3 - 3(pq - 3r) - 6r = p^3 - 3pq + 3r$.

Bình phương q : $q^2 = a^2b^2 + b^2c^2 + c^2a^2 + 2abc(a + b + c) = a^2b^2 + b^2c^2 + c^2a^2 + 2pr$.

Squaring q : $q^2 = a^2b^2 + b^2c^2 + c^2a^2 + 2abc(a + b + c) = a^2b^2 + b^2c^2 + c^2a^2 + 2pr$.

Cuối cùng $(a + b)(b + c)(c + a) = \sum_{\text{sym}} a^2b + 2abc = pq - 3r + 2r = pq - r$.

Finally $(a + b)(b + c)(c + a) = \sum_{\text{sym}} a^2b + 2abc = pq - 3r + 2r = pq - r$. ■

ĐỊNH LÝ 3.9 (Hệ thức giữa p, q, r) / THEOREM 3.9 (Relations among p, q, r) — Cho a, b, c là số thực. Khi đó $(t - a)(t - b)(t - c) = t^3 - pt^2 + qt - r$ với mọi t (hệ thức Viète), và $p^2 \geq 3q, q^2 \geq 3pr$. Nếu thêm $a, b, c \geq 0$ thì $p, q, r \geq 0$ và $p^3 - 4pq + 9r \geq 0$ (Schur).

Let a, b, c be real numbers. Then $(t - a)(t - b)(t - c) = t^3 - pt^2 + qt - r$ for all t (Viète's relations), and $p^2 \geq 3q, q^2 \geq 3pr$. If also $a, b, c \geq 0$ then $p, q, r \geq 0$ and $p^3 - 4pq + 9r \geq 0$ (Schur).

Chứng minh. / Proof.

Khai triển $(t - a)(t - b)(t - c)$ theo lũy thừa của t cho ngay hệ số $-p, q, -r$.

Expanding $(t - a)(t - b)(t - c)$ in powers of t gives the coefficients $-p, q, -r$ at once.

$$p^2 - 3q = ((a - b)^2 + (b - c)^2 + (c - a)^2)/2 \geq 0, \quad q^2 - 3pr = ((ab - bc)^2 + (bc - ca)^2 + (ca - ab)^2)/2 \geq 0$$

Hai đẳng thức này kiểm bằng khai triển (áp dụng đẳng thức đầu cho ba số ab, bc, ca , tổng của chúng là q và tổng tích đôi là $abc(a + b + c) = pr$). Phần còn lại là hiển nhiên hoặc là Schur (định lý 3.3).

Both identities are checked by expansion (apply the first to the three numbers ab, bc, ca , whose sum is q and whose sum of pairwise products is $abc(a + b + c) = pr$). The rest is immediate or is Schur (theorem 3.3). ■

BỔ ĐỀ 3.10 (Biệt thức khi $p = 0$) / LEMMA 3.10 (Discriminant when $p = 0$) — Nếu $a + b + c = 0$ thì $(a - b)^2(b - c)^2(c - a)^2 = -4q^3 - 27r^2$, và $(a^2 + b^2 + c^2)^3 - 54(abc)^2 = 2(a - b)^2(b - c)^2(c - a)^2 \geq 0$.

If $a + b + c = 0$ then $(a - b)^2(b - c)^2(c - a)^2 = -4q^3 - 27r^2$, and $(a^2 + b^2 + c^2)^3 - 54(abc)^2 = 2(a - b)^2(b - c)^2(c - a)^2 \geq 0$.

Chứng minh. / Proof.

Thay $c = -a - b$. Khi đó $q = ab - (a + b)^2 = -(a^2 + ab + b^2)$ và $r = -ab(a + b)$. Các hiệu: $b - c = a + 2b, c - a = -(2a + b)$, nên $(a - b)(b - c)(c - a) = -(a - b)(a + 2b)(2a + b) = -(2a^3 + 3a^2b - 3ab^2 - 2b^3)$.

Substitute $c = -a - b$. Then $q = ab - (a + b)^2 = -(a^2 + ab + b^2)$ and $r = -ab(a + b)$. The differences: $b - c = a + 2b$ and $c - a = -(2a + b)$, so $(a - b)(b - c)(c - a) = -(a - b)(a + 2b)(2a + b) = -(2a^3 + 3a^2b - 3ab^2 - 2b^3)$.

Vế trái là bình phương của biểu thức này, bằng $4a^6 + 12a^5b - 3a^4b^2 - 26a^3b^3 - 3a^2b^4 + 12ab^5 + 4b^6$. Vế phải là $-4q^3 - 27r^2 = 4(a^2 + ab + b^2)^3 - 27a^2b^2(a + b)^2$; khai triển cho cùng đa thức đó.

The left side is the square of this expression, equal to $4a^6 + 12a^5b - 3a^4b^2 - 26a^3b^3 - 3a^2b^4 + 12ab^5 + 4b^6$. The right side is $-4q^3 - 27r^2 = 4(a^2 + ab + b^2)^3 - 27a^2b^2(a + b)^2$; expanding gives the same polynomial.

Cuối cùng $a^2 + b^2 + c^2 = p^2 - 2q = -2q$, nên $(a^2 + b^2 + c^2)^3 = -8q^3$. Do đó $(a^2 + b^2 + c^2)^3 - 54r^2 = -8q^3 - 54r^2 = 2(-4q^3 - 27r^2)$.

Finally $a^2 + b^2 + c^2 = p^2 - 2q = -2q$, so $(a^2 + b^2 + c^2)^3 = -8q^3$. Hence $(a^2 + b^2 + c^2)^3 - 54r^2 = -8q^3 - 54r^2 = 2(-4q^3 - 27r^2)$. ■

PHÂN TÍCH / ANALYSIS — Với $p = 3$: $a^2b^2 + b^2c^2 + c^2a^2 = q^2 - 6r$, nên biểu thức cần đánh giá là $q^2 - 6r + 3r = q^2 - 3r$. Dấu trừ trước r nghĩa là cần cận dưới của r theo q : đó là Schur, $r \geq (4q - 9)/3$. Cận này chỉ có ý nghĩa khi vế phải dương, tức $q > 9/4$; với $q \leq 9/4$ ta dùng $r \geq 0$.

With $p = 3$: $a^2b^2 + b^2c^2 + c^2a^2 = q^2 - 6r$, so the expression to bound is $q^2 - 6r + 3r = q^2 - 3r$. The minus sign in front of r means we need a lower bound for r in terms of q : that is Schur, $r \geq (4q - 9)/3$. The bound is informative only when its right side is positive, $q > 9/4$; for $q \leq 9/4$ we use $r \geq 0$.

VÍ DỤ 3.10 (pqr và Schur) / EXAMPLE 3.10 (pqr with Schur) — Cho $a, b, c \geq 0$ thỏa $a + b + c = 3$. Chứng minh $a^2b^2 + b^2c^2 + c^2a^2 + 3abc \leq 6$.

Let $a, b, c \geq 0$ with $a + b + c = 3$. Prove that $a^2b^2 + b^2c^2 + c^2a^2 + 3abc \leq 6$.

Lời giải. / Solution.

Với $p = 3$, tính chất 3.8 cho vế trái bằng $q^2 - 6r + 3r = q^2 - 3r$. Vì $p^2 \geq 3q$ nên $q \leq 3$.

With $p = 3$, property 3.8 gives the left side as $q^2 - 6r + 3r = q^2 - 3r$. Since $p^2 \geq 3q$ we have $q \leq 3$.

Trường hợp $q \leq 9/4$: vì $r \geq 0$ nên $q^2 - 3r \leq q^2 \leq 81/16 < 6$.

Case $q \leq 9/4$: since $r \geq 0$, $q^2 - 3r \leq q^2 \leq 81/16 < 6$.

Trường hợp $9/4 < q \leq 3$: Schur cho $r \geq (4q - 9)/3$, nên

Case $9/4 < q \leq 3$: Schur gives $r \geq (4q - 9)/3$, so

$$q^2 - 3r \leq q^2 - (4q - 9) = q^2 - 4q + 9 = 6 + (q - 1)(q - 3) \leq 6$$

vì $1 \leq q \leq 3$ nên $(q - 1)(q - 3) \leq 0$.

because $1 \leq q \leq 3$ gives $(q - 1)(q - 3) \leq 0$.

Dấu bằng cần $q = 3$, tức $a = b = c = 1$.

Equality needs $q = 3$, that is $a = b = c = 1$. ■

PHÂN TÍCH / ANALYSIS — Hai điều kiện cho $p = 6$ và $q = 9$ nhưng không cho từng số. Cố định a : khi đó $b + c = 6 - a$ và $bc = q - a(b + c) = 9 - a(6 - a) = (a - 3)^2$. Hai số thực b, c tồn tại khi và chỉ khi $(b + c)^2 \geq 4bc$. Điều kiện này cho khoảng chạy của a , rồi $abc = a \cdot bc = a(a - 3)^2$ là hàm một biến.

The two conditions give $p = 6$ and $q = 9$ but not the numbers themselves. Fix a : then $b + c = 6 - a$ and $bc = q - a(b + c) = 9 - a(6 - a) = (a - 3)^2$. Real numbers b, c exist if and only if $(b + c)^2 \geq 4bc$. This condition gives the range of a , and then $abc = a \cdot bc = a(a - 3)^2$ is a function of one variable.

VÍ DỤ 3.11 (Điều kiện nghiệm thực) / EXAMPLE 3.11 (Condition for real roots) — Cho a, b, c là các số thực thỏa $a + b + c = 6$ và $ab + bc + ca = 9$. Chứng minh $0 \leq a, b, c \leq 4$ và $0 \leq abc \leq 4$.

Let a, b, c be real numbers with $a + b + c = 6$ and $ab + bc + ca = 9$. Prove that $0 \leq a, b, c \leq 4$ and $0 \leq abc \leq 4$.

Lời giải. / Solution.

Ta có $b + c = 6 - a$ và $bc = 9 - a(b + c) = 9 - 6a + a^2 = (a - 3)^2$. Vì b, c thực nên $(b + c)^2 \geq 4bc$:

We have $b + c = 6 - a$ and $bc = 9 - a(b + c) = 9 - 6a + a^2 = (a - 3)^2$. Since b, c are real, $(b + c)^2 \geq 4bc$:

$$(6 - a)^2 - 4(a - 3)^2 = -3a^2 + 12a = -3a(a - 4) \geq 0$$

Suy ra $0 \leq a \leq 4$. Vai trò a, b, c như nhau nên $0 \leq b, c \leq 4$.

Hence $0 \leq a \leq 4$. The roles of a, b, c are symmetric, so $0 \leq b, c \leq 4$.

Với tích: $abc = a \cdot bc = a(a - 3)^2 \geq 0$ vì $a \geq 0$. Mặt khác:

For the product: $abc = a \cdot bc = a(a - 3)^2 \geq 0$ since $a \geq 0$. On the other hand:

$$4 - abc = 4 - a(a - 3)^2 = -(a^3 - 6a^2 + 9a - 4) = (a - 1)^2(4 - a) \geq 0$$

Vậy $0 \leq abc \leq 4$. Giá trị 4 đạt tại $(1, 1, 4)$, giá trị 0 đạt tại $(0, 3, 3)$; cả hai bộ thỏa $p = 6$ và $q = 9$.

Hence $0 \leq abc \leq 4$. The value 4 is attained at $(1, 1, 4)$ and the value 0 at $(0, 3, 3)$; both triples satisfy $p = 6$ and $q = 9$. ■

NHẬN XÉT / REMARK — Ví dụ 3.11 là trường hợp riêng của sự kiện: a, b, c là ba nghiệm thực của $t^3 - pt^2 + qt - r = 0$ thì r bị chặn giữa hai giá trị khi p, q cố định. Ở đây $t^3 - 6t^2 + 9t = t(t - 3)^2$ nhận giá trị $r \in [0, 4]$ ba lần, nên $p = 6, q = 9$ xác định miền của abc .

Example 3.11 is a special case of the fact that if a, b, c are the three real roots of $t^3 - pt^2 + qt - r = 0$, then r is confined between two values when p and q are fixed. Here $t^3 - 6t^2 + 9t = t(t - 3)^2$ takes each value $r \in [0, 4]$ three times, so $p = 6, q = 9$ determines the range of abc .

LỖI HAY GẶP / COMMON MISTAKE — Dùng bất đẳng thức pqr cho số thực có thể âm, như $r \geq p(4q - p^2)/9$ (cần $a, b, c \geq 0$) hoặc $q \geq 0$, rồi viết thẳng 'vì a, b, c bất kỳ'. Nếu đề không cho a, b, c không âm thì chỉ $p^2 \geq 3q$ và $q^2 \geq 3pr$ còn dùng được.

Using pqr inequalities for real numbers that may be negative, such as $r \geq p(4q - p^2)/9$ (needs $a, b, c \geq 0$)

0) or $q \geq 0$, and then writing 'since a, b, c are arbitrary'. If the problem does not give $a, b, c \geq 0$, only $p^2 \geq 3q$ and $q^2 \geq 3pr$ remain available.

PHẢI THUỘC / MEMORISE — $\Sigma a^2 = p^2 - 2q$; $\Sigma a^3 = p^3 - 3pq + 3r$; $\Sigma a^2 b^2 = q^2 - 2pr$; $(a + b)(b + c)(c + a) = pq - r$; $p^2 \geq 3q$; $q^2 \geq 3pr$.
 $\Sigma a^2 = p^2 - 2q$; $\Sigma a^3 = p^3 - 3pq + 3r$; $\Sigma a^2 b^2 = q^2 - 2pr$; $(a + b)(b + c)(c + a) = pq - r$; $p^2 \geq 3q$; $q^2 \geq 3pr$.

3.7. Đổi biến Ravi cho cạnh tam giác — The Ravi substitution

Ba cạnh a, b, c của tam giác bị ràng buộc bởi bất đẳng thức tam giác, nên không thể coi chúng là ba số dương tùy ý. Đổi biến Ravi chuyển ràng buộc đó thành ba số dương tự do x, y, z , là độ dài các đoạn tiếp tuyến kẻ từ đỉnh tới đường tròn nội tiếp.

The sides a, b, c of a triangle are bound by the triangle inequality, so they cannot be treated as arbitrary positive numbers. The Ravi substitution turns that restriction into three free positive numbers x, y, z , the lengths of the tangent segments from the vertices to the incircle.

ĐỊNH LÝ 3.11 (Đổi biến Ravi) / THEOREM 3.11 (Ravi substitution) — Ba số dương a, b, c là độ dài ba cạnh của một tam giác (không suy biến) khi và chỉ khi tồn tại ba số dương x, y, z sao cho $a = y + z$, $b = z + x$, $c = x + y$. Khi đó $x = (b + c - a)/2$, $y = (c + a - b)/2$, $z = (a + b - c)/2$.

Three positive numbers a, b, c are the side lengths of a non-degenerate triangle if and only if there exist positive numbers x, y, z with $a = y + z$, $b = z + x$, $c = x + y$. Then $x = (b + c - a)/2$, $y = (c + a - b)/2$, $z = (a + b - c)/2$.

Chứng minh. / Proof.

Nếu $a = y + z$, $b = z + x$, $c = x + y$ với $x, y, z > 0$ thì $b + c - a = 2x > 0$, $c + a - b = 2y > 0$, $a + b - c = 2z > 0$: ba bất đẳng thức tam giác đúng ngặt.

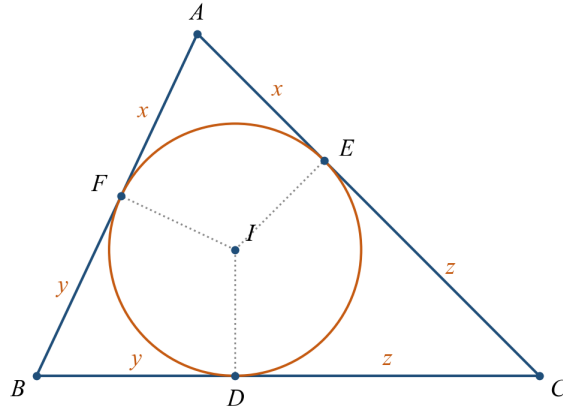
If $a = y + z$, $b = z + x$, $c = x + y$ with $x, y, z > 0$ then $b + c - a = 2x > 0$, $c + a - b = 2y > 0$, $a + b - c = 2z > 0$: all three triangle inequalities hold strictly.

Ngược lại, nếu a, b, c là cạnh tam giác, đặt $x = (b + c - a)/2$, $y = (c + a - b)/2$, $z = (a + b - c)/2$; chúng dương theo bất đẳng thức tam giác, và $y + z = a$, $z + x = b$, $x + y = c$.

Conversely, if a, b, c are sides of a triangle, put $x = (b + c - a)/2$, $y = (c + a - b)/2$, $z = (a + b - c)/2$; they are positive by the triangle inequality, and $y + z = a$, $z + x = b$, $x + y = c$. ■

Ý nghĩa hình học: gọi D, E, F là tiếp điểm của đường tròn nội tiếp với BC, CA, AB . Hai tiếp tuyến cùng kẻ từ một đỉnh bằng nhau nên $AE = AF = x$, $BD = BF = y$, $CD = CE = z$, và $BC = y + z$.

Geometric meaning: let D, E, F be the points where the incircle touches BC, CA, AB . Two tangents from the same vertex are equal, so $AE = AF = x$, $BD = BF = y$, $CD = CE = z$, and $BC = y + z$.



Hình 3.3. Đổi biến Ravi: các đoạn tiếp tuyến $AE = AF = x$, $BD = BF = y$, $CD = CE = z$; $BC = y + z$, $CA = z + x$, $AB = x + y$.

Figure 3.3. The Ravi substitution: tangent segments $AE = AF = x$, $BD = BF = y$, $CD = CE = z$; $BC = y + z$, $CA = z + x$, $AB = x + y$.

HỆ QUẢ 3.12 / COROLLARY 3.12 — Với a, b, c là ba cạnh của một tam giác: (1) $abc \geq (b + c - a)(c + a - b)(a + b - c)$; (2) $2(ab + bc + ca) - (a^2 + b^2 + c^2) = 4(xy + yz + zx) > 0$, trong đó x, y, z là các số Ravi.

For a, b, c the sides of a triangle: (1) $abc \geq (b + c - a)(c + a - b)(a + b - c)$; (2) $2(ab + bc + ca) - (a^2 + b^2 + c^2) = 4(xy + yz + zx) > 0$, where x, y, z are the Ravi numbers.

Chứng minh. / Proof.

(1) Theo đổi biến Ravi, bất đẳng thức thành $(y + z)(z + x)(x + y) \geq 8xyz$. Mà $(y + z)(z + x)(x + y) - 8xyz = x(y - z)^2 + y(z - x)^2 + z(x - y)^2 \geq 0$.

(1) By the Ravi substitution the inequality becomes $(y + z)(z + x)(x + y) \geq 8xyz$. And $(y + z)(z + x)(x + y) - 8xyz = x(y - z)^2 + y(z - x)^2 + z(x - y)^2 \geq 0$.

(2) Thay $a = y + z$, $b = z + x$, $c = x + y$: $a^2 + b^2 + c^2 = 2(x^2 + y^2 + z^2) + 2(xy + yz + zx)$ và $ab + bc + ca = x^2 + y^2 + z^2 + 3(xy + yz + zx)$. Trừ ra $2(ab + bc + ca) - (a^2 + b^2 + c^2) = 4(xy + yz + zx)$.

(2) Substituting $a = y + z$, $b = z + x$, $c = x + y$: $a^2 + b^2 + c^2 = 2(x^2 + y^2 + z^2) + 2(xy + yz + zx)$ and $ab + bc + ca = x^2 + y^2 + z^2 + 3(xy + yz + zx)$. Subtracting gives $2(ab + bc + ca) - (a^2 + b^2 + c^2) = 4(xy + yz + zx)$. ■

PHÂN TÍCH / ANALYSIS — Mẫu $b + c - a$, $c + a - b$, $a + b - c$ chính là $2x$, $2y$, $2z$: đúng điều Ravi làm gọn. Thay $a = y + z$, tử số thành tổng hai biến, và mỗi phân thức thành $(y + z)/(2x)$. Khi đó chỉ còn các tỉ số y/x dạng nghịch đảo của nhau, và AM–GM cho tổng của hai nghịch đảo ≥ 2 .

The denominators $b + c - a$, $c + a - b$, $a + b - c$ are exactly $2x$, $2y$, $2z$, which is what Ravi simplifies. With $a = y + z$ each numerator is a sum of two variables and each fraction becomes $(y + z)/(2x)$. Only ratios y/x and their reciprocals remain, and AM–GM bounds the sum of two reciprocals by at least 2.

VÍ DỤ 3.12 (Ravi cho phân thức) / EXAMPLE 3.12 (Ravi for fractions) — Cho a, b, c là ba cạnh của một tam giác. Chứng minh $a/(b+c-a) + b/(c+a-b) + c/(a+b-c) \geq 3$.
Let a, b, c be the sides of a triangle. Prove that $a/(b+c-a) + b/(c+a-b) + c/(a+b-c) \geq 3$.

Lời giải. / Solution.

Đặt $a = y + z, b = z + x, c = x + y$ với $x, y, z > 0$. Khi đó $b + c - a = 2x, c + a - b = 2y, a + b - c = 2z$ và vế trái bằng:

Put $a = y + z, b = z + x, c = x + y$ with $x, y, z > 0$. Then $b + c - a = 2x, c + a - b = 2y, a + b - c = 2z$ and the left side equals:

$$(y+z)/(2x) + (z+x)/(2y) + (x+y)/(2z) = (1/2) \cdot [(x/y + y/x) + (y/z + z/y) + (z/x + x/z)]$$

Với $u, v > 0$: $u/v + v/u \geq 2$ (vì $(u-v)^2 \geq 0$). Do đó tổng trong ngoặc ≥ 6 và vế trái ≥ 3 .

For $u, v > 0$: $u/v + v/u \geq 2$ (because $(u-v)^2 \geq 0$). So the bracket is at least 6 and the left side is at least 3.

Dấu bằng khi $x = y = z$, tức $a = b = c$.

Equality holds when $x = y = z$, that is $a = b = c$. ■

PHÂN TÍCH / ANALYSIS — Chu vi bằng 2 cho $x + y + z = 1$ và các cạnh $a = 1 - x, b = 1 - y, c = 1 - z$. Biểu thức $ab + bc + ca - abc$ là đa thức đối xứng bậc 3 của $1 - x, 1 - y, 1 - z$; khai triển theo $u = xy + yz + zx$ và $v = xyz$ sẽ triệt tiêu u .
Perimeter 2 gives $x + y + z = 1$ and sides $a = 1 - x, b = 1 - y, c = 1 - z$. The expression $ab + bc + ca - abc$ is a symmetric polynomial of degree 3 in $1 - x, 1 - y, 1 - z$; expanding in $u = xy + yz + zx$ and $v = xyz$ makes u cancel.

VÍ DỤ 3.13 (Ravi và chu vi cố định) / EXAMPLE 3.13 (Ravi with fixed perimeter) — Cho a, b, c là ba cạnh của một tam giác có chu vi bằng 2. Chứng minh $1 < ab + bc + ca - abc \leq 28/27$.
Let a, b, c be the sides of a triangle with perimeter 2. Prove that $1 < ab + bc + ca - abc \leq 28/27$.

Lời giải. / Solution.

Đổi biến Ravi: $a + b + c = 2(x + y + z) = 2$ nên $x + y + z = 1$, và $a = y + z = 1 - x, b = 1 - y, c = 1 - z$. Đặt $u = xy + yz + zx, v = xyz$.

Ravi substitution: $a + b + c = 2(x + y + z) = 2$, so $x + y + z = 1$, and $a = y + z = 1 - x, b = 1 - y, c = 1 - z$. Put $u = xy + yz + zx, v = xyz$.

Khai triển:

Expanding:

$$ab + bc + ca = 3 - 2(x + y + z) + u = 1 + u, \quad abc = 1 - (x + y + z) + u - v = u - v$$

Do đó $ab + bc + ca - abc = 1 + v$. Vì $x, y, z > 0$ nên $v > 0$, suy ra vế trái > 1 .

Hence $ab + bc + ca - abc = 1 + v$. Since $x, y, z > 0$ we have $v > 0$, so the left side exceeds 1.

Theo AM–GM, $1 = x + y + z \geq 3 \cdot (xyz)^{1/3}$, nên $v \leq 1/27$ và $ab + bc + ca - abc \leq 28/27$.

By AM–GM, $1 = x + y + z \geq 3 \cdot (xyz)^{1/3}$, so $v \leq 1/27$ and $ab + bc + ca - abc \leq 28/27$.

Dấu bằng bên phải khi $x = y = z = 1/3$, tức $a = b = c = 2/3$. Cận 1 không đạt được vì $v > 0$ luôn đúng.

Equality on the right occurs when $x = y = z = 1/3$, that is $a = b = c = 2/3$. The bound 1 is never attained since $v > 0$ always. ■

NHẬN XÉT / REMARK — Tam giác chỉ cần thiết khi bất đẳng thức dùng điều kiện tam giác. Bất đẳng thức $abc \geq (b + c - a)(c + a - b)(a + b - c)$ còn đúng với mọi $a, b, c \geq 0$ (tương đương Schur), nhưng chứng minh bằng Ravi gọn hơn và chỉ dùng AM–GM.

The triangle condition is needed only when the inequality uses it. The inequality $abc \geq (b + c - a)(c + a - b)(a + b - c)$ holds for all $a, b, c \geq 0$ (equivalent to Schur), but the Ravi proof is shorter and uses only AM–GM.

LỖI HAY GẶP / COMMON MISTAKE — Đổi biến Ravi khi đề chỉ cho $a, b, c > 0$ mà không có điều kiện tam giác, hoặc đổi chiều (cho x, y, z rồi nói a, b, c là cạnh tam giác) mà quên x, y, z phải dương.

Applying the Ravi substitution when the problem gives only $a, b, c > 0$ with no triangle condition, or going the other way (starting from x, y, z) and forgetting that x, y, z must be positive.

3.8. Hàm lồi và bất đẳng thức Jensen rời rạc — Convex functions and discrete Jensen

Đánh giá tiếp tuyến ở mục 3.4 là hệ quả của tính lồi. Công cụ tổng quát hơn không cần đạo hàm: kiểm tra tính lồi bằng định nghĩa trung điểm, rồi suy ra bất đẳng thức cho n số bất kỳ.

The tangent estimate of section 3.4 is a consequence of convexity. The more general tool needs no derivatives: check convexity from the midpoint definition, then deduce an inequality for any number of terms.

ĐỊNH NGHĨA 3.13 (Hàm lồi) / DEFINITION 3.13 (Convex function) — Hàm f xác định trên khoảng I gọi là lồi trên I nếu $f((x + y)/2) \leq (f(x) + f(y))/2$ với mọi $x, y \in I$. Hàm f gọi là lõm nếu bất đẳng thức đảo chiều, tức $-f$ lồi.

A function f defined on an interval I is called convex on I if $f((x + y)/2) \leq (f(x) + f(y))/2$ for all $x, y \in I$. It is called concave if the inequality is reversed, that is, if $-f$ is convex.

Định nghĩa thông thường của hàm lồi đòi hỏi $f(\lambda x + (1 - \lambda)y) \leq \lambda f(x) + (1 - \lambda)f(y)$ với mọi $\lambda \in [0, 1]$. Lấy $\lambda = 1/2$ ta được định nghĩa trên, nên mọi hàm lồi theo nghĩa thông thường đều lồi theo nghĩa của sách này. Chứng minh bất đẳng thức Jensen chỉ dùng $\lambda = 1/2$.

The usual definition of a convex function requires $f(\lambda x + (1 - \lambda)y) \leq \lambda f(x) + (1 - \lambda)f(y)$ for all $\lambda \in [0, 1]$. Taking $\lambda = 1/2$ gives the definition above, so every function convex in the usual sense is convex in the sense of this book. The proof of Jensen's inequality uses only $\lambda = 1/2$.

BỔ ĐỀ 3.14 (Kiểm tra hàm lồi) / LEMMA 3.14 (Checking convexity) — (a) $f(x) = x^2$ lồi trên $\mathbb{R}$; (b) $f(x) = 1/x$ lồi trên $(0, +\infty)$; (c) $f(x) = x^3$ lồi trên $[0, +\infty)$; (d) tổng hai hàm lồi, tích

của hàm lồi với số dương, và hàm lồi hợp với phép thế bậc nhất $f(\alpha x + \beta)$ đều lồi (trên tập thích hợp).

(a) $f(x) = x^2$ is convex on $\mathbb{R}$; (b) $f(x) = 1/x$ is convex on $(0, +\infty)$; (c) $f(x) = x^3$ is convex on $[0, +\infty)$; (d) a sum of convex functions, a convex function times a positive number, and a convex function composed with a linear substitution $f(\alpha x + \beta)$ are convex (on a suitable set).

Chứng minh. / Proof.

$$(a) (x^2 + y^2)/2 - ((x + y)/2)^2 = (x - y)^2/4 \geq 0.$$

$$(a) (x^2 + y^2)/2 - ((x + y)/2)^2 = (x - y)^2/4 \geq 0.$$

$$(b) \text{ Với } x, y > 0: (1/x + 1/y)/2 - 2/(x + y) = (x - y)^2/(2xy(x + y)) \geq 0.$$

$$(b) \text{ For } x, y > 0: (1/x + 1/y)/2 - 2/(x + y) = (x - y)^2/(2xy(x + y)) \geq 0.$$

$$(c) \text{ Với } x, y \geq 0: (x^3 + y^3)/2 - ((x + y)/2)^3 = 3(x + y)(x - y)^2/8 \geq 0.$$

$$(c) \text{ For } x, y \geq 0: (x^3 + y^3)/2 - ((x + y)/2)^3 = 3(x + y)(x - y)^2/8 \geq 0.$$

(d) Với tổng và bội dương, cộng hoặc nhân các bất đẳng thức trung điểm. Với phép thế bậc nhất, trung điểm của $\alpha x + \beta$ và $\alpha y + \beta$ là $\alpha(x + y)/2 + \beta$, nên bất đẳng thức trung điểm của f áp dụng được.

(d) For sums and positive multiples, add or multiply the midpoint inequalities. For a linear substitution, the midpoint of $\alpha x + \beta$ and $\alpha y + \beta$ is $\alpha(x + y)/2 + \beta$, so the midpoint inequality for f applies. ■

ĐỊNH LÝ 3.15 (Bất đẳng thức Jensen) / THEOREM 3.15 (Jensen's inequality) — Cho f lồi trên khoảng I . Với mọi $x_1, \dots, x_n \in I$ ($n \geq 2$): $f((x_1 + \dots + x_n)/n) \leq (f(x_1) + \dots + f(x_n))/n$. Nếu f lõm thì bất đẳng thức đảo chiều.

Let f be convex on an interval I . For all $x_1, \dots, x_n \in I$ ($n \geq 2$): $f((x_1 + \dots + x_n)/n) \leq (f(x_1) + \dots + f(x_n))/n$. If f is concave the inequality is reversed.

$$f((x_1 + x_2 + \dots + x_n)/n) \leq (f(x_1) + f(x_2) + \dots + f(x_n))/n \quad (3.3)$$

Chứng minh. / Proof.

Bước 1: $n = 2^k$. Quy nạp theo k , đặt $m = 2^k$. Với $k = 1$ đó là định nghĩa. Giả sử đúng cho m số; với $2m$ số, gọi A là trung bình của m số đầu, B là trung bình của m số sau. Khi đó trung bình của cả $2m$ số là $(A + B)/2$ và

Step 1: $n = 2^k$. Induction on k , put $m = 2^k$. For $k = 1$ this is the definition. Assume it for m numbers; given $2m$ numbers, let A be the mean of the first m and B the mean of the last m . The mean of all $2m$ numbers is $(A + B)/2$ and

$$f((A + B)/2) \leq (f(A) + f(B))/2 \leq (1/2) \cdot [(f(x_1) + \dots + f(x_m))/m + (f(x_{m+1}) + \dots + f(x_{2m}))/m]$$

Vế phải là trung bình của $f(x_i)$ trên cả $2m$ số.

The right side is the mean of the $f(x_i)$ over all $2m$ numbers.

Bước 2: n bất kỳ. Chọn $m = 2^k \geq n$, đặt $A = (x_1 + \dots + x_n)/n \in I$ và bổ sung $m - n$ số $x_{n+1} = \dots = x_m = A$. Trung bình của m số là $(nA + (m - n)A)/m = A$. Theo bước 1:

Step 2: arbitrary n . Choose $m = 2^k \geq n$, put $A = (x_1 + \dots + x_n)/n \in I$ and append $m - n$ numbers $x_{n+1} = \dots = x_m = A$. The mean of the m numbers is $(nA + (m - n)A)/m = A$. By step 1:

$$f(A) \leq (f(x_1) + \dots + f(x_n) + (m - n)f(A))/m$$

Nhân m , chuyển $(m - n)f(A)$ sang trái được $n \cdot f(A) \leq f(x_1) + \dots + f(x_n)$. Chia cho n ta có (3.3).

Multiply by m and move $(m - n)f(A)$ to the left to get $n \cdot f(A) \leq f(x_1) + \dots + f(x_n)$. Dividing by n gives (3.3). ■

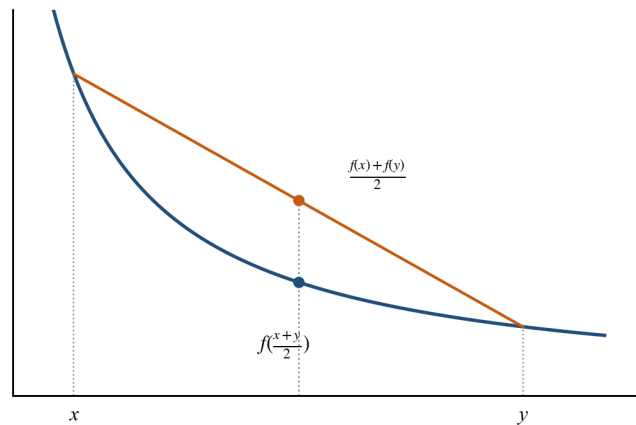
HỆ QUẢ 3.16 / COROLLARY 3.16 — Cho f lồi trên I , các số hữu tỉ dương $w_1, \dots, w_n$ có tổng bằng 1 và $x_1, \dots, x_n \in I$. Khi đó $f(w_1x_1 + \dots + w_nx_n) \leq w_1f(x_1) + \dots + w_nf(x_n)$.

Let f be convex on I , let $w_1, \dots, w_n$ be positive rationals with sum 1 and $x_1, \dots, x_n \in I$. Then $f(w_1x_1 + \dots + w_nx_n) \leq w_1f(x_1) + \dots + w_nf(x_n)$.

Chứng minh. / Proof.

Viết $w_i = m_i/N$ với m_i nguyên dương, $m_1 + \dots + m_n = N$. Áp dụng định lý 3.15 cho N số, trong đó x_i xuất hiện m_i lần: vế trái là f của trung bình có trọng số, vế phải là trung bình có trọng số của $f(x_i)$.

Write $w_i = m_i/N$ with positive integers m_i , $m_1 + \dots + m_n = N$. Apply theorem 3.15 to N numbers in which x_i appears m_i times: the left side is f of the weighted mean, the right side is the weighted mean of the $f(x_i)$. ■



Hình 3.4. Đồ thị hàm lồi $f(x) = 1/x$: điểm giữa của dây cung nằm trên đồ thị tại trung điểm, $f((x + y)/2) \leq (f(x) + f(y))/2$.

Figure 3.4. Graph of the convex function $f(x) = 1/x$: the midpoint of the chord lies above the graph at the midpoint, $f((x + y)/2) \leq (f(x) + f(y))/2$.

PHÂN TÍCH / ANALYSIS — Điều kiện $x + y + z = 1$ là tổng cố định và vế trái là tổng của cùng một hàm tại ba biến. Viết $x/(1 - x) = 1/(1 - x) - 1$. Hàm $1/u$ lồi với $u > 0$ (bổ đề 3.14b); đổi biến $u = 1 - x$ là phép thế bậc nhất nên $f(x) = 1/(1 - x)$ lồi trên $(-\infty, 1)$.

The condition $x + y + z = 1$ fixes the sum and the left side is a sum of the same function at three variables. Write $x/(1 - x) = 1/(1 - x) - 1$. The function $1/u$ is convex for $u > 0$ (lemma 3.14b); $u = 1 - x$ is a linear substitution, so $f(x) = 1/(1 - x)$ is convex on $(-\infty, 1)$.

VÍ DỤ 3.14 (Jensen cho ba biến) / EXAMPLE 3.14 (Jensen for three variables) — Cho $x, y, z \in (0, 1)$ thỏa $x + y + z = 1$. Chứng minh $x/(1-x) + y/(1-y) + z/(1-z) \geq 3/2$.
Let $x, y, z \in (0, 1)$ with $x + y + z = 1$. Prove that $x/(1-x) + y/(1-y) + z/(1-z) \geq 3/2$.

Lời giải. / Solution.

Xét $f(t) = t/(1-t) = 1/(1-t) - 1$ trên $I = (0, 1)$. Theo bổ đề 3.14 (b) và (d), f lồi trên I .
Consider $f(t) = t/(1-t) = 1/(1-t) - 1$ on $I = (0, 1)$. By lemma 3.14 (b) and (d), f is convex on I .

Áp dụng định lý 3.15 với $n = 3$:

Apply theorem 3.15 with $n = 3$:

$$f(x) + f(y) + f(z) \geq 3 \cdot f((x+y+z)/3) = 3 \cdot f(1/3) = 3 \cdot (1/3)/(2/3) = 3/2$$

Dấu bằng khi $x = y = z = 1/3$.

Equality holds when $x = y = z = 1/3$. ■

NHẬN XÉT / REMARK — Jensen mạnh hơn tiếp tuyến ở chỗ không cần tìm hệ số α ; nhưng tiếp tuyến cho phép dùng hàm không lồi trên cả miền miễn là $g(x) \geq \alpha x + \beta$ đúng trên I (như $1/(x^2+1)$ ở ví dụ 3.7, không lồi trên $[0, 3]$).

Jensen is stronger than the tangent line in that no slope α has to be found; the tangent line, however, works for functions that are not convex on the whole range as long as $g(x) \geq \alpha x + \beta$ holds on I (such as $1/(x^2+1)$ in example 3.7, which is not convex on $[0, 3]$).

NHẬN XÉT / REMARK — Với hàm lõm, Jensen cho cận trên. Hàm $\sqrt{x}$ lõm trên $[0, +\infty)$ vì $(\sqrt{x} + \sqrt{y})/2 \leq \sqrt{(x+y)/2}$ (bình phương hai vế, quy về $2\sqrt{xy} \leq x+y$). Do đó $\sqrt{a} + \sqrt{b} + \sqrt{c} \leq 3 \cdot \sqrt{(a+b+c)/3}$ với $a, b, c \geq 0$.

For a concave function Jensen gives an upper bound. The function $\sqrt{x}$ is concave on $[0, +\infty)$ because $(\sqrt{x} + \sqrt{y})/2 \leq \sqrt{(x+y)/2}$ (square both sides and reduce to $2\sqrt{xy} \leq x+y$). Hence $\sqrt{a} + \sqrt{b} + \sqrt{c} \leq 3 \cdot \sqrt{(a+b+c)/3}$ for $a, b, c \geq 0$.

LỖI HAY GẶP / COMMON MISTAKE — Dùng Jensen mà không kiểm tra hàm lồi trên đúng khoảng chứa các biến. Hàm $1/(x^2+1)$ không lồi trên $[0, 3]$, và bất đẳng thức Jensen cho nó không áp dụng được.

Using Jensen without checking that the function is convex on the exact interval containing the variables. The function $1/(x^2+1)$ is not convex on $[0, 3]$, so Jensen does not apply to it.

3.9. Bảng dấu hiệu và kỹ thuật — Signs and techniques at a glance

Dấu hiệu trong đề <i>Sign in the problem</i>	Công cụ nên thử <i>Tool to try</i>	Ví dụ <i>Example</i>
Điều kiện $abc = 1, ab + bc + ca = 3$ hay $a^2 + b^2 + c^2 = 3$; các số hạng khác bậc <i>Constraint such as $abc = 1, ab + bc + ca = 3$ or $a^2 + b^2 + c^2 = 3$; terms of different degrees</i>	Thuần nhất hóa bằng điều kiện, hoặc chuẩn hóa <i>Homogenise with the constraint, or normalise</i>	Ví dụ 3.1, 3.2 <i>Examples 3.1, 3.2</i>

Dấu hiệu trong đề <i>Sign in the problem</i>	Công cụ nên thử <i>Tool to try</i>	Ví dụ <i>Example</i>
Dấu bằng tại $a = b = c$ và tại $(1, 1, 0)$; biểu thức bậc ba hoặc bậc bốn <i>Equality at $a = b = c$ and at $(1, 1, 0)$; cubic or quartic expression</i>	Bất đẳng thức Schur <i>Schur's inequality</i>	Ví dụ 3.3, 3.4 <i>Examples 3.3, 3.4</i>
Hiệu hai vế chia hết cho $(a - b)^2$, $(b - c)^2$, $(c - a)^2$ <i>The difference of the sides is divisible by $(a - b)^2$, $(b - c)^2$, $(c - a)^2$</i>	Phương pháp SOS, tiêu chuẩn S_a, S_b, S_c <i>SOS method, criteria on S_a, S_b, S_c</i>	Ví dụ 3.5, 3.6 <i>Examples 3.5, 3.6</i>
Tổng của cùng một hàm tại từng biến, tổng các biến cố định <i>Sum of the same function at each variable, sum of the variables fixed</i>	Đánh giá tiếp tuyến; nếu hàm lồi thì Jensen <i>Tangent-line estimate; if the function is convex, Jensen</i>	Ví dụ 3.7, 3.8, 3.14 <i>Examples 3.7, 3.8, 3.14</i>
Biểu thức đối xứng, đặt c nhỏ nhất thì phụ thuộc đơn giản vào ab <i>Symmetric expression which, with c smallest, depends simply on ab</i>	Đồn hai biến về trung bình <i>Mix two variables to their mean</i>	Ví dụ 3.9 <i>Example 3.9</i>
Bất đẳng thức đối xứng ba biến, đề cho p hoặc q , hoặc có Σa^2b^2 , Σa^3 <i>Symmetric inequality in three variables, with p or q given, or containing Σa^2b^2, Σa^3</i>	Đổi biến p, q, r kèm Schur và $p^2 \geq 3q$ <i>The p, q, r substitution with Schur and $p^2 \geq 3q$</i>	Ví dụ 3.10, 3.11 <i>Examples 3.10, 3.11</i>
Đề cho a, b, c là ba cạnh tam giác <i>The problem says a, b, c are sides of a triangle</i>	Đổi biến Ravi $a = y + z$, $b = z + x$, $c = x + y$ <i>Ravi substitution $a = y + z$, $b = z + x$, $c = x + y$</i>	Ví dụ 3.12, 3.13 <i>Examples 3.12, 3.13</i>
Tiếp tuyến cho hiệu đổi dấu trong miền <i>The tangent line gives a difference that changes sign in the range</i>	Chia miền, hoặc chuyển sang SOS hoặc pqr <i>Split the range, or switch to SOS or pqr</i>	Nhận xét sau ví dụ 3.8 <i>Remark after example 3.8</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Thuần nhất hóa	Homogenisation	dùng điều kiện để các số hạng cùng bậc <i>making all terms of the same degree using the condition</i>
Chuẩn hóa	Normalisation	thêm điều kiện gọn vào đề thuần nhất <i>adding a convenient condition to a homogeneous problem</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Đa thức thuần nhất	Homogeneous polynomial	$P(ta, tb, tc) = t^k \cdot P(a, b, c)$
Điểm rơi	Equality point	bộ biến làm bất đẳng thức thành đẳng thức <i>the values of the variables that make the inequality an equality</i>
Bất đẳng thức Schur	Schur's inequality	$\sum a(a-b)(a-c) \geq 0$ với $a, b, c \geq 0$ <i>$\sum a(a-b)(a-c) \geq 0$ for $a, b, c \geq 0$</i>
Phương pháp SOS	SOS method	viết hiệu hai vế thành $\sum S_c(a-b)^2$ <i>writing the difference of the sides as $\sum S_c(a-b)^2$</i>
Tổng các bình phương	Sum of squares	biểu thức là tổng của các bình phương nhân hệ số <i>an expression that is a sum of squares times coefficients</i>
Tiếp tuyến	Tangent line	đường thẳng $ax + \beta$ chạm đồ thị tại điểm rơi <i>the line $ax + \beta$ touching the graph at the equality point</i>
Dồn biến	Mixing variables	thay hai biến bằng trung bình cộng của chúng <i>replacing two variables by their arithmetic mean</i>
Đa thức đối xứng	Symmetric polynomial	không đổi khi hoán vị các biến <i>unchanged under permutations of the variables</i>
Hệ thức Viète	Viète's relations	liên hệ nghiệm với hệ số của đa thức <i>relations between roots and coefficients of a polynomial</i>
Biệt thức	Discriminant	tích các bình phương hiệu các nghiệm <i>the product of the squared differences of the roots</i>
Đổi biến Ravi	Ravi substitution	$a = y + z, b = z + x, c = x + y$ với $x, y, z > 0$ <i>$a = y + z, b = z + x, c = x + y$ with $x, y, z > 0$</i>
Bất đẳng thức tam giác	Triangle inequality	mỗi cạnh nhỏ hơn tổng hai cạnh kia <i>each side is less than the sum of the other two</i>
Đường tròn nội tiếp	Incircle	đường tròn tiếp xúc ba cạnh trong tam giác <i>the circle tangent to the three sides inside the triangle</i>
Hàm lồi	Convex function	$f((x+y)/2) \leq (f(x) + f(y))/2$

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Hàm lõm	Concave function	hàm có $-f$ lồi <i>a function whose negative is convex</i>
Bất đẳng thức Jensen	Jensen's inequality	$f(\text{trung bình}) \leq \text{trung bình của } f$ với f lồi <i>$f(\text{mean}) \leq \text{mean of } f$ for convex f</i>
Trung điểm	Midpoint	điểm $(x + y)/2$ nằm giữa x và y <i>the point $(x + y)/2$ halfway between x and y</i>
Phản ví dụ	Counterexample	bộ số làm một mệnh đề sai <i>a choice of values that makes a statement false</i>
Hoán vị các biến	Permutation of variables	đổi chỗ a, b, c cho nhau <i>interchanging a, b and c</i>

3.10. Bài tự luyện — Practice problems

Mức 1 — Học sinh giỏi cấp tỉnh — Level 1 — Provincial olympiad

Bài 3.1 / Problem 3.1 — Chứng minh với mọi $a, b, c \geq 0$: $(a + b + c)(a^2 + b^2 + c^2) \leq 3(a^3 + b^3 + c^3)$. Dấu bằng xảy ra khi nào?

Prove that for all $a, b, c \geq 0$: $(a + b + c)(a^2 + b^2 + c^2) \leq 3(a^3 + b^3 + c^3)$. When does equality hold?

Bài 3.2 / Problem 3.2 — Cho $x, y, z \geq 0$ thỏa $x + y + z = 3$. Chứng minh $1/(x^2 + x + 1) + 1/(y^2 + y + 1) + 1/(z^2 + z + 1) \geq 1$.

Let $x, y, z \geq 0$ with $x + y + z = 3$. Prove that $1/(x^2 + x + 1) + 1/(y^2 + y + 1) + 1/(z^2 + z + 1) \geq 1$.

Bài 3.3 / Problem 3.3 — Cho a, b, c là ba cạnh của một tam giác. Chứng minh $(b + c - a)/a + (c + a - b)/b + (a + b - c)/c \geq 3$.

Let a, b, c be the sides of a triangle. Prove that $(b + c - a)/a + (c + a - b)/b + (a + b - c)/c \geq 3$.

Bài 3.4 / Problem 3.4 — Cho $a, b, c > 0$ thỏa $abc = 1$. Chứng minh $a^2 + b^2 + c^2 \geq a + b + c$.

Let $a, b, c > 0$ with $abc = 1$. Prove that $a^2 + b^2 + c^2 \geq a + b + c$.

Mức 2 — Học sinh giỏi quốc gia — Level 2 — National olympiad

Bài 3.5 / Problem 3.5 — Tìm số thực k lớn nhất sao cho với mọi $a, b, c \geq 0$: $(a - b)^2(a + b - kc) + (b - c)^2(b + c - ka) + (c - a)^2(c + a - kb) \geq 0$.

Find the largest real k such that for all $a, b, c \geq 0$: $(a - b)^2(a + b - kc) + (b - c)^2(b + c - ka) + (c - a)^2(c + a - kb) \geq 0$.

Bài 3.6 / Problem 3.6 — Cho a, b, c là các số thực thỏa $a + b + c = 3$ và $ab + bc + ca = 2$. Tìm giá trị lớn nhất và nhỏ nhất của abc .

Let a, b, c be real numbers with $a + b + c = 3$ and $ab + bc + ca = 2$. Find the largest and smallest values of abc .

Bài 3.7 / Problem 3.7 — Cho $a, b, c \geq 0$ thỏa $a + b + c = 3$. Chứng minh $3(ab + bc + ca) - 2abc \leq 7$.

Let $a, b, c \geq 0$ with $a + b + c = 3$. Prove that $3(ab + bc + ca) - 2abc \leq 7$.

Bài 3.8 / Problem 3.8 — Cho $a, b, c, d > 0$ thỏa $a + b + c + d = 4$. Chứng minh $a^2/(1+a) + b^2/(1+b) + c^2/(1+c) + d^2/(1+d) \geq 2$.

Let $a, b, c, d > 0$ with $a + b + c + d = 4$. Prove that $a^2/(1+a) + b^2/(1+b) + c^2/(1+c) + d^2/(1+d) \geq 2$.

Mức 3 — Olympic quốc tế — Level 3 — International olympiad

Bài 3.9 / Problem 3.9 — Cho $a, b, c \geq 0$ thỏa $a + b + c = 4$. Chứng minh $4(a^2b^2 + b^2c^2 + c^2a^2) + 11abc \leq 64$. Tìm mọi trường hợp dấu bằng.

Let $a, b, c \geq 0$ with $a + b + c = 4$. Prove that $4(a^2b^2 + b^2c^2 + c^2a^2) + 11abc \leq 64$. Find all equality cases.

Bài 3.10 / Problem 3.10 — Tìm số thực k lớn nhất sao cho với mọi $a, b, c \geq 0$: $a^4 + b^4 + c^4 + k \cdot abc(a + b + c) \geq (1 + k)(a^2b^2 + b^2c^2 + c^2a^2)$.

Find the largest real k such that for all $a, b, c \geq 0$: $a^4 + b^4 + c^4 + k \cdot abc(a + b + c) \geq (1 + k)(a^2b^2 + b^2c^2 + c^2a^2)$.

Bài 3.11 / Problem 3.11 — Cho a, b, c là các số thực thỏa $a + b + c = 3$ và $ab + bc + ca = 0$. Chứng minh $-4 \leq abc \leq 0$ và chỉ ra các bộ số đạt hai cận.

Let a, b, c be real numbers with $a + b + c = 3$ and $ab + bc + ca = 0$. Prove that $-4 \leq abc \leq 0$ and exhibit triples attaining both bounds.

Bài 3.12 / Problem 3.12 — Cho $a, b, c, d \geq 0$ thỏa $a + b + c + d = 4$. Chứng minh $abc + abd + acd + bcd - abcd \leq 3$. Tìm mọi trường hợp dấu bằng.

Let $a, b, c, d \geq 0$ with $a + b + c + d = 4$. Prove that $abc + abd + acd + bcd - abcd \leq 3$. Find all equality cases.

3.11. Lời giải bài tự luyện — Solutions to practice problems

Bài 3.1 — Problem 3.1

Khai triển: $(a + b + c)(a^2 + b^2 + c^2) = a^3 + b^3 + c^3 + \sum_{\text{sym}} a^2b$. Vậy hiệu hai vế bằng $2(a^3 + b^3 + c^3) - \sum_{\text{sym}} a^2b$.

Expanding: $(a + b + c)(a^2 + b^2 + c^2) = a^3 + b^3 + c^3 + \sum_{\text{sym}} a^2b$. So the difference of the sides is $2(a^3 + b^3 + c^3) - \sum_{\text{sym}} a^2b$.

Với mỗi cặp, $(a + b)(a - b)^2 = a^3 + b^3 - a^2b - ab^2$. Cộng ba cặp, mỗi lập phương xuất hiện hai lần:

For each pair, $(a + b)(a - b)^2 = a^3 + b^3 - a^2b - ab^2$. Adding the three pairs, each cube appears twice:

$$3(a^3 + b^3 + c^3) - (a + b + c)(a^2 + b^2 + c^2) = (a + b)(a - b)^2 + (b + c)(b - c)^2 + (c + a)(c - a)^2 \geq 0$$

Dấu bằng cần cả ba số hạng bằng 0. Nếu $a \neq b$ thì phải có $a + b = 0$, với $a, b \geq 0$ suy ra $a = b = 0$, mâu thuẫn. Vậy $a = b$; tương tự $b = c$. Dấu bằng xảy ra khi và chỉ khi $a = b = c$.

Equality needs all three terms to vanish. If $a \neq b$ then $a + b = 0$, which for $a, b \geq 0$ gives $a = b = 0$, a contradiction. So $a = b$; similarly $b = c$. Equality holds if and only if $a = b = c$. ■

Bài 3.2 — Problem 3.2

Điểm rơi $x = y = z = 1$, $g(1) = 1/3$. Rút gọn $g(t) - 1/3 = (2 - t - t^2)/(3(t^2 + t + 1)) = (t - 1)(-t - 2)/(3(t^2 + t + 1))$, nên $h(t) = -(t + 2)/(3(t^2 + t + 1))$ và $\alpha = h(1) = -1/3$. Tiếp tuyến: $(2 - t)/3$.

Equality point $x = y = z = 1$, $g(1) = 1/3$. Simplify $g(t) - 1/3 = (2 - t - t^2)/(3(t^2 + t + 1)) = (t - 1)(-t - 2)/(3(t^2 + t + 1))$, so $h(t) = -(t + 2)/(3(t^2 + t + 1))$ and $\alpha = h(1) = -1/3$. The tangent line: $(2 - t)/3$.

Với mọi $t \geq 0$:

For every $t \geq 0$:

$$1/(t^2 + t + 1) - (2 - t)/3 = (t - 1)^2(t + 1)/(3(t^2 + t + 1)) \geq 0$$

Cộng ba bất đẳng thức cho x, y, z : vế trái $\geq (6 - (x + y + z))/3 = 1$. Dấu bằng khi $x = y = z = 1$.

Adding the three inequalities for x, y, z : the left side is at least $(6 - (x + y + z))/3 = 1$. Equality holds when $x = y = z = 1$. ■

Bài 3.3 — Problem 3.3

Đổi biến Ravi: $a = y + z$, $b = z + x$, $c = x + y$ với $x, y, z > 0$. Khi đó $(b + c - a)/a = 2x/(y + z)$ và tương tự. Cần chứng minh $x/(y + z) + y/(z + x) + z/(x + y) \geq 3/2$.

Ravi substitution: $a = y + z$, $b = z + x$, $c = x + y$ with $x, y, z > 0$. Then $(b + c - a)/a = 2x/(y + z)$ and similarly for the others. It suffices to prove $x/(y + z) + y/(z + x) + z/(x + y) \geq 3/2$.

Đặt $s = x + y + z$. Vì $x/(y + z) = s/(y + z) - 1$ nên tổng bằng $s \cdot (1/(y + z) + 1/(z + x) + 1/(x + y)) - 3$.

Put $s = x + y + z$. Since $x/(y + z) = s/(y + z) - 1$, the sum equals $s \cdot (1/(y + z) + 1/(z + x) + 1/(x + y)) - 3$.

Theo bổ đề 3.14 (b) hoặc AM–HM, $1/(y + z) + 1/(z + x) + 1/(x + y) \geq 9/((y + z) + (z + x) + (x + y)) = 9/(2s)$.

By lemma 3.14 (b) or AM–HM, $1/(y + z) + 1/(z + x) + 1/(x + y) \geq 9/((y + z) + (z + x) + (x + y)) = 9/(2s)$.

Do đó tổng $\geq s \cdot 9/(2s) - 3 = 3/2$, và biểu thức đề bài $\geq 2 \cdot (3/2) = 3$. Dấu bằng khi $x = y = z$, tức tam giác đều.

Hence the sum is at least $s \cdot 9/(2s) - 3 = 3/2$, and the expression in the problem is at least $2 \cdot (3/2) = 3$. Equality holds when $x = y = z$, that is the triangle is equilateral. ■

Bài 3.4 — Problem 3.4

Đặt $p = a + b + c$. Theo AM–GM cho ba số (Chương 2), $p \geq 3 \cdot (abc)^{1/3} = 3$.

Put $p = a + b + c$. By three-term AM–GM (Chapter 2), $p \geq 3 \cdot (abc)^{1/3} = 3$.

Mặt khác $3(a^2 + b^2 + c^2) - p^2 = (a - b)^2 + (b - c)^2 + (c - a)^2 \geq 0$, nên $a^2 + b^2 + c^2 \geq p^2/3$.

Also $3(a^2 + b^2 + c^2) - p^2 = (a - b)^2 + (b - c)^2 + (c - a)^2 \geq 0$, so $a^2 + b^2 + c^2 \geq p^2/3$.

Vì $p \geq 3$ nên $p^2/3 = p \cdot (p/3) \geq p$. Vậy $a^2 + b^2 + c^2 \geq p$. Dấu bằng khi $a = b = c = 1$.

Since $p \geq 3$ we have $p^2/3 = p \cdot (p/3) \geq p$. Hence $a^2 + b^2 + c^2 \geq p$. Equality holds when $a = b = c = 1$. ■

Bài 3.5 — Problem 3.5

Gọi F_k là vế trái. Lấy $a = b = 1, c = 0$: $(a - b)^2 = 0$, còn $(b - c)^2(b + c - ka) = 1 - k$ và $(c - a)^2(c + a - kb) = 1 - k$. Vậy $F_k = 2(1 - k)$, và $F_k \geq 0$ buộc $k \leq 1$.

Let F_k be the left side. Take $a = b = 1, c = 0$: $(a - b)^2 = 0$, while $(b - c)^2(b + c - ka) = 1 - k$ and $(c - a)^2(c + a - kb) = 1 - k$. So $F_k = 2(1 - k)$, and $F_k \geq 0$ forces $k \leq 1$.

Ngược lại, tách $F_k = \Sigma(a - b)^2(a + b - c) + (1 - k)\Sigma(a - b)^2c$. Tổng đầu bằng $2[a(a - b)(a - c) + b(b - a)(b - c) + c(c - a)(c - b)]$, vì

Conversely, split $F_k = \Sigma(a - b)^2(a + b - c) + (1 - k)\Sigma(a - b)^2c$. The first sum equals $2[a(a - b)(a - c) + b(b - a)(b - c) + c(c - a)(c - b)]$, because

$$\Sigma(a - b)^2(a + b) = 2(a^3 + b^3 + c^3) - \Sigma_{\text{sym}} a^2b, \quad \Sigma(a - b)^2c = \Sigma_{\text{sym}} a^2b - 6abc$$

Trừ hai đẳng thức: $\Sigma(a - b)^2(a + b - c) = 2(a^3 + b^3 + c^3) - 2\Sigma_{\text{sym}} a^2b + 6abc$, đúng bằng hai lần vế trái của bất đẳng thức Schur, không âm (định lý 3.3).

Subtracting: $\Sigma(a - b)^2(a + b - c) = 2(a^3 + b^3 + c^3) - 2\Sigma_{\text{sym}} a^2b + 6abc$, which is exactly twice the left side of Schur's inequality and is non-negative (theorem 3.3).

Với $k \leq 1$ thì $(1 - k)\Sigma(a - b)^2c \geq 0$, nên $F_k \geq 0$ với mọi $a, b, c \geq 0$. Vậy số k lớn nhất là $k = 1$.

For $k \leq 1$ we have $(1 - k)\Sigma(a - b)^2c \geq 0$, so $F_k \geq 0$ for all $a, b, c \geq 0$. Hence the largest k is $k = 1$. ■

Bài 3.6 — Problem 3.6

Đặt $s = \sqrt{3}/3 = 1/\sqrt{3}$ và $m = 2\sqrt{3}/9$. Cố định a : $b + c = 3 - a$ và $bc = 2 - a(3 - a) = a^2 - 3a + 2 = (a - 1)(a - 2)$. Hai số thực b, c tồn tại khi $(3 - a)^2 \geq 4(a^2 - 3a + 2)$, tức:

Put $s = \sqrt{3}/3 = 1/\sqrt{3}$ and $m = 2\sqrt{3}/9$. Fix a : $b + c = 3 - a$ and $bc = 2 - a(3 - a) = a^2 - 3a + 2 = (a - 1)(a - 2)$. Real numbers b, c exist when $(3 - a)^2 \geq 4(a^2 - 3a + 2)$, that is:

$$3a^2 - 6a - 1 \leq 0 \Leftrightarrow 3(a - 1)^2 \leq 4 \Leftrightarrow 1 - 2s \leq a \leq 1 + 2s$$

Khi đó $abc = a(a - 1)(a - 2) = a^3 - 3a^2 + 2a$. Ta có hai đẳng thức (kiểm bằng khai triển, dùng $3s^2 = 1$):

Then $abc = a(a - 1)(a - 2) = a^3 - 3a^2 + 2a$. There are two identities (check by expansion, using $3s^2 = 1$):

$$abc - m = (a - 1 + s)^2(a - 1 - 2s), \quad abc + m = (a - 1 - s)^2(a - 1 + 2s)$$

Trên đoạn $1 - 2s \leq a \leq 1 + 2s$: thừa số $a - 1 - 2s \leq 0$ nên $abc \leq m$; thừa số $a - 1 + 2s \geq 0$ nên $abc \geq -m$.

On the interval $1 - 2s \leq a \leq 1 + 2s$: the factor $a - 1 - 2s \leq 0$ so $abc \leq m$; the factor $a - 1 + 2s \geq 0$ so $abc \geq -m$.

Các giá trị đạt được: với $a = 1 - s$ thì $b + c = 2 + s$, $bc = s(1 + s)$, biệt thức $(2 + s)^2 - 4s(1 + s) = 4 - 3s^2 = 3 > 0$ nên b, c thực, và $abc = m$. Với $a = 1 + s$ thì $b + c = 2 - s$, $bc = s(s - 1)$, biệt thức cũng bằng $3 > 0$, và $abc = -m$.

Both values are attained: for $a = 1 - s$ we get $b + c = 2 + s$, $bc = s(1 + s)$, discriminant $(2 + s)^2 - 4s(1 + s) = 4 - 3s^2 = 3 > 0$, so b, c are real and $abc = m$. For $a = 1 + s$ we get $b + c = 2 - s$, $bc = s(s - 1)$, discriminant again $3 > 0$, and $abc = -m$.

Vậy giá trị lớn nhất của abc là $2\sqrt{3}/9$ và giá trị nhỏ nhất là $-2\sqrt{3}/9$.

Hence the largest value of abc is $2\sqrt{3}/9$ and the smallest is $-2\sqrt{3}/9$. ■

Bài 3.7 — Problem 3.7

Giả sử $c = \min\{a, b, c\}$, nên $0 \leq c \leq 1$. Đặt $F = 3(ab + bc + ca) - 2abc$. Vì $a + b = 3 - c$:

Assume $c = \min\{a, b, c\}$, so $0 \leq c \leq 1$. Put $F = 3(ab + bc + ca) - 2abc$. Since $a + b = 3 - c$:

$$F = (3 - 2c)ab + 3c(3 - c)$$

Do $3 - 2c \geq 1 > 0$ và $ab \leq (3 - c)^2/4$ (bổ đề 3.7), ta có:

Since $3 - 2c \geq 1 > 0$ and $ab \leq (3 - c)^2/4$ (lemma 3.7), we get:

$$F \leq (3 - 2c)(3 - c)^2/4 + 3c(3 - c) = (27 + 3c^2 - 2c^3)/4$$

Cuối cùng $7 - (27 + 3c^2 - 2c^3)/4 = (2c^3 - 3c^2 + 1)/4 = (c - 1)^2(2c + 1)/4 \geq 0$.

Finally $7 - (27 + 3c^2 - 2c^3)/4 = (2c^3 - 3c^2 + 1)/4 = (c - 1)^2(2c + 1)/4 \geq 0$.

Vậy $F \leq 7$, dấu bằng khi $a = b = c = 1$.

Hence $F \leq 7$, with equality when $a = b = c = 1$. ■

Bài 3.8 — Problem 3.8

Viết $f(t) = t^2/(1 + t) = t - 1 + 1/(1 + t)$ trên $(0, +\infty)$, vì $t^2 = (t + 1)(t - 1) + 1$.

Write $f(t) = t^2/(1 + t) = t - 1 + 1/(1 + t)$ on $(0, +\infty)$, because $t^2 = (t + 1)(t - 1) + 1$.

Hàm $t - 1$ là bậc nhất nên vừa lồi vừa lõm (bất đẳng thức trung điểm thành đẳng thức). Hàm $1/(1 + t)$ lồi theo bổ đề 3.14 (b) với phép thế bậc nhất $u = 1 + t > 0$. Do đó f lồi trên $(0, +\infty)$.

The function $t - 1$ is linear, so it is both convex and concave (the midpoint inequality is an equality). The function $1/(1 + t)$ is convex by lemma 3.14 (b) with the linear substitution $u = 1 + t > 0$. Hence f is convex on $(0, +\infty)$.

Theo định lý 3.15 với $n = 4$:

By theorem 3.15 with $n = 4$:

$$f(a) + f(b) + f(c) + f(d) \geq 4 \cdot f((a + b + c + d)/4) = 4 \cdot f(1) = 4 \cdot (1/2) = 2$$

Vậy bất đẳng thức đúng; dấu bằng khi $a = b = c = d = 1$.

Hence the inequality holds, with equality when $a = b = c = d = 1$. ■

Bài 3.9 — Problem 3.9

Với $p = 4$, tính chất 3.8 cho $a^2b^2 + b^2c^2 + c^2a^2 = q^2 - 8r$. Vế trái bằng $4q^2 - 32r + 11r = 4q^2 - 21r$. Vì $p^2 \geq 3q$ nên $q \leq 16/3$.

With $p = 4$, property 3.8 gives $a^2b^2 + b^2c^2 + c^2a^2 = q^2 - 8r$. The left side is $4q^2 - 32r + 11r = 4q^2 - 21r$. Since $p^2 \geq 3q$ we have $q \leq 16/3$.

Trường hợp $q < 4$: vì $r \geq 0$ nên $4q^2 - 21r \leq 4q^2 < 64$.

Case $q < 4$: since $r \geq 0$, $4q^2 - 21r \leq 4q^2 < 64$.

Trường hợp $4 \leq q \leq 16/3$: dạng (2) của hệ quả 3.4 cho $r \geq 4(4q - 16)/9 = (16q - 64)/9$. Do đó $21r \geq (7/3)(16q - 64)$ và

Case $4 \leq q \leq 16/3$: form (2) of corollary 3.4 gives $r \geq 4(4q - 16)/9 = (16q - 64)/9$. Hence $21r \geq (7/3)(16q - 64)$ and

$$64 - (4q^2 - 21r) \geq 64 - 4q^2 + (7/3)(16q - 64) = -(4/3)(3q^2 - 28q + 64) = (4/3)(16 - 3q)(q - 4) \geq 0$$

Dòng cuối đúng vì $4 \leq q \leq 16/3$. Vậy bất đẳng thức đúng trong cả hai trường hợp.

The last line holds because $4 \leq q \leq 16/3$. So the inequality holds in both cases.

Dấu bằng. Trường hợp $q < 4$ cho bất đẳng thức ngặt. Trường hợp $q \geq 4$ cần $(16 - 3q)(q - 4) = 0$ và $r = (16q - 64)/9$. Nếu $q = 16/3$ thì $p^2 = 3q$ nên $a = b = c = 4/3$. Nếu $q = 4$ thì $r = 0$, tức một số bằng 0, chẳng hạn $c = 0$, khi đó $a + b = 4$, $ab = 4$ nên $a = b = 2$.

Equality. The case $q < 4$ gives a strict inequality. The case $q \geq 4$ needs $(16 - 3q)(q - 4) = 0$ and $r = (16q - 64)/9$. If $q = 16/3$ then $p^2 = 3q$, so $a = b = c = 4/3$. If $q = 4$ then $r = 0$, so one number is 0, say $c = 0$; then $a + b = 4$, $ab = 4$ and $a = b = 2$.

Vậy dấu bằng xảy ra tại $(4/3, 4/3, 4/3)$ và các hoán vị của $(2, 2, 0)$.

Hence equality holds at $(4/3, 4/3, 4/3)$ and at the permutations of $(2, 2, 0)$. ■

Bài 3.10 — Problem 3.10

Gọi H_k là hiệu hai vế. Lấy $a = b = 1$, $c = 0$: $H_k = 2 - (1 + k) = 1 - k$. Vậy $H_k \geq 0$ buộc $k \leq 1$.

Let H_k be the difference of the sides. Take $a = b = 1$, $c = 0$: $H_k = 2 - (1 + k) = 1 - k$. So $H_k \geq 0$ forces $k \leq 1$.

Với $k = 1$, ta tách H_1 thành hai phần không âm. Phần thứ nhất là bất đẳng thức Schur bậc 4 của ví dụ 3.6. Phần thứ hai là $\sum ab(a - b)^2$:

For $k = 1$ split H_1 into two non-negative parts. The first is the degree-4 Schur inequality of example 3.6. The second is $\sum ab(a - b)^2$:

$$H_1 = [a^4 + b^4 + c^4 + abc(a + b + c) - \sum_{\text{sym}} a^3b] + [ab(a - b)^2 + bc(b - c)^2 + ca(c - a)^2]$$

Thật vậy $ab(a - b)^2 = a^3b + ab^3 - 2a^2b^2$, cộng ba cặp cho $\sum_{\text{sym}} a^3b - 2(a^2b^2 + b^2c^2 + c^2a^2)$; cộng với phần đầu được đúng H_1 .

Indeed $ab(a - b)^2 = a^3b + ab^3 - 2a^2b^2$; adding the three pairs gives $\sum_{\text{sym}} a^3b - 2(a^2b^2 + b^2c^2 + c^2a^2)$; adding the first part gives exactly H_1 .

Với $k < 1$: $H_k = H_1 + (1 - k) \cdot (a^2b^2 + b^2c^2 + c^2a^2 - abc(a + b + c))$, và $a^2b^2 + b^2c^2 + c^2a^2 - abc(a + b + c) = ((ab - bc)^2 + (bc - ca)^2 + (ca - ab)^2)/2 \geq 0$. Vậy $H_k \geq 0$ với mọi $k \leq 1$.

For $k < 1$: $H_k = H_1 + (1 - k) \cdot (a^2b^2 + b^2c^2 + c^2a^2 - abc(a + b + c))$, and $a^2b^2 + b^2c^2 + c^2a^2 - abc(a + b + c) = ((ab - bc)^2 + (bc - ca)^2 + (ca - ab)^2)/2 \geq 0$. So $H_k \geq 0$ for every $k \leq 1$.

Số k lớn nhất là $k = 1$.

The largest k is $k = 1$. ■

Bài 3.11 — Problem 3.11

Tính tiền: đặt $x = a - 1$, $y = b - 1$, $z = c - 1$. Khi đó $x + y + z = 0$. Hơn nữa $a^2 + b^2 + c^2 = p^2 - 2q = 9$, nên $x^2 + y^2 + z^2 = (a^2 + b^2 + c^2) - 2(a + b + c) + 3 = 9 - 6 + 3 = 6$.

Translate: put $x = a - 1$, $y = b - 1$, $z = c - 1$. Then $x + y + z = 0$. Moreover $a^2 + b^2 + c^2 = p^2 - 2q = 9$, so $x^2 + y^2 + z^2 = (a^2 + b^2 + c^2) - 2(a + b + c) + 3 = 9 - 6 + 3 = 6$.

Khai triển $abc = (x + 1)(y + 1)(z + 1) = xyz + (xy + yz + zx) + (x + y + z) + 1$. Với $x + y + z = 0$ ta có $xy + yz + zx = -(x^2 + y^2 + z^2)/2 = -3$, nên $abc = xyz - 3 + 0 + 1 = xyz - 2$.

Expand $abc = (x + 1)(y + 1)(z + 1) = xyz + (xy + yz + zx) + (x + y + z) + 1$. With $x + y + z = 0$ we have $xy + yz + zx = -(x^2 + y^2 + z^2)/2 = -3$, so $abc = xyz - 3 + 0 + 1 = xyz - 2$.

Áp dụng bổ đề 3.10 cho x, y, z (tổng bằng 0):

Apply lemma 3.10 to x, y, z (sum zero):

$$6^3 - 54(xyz)^2 \geq 0 \Rightarrow (xyz)^2 \leq 4 \Rightarrow -2 \leq xyz \leq 2$$

Do đó $-4 \leq abc = xyz - 2 \leq 0$.

Therefore $-4 \leq abc = xyz - 2 \leq 0$.

Đạt cận: $(a, b, c) = (3, 0, 0)$ có tổng 3, $ab + bc + ca = 0$, $abc = 0$. Bộ $(a, b, c) = (-1, 2, 2)$ có tổng 3, $ab + bc + ca = -2 - 2 + 4 = 0$, $abc = -4$.

Bounds attained: $(a, b, c) = (3, 0, 0)$ has sum 3, $ab + bc + ca = 0$, $abc = 0$. The triple $(a, b, c) = (-1, 2, 2)$ has sum 3, $ab + bc + ca = -2 - 2 + 4 = 0$, $abc = -4$. ■

Bài 3.12 — Problem 3.12

Sắp thứ tự $a \geq b \geq c \geq d$. Đặt $s = a + b$, $u = c + d$, $v = cd$. Vì $c + d \leq a + b$ và tổng bằng 4 nên $0 \leq u \leq 2$, $s = 4 - u$. Biểu thức bằng:

Order $a \geq b \geq c \geq d$. Put $s = a + b$, $u = c + d$, $v = cd$. Since $c + d \leq a + b$ and the sum is 4, we have $0 \leq u \leq 2$ and $s = 4 - u$. The expression equals:

$$F = ab(c + d) + cd(a + b) - abcd = ab(u - v) + vs$$

Bước 1 (đòn a, b). Vì $v \leq u^2/4$ (bổ đề 3.7) nên $u - v \geq u - u^2/4 = u(4 - u)/4 \geq 0$. Thay ab bằng giá trị lớn nhất $s^2/4$:

Step 1 (mix a, b). Since $v \leq u^2/4$ (lemma 3.7) we get $u - v \geq u - u^2/4 = u(4 - u)/4 \geq 0$. Replacing ab by its largest value $s^2/4$:

$$F \leq (s^2/4)(u - v) + vs = s^2u/4 + v \cdot s(4 - s)/4 = s^2u/4 + v \cdot su/4$$

Bước 2 (đòn c, d). Hệ số của v là $su/4 \geq 0$, và $v \leq u^2/4$, nên $F \leq s^2u/4 + su^3/16$. Thay $s = 4 - u$:

Step 2 (mix c, d). The coefficient of v is $su/4 \geq 0$ and $v \leq u^2/4$, so $F \leq s^2u/4 + su^3/16$. Substituting $s = 4 - u$:

$$F \leq (4 - u)^2 u / 4 + (4 - u) u^3 / 16 = (4 - u) u (u^2 - 4u + 16) / 16$$

Bước 3 (một biến). Ta có $48 - (4 - u)u(u^2 - 4u + 16) = u^4 - 8u^3 + 32u^2 - 64u + 48 = (u - 2)^2(u^2 - 4u + 12)$, kiểm bằng khai triển, và $u^2 - 4u + 12 = (u - 2)^2 + 8 > 0$. Do đó $(4 - u)u(u^2 - 4u + 16)/16 \leq 3$, suy ra $F \leq 3$.

Step 3 (one variable). We have $48 - (4 - u)u(u^2 - 4u + 16) = u^4 - 8u^3 + 32u^2 - 64u + 48 = (u - 2)^2(u^2 - 4u + 12)$, checked by expansion, and $u^2 - 4u + 12 = (u - 2)^2 + 8 > 0$. Hence $(4 - u)u(u^2 - 4u + 16)/16 \leq 3$, so $F \leq 3$.

Dấu bằng cần $u = 2$, $ab = s^2/4 = 1$ với $a + b = 2$ nên $a = b = 1$, và $cd = u^2/4 = 1$ với $c + d = 2$ nên $c = d = 1$. Vậy dấu bằng chỉ xảy ra khi $a = b = c = d = 1$.

Equality needs $u = 2$, $ab = s^2/4 = 1$ with $a + b = 2$ so $a = b = 1$, and $cd = u^2/4 = 1$ with $c + d = 2$ so $c = d = 1$. Hence equality holds only when $a = b = c = d = 1$. ■

Chương 4. Phương trình, bất phương trình và hệ phương trình

— Chapter 4. Equations, inequations and systems

Mục tiêu chương — Chapter objectives

- Xét dấu tam thức bậc hai, dùng định lý Viète và so sánh nghiệm với một số α để biện luận theo tham số.
Determine the sign of a quadratic, and use Viète's theorem and comparison of roots with a number α to discuss a parameter.
- Giải phương trình và bất phương trình vô tỉ bằng nâng lũy thừa có điều kiện, ẩn phụ, liên hợp và đánh giá.
Solve irrational equations and inequations by conditional squaring, substitution, conjugates and estimation.
- Giải phương trình bậc cao có cấu trúc: đối xứng, hồi quy, đặt ẩn theo nhóm nhân tử.
Solve structured higher-degree equations: symmetric, reciprocal, and substitution on grouped factors.
- Giải hệ đối xứng loại I, loại II, hệ đẳng cấp, hệ bậc nhất ba ẩn và hệ giải bằng đánh giá.
Solve symmetric systems of types I and II, homogeneous systems, linear systems in three unknowns, and systems solved by estimation.
- Dùng tính đơn điệu theo định nghĩa: $f(u) = f(v) \Rightarrow u = v$, để giải phương trình và hệ vòng quanh.
Use monotonicity from the definition: $f(u) = f(v) \Rightarrow u = v$, to solve equations and cyclic systems.

4.1. Hàm số bậc hai và dấu của tam thức bậc hai — The quadratic function and the sign of a quadratic trinomial

Mọi bài toán biện luận nghiệm của phương trình bậc hai đều quy về việc đọc dấu của một tam thức, nên phần nền được chứng minh đầy đủ.

Every discussion of the roots of a quadratic comes down to reading the sign of a trinomial, so the basics are proved in full.

ĐỊNH NGHĨA 4.1 (Tam thức bậc hai) / DEFINITION 4.1 (Quadratic trinomial) — Tam thức bậc hai là biểu thức $f(x) = ax^2 + bx + c$ với $a, b, c \in \mathbb{R}$ và $a \neq 0$. Biệt thức là $\Delta = b^2 - 4ac$. Khi $b = 2b'$ ta dùng biệt thức thu gọn $\Delta' = b'^2 - ac$, cùng dấu với Δ . Nghiệm của f là số x_0 sao cho $f(x_0) = 0$.

A quadratic trinomial is an expression $f(x) = ax^2 + bx + c$ with $a, b, c \in \mathbb{R}$ and $a \neq 0$. Its discriminant is $\Delta = b^2 - 4ac$. When $b = 2b'$ we use the reduced discriminant $\Delta' = b'^2 - ac$, which has the same sign as Δ . A root of f is a number x_0 with $f(x_0) = 0$.

ĐỊNH LÝ 4.2 (Dạng chính tắc) / THEOREM 4.2 (Completed-square form) — Với mọi x : $f(x) = a[(x + b/(2a))^2 - \Delta/(4a^2)]$. Do đó đồ thị $y = f(x)$ là parabol có đỉnh $(-b/(2a); -\Delta/(4a))$, trục đối xứng $x = -b/(2a)$. Nếu $a > 0$ thì f đạt giá trị nhỏ nhất $-\Delta/(4a)$ tại $x = -b/(2a)$; nếu $a < 0$ thì f đạt giá trị lớn nhất $-\Delta/(4a)$ tại điểm đó.

For every x : $f(x) = a[(x + b/(2a))^2 - \Delta/(4a^2)]$. Hence the graph $y = f(x)$ is a parabola with vertex

$(-b/(2a), -\Delta/(4a))$ and axis $x = -b/(2a)$. If $a > 0$ then f attains its minimum $-\Delta/(4a)$ at $x = -b/(2a)$; if $a < 0$ it attains its maximum $-\Delta/(4a)$ there.

Chứng minh. / Proof.

Khai triển bình phương và rút gọn:

Expand the square and simplify:

$$a[(x + b/(2a))^2 - (b^2 - 4ac)/(4a^2)] = a[x^2 + (b/a)x + b^2/(4a^2) - b^2/(4a^2) + c/a] = ax^2 + bx + c \quad (4.1)$$

Bình phương luôn không âm và bằng 0 đúng khi $x = -b/(2a)$. Với $a > 0$, $f(x) \geq -\Delta/(4a)$, dấu bằng tại $x = -b/(2a)$; với $a < 0$ bất đẳng thức đổi chiều.

A square is never negative and vanishes exactly at $x = -b/(2a)$. For $a > 0$, $f(x) \geq -\Delta/(4a)$ with equality at $x = -b/(2a)$; for $a < 0$ the inequality reverses. ■

ĐỊNH LÝ 4.3 (Định lý về dấu tam thức bậc hai) / THEOREM 4.3 (Sign of a quadratic trinomial) — Gọi a là hệ số bậc hai của f . (i) Nếu $\Delta < 0$ thì $a \cdot f(x) > 0$ với mọi $x \in \mathbb{R}$; (ii) Nếu $\Delta = 0$ thì $a \cdot f(x) \geq 0$ với mọi x , và $f(x) = 0$ chỉ tại $x = -b/(2a)$; (iii) Nếu $\Delta > 0$ thì f có hai nghiệm $x_1 < x_2$, $f(x) = a(x - x_1)(x - x_2)$; $a \cdot f(x) < 0$ khi $x_1 < x < x_2$, $a \cdot f(x) > 0$ khi $x < x_1$ hoặc $x > x_2$.

Let a be the leading coefficient of f . (i) If $\Delta < 0$ then $a \cdot f(x) > 0$ for all $x \in \mathbb{R}$; (ii) If $\Delta = 0$ then $a \cdot f(x) \geq 0$ for all x , and $f(x) = 0$ only at $x = -b/(2a)$; (iii) If $\Delta > 0$ then f has two roots $x_1 < x_2$ and $f(x) = a(x - x_1)(x - x_2)$; $a \cdot f(x) < 0$ for $x_1 < x < x_2$, and $a \cdot f(x) > 0$ for $x < x_1$ or $x > x_2$.

Chứng minh. / Proof.

Nhân (4.1) với a : $a \cdot f(x) = a^2[(x + b/(2a))^2 - \Delta/(4a^2)]$. Vì $a^2 > 0$ nên dấu của $a \cdot f(x)$ là dấu của $(x + b/(2a))^2 - \Delta/(4a^2)$.

Multiply (4.1) by a : $a \cdot f(x) = a^2[(x + b/(2a))^2 - \Delta/(4a^2)]$. Since $a^2 > 0$, the sign of $a \cdot f(x)$ is the sign of $(x + b/(2a))^2 - \Delta/(4a^2)$.

Nếu $\Delta < 0$ thì $-\Delta/(4a^2) > 0$, tổng của một số không âm và một số dương là dương: (i).

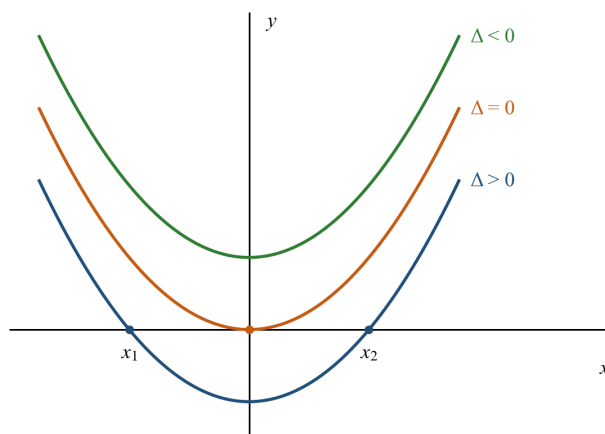
If $\Delta < 0$ then $-\Delta/(4a^2) > 0$, and a non-negative number plus a positive one is positive: (i).

Nếu $\Delta = 0$ thì $a \cdot f(x) = a^2(x + b/(2a))^2 \geq 0$, bằng 0 đúng khi $x = -b/(2a)$: (ii).

If $\Delta = 0$ then $a \cdot f(x) = a^2(x + b/(2a))^2 \geq 0$, with equality exactly at $x = -b/(2a)$: (ii).

Nếu $\Delta > 0$ đặt $x_{1,2} = (-b \mp \sqrt{\Delta})/(2a)$ (sắp để $x_1 < x_2$). Khi đó $(x + b/(2a))^2 - \Delta/(4a^2) = (x - x_1)(x - x_2)$ theo hằng đẳng thức hiệu hai bình phương, nên $f(x) = a(x - x_1)(x - x_2)$ và $a \cdot f(x) = a^2(x - x_1)(x - x_2)$. Tích $(x - x_1)(x - x_2)$ âm khi hai thừa số trái dấu, tức $x_1 < x < x_2$, và dương khi hai thừa số cùng dấu, tức x nằm ngoài $[x_1, x_2]$: (iii).

If $\Delta > 0$ put $x_{1,2} = (-b \mp \sqrt{\Delta})/(2a)$, ordered so that $x_1 < x_2$. By the difference of squares, $(x + b/(2a))^2 - \Delta/(4a^2) = (x - x_1)(x - x_2)$, so $f(x) = a(x - x_1)(x - x_2)$ and $a \cdot f(x) = a^2(x - x_1)(x - x_2)$. The product $(x - x_1)(x - x_2)$ is negative when the factors have opposite signs, that is $x_1 < x < x_2$, and positive when they have equal signs, that is x outside $[x_1, x_2]$: (iii). ■



Hình 4.1. Ba vị trí của parabol $y = ax^2 + bx + c$ ($a > 0$) so với trục hoành, theo dấu của Δ .

Figure 4.1. Three positions of the parabola $y = ax^2 + bx + c$ ($a > 0$) relative to the x -axis, according to the sign of Δ .

HỆ QUẢ 4.4 / COROLLARY 4.4 — Với $a \neq 0$: $f(x) \geq 0$ với mọi $x \in \mathbb{R}$ khi và chỉ khi $a > 0$ và $\Delta \leq 0$; $f(x) > 0$ với mọi x khi và chỉ khi $a > 0$ và $\Delta < 0$. Hai điều kiện tương tự cho $f(x) \leq 0$ và $f(x) < 0$ đổi $a > 0$ thành $a < 0$.

For $a \neq 0$: $f(x) \geq 0$ for all $x \in \mathbb{R}$ if and only if $a > 0$ and $\Delta \leq 0$; $f(x) > 0$ for all x if and only if $a > 0$ and $\Delta < 0$. The analogous conditions for $f(x) \leq 0$ and $f(x) < 0$ replace $a > 0$ by $a < 0$.

Chứng minh. / Proof.

Giả sử $a > 0$ và $\Delta \leq 0$. Theo Định lý 4.3 (i), (ii), $a \cdot f(x) \geq 0$, mà $a > 0$ nên $f(x) \geq 0$; khi $\Delta < 0$ thì $f(x) > 0$.

Suppose $a > 0$ and $\Delta \leq 0$. By Theorem 4.3 (i), (ii), $a \cdot f(x) \geq 0$, and $a > 0$, so $f(x) \geq 0$; when $\Delta < 0$, $f(x) > 0$.

Ngược lại giả sử $f(x) \geq 0$ với mọi x . Theo Định lý 4.3 luôn có điểm x với $a \cdot f(x) > 0$ (mọi x khác $-b/(2a)$ nếu $\Delta \leq 0$, mọi x ngoài $[x_1, x_2]$ nếu $\Delta > 0$). Tại điểm đó $f(x) \geq 0$ nên $a > 0$. Nếu $\Delta > 0$, phần (iii) cho $a \cdot f(x) < 0$ ở giữa hai nghiệm, tức $f(x) < 0$ vì $a > 0$, trái giả thiết. Vậy $\Delta \leq 0$. Trường hợp $f(x) > 0$ với mọi x tương tự, loại thêm $\Delta = 0$ vì khi đó $f(-b/(2a)) = 0$.

Conversely suppose $f(x) \geq 0$ for all x . By Theorem 4.3 there is always a point with $a \cdot f(x) > 0$ (every x other than $-b/(2a)$ if $\Delta \leq 0$, every x outside $[x_1, x_2]$ if $\Delta > 0$). At that point $f(x) \geq 0$, so $a > 0$. If $\Delta > 0$, part (iii) gives $a \cdot f(x) < 0$ between the roots, that is $f(x) < 0$ since $a > 0$, contradicting the hypothesis. Hence $\Delta \leq 0$. The case $f(x) > 0$ for all x is similar, with $\Delta = 0$ excluded because then $f(-b/(2a)) = 0$. ■

PHẢI THUỘC / MEMORISE — $f(x) = ax^2 + bx + c$ luôn cùng dấu a khi $\Delta < 0$; chỉ trái dấu a trong khoảng giữa hai nghiệm khi $\Delta > 0$.

$f(x) = ax^2 + bx + c$ always has the sign of a when $\Delta < 0$; it has the opposite sign only between the two roots when $\Delta > 0$.

VÍ DỤ 4.1 (Tam thức không đổi dấu) / EXAMPLE 4.1 (Trinomial of constant sign) —

Cho $f(x) = x^2 - 2(m+1)x + 3m + 7$. (a) Tìm m để $f(x) > 0$ với mọi $x \in \mathbb{R}$. (b) Tìm m để giá trị

nhỏ nhất của f bằng 1.

Let $f(x) = x^2 - 2(m+1)x + 3m + 7$. (a) Find m such that $f(x) > 0$ for all $x \in \mathbb{R}$. (b) Find m such that the minimum of f equals 1.

Lời giải. / Solution.

(a) Hệ số bậc hai bằng $1 > 0$. Theo Hệ quả 4.4, $f(x) > 0$ với mọi x khi và chỉ khi $\Delta' < 0$. Ở đây $\Delta' = (m+1)^2 - (3m+7) = m^2 - m - 6 = (m-3)(m+2)$.

(a) The leading coefficient is $1 > 0$. By Corollary 4.4, $f(x) > 0$ for all x if and only if $\Delta' < 0$. Here $\Delta' = (m+1)^2 - (3m+7) = m^2 - m - 6 = (m-3)(m+2)$.

Tích $(m-3)(m+2)$ âm khi $-2 < m < 3$. Vậy $f(x) > 0$ với mọi x khi và chỉ khi $-2 < m < 3$.

The product $(m-3)(m+2)$ is negative when $-2 < m < 3$. Hence $f(x) > 0$ for all x if and only if $-2 < m < 3$.

(b) Theo Định lý 4.2, giá trị nhỏ nhất là $f(m+1) = -\Delta' = -m^2 + m + 6$, vì $a = 1$. Điều kiện $-m^2 + m + 6 = 1$ cho $m^2 - m - 5 = 0$, tức $m = (1 \pm \sqrt{21})/2$.

(b) By Theorem 4.2 the minimum is $f(m+1) = -\Delta' = -m^2 + m + 6$, because $a = 1$. The condition $-m^2 + m + 6 = 1$ gives $m^2 - m - 5 = 0$, so $m = (1 \pm \sqrt{21})/2$.

Vậy $m = (1 + \sqrt{21})/2$ hoặc $m = (1 - \sqrt{21})/2$. Cả hai đều nằm trong $(-2; 3)$, nên với chúng f cũng dương với mọi x , phù hợp với (a).

Hence $m = (1 + \sqrt{21})/2$ or $m = (1 - \sqrt{21})/2$. Both lie in $(-2, 3)$, so f is also positive everywhere for them, consistent with (a). ■

LỖI HAY GẶP / COMMON MISTAKE — Dùng $\Delta \geq 0$ hay $\Delta > 0$ cho cả hai ý của một đề: $f(x) \geq 0$ với mọi x cho phép $\Delta = 0$ (parabol tiếp xúc trục), còn $f(x) > 0$ với mọi x thì không. Quên xét $a = 0$ khi hệ số bậc hai chứa tham số cũng mất điểm.

Using $\Delta \geq 0$ or $\Delta > 0$ for both parts of a problem: $f(x) \geq 0$ for all x allows $\Delta = 0$ (the parabola touches the axis) while $f(x) > 0$ for all x does not. Forgetting the case $a = 0$ when the leading coefficient contains the parameter also loses marks.

4.2. Định lý Viète và so sánh nghiệm với một số α — Viète's theorem and comparing roots with a number α

ĐỊNH LÝ 4.5 (Định lý Viète) / THEOREM 4.5 (Viète's theorem) — Nếu $f(x) = ax^2 + bx + c$ có hai nghiệm x_1, x_2 (kể cả nghiệm kép) thì $x_1 + x_2 = -b/a$ và $x_1x_2 = c/a$. Ngược lại, hai số thực có tổng S và tích P là hai nghiệm của $X^2 - SX + P = 0$, và hai số thực như vậy tồn tại khi và chỉ khi $S^2 \geq 4P$.

If $f(x) = ax^2 + bx + c$ has roots x_1, x_2 (a double root counted twice) then $x_1 + x_2 = -b/a$ and $x_1x_2 = c/a$. Conversely, two real numbers with sum S and product P are the roots of $X^2 - SX + P = 0$, and such real numbers exist if and only if $S^2 \geq 4P$.

Chứng minh. / Proof.

Theo Định lý 4.3, nghiệm là

By Theorem 4.3 the roots are

$$x_{1,2} = (-b \pm \sqrt{\Delta})/(2a) \quad (4.2)$$

Cộng hai nghiệm: $(-b + \sqrt{\Delta} - b - \sqrt{\Delta})/(2a) = -b/a$. Nhân hai nghiệm: $(b^2 - \Delta)/(4a^2) = 4ac/(4a^2) = c/a$.

Adding the roots gives $(-b + \sqrt{\Delta} - b - \sqrt{\Delta})/(2a) = -b/a$. Multiplying them gives $(b^2 - \Delta)/(4a^2) = 4ac/(4a^2) = c/a$.

Phần đảo: nếu $u + v = S$ và $uv = P$ thì $(X - u)(X - v) = X^2 - SX + P$, nên u, v là nghiệm của tam thức này. Tam thức $X^2 - SX + P$ có nghiệm thực khi và chỉ khi biệt thức $S^2 - 4P \geq 0$, và khi đó hai nghiệm có tổng S , tích P theo phần thuận.

For the converse: if $u + v = S$ and $uv = P$ then $(X - u)(X - v) = X^2 - SX + P$, so u and v are roots of this trinomial. $X^2 - SX + P$ has real roots if and only if its discriminant $S^2 - 4P \geq 0$, and then the roots have sum S and product P by the direct part. ■

Đặt $S = x_1 + x_2$ và $P = x_1x_2$. Các biểu thức đối xứng của hai nghiệm đều tính được từ S và P , không cần giải ra nghiệm:

Put $S = x_1 + x_2$ and $P = x_1x_2$. Every symmetric expression in the two roots can be computed from S and P without solving for the roots:

$$x_1^2 + x_2^2 = S^2 - 2P \quad (4.3)$$

$$x_1^3 + x_2^3 = S^3 - 3SP \quad (4.4)$$

$$|x_1 - x_2| = \sqrt{(S^2 - 4P)} = \sqrt{\Delta}/|a| \quad (4.5)$$

ĐỊNH LÝ 4.6 (So sánh nghiệm với một số) / THEOREM 4.6 (Comparing roots with a number) — Cho $f(x) = ax^2 + bx + c$, $a \neq 0$, và số thực α . (i) f có hai nghiệm $x_1 < \alpha < x_2$ khi và chỉ khi $a \cdot f(\alpha) < 0$; (ii) f có hai nghiệm $x_1 \leq x_2$ (kể cả nghiệm kép) cùng lớn hơn α khi và chỉ khi $\Delta \geq 0$, $a \cdot f(\alpha) > 0$ và $-b/(2a) > \alpha$; (iii) f có hai nghiệm $x_1 \leq x_2$ cùng nhỏ hơn α khi và chỉ khi $\Delta \geq 0$, $a \cdot f(\alpha) > 0$ và $-b/(2a) < \alpha$.

Let $f(x) = ax^2 + bx + c$ with $a \neq 0$, and let α be real. (i) f has two roots $x_1 < \alpha < x_2$ if and only if $a \cdot f(\alpha) < 0$. (ii) f has two roots $x_1 \leq x_2$ (a double root allowed) both greater than α if and only if $\Delta \geq 0$, $a \cdot f(\alpha) > 0$ and $-b/(2a) > \alpha$. (iii) f has two roots $x_1 \leq x_2$ both less than α if and only if $\Delta \geq 0$, $a \cdot f(\alpha) > 0$ and $-b/(2a) < \alpha$.

Chứng minh. / Proof.

Khi $\Delta \geq 0$, $f(x) = a(x - x_1)(x - x_2)$ nên $a \cdot f(\alpha) = a^2(\alpha - x_1)(\alpha - x_2)$, cùng dấu với $(\alpha - x_1)(\alpha - x_2)$.

When $\Delta \geq 0$, $f(x) = a(x - x_1)(x - x_2)$, so $a \cdot f(\alpha) = a^2(\alpha - x_1)(\alpha - x_2)$ has the sign of $(\alpha - x_1)(\alpha - x_2)$.

(i) Nếu $a \cdot f(\alpha) < 0$ thì $\Delta > 0$, vì với $\Delta \leq 0$ ta có $a \cdot f(\alpha) \geq 0$ theo Định lý 4.3. Khi đó $(\alpha - x_1)(\alpha - x_2) < 0$, tức hai thừa số trái dấu: $x_1 < \alpha < x_2$. Chiều ngược lại là cùng đẳng thức trên.

(i) If $a \cdot f(\alpha) < 0$ then $\Delta > 0$, because $\Delta \leq 0$ gives $a \cdot f(\alpha) \geq 0$ by Theorem 4.3. Then $(\alpha - x_1)(\alpha - x_2) < 0$, so the factors have opposite signs: $x_1 < \alpha < x_2$. The converse is the same identity.

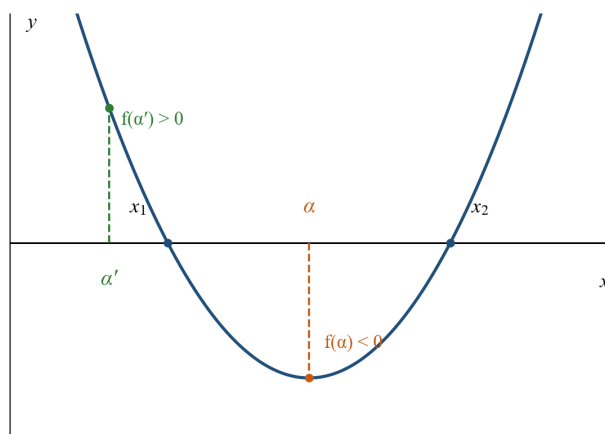
(ii) Nếu $\alpha < x_1 \leq x_2$ thì cả hai thừa số $\alpha - x_1$, $\alpha - x_2$ đều âm, tích dương, nên $a \cdot f(\alpha) > 0$; trung điểm $(x_1 + x_2)/2 = -b/(2a)$ lớn hơn α . Ngược lại, $a \cdot f(\alpha) > 0$ cho hai thừa số cùng

dấu: hoặc $\alpha < x_1$, hoặc $\alpha > x_2$. Trường hợp $\alpha > x_2$ kéo theo $\alpha > x_2 \geq (x_1 + x_2)/2 = -b/(2a)$, trái với $-b/(2a) > \alpha$. Vậy $\alpha < x_1 \leq x_2$.

(ii) If $\alpha < x_1 \leq x_2$ then both factors $\alpha - x_1$ and $\alpha - x_2$ are negative, the product is positive, so $a \cdot f(\alpha) > 0$; and the midpoint $(x_1 + x_2)/2 = -b/(2a)$ exceeds α . Conversely, $a \cdot f(\alpha) > 0$ gives two factors of equal sign: either $\alpha < x_1$ or $\alpha > x_2$. The case $\alpha > x_2$ would give $\alpha > x_2 \geq (x_1 + x_2)/2 = -b/(2a)$, contradicting $-b/(2a) > \alpha$. Hence $\alpha < x_1 \leq x_2$.

(iii) Chứng minh đối xứng với (ii): đổi chiều mọi bất đẳng thức so với α .

(iii) Symmetric to (ii): reverse every inequality involving α . ■



Hình 4.2. Parabol $y = x^2 - 6x + 7$ ($a = 1$): số α nằm giữa hai nghiệm khi $f(\alpha) < 0$; số α' nằm ngoài, bên trái cả hai nghiệm, khi $f(\alpha') > 0$ và $\alpha' < -b/(2a)$.

Figure 4.2. The parabola $y = x^2 - 6x + 7$ ($a = 1$): the number α lies between the roots when $f(\alpha) < 0$; the number α' lies to the left of both roots when $f(\alpha') > 0$ and $\alpha' < -b/(2a)$.

PHÂN TÍCH / ANALYSIS — Đề cho nghiệm “lớn hơn 1” không cần giải ra nghiệm. Ba phép thử chạy theo đúng Định lý 4.6 (ii): nghiệm có tồn tại (Δ), số 1 nằm ngoài khoảng hai nghiệm (dấu $a \cdot f(1)$), và nó nằm bên trái (so với trung điểm).

A statement such as “both roots exceed 1” needs no explicit roots. Three tests follow Theorem 4.6 (ii) exactly: the roots exist (Δ), the number 1 lies outside the interval between them (sign of $a \cdot f(1)$), and it lies on the left (compare with the midpoint).

VÍ DỤ 4.2 (So sánh nghiệm với số 1) / EXAMPLE 4.2 (Comparing roots with 1) — Cho phương trình $x^2 - 2mx + 3m - 2 = 0$. (a) Tìm m để phương trình có hai nghiệm (kể cả nghiệm kép) đều lớn hơn 1. (b) Tìm m để phương trình có nghiệm $x_1 < 1 < x_2$.

Consider $x^2 - 2mx + 3m - 2 = 0$. (a) Find m such that both roots (a double root allowed) exceed 1. (b) Find m such that the roots satisfy $x_1 < 1 < x_2$.

Lời giải. / Solution.

Đặt $f(x) = x^2 - 2mx + 3m - 2$. Hệ số bậc hai bằng 1, $f(1) = 1 - 2m + 3m - 2 = m - 1$, $\Delta' = m^2 - (3m - 2) = (m - 1)(m - 2)$, trung điểm hai nghiệm là m .

Put $f(x) = x^2 - 2mx + 3m - 2$. The leading coefficient is 1, $f(1) = 1 - 2m + 3m - 2 = m - 1$, $\Delta' = m^2 - (3m - 2) = (m - 1)(m - 2)$, and the midpoint of the roots is m .

(a) Theo Định lý 4.6 (ii) cần đồng thời: $\Delta' \geq 0$, tức $m \leq 1$ hoặc $m \geq 2$; $f(1) > 0$, tức $m > 1$; $m > 1$. Giao ba điều kiện là $m \geq 2$.

(a) By Theorem 4.6 (ii) we need simultaneously: $\Delta' \geq 0$, that is $m \leq 1$ or $m \geq 2$; $f(1) > 0$, that is $m > 1$; and $m > 1$. The intersection is $m \geq 2$.

Kiểm tra $m = 2$: phương trình thành $(x - 2)^2 = 0$, nghiệm kép $x = 2 > 1$, đúng.

Check $m = 2$: the equation becomes $(x - 2)^2 = 0$, double root $x = 2 > 1$, as required.

(b) Theo Định lý 4.6 (i) cần $f(1) < 0$, tức $m < 1$. Khi đó $\Delta' = (m - 1)(m - 2) > 0$ tự có, hai nghiệm phân biệt nằm hai phía của 1.

(b) By Theorem 4.6 (i) we need $f(1) < 0$, that is $m < 1$. Then $\Delta' = (m - 1)(m - 2) > 0$ holds automatically and the two distinct roots lie on either side of 1.

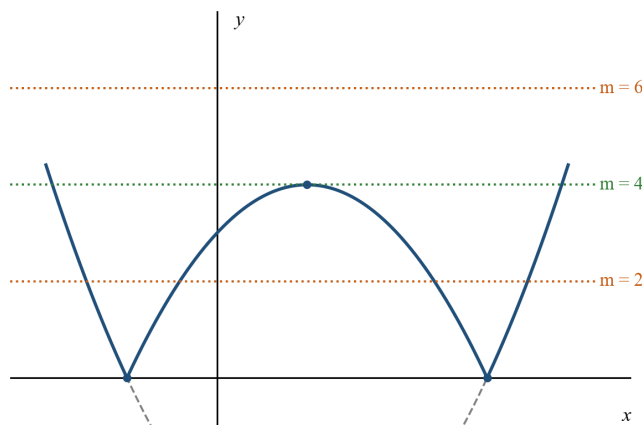
Vậy (a) $m \geq 2$; (b) $m < 1$.

Hence (a) $m \geq 2$; (b) $m < 1$. ■

Biện luận số nghiệm bằng đồ thị — Counting solutions graphically

Khi tham số m tách được về một vế, số nghiệm của $f(x) = m$ là số giao điểm của đồ thị $y = f(x)$ với đường ngang $y = m$. Với $f(x) = |x^2 - 2x - 3| = |(x - 1)^2 - 4|$, đồ thị gồm phần parabol $y = x^2 - 2x - 3$ nằm trên trục hoành, cộng phần còn lại lật lên qua trục hoành; điểm cực đại địa phương là $(1; 4)$.

When the parameter m can be isolated on one side, the number of solutions of $f(x) = m$ is the number of intersections of $y = f(x)$ with the horizontal line $y = m$. For $f(x) = |x^2 - 2x - 3| = |(x - 1)^2 - 4|$ the graph consists of the part of $y = x^2 - 2x - 3$ above the axis together with the rest reflected upwards; the local maximum is the point $(1, 4)$.



Hình 4.3. Đồ thị $y = |x^2 - 2x - 3|$ (nét liền) và parabol gốc (nét đứt); các đường ngang $y = 2, 4, 6$ cắt đồ thị tại 4, 3, 2 điểm.

Figure 4.3. The graph of $y = |x^2 - 2x - 3|$ (solid) and the original parabola (dashed); the horizontal lines $y = 2, 4, 6$ meet it in 4, 3, 2 points.

Từ hình: phương trình $|x^2 - 2x - 3| = m$ vô nghiệm khi $m < 0$; có 2 nghiệm khi $m = 0$ hoặc $m > 4$; có 4 nghiệm khi $0 < m < 4$; có 3 nghiệm khi $m = 4$. Mỗi kết quả kiểm lại được bằng Định lý 4.6: với $m > 0$, hai phương trình $x^2 - 2x - 3 = \pm m$ cho các nghiệm phải đếm riêng.

From the picture: $|x^2 - 2x - 3| = m$ has no solution for $m < 0$; two solutions for $m = 0$ or $m > 4$; four solutions for $0 < m < 4$; three solutions for $m = 4$. Each claim can be rechecked with Theorem 4.6: for $m > 0$ the two equations $x^2 - 2x - 3 = \pm m$ must be counted separately.

NHẬN XÉT / REMARK — Hình vẽ chỉ gợi ý đáp số. Trong bài thi phải đi kèm lập luận bằng bảng biến thiên của hàm hoặc bằng điều kiện Δ , vì đồ thị “trông như cắt” không phải là chứng minh. Ở ví dụ trên, với $m = 4$ hai phương trình $x^2 - 2x - 3 = 4$ ($\Delta' = 8 > 0$, hai nghiệm) và $x^2 - 2x - 3 = -4$ ($\Delta' = 0$, nghiệm kép $x = 1$) cho tổng cộng 3 nghiệm khác nhau.

A picture only suggests the answer. In an exam it must be backed by monotonicity of the function or by the condition on Δ , because “it looks like it crosses” is not a proof. In the example above, for $m = 4$ the equations $x^2 - 2x - 3 = 4$ ($\Delta' = 8 > 0$, two roots) and $x^2 - 2x - 3 = -4$ ($\Delta' = 0$, double root $x = 1$) give three distinct solutions in all.

4.3. Phương trình vô tỉ — Irrational equations

Bốn kỹ thuật chiếm gần hết các đề: nâng lũy thừa có điều kiện, đặt ẩn phụ, nhân liên hợp, đánh giá. Điểm mất nhiều nhất là bước nâng lũy thừa không kèm điều kiện, sinh nghiệm ngoại lai, hoặc kiểm nghiệm sai chỗ.

Four techniques cover most problems: conditional squaring, substitution, conjugates and estimation. Most marks are lost in squaring without a condition, which creates extraneous roots, or in checking roots in the wrong equation.

BỔ ĐỀ 4.7 (Nâng lũy thừa tương đương) / LEMMA 4.7 (Equivalent squaring) — Với các biểu thức A, B : (a) $\sqrt{A} = B$ khi và chỉ khi $B \geq 0$ và $A = B^2$; (b) $\sqrt{A} = \sqrt{B}$ khi và chỉ khi $A = B \geq 0$.

For expressions A, B : (a) $\sqrt{A} = B$ if and only if $B \geq 0$ and $A = B^2$; (b) $\sqrt{A} = \sqrt{B}$ if and only if $A = B \geq 0$.

Chứng minh. / Proof.

(a) Nếu $\sqrt{A} = B$ thì B là căn bậc hai số học nên $B \geq 0$, và bình phương hai vế cho $A = B^2$. Ngược lại, nếu $B \geq 0$ và $A = B^2$ thì $A \geq 0$ và $\sqrt{A} = \sqrt{(B^2)} = |B| = B$.

(a) If $\sqrt{A} = B$ then B is an arithmetic square root, so $B \geq 0$, and squaring gives $A = B^2$. Conversely, if $B \geq 0$ and $A = B^2$ then $A \geq 0$ and $\sqrt{A} = \sqrt{(B^2)} = |B| = B$.

(b) Nếu $\sqrt{A} = \sqrt{B}$ thì cả hai vế xác định, hai căn không âm và bình phương cho $A = B \geq 0$. Ngược lại $A = B \geq 0$ cho $\sqrt{A} = \sqrt{B}$ hiển nhiên.

(b) If $\sqrt{A} = \sqrt{B}$ then both sides are defined and non-negative, and squaring gives $A = B \geq 0$. The converse is immediate. ■

TÍNH CHẤT 4.8 (Biểu thức liên hợp và đánh giá hai căn) / PROPERTY 4.8 (Conjugate and two-root estimate) — Với $A, B \geq 0$ và $A \neq B$: $\sqrt{A} - \sqrt{B} = (A - B)/(\sqrt{A} + \sqrt{B})$. Với $a, b \geq 0$: $(\sqrt{a} + \sqrt{b})^2 \leq 2(a + b)$, dấu bằng khi và chỉ khi $a = b$.

For $A, B \geq 0$ with $A \neq B$: $\sqrt{A} - \sqrt{B} = (A - B)/(\sqrt{A} + \sqrt{B})$. For $a, b \geq 0$: $(\sqrt{a} + \sqrt{b})^2 \leq 2(a + b)$, with equality if and only if $a = b$.

Chứng minh. / Proof.

Vì $A \neq B$ nên $\sqrt{A} + \sqrt{B} > 0$ (hai căn không cùng bằng 0). Nhân tử và mẫu của vế phải với $\sqrt{A} + \sqrt{B}$, hoặc đơn giản hơn nhân chéo:

Since $A \neq B$, $\sqrt{A} + \sqrt{B} > 0$ (the two roots are not both zero). Cross-multiplying:

$$(\sqrt{A} - \sqrt{B})(\sqrt{A} + \sqrt{B}) = A - B \quad (4.6)$$

Bất đẳng thức thứ hai: $2(a + b) - (\sqrt{a} + \sqrt{b})^2 = a + b - 2\sqrt{ab} = (\sqrt{a} - \sqrt{b})^2 \geq 0$, bằng 0 đúng khi $\sqrt{a} = \sqrt{b}$.

For the inequality: $2(a + b) - (\sqrt{a} + \sqrt{b})^2 = a + b - 2\sqrt{ab} = (\sqrt{a} - \sqrt{b})^2 \geq 0$, with equality exactly when $\sqrt{a} = \sqrt{b}$. ■

PHÂN TÍCH / ANALYSIS — Hai căn lệch nhau đúng 2, và biểu thức trong căn đều bậc nhất. Cô lập một căn rồi bình phương hai vế bỏ được một căn, để lại một căn duy nhất; lần bình phương thứ hai bỏ hẳn căn. Vế phải sau khi cô lập là $2 + \sqrt{x+1} \geq 2 > 0$ nên Bỏ đề 4.7 (a) cho phép bình phương mà không sinh nghiệm ngoại lai.

The two radicals differ by exactly 2 and their radicands are linear. Isolating one radical and squaring removes one radical and leaves exactly one; a second squaring removes the last. After isolating, the right side is $2 + \sqrt{x+1} \geq 2 > 0$, so Lemma 4.7 (a) lets us square without creating extraneous roots.

VÍ DỤ 4.3 (Nâng lũy thừa có điều kiện) / EXAMPLE 4.3 (Conditional squaring) — Giải phương trình $\sqrt{3x+7} - \sqrt{x+1} = 2$.

Solve the equation $\sqrt{3x+7} - \sqrt{x+1} = 2$.

Lời giải. / Solution.

Điều kiện xác định: $x+1 \geq 0$ và $3x+7 \geq 0$, tức $x \geq -1$. Chuyển vế: $\sqrt{3x+7} = 2 + \sqrt{x+1}$. Vế phải $\geq 2 > 0$ nên theo Bỏ đề 4.7 (a), phương trình tương đương với $3x+7 = 4 + 4\sqrt{x+1} + x+1$.

Domain: $x+1 \geq 0$ and $3x+7 \geq 0$, that is $x \geq -1$. Rearranging: $\sqrt{3x+7} = 2 + \sqrt{x+1}$. The right side is $\geq 2 > 0$, so by Lemma 4.7 (a) the equation is equivalent to $3x+7 = 4 + 4\sqrt{x+1} + x+1$.

Rút gọn: $2x+2 = 4\sqrt{x+1}$, tức $x+1 = 2\sqrt{x+1}$. Đặt $v = \sqrt{x+1} \geq 0$: $v^2 = 2v$, nên $v = 0$ hoặc $v = 2$.

Simplifying: $2x+2 = 4\sqrt{x+1}$, that is $x+1 = 2\sqrt{x+1}$. Put $v = \sqrt{x+1} \geq 0$: $v^2 = 2v$, so $v = 0$ or $v = 2$.

Với $v = 0$: $x = -1$. Với $v = 2$: $x+1 = 4$, $x = 3$. Cả hai thỏa $x \geq -1$. Kiểm tra trong đề: $x = -1$ cho $\sqrt{4} - 0 = 2$; $x = 3$ cho $\sqrt{16} - \sqrt{4} = 2$.

For $v = 0$: $x = -1$. For $v = 2$: $x+1 = 4$, $x = 3$. Both satisfy $x \geq -1$. Check in the original: $x = -1$ gives $\sqrt{4} - 0 = 2$; $x = 3$ gives $\sqrt{16} - \sqrt{4} = 2$.

Vậy tập nghiệm là $\{-1; 3\}$.

Hence the solution set is $\{-1, 3\}$. ■

PHÂN TÍCH / ANALYSIS — Trong đề, $x^2 + 5x$ xuất hiện ở cả hai vế: ngoài căn là $x^2 + 5x + 4$ và trong căn là $x^2 + 5x + 10$. Hiệu hai biểu thức đó là hằng số 6, nên đặt t là căn thì $x^2 + 5x + 4 = t^2 - 6$, và phương trình thành phương trình bậc hai theo t . Điều kiện $t \geq 0$ phải được giữ lại để loại nghiệm.

In the statement $x^2 + 5x$ occurs on both sides: $x^2 + 5x + 4$ outside the root and $x^2 + 5x + 10$ inside.

The two differ by the constant 6, so with t the root, $x^2 + 5x + 4 = t^2 - 6$ and the equation becomes quadratic in t . The condition $t \geq 0$ must be kept to discard roots.

VÍ DỤ 4.4 (Đặt ẩn phụ là căn) / EXAMPLE 4.4 (Radical as the new unknown) — Giải phương trình $x^2 + 5x + 4 = \sqrt{x^2 + 5x + 10}$.
Solve the equation $x^2 + 5x + 4 = \sqrt{x^2 + 5x + 10}$.

Lời giải. / Solution.

Biểu thức dưới căn $x^2 + 5x + 10 = (x + 5/2)^2 + 15/4 > 0$ nên phương trình xác định với mọi x . Đặt $t = \sqrt{x^2 + 5x + 10} \geq 0$, khi đó $x^2 + 5x + 4 = t^2 - 6$.

The radicand $x^2 + 5x + 10 = (x + 5/2)^2 + 15/4$ is positive, so the equation is defined for all x . Put $t = \sqrt{x^2 + 5x + 10} \geq 0$; then $x^2 + 5x + 4 = t^2 - 6$.

Phương trình thành $t^2 - 6 = t$, tức $t^2 - t - 6 = (t - 3)(t + 2) = 0$. Vì $t \geq 0$ nên $t = 3$.

The equation becomes $t^2 - 6 = t$, that is $t^2 - t - 6 = (t - 3)(t + 2) = 0$. Since $t \geq 0$, $t = 3$.

Từ $t = 3$: $x^2 + 5x + 10 = 9$, tức $x^2 + 5x + 1 = 0$ với $\Delta = 21 > 0$, nên $x = (-5 \pm \sqrt{21})/2$. Với hai giá trị này $x^2 + 5x + 4 = 3 > 0$ và $\sqrt{x^2 + 5x + 10} = 3$, đúng.

From $t = 3$: $x^2 + 5x + 10 = 9$, that is $x^2 + 5x + 1 = 0$ with $\Delta = 21 > 0$, so $x = (-5 \pm \sqrt{21})/2$. For both values $x^2 + 5x + 4 = 3 > 0$ and $\sqrt{x^2 + 5x + 10} = 3$, as required.

Vậy tập nghiệm là $\{(-5 - \sqrt{21})/2; (-5 + \sqrt{21})/2\}$.

Hence the solution set is $\{(-5 - \sqrt{21})/2, (-5 + \sqrt{21})/2\}$. ■

PHÂN TÍCH / ANALYSIS — Thử $x = 1$ cho cả hai căn bằng 3 và 3, hai vế đều 0. Nghiệm đoán được là dấu hiệu nên tách thừa số $x - 1$. Hiệu hai biểu thức trong căn là $4(x - 1)$ chia hết cho $x - 1$, nên nhân liên hợp đưa về trái về dạng có nhân tử $x - 1$. Phần còn lại phải được đánh giá để chỉ ra nó không triệt tiêu.

Trying $x = 1$ gives both radicals equal to 3, and both sides 0. A guessed root signals a factor $x - 1$.

The difference of the radicands is $4(x - 1)$, divisible by $x - 1$, so multiplying by the conjugate puts the left side in a form with the factor $x - 1$. The remaining factor must be estimated to show it never vanishes.

VÍ DỤ 4.5 (Nhân liên hợp, tách nhân tử) / EXAMPLE 4.5 (Conjugate and factor extraction) — Giải phương trình $\sqrt{5x + 4} - \sqrt{x + 8} = 2x - 2$.
Solve the equation $\sqrt{5x + 4} - \sqrt{x + 8} = 2x - 2$.

Lời giải. / Solution.

Điều kiện: $5x + 4 \geq 0$ và $x + 8 \geq 0$, tức $x \geq -4/5$. Đặt $T = \sqrt{5x + 4} + \sqrt{x + 8}$. Với $x \geq -4/5$: $x + 8 \geq 36/5 > 4$ nên $\sqrt{x + 8} > 2$ và $T > 2$.

Domain: $5x + 4 \geq 0$ and $x + 8 \geq 0$, that is $x \geq -4/5$. Put $T = \sqrt{5x + 4} + \sqrt{x + 8}$. For $x \geq -4/5$ we have $x + 8 \geq 36/5 > 4$, so $\sqrt{x + 8} > 2$ and $T > 2$.

Theo (4.6): $\sqrt{5x + 4} - \sqrt{x + 8} = (5x + 4 - x - 8)/T = 4(x - 1)/T$. Chuyển mọi hạng tử sang một vế:

By (4.6): $\sqrt{5x + 4} - \sqrt{x + 8} = (5x + 4 - x - 8)/T = 4(x - 1)/T$. Moving everything to one side:

$$4(x-1)/T - 2(x-1) = 2(x-1)(2-T)/T = 0$$

Vì $T > 2$ nên $2 - T \neq 0$ và $T \neq 0$, do đó phương trình tương đương $x - 1 = 0$. Nghiệm $x = 1$ thỏa điều kiện; trong đề, vế trái là $3 - 3 = 0$ và vế phải là 0.

Since $T > 2$, we have $2 - T \neq 0$ and $T \neq 0$, so the equation is equivalent to $x - 1 = 0$. The root $x = 1$ satisfies the domain; in the original, the left side is $3 - 3 = 0$ and the right side is 0.

Vậy phương trình có nghiệm duy nhất $x = 1$.

Hence the equation has the single root $x = 1$. ■

PHÂN TÍCH / ANALYSIS — Vế trái là tổng hai căn có tổng hai biểu thức trong căn là hằng số $(x-2) + (4-x) = 2$. Khi đó Tính chất 4.8 chặn vế trái từ trên bằng một hằng số. Vế phải $x^2 - 6x + 11$ là tam thức bậc hai, đưa về bình phương cộng hằng số thì chặn được từ dưới. Nếu hai chặn gặp nhau thì mọi dấu bằng phải xảy ra đồng thời.

The left side is a sum of two roots whose radicands add to the constant $(x-2) + (4-x) = 2$. Property 4.8 then bounds it above by a constant. The right side $x^2 - 6x + 11$ is a quadratic; completing the square bounds it below. If the two bounds meet, every equality must hold at once.

VÍ DỤ 4.6 (Đánh giá hai vế) / EXAMPLE 4.6 (Estimating both sides) — Giải phương trình $\sqrt{x-2} + \sqrt{4-x} = x^2 - 6x + 11$.

Solve the equation $\sqrt{x-2} + \sqrt{4-x} = x^2 - 6x + 11$.

Lời giải. / Solution.

Điều kiện: $x - 2 \geq 0$ và $4 - x \geq 0$, tức $2 \leq x \leq 4$.

Domain: $x - 2 \geq 0$ and $4 - x \geq 0$, that is $2 \leq x \leq 4$.

Theo Tính chất 4.8 với $a = x - 2$, $b = 4 - x$: $(\sqrt{x-2} + \sqrt{4-x})^2 \leq 2((x-2) + (4-x)) = 4$, nên vế trái ≤ 2 , dấu bằng khi $x - 2 = 4 - x$, tức $x = 3$.

By Property 4.8 with $a = x - 2$, $b = 4 - x$: $(\sqrt{x-2} + \sqrt{4-x})^2 \leq 2((x-2) + (4-x)) = 4$, so the left side is ≤ 2 , with equality when $x - 2 = 4 - x$, that is $x = 3$.

Vế phải: $x^2 - 6x + 11 = (x-3)^2 + 2 \geq 2$, dấu bằng khi $x = 3$.

Right side: $x^2 - 6x + 11 = (x-3)^2 + 2 \geq 2$, with equality when $x = 3$.

Hai vế bằng nhau chỉ khi cùng bằng 2, tức đồng thời đạt dấu bằng, nghĩa là $x = 3$. Kiểm tra: $\sqrt{1} + \sqrt{1} = 2$ và $9 - 18 + 11 = 2$. Vậy phương trình có nghiệm duy nhất $x = 3$.

The two sides are equal only when both equal 2, that is when both equalities hold, which means $x = 3$. Check: $\sqrt{1} + \sqrt{1} = 2$ and $9 - 18 + 11 = 2$. Hence the equation has the single root $x = 3$.

■

NHẬN XÉT / REMARK — Khi bình phương, mỗi lần bình phương cần ghi dấu của hai vế. Ở Ví dụ 4.3 vế phải dương nên mọi bước là tương đương; nếu vế phải có thể âm, phương trình sau bình phương chỉ là hệ quả và bắt buộc thử nghiệm lại vào đề gốc.

Each time you square, record the signs of both sides. In Example 4.3 the right side is positive, so every step is an equivalence; if the right side can be negative, the squared equation is only a consequence and roots must be tested in the original equation.

LỖI HAY GẶP / COMMON MISTAKE — Bình phương hai vế rồi quên điều kiện vế còn lại không âm: $x = -3$ là nghiệm ngoại lai của $\sqrt{x+7} = x+1$ vì vế phải bằng -2 . Kết luận mà không thử lại là mất điểm.

Squaring and forgetting that the other side must be non-negative: $x = -3$ is extraneous for $\sqrt{x+7} = x+1$ because the right side equals -2 . Concluding without testing loses marks.

4.4. Phương trình bậc cao: đối xứng, hồi quy và đặt ẩn — Higher-degree equations: symmetric, reciprocal and grouped substitution

Phương trình bậc ba trở lên chỉ giải được bằng kỹ thuật sơ cấp khi có cấu trúc. Ba cấu trúc hay gặp: các nghiệm đi theo cặp nghịch đảo (hồi quy), các thừa số ghép được thành hai nhóm cùng một biểu thức, và dạng trùng phương.

A cubic or higher-degree equation yields to elementary methods only when it has structure. Three structures are common: roots in reciprocal pairs (reciprocal equations), factors that group into two blocks sharing one expression, and biquadratic forms.

BỔ ĐỀ 4.9 (Bất đẳng thức $x + 1/x$) / LEMMA 4.9 (The inequality $x + 1/x$) — Với $x \neq 0$ ta có $|x + 1/x| \geq 2$, dấu bằng khi và chỉ khi $x = 1$ hoặc $x = -1$. Với số thực t , phương trình $x + 1/x = t$ có nghiệm thực khi và chỉ khi $|t| \geq 2$; khi $|t| > 2$ có hai nghiệm phân biệt có tích bằng 1, khi $|t| = 2$ có nghiệm kép $x = t/2$.

For $x \neq 0$, $|x + 1/x| \geq 2$, with equality if and only if $x = 1$ or $x = -1$. For real t , the equation $x + 1/x = t$ has a real solution if and only if $|t| \geq 2$; for $|t| > 2$ it has two distinct roots with product 1, and for $|t| = 2$ a double root $x = t/2$.

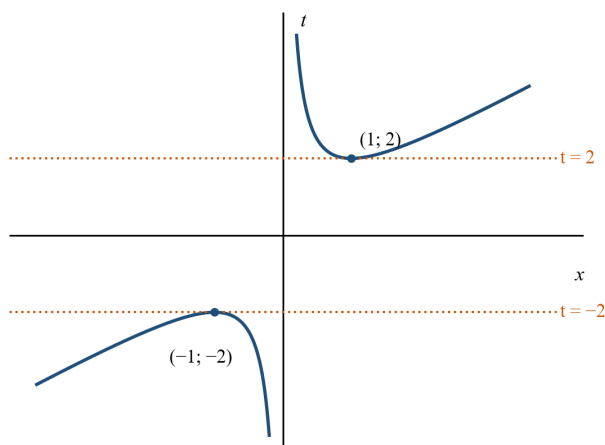
Chứng minh. / Proof.

Nhân phương trình $x + 1/x = t$ với $x \neq 0$: $x^2 - tx + 1 = 0$, biệt thức $t^2 - 4$. Phương trình có nghiệm thực khi và chỉ khi $t^2 \geq 4$, tức $|t| \geq 2$. Theo Viète, tích hai nghiệm bằng 1; khi $t^2 = 4$ nghiệm kép là $x = t/2 \in \{1, -1\}$.

Multiply $x + 1/x = t$ by $x \neq 0$: $x^2 - tx + 1 = 0$, with discriminant $t^2 - 4$. It has a real root if and only if $t^2 \geq 4$, that is $|t| \geq 2$. By Viète the product of the roots is 1; when $t^2 = 4$ the double root is $x = t/2 \in \{1, -1\}$.

Mọi $x \neq 0$ cho một giá trị $t = x + 1/x$ mà phương trình có nghiệm x , nên $|t| \geq 2$: đó là bất đẳng thức đã nêu.

Every $x \neq 0$ gives a value $t = x + 1/x$ for which the equation has the root x , so $|t| \geq 2$: this is the stated inequality. ■



Hình 4.4. Đồ thị $t = x + 1/x$: không có điểm nào trong dải $-2 < t < 2$, nên phương trình hồi quy theo t chỉ nhận nghiệm t với $|t| \geq 2$.

Figure 4.4. The graph of $t = x + 1/x$: no point lies in the strip $-2 < t < 2$, so a reciprocal equation in t admits only roots with $|t| \geq 2$.

ĐỊNH LÝ 4.10 (Phương trình hồi quy bậc bốn) / THEOREM 4.10 (Reciprocal quartic)

— Phương trình hồi quy bậc bốn $ax^4 + bx^3 + cx^2 + bx + a = 0$ ($a \neq 0$) không nhận $x = 0$ làm nghiệm. Đặt $t = x + 1/x$, phương trình tương đương $at^2 + bt + c - 2a = 0$ với điều kiện $|t| \geq 2$. Mỗi nghiệm t với $|t| > 2$ cho hai nghiệm x nghịch đảo nhau; mỗi nghiệm $t = \pm 2$ cho nghiệm $x = \pm 1$.

The reciprocal quartic $ax^4 + bx^3 + cx^2 + bx + a = 0$ ($a \neq 0$) does not have $x = 0$ as a root. With $t = x + 1/x$ the equation is equivalent to $at^2 + bt + c - 2a = 0$ under the condition $|t| \geq 2$. Each root t with $|t| > 2$ gives two reciprocal roots x ; each root $t = \pm 2$ gives $x = \pm 1$.

Chứng minh. / Proof.

Thay $x = 0$ cho $a = 0$, trái giả thiết. Với $x \neq 0$ chia hai vế cho x^2 :

Substituting $x = 0$ gives $a = 0$, contrary to the hypothesis. For $x \neq 0$ divide by x^2 :

$$a(x^2 + 1/x^2) + b(x + 1/x) + c = 0 \quad (4.7)$$

Vì $x^2 + 1/x^2 = (x + 1/x)^2 - 2 = t^2 - 2$, ta được $a(t^2 - 2) + bt + c = 0$, tức $at^2 + bt + c - 2a = 0$. Theo Bổ đề 4.9, mỗi t với $|t| \geq 2$ ứng với nghiệm x của $x + 1/x = t$, còn mỗi t với $|t| < 2$ không ứng với x thực nào.

Since $x^2 + 1/x^2 = (x + 1/x)^2 - 2 = t^2 - 2$, we get $a(t^2 - 2) + bt + c = 0$, that is $at^2 + bt + c - 2a = 0$. By Lemma 4.9 each t with $|t| \geq 2$ corresponds to roots x of $x + 1/x = t$, while each t with $|t| < 2$ corresponds to no real x . ■

PHÂN TÍCH / ANALYSIS — Hệ số 2, 3, -16, 3, 2 đối xứng qua giữa. Đó là dấu hiệu duy nhất cần để chia cho x^2 và đặt $t = x + 1/x$. Sau khi giải theo t , đừng quên bước hai: giải $x + 1/x = t$, và kiểm tra $|t| \geq 2$.

The coefficients 2, 3, -16, 3, 2 are symmetric about the middle. That is the only sign needed to divide by x^2 and put $t = x + 1/x$. After solving for t , do not forget the second step: solve $x + 1/x = t$ and check $|t| \geq 2$.

VÍ DỤ 4.7 (Phương trình hồi quy) / EXAMPLE 4.7 (Reciprocal equation) — Giải phương trình $2x^4 + 3x^3 - 16x^2 + 3x + 2 = 0$.
Solve the equation $2x^4 + 3x^3 - 16x^2 + 3x + 2 = 0$.

Lời giải. / Solution.

$x = 0$ không là nghiệm (vế trái bằng 2). Chia hai vế cho x^2 và đặt $t = x + 1/x$ theo Định lý 4.10: $2(t^2 - 2) + 3t - 16 = 0$, tức $2t^2 + 3t - 20 = 0$.

$x = 0$ is not a root (the left side equals 2). Divide by x^2 and put $t = x + 1/x$ as in Theorem 4.10: $2(t^2 - 2) + 3t - 16 = 0$, that is $2t^2 + 3t - 20 = 0$.

Biệt thức $9 + 160 = 169 = 13^2$, nên $t = (-3 + 13)/4 = 5/2$ hoặc $t = (-3 - 13)/4 = -4$. Cả hai thỏa $|t| \geq 2$.

The discriminant is $9 + 160 = 169 = 13^2$, so $t = (-3 + 13)/4 = 5/2$ or $t = (-3 - 13)/4 = -4$. Both satisfy $|t| \geq 2$.

Với $t = 5/2$: $x^2 - (5/2)x + 1 = 0$, tức $2x^2 - 5x + 2 = 0$, nghiệm $x = 2$ và $x = 1/2$. Với $t = -4$: $x^2 + 4x + 1 = 0$, nghiệm $x = -2 \pm \sqrt{3}$.

For $t = 5/2$: $x^2 - (5/2)x + 1 = 0$, that is $2x^2 - 5x + 2 = 0$, with roots $x = 2$ and $x = 1/2$. For $t = -4$: $x^2 + 4x + 1 = 0$, with roots $x = -2 \pm \sqrt{3}$.

Vậy tập nghiệm là $\{2; 1/2; -2 + \sqrt{3}; -2 - \sqrt{3}\}$.

Hence the solution set is $\{2, 1/2, -2 + \sqrt{3}, -2 - \sqrt{3}\}$. ■

NHẬN XÉT / REMARK — Nghiệm của phương trình hồi quy đi theo cặp $(x; 1/x)$. Ở Ví dụ 4.7 các cặp là $(2; 1/2)$ và $(-2 + \sqrt{3}; -2 - \sqrt{3})$, vì $(-2 + \sqrt{3})(-2 - \sqrt{3}) = 4 - 3 = 1$. Quan sát này cho cách kiểm tra nghiệm nhanh.

The roots of a reciprocal equation come in pairs $(x, 1/x)$. In Example 4.7 the pairs are $(2, 1/2)$ and $(-2 + \sqrt{3}, -2 - \sqrt{3})$, since $(-2 + \sqrt{3})(-2 - \sqrt{3}) = 4 - 3 = 1$. This observation gives a fast check on the roots.

NHẬN XÉT / REMARK — Khi bốn thừa số bậc nhất có tổng hai cặp bằng nhau, ghép chúng thành hai nhóm cùng phần $x^2 + kx$. Ví dụ $(x + 1)(x + 2)(x + 4)(x + 5)$: ghép $(x + 1)(x + 5) = x^2 + 6x + 5$ và $(x + 2)(x + 4) = x^2 + 6x + 8$, rồi đặt $y = x^2 + 6x$. Điều kiện $y \geq -9$ (vì $y = (x + 3)^2 - 9$) phải được giữ khi kết luận.

When four linear factors can be paired with equal sums, group them into two blocks sharing the part $x^2 + kx$. For $(x + 1)(x + 2)(x + 4)(x + 5)$: pair $(x + 1)(x + 5) = x^2 + 6x + 5$ and $(x + 2)(x + 4) = x^2 + 6x + 8$, then put $y = x^2 + 6x$. The condition $y \geq -9$ (because $y = (x + 3)^2 - 9$) must be kept when concluding.

LỖI HAY GẶP / COMMON MISTAKE — Đặt $t = x + 1/x$ rồi giải ra $t = 1$ và coi như xong: phương trình $x + 1/x = 1$ vô nghiệm thực vì $|1| < 2$. Mọi giá trị t phải được kiểm tra điều kiện $|t| \geq 2$ trước khi quay lại biến x .

Putting $t = x + 1/x$, finding $t = 1$ and stopping: $x + 1/x = 1$ has no real solution because $|1| < 2$. Every value of t must be tested against $|t| \geq 2$ before returning to x .

PHẢI THUỘC / MEMORISE — Phương trình hồi quy bậc bốn: chia x^2 , đặt $t = x + 1/x$, rồi giải $x + 1/x = t$ chỉ khi $|t| \geq 2$. Hai nghiệm cùng t có tích bằng 1.

Reciprocal quartic: divide by x^2 , put $t = x + 1/x$, then solve $x + 1/x = t$ only when $|t| \geq 2$. Two roots sharing the same t have product 1.

4.5. Hệ phương trình: đối xứng, đẳng cấp, bậc nhất ba ẩn — *Systems: symmetric, homogeneous, linear in three unknowns*

Hệ đối xứng loại I — *Symmetric systems of type I*

Hệ gồm các phương trình không đổi khi hoán vị x và y gọi là hệ đối xứng loại I. Các tổng $x^2 + y^2$, $x^3 + y^3$, $x^4 + y^4$ đều biểu diễn được qua $S = x + y$ và $P = xy$:

A system whose equations do not change when x and y are swapped is a symmetric system of type I. The sums $x^2 + y^2$, $x^3 + y^3$, $x^4 + y^4$ can all be written with $S = x + y$ and $P = xy$:

$$x^2 + y^2 = S^2 - 2P, \quad x^3 + y^3 = S^3 - 3SP, \quad x^4 + y^4 = S^4 - 4S^2P + 2P^2 \quad (4.8)$$

ĐỊNH LÝ 4.11 (Hệ đối xứng loại I) / THEOREM 4.11 (Symmetric system of type I) —

Cho hệ hai phương trình đối xứng theo x, y , viết được thành hệ (H) theo $S = x + y$ và $P = xy$. Khi đó $(x; y)$ là nghiệm thực của hệ ban đầu khi và chỉ khi $(S; P) = (x + y; xy)$ là nghiệm của (H) với $S^2 \geq 4P$. Với mỗi nghiệm $(S; P)$ của (H) thỏa $S^2 \geq 4P$, hai số x, y là hai nghiệm của $X^2 - SX + P = 0$, và hệ ban đầu nhận $(x; y)$ và $(y; x)$.

Let a pair of equations symmetric in x, y be rewritten as a system (H) in $S = x + y$ and $P = xy$. Then (x, y) is a real solution of the original system if and only if $(S, P) = (x + y, xy)$ solves (H) with $S^2 \geq 4P$.

For each solution (S, P) of (H) with $S^2 \geq 4P$, the numbers x, y are the two roots of $X^2 - SX + P = 0$, and the original system has both (x, y) and (y, x) .

Chứng minh. / *Proof.*

Nếu $(x; y)$ là nghiệm thực thì $S = x + y$, $P = xy$ thỏa (H), và hai số thực x, y có tổng S , tích P nên $S^2 \geq 4P$ theo Định lý 4.5.

If (x, y) is a real solution then $S = x + y$, $P = xy$ satisfy (H), and the real numbers x, y have sum S and product P , so $S^2 \geq 4P$ by Theorem 4.5.

Ngược lại, nếu $(S; P)$ thỏa (H) và $S^2 \geq 4P$ thì $X^2 - SX + P = 0$ có hai nghiệm thực, gọi là x, y ; theo Viète $x + y = S$, $xy = P$, và vì hệ ban đầu chỉ phụ thuộc S, P nên $(x; y)$ thỏa nó. Hoán vị x, y không đổi S, P nên $(y; x)$ cũng là nghiệm.

Conversely, if (S, P) satisfies (H) and $S^2 \geq 4P$ then $X^2 - SX + P = 0$ has two real roots, call them x and y ; by Viète $x + y = S$ and $xy = P$, and since the original system depends only on S and P , (x, y) satisfies it. Swapping x and y leaves S and P unchanged, so (y, x) is also a solution. ■

VÍ DỤ 4.8 (Hệ đối xứng loại I) / EXAMPLE 4.8 (Symmetric system of type I) — Giải hệ

$x + y + xy = 11$ và $x^2 + y^2 + x + y = 32$.

Solve the system $x + y + xy = 11$ and $x^2 + y^2 + x + y = 32$.

Lời giải. / *Solution.*

Đặt $S = x + y$, $P = xy$. Theo (4.8) hệ thành $S + P = 11$ và $S^2 - 2P + S = 32$. Thế $P = 11 - S$: $S^2 - 22 + 2S + S = 32$, tức $S^2 + 3S - 54 = 0$, hay $(S - 6)(S + 9) = 0$.

Put $S = x + y$, $P = xy$. By (4.8) the system becomes $S + P = 11$ and $S^2 - 2P + S = 32$. Substituting $P = 11 - S$: $S^2 - 22 + 2S + S = 32$, that is $S^2 + 3S - 54 = 0$, or $(S - 6)(S + 9) = 0$.

Với $S = 6, P = 5$: $S^2 - 4P = 16 \geq 0, X^2 - 6X + 5 = 0$ cho $X = 1$ hoặc $X = 5$, được $(1; 5)$ và $(5; 1)$.

For $S = 6, P = 5$: $S^2 - 4P = 16 \geq 0, X^2 - 6X + 5 = 0$ gives $X = 1$ or $X = 5$, so $(1, 5)$ and $(5, 1)$.

Với $S = -9, P = 20$: $S^2 - 4P = 81 - 80 = 1 \geq 0, X^2 + 9X + 20 = 0$ cho $X = -4$ hoặc $X = -5$, được $(-4; -5)$ và $(-5; -4)$.

For $S = -9, P = 20$: $S^2 - 4P = 81 - 80 = 1 \geq 0, X^2 + 9X + 20 = 0$ gives $X = -4$ or $X = -5$, so $(-4, -5)$ and $(-5, -4)$.

Vậy hệ có bốn nghiệm $(1; 5), (5; 1), (-4; -5), (-5; -4)$.

Hence the system has four solutions $(1, 5), (5, 1), (-4, -5), (-5, -4)$. ■

Hệ đối xứng loại II — Symmetric systems of type II

TÍNH CHẤT 4.12 (Hệ đối xứng loại II) / PROPERTY 4.12 (Symmetric system of type II) — Hệ $F(x, y) = 0, F(y, x) = 0$ (loại II) tương đương với hệ $F(x, y) = 0, F(x, y) - F(y, x) = 0$. Với F là đa thức, $G(x, y) = F(x, y) - F(y, x)$ chia hết cho $x - y$; hệ tách thành hai trường hợp $x = y$ và $G(x, y)/(x - y) = 0$.

The system $F(x, y) = 0, F(y, x) = 0$ (type II) is equivalent to $F(x, y) = 0, F(x, y) - F(y, x) = 0$. For a polynomial F , $G(x, y) = F(x, y) - F(y, x)$ is divisible by $x - y$, so the system splits into the cases $x = y$ and $G(x, y)/(x - y) = 0$.

Chứng minh. / Proof.

Tương đương: nếu $F(x, y) = 0$ thì $F(y, x) = 0$ khi và chỉ khi $F(x, y) - F(y, x) = 0$.

Equivalence: if $F(x, y) = 0$ then $F(y, x) = 0$ if and only if $F(x, y) - F(y, x) = 0$.

Chia hết: viết $F(x, y) = \sum c_{ij}x^i y^j$. Khi đó $G(x, y) = \sum c_{ij}(x^i y^j - x^j y^i)$. Số hạng $i = j$ bằng 0. Với $i \neq j$, đặt $m = \min(i, j), k = |i - j|$: $x^i y^j - x^j y^i = \pm x^m y^m (x^k - y^k)$, và $x^k - y^k = (x - y)(x^{k-1} + x^{k-2}y + \dots + y^{k-1})$. Vậy mỗi số hạng, nên cả G , chia hết cho $x - y$.

Divisibility: write $F(x, y) = \sum c_{ij}x^i y^j$. Then $G(x, y) = \sum c_{ij}(x^i y^j - x^j y^i)$. Terms with $i = j$ vanish. For $i \neq j$ put $m = \min(i, j), k = |i - j|$: $x^i y^j - x^j y^i = \pm x^m y^m (x^k - y^k)$, and $x^k - y^k = (x - y)(x^{k-1} + x^{k-2}y + \dots + y^{k-1})$. So every term, hence G , is divisible by $x - y$. ■

PHÂN TÍCH / ANALYSIS — Hai phương trình hoán đổi cho nhau khi đổi x và y . Trừ vế cho vế thì các hạng tử đối xứng triệt tiêu, còn lại tích $(x - y)(x + y + 3)$ theo Tính chất 4.12. Hai nhân tử cho hai nhánh: $x = y$ đưa về một ẩn, $x + y = -3$ cho phép thế y .

The two equations swap when x and y are exchanged. Subtracting them cancels the symmetric terms, leaving the product $(x - y)(x + y + 3)$ by Property 4.12. The two factors give two branches: $x = y$ reduces to one unknown, $x + y = -3$ lets us substitute for y .

VÍ DỤ 4.9 (Hệ đối xứng loại II) / EXAMPLE 4.9 (Symmetric system of type II) — Giải hệ $x^2 + x = 2y + 6$ và $y^2 + y = 2x + 6$.

Solve the system $x^2 + x = 2y + 6$ and $y^2 + y = 2x + 6$.

Lời giải. / Solution.

Trừ vế cho vế: $x^2 - y^2 + x - y = 2y - 2x$, tức $(x - y)(x + y) + 3(x - y) = 0$, hay $(x - y)(x + y + 3) = 0$.

Subtracting: $x^2 - y^2 + x - y = 2y - 2x$, that is $(x - y)(x + y) + 3(x - y) = 0$, or $(x - y)(x + y + 3) = 0$.

Trường hợp $x = y$: $x^2 + x = 2x + 6$, tức $x^2 - x - 6 = 0$, nghiệm $x = 3$ hoặc $x = -2$. Được $(3; 3)$ và $(-2; -2)$.

Case $x = y$: $x^2 + x = 2x + 6$, that is $x^2 - x - 6 = 0$, with $x = 3$ or $x = -2$. This gives $(3, 3)$ and $(-2, -2)$.

Trường hợp $y = -3 - x$: thế vào phương trình đầu, $x^2 + x = 2(-3 - x) + 6 = -2x$, tức $x^2 + 3x = 0$, nghiệm $x = 0$ ($y = -3$) hoặc $x = -3$ ($y = 0$). Được $(0; -3)$ và $(-3; 0)$.

Case $y = -3 - x$: substituting into the first equation, $x^2 + x = 2(-3 - x) + 6 = -2x$, that is $x^2 + 3x = 0$, with $x = 0$ ($y = -3$) or $x = -3$ ($y = 0$). This gives $(0, -3)$ and $(-3, 0)$.

Vì hệ ban đầu tương đương với phương trình đầu cùng hiệu hai phương trình, mỗi cặp tìm được thỏa cả hai phương trình; chẳng hạn $(0; -3)$: $0 = -6 + 6$ và $9 - 3 = 6 = 0 + 6$. Vậy hệ có bốn nghiệm $(3; 3)$, $(-2; -2)$, $(0; -3)$, $(-3; 0)$.

Since the original system is equivalent to the first equation together with the difference, each pair found satisfies both equations; for instance $(0, -3)$: $0 = -6 + 6$ and $9 - 3 = 6 = 0 + 6$. Hence the system has four solutions $(3, 3)$, $(-2, -2)$, $(0, -3)$, $(-3, 0)$. ■

Hệ đẳng cấp — Homogeneous systems

Nếu một phương trình của hệ chỉ gồm các hạng tử cùng bậc (không có hạng tử tự do hay bậc thấp hơn) thì nó phân tích được thành nhân tử hoặc cho tỉ số $x : y$. Khi cả hai phương trình đều có vế phải khác 0, lấy $d_2 \cdot (\text{phương trình 1}) - d_1 \cdot (\text{phương trình 2})$ để triệt hằng số, ra một phương trình đẳng cấp.

If one equation of the system consists only of terms of the same degree (no constant or lower-degree term) it factors, or gives the ratio $x : y$. When both right-hand sides are non-zero, take $d_2 \cdot (\text{equation 1}) - d_1 \cdot (\text{equation 2})$ to cancel the constants and obtain a homogeneous equation.

PHÂN TÍCH / ANALYSIS — Phương trình đầu không có hạng tử tự do và mọi hạng tử bậc hai, nên là tam thức bậc hai theo x/y . Phân tích $x^2 - 5xy + 6y^2 = (x - 2y)(x - 3y)$ cho hai tỉ số. Mỗi tỉ số thế vào phương trình thứ hai cho một phương trình một ẩn.

The first equation has no constant term and all terms are of degree two, so it is a quadratic in x/y .

Factoring $x^2 - 5xy + 6y^2 = (x - 2y)(x - 3y)$ gives two ratios. Each ratio substituted into the second equation gives an equation in one unknown.

VÍ DỤ 4.10 (Hệ đẳng cấp) / EXAMPLE 4.10 (Homogeneous system) — Giải hệ $x^2 - 5xy + 6y^2 = 0$ và $x^2 + y^2 = 20$.

Solve the system $x^2 - 5xy + 6y^2 = 0$ and $x^2 + y^2 = 20$.

Lời giải. / Solution.

Phương trình đầu: $(x - 2y)(x - 3y) = 0$, nên $x = 2y$ hoặc $x = 3y$.

First equation: $(x - 2y)(x - 3y) = 0$, so $x = 2y$ or $x = 3y$.

Nếu $x = 2y$: $4y^2 + y^2 = 20$, $y^2 = 4$, $y = \pm 2$. Được $(4; 2)$ và $(-4; -2)$.

If $x = 2y$: $4y^2 + y^2 = 20$, $y^2 = 4$, $y = \pm 2$. This gives $(4, 2)$ and $(-4, -2)$.

Nếu $x = 3y$: $9y^2 + y^2 = 20$, $y^2 = 2$, $y = \pm\sqrt{2}$. Được $(3\sqrt{2}; \sqrt{2})$ và $(-3\sqrt{2}; -\sqrt{2})$.

If $x = 3y$: $9y^2 + y^2 = 20$, $y^2 = 2$, $y = \pm\sqrt{2}$. This gives $(3\sqrt{2}, \sqrt{2})$ and $(-3\sqrt{2}, -\sqrt{2})$.

Vậy hệ có bốn nghiệm $(4; 2)$, $(-4; -2)$, $(3\sqrt{2}; \sqrt{2})$, $(-3\sqrt{2}; -\sqrt{2})$.

Hence the system has four solutions $(4, 2)$, $(-4, -2)$, $(3\sqrt{2}, \sqrt{2})$, $(-3\sqrt{2}, -\sqrt{2})$. ■

Hệ bậc nhất ba ẩn: phép khử Gauss — *Linear systems in three unknowns: Gaussian elimination*

TÍNH CHẤT 4.13 (Phép khử Gauss) / PROPERTY 4.13 (Gaussian elimination) — Ba phép biến đổi sau không làm thay đổi tập nghiệm của hệ phương trình tuyến tính: (1) đổi chỗ hai phương trình; (2) nhân một phương trình với số khác 0; (3) cộng vào một phương trình một bội của phương trình khác.

The following three operations do not change the solution set of a linear system: (1) swapping two equations; (2) multiplying an equation by a non-zero number; (3) adding to one equation a multiple of another.

Chứng minh. / Proof.

Mỗi phép đều làm cho nghiệm cũ vẫn là nghiệm của hệ mới: đổi chỗ không đổi tập phương trình; nhân với $c \neq 0$ thì cả hai vế cùng được nhân với c ; cộng bội thì cộng hai đẳng thức đúng cho đẳng thức đúng. Mỗi phép có phép ngược cùng loại (đổi chỗ lần nữa, nhân với $1/c$, trừ cùng bội), nên nghiệm của hệ mới cũng là nghiệm của hệ cũ.

Each operation keeps every old solution a solution of the new system: swapping leaves the set of equations unchanged; multiplying by $c \neq 0$ multiplies both sides by c ; adding a multiple adds true equalities to true equalities. Each has an inverse operation of the same kind (swap again, multiply by $1/c$, subtract the same multiple), so every solution of the new system is also a solution of the old one. ■

VÍ DỤ 4.11 (Khử Gauss ba ẩn) / EXAMPLE 4.11 (Gaussian elimination in three unknowns) — Giải hệ $x + 2y + z = 3$, $2x - y + z = 8$, $3x + y - 2z = -1$.

Solve the system $x + 2y + z = 3$, $2x - y + z = 8$, $3x + y - 2z = -1$.

Lời giải. / Solution.

Ký hiệu ba phương trình là (E1), (E2), (E3). Khử x : (E2) $- 2$ (E1) cho $-5y - z = 2$; (E3) $- 3$ (E1) cho $-5y - 5z = -10$, tức $y + z = 2$.

Call the equations (E1), (E2), (E3). Eliminate x : (E2) $- 2$ (E1) gives $-5y - z = 2$; (E3) $- 3$ (E1) gives $-5y - 5z = -10$, that is $y + z = 2$.

Cộng $-5y - z = 2$ với $y + z = 2$ được $-4y = 4$, nên $y = -1$, rồi $z = 2 - y = 3$.

Adding $-5y - z = 2$ and $y + z = 2$ gives $-4y = 4$, so $y = -1$, and then $z = 2 - y = 3$.

Từ (E1): $x = 3 - 2y - z = 3 + 2 - 3 = 2$. Theo Tính chất 4.13 các phép đã dùng bảo toàn tập nghiệm, nên nghiệm duy nhất là $(2; -1; 3)$. Thử lại: $2 - 2 + 3 = 3$, $4 + 1 + 3 = 8$, $6 - 1 - 6 = -1$.

From (E1): $x = 3 - 2y - z = 3 + 2 - 3 = 2$. By Property 4.13 the operations used preserve the solution set, so the unique solution is $(2, -1, 3)$. Back-substitution: $2 - 2 + 3 = 3$, $4 + 1 + 3 = 8$, $6 - 1 - 6 = -1$.

Vậy $(x; y; z) = (2; -1; 3)$.

Hence $(x, y, z) = (2, -1, 3)$. ■

NHẬN XÉT / REMARK — Hệ ba phương trình bậc nhất ba ẩn có thể vô nghiệm hoặc vô số nghiệm: khi khử xong gặp $0 = c$ với $c \neq 0$ thì vô nghiệm; gặp $0 = 0$ thì còn một ẩn tự do. Khi hệ có tham số, đừng chia cho biểu thức chứa tham số trước khi xét trường hợp nó bằng 0.

A system of three linear equations in three unknowns may have no solution or infinitely many: reaching $0 = c$ with $c \neq 0$ means no solution, reaching $0 = 0$ leaves a free unknown. With a parameter, do not divide by an expression containing it before treating the case where it equals 0.

Hệ giải bằng đánh giá — Systems solved by estimation

Khi các phương trình cho hai đại lượng liên hệ chặt, một bất đẳng thức ép các biến bằng nhau. Với ba số thực x, y, z :

When the equations tie two quantities tightly, an inequality forces the variables to be equal. For three real numbers x, y, z :

$$(x - y)^2 + (y - z)^2 + (z - x)^2 = 2(x^2 + y^2 + z^2) - 2(xy + yz + zx) \quad (4.9)$$

Nếu hệ cho $x + y + z = 6$ và $xy + yz + zx = 12$ thì $x^2 + y^2 + z^2 = 36 - 24 = 12$ và vế phải của (4.9) bằng $24 - 24 = 0$. Tổng ba bình phương bằng 0 nên $x = y = z$, và $3x = 6$ cho $x = y = z = 2$.

If a system gives $x + y + z = 6$ and $xy + yz + zx = 12$ then $x^2 + y^2 + z^2 = 36 - 24 = 12$ and the right side of (4.9) equals $24 - 24 = 0$. A sum of three squares equal to 0 forces $x = y = z$, and $3x = 6$ gives $x = y = z = 2$.

LỖI HAY GẶP / COMMON MISTAKE — Giải hệ đối xứng loại I mà quên điều kiện $S^2 \geq 4P$: cặp $(S; P)$ tìm được có thể không ứng với số thực nào. Ví dụ $S = 1, P = 1$ cho $X^2 - X + 1 = 0$ vô nghiệm thực.

Solving a type I symmetric system and forgetting the condition $S^2 \geq 4P$: a pair (S, P) found may correspond to no real numbers. For instance $S = 1, P = 1$ gives $X^2 - X + 1 = 0$, which has no real root.

4.6. Hàm đơn điệu và phương trình $f(u) = f(v)$ — Monotone functions and the equation $f(u) = f(v)$

Lớp 10 chưa có đạo hàm, nên tính đơn điệu luôn được chứng minh trực tiếp từ định nghĩa. Với những hàm quen thuộc, phép chứng minh chỉ là một lần phân tích hiệu $f(v) - f(u)$ thành nhân tử.

Grade 10 has no derivative, so monotonicity is always proved directly from the definition. For familiar functions the proof is a single factorisation of the difference $f(v) - f(u)$.

ĐỊNH NGHĨA 4.14 (Hàm đơn điệu) / DEFINITION 4.14 (Monotone function) — Hàm số f xác định trên khoảng (hoặc đoạn, nửa khoảng) I gọi là đồng biến trên I nếu với mọi $u, v \in I$ mà $u < v$ thì $f(u) < f(v)$; gọi là nghịch biến trên I nếu $u < v$ kéo theo $f(u) > f(v)$. Đồng biến hoặc nghịch biến gọi chung là đơn điệu.

A function f defined on an interval I is increasing on I if $u < v$ in I implies $f(u) < f(v)$; it is decreasing on I if $u < v$ implies $f(u) > f(v)$. Increasing or decreasing is called monotone.

ĐỊNH LÝ 4.15 (Hàm đơn điệu là đơn ánh) / THEOREM 4.15 (A monotone function is injective) — Cho f đồng biến trên I và $u, v \in I$. Khi đó $f(u) = f(v)$ khi và chỉ khi $u = v$; $f(u) < f(v)$ khi và chỉ khi $u < v$; $f(u) \leq f(v)$ khi và chỉ khi $u \leq v$. Với f nghịch biến, hai bất đẳng thức sau đổi chiều.

Let f be increasing on I and $u, v \in I$. Then $f(u) = f(v)$ if and only if $u = v$; $f(u) < f(v)$ if and only if $u < v$; $f(u) \leq f(v)$ if and only if $u \leq v$. For f decreasing, the last two inequalities reverse.

Chứng minh. / Proof.

Giả sử $u \neq v$, chẳng hạn $u < v$. Vì f đồng biến, $f(u) < f(v)$, nên $f(u) \neq f(v)$. Vậy $f(u) = f(v)$ chỉ xảy ra khi $u = v$; chiều ngược lại hiển nhiên.

Suppose $u \neq v$, say $u < v$. Since f is increasing, $f(u) < f(v)$, so $f(u) \neq f(v)$. Thus $f(u) = f(v)$ happens only when $u = v$; the converse is clear.

Với bất đẳng thức: $u < v \Rightarrow f(u) < f(v)$ theo định nghĩa. Nếu $f(u) < f(v)$ mà $u \geq v$ thì hoặc $u = v$, cho $f(u) = f(v)$, hoặc $u > v$, cho $f(u) > f(v)$; cả hai đều mâu thuẫn. Vậy $u < v$. Trường hợp $\leq$ ghép hai kết quả trên.

For the inequalities: $u < v \Rightarrow f(u) < f(v)$ by definition. If $f(u) < f(v)$ but $u \geq v$ then either $u = v$, giving $f(u) = f(v)$, or $u > v$, giving $f(u) > f(v)$; both are contradictions. So $u < v$. The case $\leq$ combines the two results. ■

Đẳng thức sau dùng cho các hàm lũy thừa lẻ:

The following identity serves the odd powers:

$$v^3 - u^3 = (v - u)(v^2 + uv + u^2), \quad v^2 + uv + u^2 = (v + u/2)^2 + 3u^2/4 \quad (4.10)$$

TÍNH CHẤT 4.16 / PROPERTY 4.16 — (a) Tổng hai hàm đồng biến trên I là hàm đồng biến trên I . (b) Hợp của hai hàm đồng biến là hàm đồng biến. (c) Các hàm t^3 và $t^3 + kt$ ($k \geq 0$) đồng biến trên $\mathbb{R}$, hàm $\sqrt{t}$ đồng biến trên $[0; +\infty)$.

(a) The sum of two increasing functions on I is increasing on I . (b) The composite of two increasing functions is increasing. (c) The functions t^3 and $t^3 + kt$ ($k \geq 0$) are increasing on $\mathbb{R}$, and the function $\sqrt{t}$ is increasing on $[0, +\infty)$.

Chứng minh. / Proof.

(a), (b) suy ngay từ định nghĩa: nếu $u < v$ thì $f(u) < f(v)$ và $g(u) < g(v)$, cộng lại; còn $g(f(u)) < g(f(v))$ vì $f(u) < f(v)$ và g đồng biến.

(a), (b) follow from the definition: if $u < v$ then $f(u) < f(v)$ and $g(u) < g(v)$, add them; and $g(f(u)) < g(f(v))$ because $f(u) < f(v)$ and g is increasing.

(c) Với $u < v$, theo (4.10) $v^3 - u^3 = (v - u)[(v + u/2)^2 + 3u^2/4]$. Thừa số đầu dương; thừa số sau không âm, và chỉ bằng 0 khi $u = 0$ và $v = -u/2 = 0$, mâu thuẫn $u < v$. Vậy $v^3 > u^3$. Hàm kt không giảm ($k \geq 0$), nên theo (a) tổng $t^3 + kt$ đồng biến.

(c) For $u < v$, by (4.10) $v^3 - u^3 = (v - u)[(v + u/2)^2 + 3u^2/4]$. The first factor is positive; the second is non-negative and vanishes only if $u = 0$ and $v = -u/2 = 0$, contradicting $u < v$. So $v^3 > u^3$. The function kt is non-decreasing ($k \geq 0$), so by (a) the sum $t^3 + kt$ is increasing.

Với $0 \leq u < v$: $\sqrt{v} - \sqrt{u} = (v - u)/(\sqrt{v} + \sqrt{u}) > 0$ theo (4.6).

For $0 \leq u < v$: $\sqrt{v} - \sqrt{u} = (v - u)/(\sqrt{v} + \sqrt{u}) > 0$ by (4.6). ■

PHÂN TÍCH / ANALYSIS — Vế trái $(2x - 1)^3 + (2x - 1)$ có dạng $t^3 + t$ với $t = 2x - 1$. Ở vế phải, $(3x - 1)\sqrt[3]{3x - 2}$: đặt $v = \sqrt[3]{3x - 2}$ thì $3x - 1 = v^2 + 1$, nên vế phải là $(v^2 + 1)v = v^3 + v$. Hai vế cùng dạng $f(t) = t^3 + t$, mà f đồng biến theo Tính chất 4.16, nên $t = v$.
The left side $(2x - 1)^3 + (2x - 1)$ has the form $t^3 + t$ with $t = 2x - 1$. On the right, $(3x - 1)\sqrt[3]{3x - 2}$: put $v = \sqrt[3]{3x - 2}$; then $3x - 1 = v^2 + 1$, so the right side is $(v^2 + 1)v = v^3 + v$. Both sides have the form $f(t) = t^3 + t$, and f is increasing by Property 4.16, so $t = v$.

VÍ DỤ 4.12 ($f(u) = f(v)$ với f đồng biến) / EXAMPLE 4.12 ($f(u) = f(v)$ with f increasing)

— Giải phương trình $(2x - 1)^3 + (2x - 1) = (3x - 1)\sqrt[3]{3x - 2}$.

Solve the equation $(2x - 1)^3 + (2x - 1) = (3x - 1)\sqrt[3]{3x - 2}$.

Lời giải. / Solution.

Điều kiện: $3x - 2 \geq 0$, tức $x \geq 2/3$. Đặt $v = \sqrt[3]{3x - 2} \geq 0$, khi đó $3x - 1 = v^2 + 1$ và vế phải bằng $(v^2 + 1)v = v^3 + v$.

Domain: $3x - 2 \geq 0$, that is $x \geq 2/3$. Put $v = \sqrt[3]{3x - 2} \geq 0$; then $3x - 1 = v^2 + 1$ and the right side equals $(v^2 + 1)v = v^3 + v$.

Với $f(t) = t^3 + t$, phương trình là $f(2x - 1) = f(v)$. Theo Tính chất 4.16 f đồng biến trên $\mathbb{R}$, nên theo Định lý 4.15, $2x - 1 = v = \sqrt[3]{3x - 2}$.

With $f(t) = t^3 + t$ the equation reads $f(2x - 1) = f(v)$. By Property 4.16 f is increasing on $\mathbb{R}$, so by Theorem 4.15, $2x - 1 = v = \sqrt[3]{3x - 2}$.

Theo Bổ đề 4.7 (a) phương trình này tương đương $2x - 1 \geq 0$ và $(2x - 1)^2 = 3x - 2$, tức $x \geq 1/2$ và $4x^2 - 7x + 3 = 0$. Phương trình bậc hai có nghiệm $x = 1$ và $x = 3/4$ [vì $(4x - 3)(x - 1) = 4x^2 - 7x + 3$].

By Lemma 4.7 (a) this equation is equivalent to $2x - 1 \geq 0$ and $(2x - 1)^2 = 3x - 2$, that is $x \geq 1/2$ and $4x^2 - 7x + 3 = 0$. The quadratic has roots $x = 1$ and $x = 3/4$ [because $(4x - 3)(x - 1) = 4x^2 - 7x + 3$].

Cả hai thỏa $x \geq 2/3$ ($3/4 > 2/3$) và $x \geq 1/2$. Kiểm tra $x = 3/4$: $2x - 1 = 1/2$ và $\sqrt[3]{3x - 2} = \sqrt[3]{1/4} = 1/2$. Vậy tập nghiệm là $\{3/4, 1\}$.

Both satisfy $x \geq 2/3$ (since $3/4 > 2/3$) and $x \geq 1/2$. Check $x = 3/4$: $2x - 1 = 1/2$ and $\sqrt[3]{3x - 2} = \sqrt[3]{1/4} = 1/2$. Hence the solution set is $\{3/4, 1\}$. ■

BỔ ĐỀ 4.17 (Hệ vòng quanh) / LEMMA 4.17 (Cyclic system) — Cho f đồng biến trên I và $x, y, z \in I$ thỏa $y = f(x)$, $z = f(y)$, $x = f(z)$. Khi đó $x = y = z$, và mỗi giá trị chung là nghiệm của phương trình $f(t) = t$.

Let f be increasing on I and $x, y, z \in I$ with $y = f(x)$, $z = f(y)$, $x = f(z)$. Then $x = y = z$, and the common value solves $f(t) = t$.

Chứng minh. / Proof.

Nếu $x \leq y$ thì theo Định lý 4.15, $f(x) \leq f(y)$, tức $y \leq z$; tiếp tục $f(y) \leq f(z)$, tức $z \leq x$. Vậy $x \leq y \leq z \leq x$, suy ra $x = y = z$.

If $x \leq y$ then by Theorem 4.15 $f(x) \leq f(y)$, that is $y \leq z$; then $f(y) \leq f(z)$, that is $z \leq x$. So $x \leq y \leq z \leq x$, which gives $x = y = z$.

Nếu $x \geq y$ thì mọi bất đẳng thức đổi chiều và kết luận như cũ. Hai trường hợp bao hết các khả năng. Khi $x = y = z$ thì $y = f(x)$ trở thành $x = f(x)$.

If $x \geq y$ every inequality reverses with the same conclusion. The two cases cover everything. When $x = y = z$, $y = f(x)$ becomes $x = f(x)$. ■

PHÂN TÍCH / ANALYSIS — Ba phương trình cùng dạng và luân phiên: biến sau là f của biến trước, với $f(t) = (t^3 + t)/2$. Đây chính là cấu trúc của Bổ đề 4.17. Cần kiểm tra f đồng biến (Tính chất 4.16 với $k = 1$, nhân thêm $1/2$ dương) và giải $f(t) = t$.

The three equations have the same form and rotate: each variable is f of the previous one, with $f(t) = (t^3 + t)/2$. This is exactly the structure of Lemma 4.17. We must check that f is increasing (Property 4.16 with $k = 1$, multiplied by the positive number $1/2$) and solve $f(t) = t$.

VÍ DỤ 4.13 (Hệ vòng quanh và hàm đồng biến) / EXAMPLE 4.13 (Cyclic system with an increasing function) — Giải hệ $x^3 + x = 2y$, $y^3 + y = 2z$, $z^3 + z = 2x$ trên $\mathbb{R}$.

Solve the system $x^3 + x = 2y$, $y^3 + y = 2z$, $z^3 + z = 2x$ over $\mathbb{R}$.

Lời giải. / Solution.

Đặt $f(t) = (t^3 + t)/2$. Hệ là $y = f(x)$, $z = f(y)$, $x = f(z)$. Theo Tính chất 4.16, $t^3 + t$ đồng biến trên $\mathbb{R}$, nhân với $1/2 > 0$ vẫn đồng biến, nên f đồng biến trên $\mathbb{R}$.

Put $f(t) = (t^3 + t)/2$. The system reads $y = f(x)$, $z = f(y)$, $x = f(z)$. By Property 4.16, $t^3 + t$ is increasing on $\mathbb{R}$, and multiplying by $1/2 > 0$ keeps it increasing, so f is increasing on $\mathbb{R}$.

Theo Bổ đề 4.17, $x = y = z = t$ với $f(t) = t$, tức $t^3 + t = 2t$, hay $t^3 - t = t(t - 1)(t + 1) = 0$.

By Lemma 4.17, $x = y = z = t$ with $f(t) = t$, that is $t^3 + t = 2t$, or $t^3 - t = t(t - 1)(t + 1) = 0$.

Vậy $t \in \{-1; 0; 1\}$. Ngược lại, mỗi bộ $(t; t; t)$ với $t \in \{-1; 0; 1\}$ thỏa hệ vì $t^3 + t = 2t$. Hệ có ba nghiệm $(-1; -1; -1)$, $(0; 0; 0)$, $(1; 1; 1)$.

So $t \in \{-1, 0, 1\}$. Conversely each triple (t, t, t) with $t \in \{-1, 0, 1\}$ satisfies the system because $t^3 + t = 2t$. The system has three solutions $(-1, -1, -1)$, $(0, 0, 0)$, $(1, 1, 1)$. ■

NHẬN XÉT / REMARK — Bổ đề 4.17 cần f đồng biến. Với $f(t) = -t$ (nghịch biến), vòng hai phương trình $y = -x$, $x = -y$ có mọi cặp $(x; -x)$ là nghiệm, nên không buộc $x = y$. Vòng ba phương trình $y = -x$, $z = -y$, $x = -z$ buộc $x = 0$, nhưng do số lẻ phép đổi dấu chứ không do đơn điệu.

Lemma 4.17 needs f increasing. With $f(t) = -t$ (decreasing), the two-equation cycle $y = -x$, $x = -y$ has every pair $(x, -x)$ as a solution, so $x = y$ is not forced. The three-equation cycle $y = -x$, $z = -y$, $x = -z$ forces $x = 0$, but because of the odd number of sign changes, not because of monotonicity.

LỖI HAY GẶP / COMMON MISTAKE — Tuyên bố hàm đơn điệu mà không nói trên khoảng nào. Hàm $1/t$ giảm trên $(0; +\infty)$ và trên $(-\infty; 0)$ nhưng không đơn điệu trên $\mathbb{R} \setminus \{0\}$: $1/(-1) < 1/1$ dù $-1 < 1$. Dùng $f(u) = f(v) \Rightarrow u = v$ phải kiểm tra u, v cùng thuộc một khoảng đơn điệu.

Declaring a function monotone without naming the interval. The function $1/t$ decreases on $(0, +\infty)$ and on $(-\infty, 0)$ but is not monotone on $\mathbb{R} \setminus \{0\}$: $1/(-1) < 1/1$ although $-1 < 1$. Using $f(u) = f(v) \Rightarrow u = v$ requires u, v to lie in one interval of monotonicity.

4.7. Bất phương trình vô tỉ — Irrational inequations

BỔ ĐỀ 4.18 (Bất phương trình vô tỉ cơ bản) / LEMMA 4.18 (Basic irrational

inequations) — Với các biểu thức A, B : (a) $\sqrt{A} < B$ khi và chỉ khi $A \geq 0, B > 0$ và $A < B^2$. (b) $\sqrt{A} \geq B$ khi và chỉ khi $[B < 0$ và $A \geq 0]$ hoặc $[B \geq 0$ và $A \geq B^2]$. (c) $\sqrt{A} > B$ khi và chỉ khi $[B < 0$ và $A \geq 0]$ hoặc $[B \geq 0$ và $A > B^2]$.

For expressions A, B : (a) $\sqrt{A} < B$ if and only if $A \geq 0, B > 0$ and $A < B^2$. (b) $\sqrt{A} \geq B$ if and only if $[B < 0$ and $A \geq 0]$ or $[B \geq 0$ and $A \geq B^2]$. (c) $\sqrt{A} > B$ if and only if $[B < 0$ and $A \geq 0]$ or $[B \geq 0$ and $A > B^2]$.

Chứng minh. / Proof.

(a) $\sqrt{A}$ xác định khi $A \geq 0$ và $\sqrt{A} \geq 0$, nên $\sqrt{A} < B$ buộc $B > 0$. Với $A \geq 0$ và $B > 0$, hai vế không âm và phép bình phương giữ thứ tự trên $[0; +\infty)$ vì với $0 \leq u < v$ ta có $v^2 - u^2 = (v - u)(v + u) > 0$, nên $\sqrt{A} < B$ tương đương $A < B^2$.

(a) $\sqrt{A}$ is defined when $A \geq 0$ and $\sqrt{A} \geq 0$, so $\sqrt{A} < B$ forces $B > 0$. With $A \geq 0$ and $B > 0$ both sides are non-negative and squaring preserves order on $[0, +\infty)$ because for $0 \leq u < v$ we have $v^2 - u^2 = (v - u)(v + u) > 0$, so $\sqrt{A} < B$ is equivalent to $A < B^2$.

(b), (c) Nếu $B < 0$ thì mọi giá trị xác định của $\sqrt{A} \geq 0 > B$ đều thỏa, tức điều kiện $A \geq 0$. Nếu $B \geq 0$ thì hai vế không âm, bình phương tương đương: $\sqrt{A} \geq B \Leftrightarrow A \geq B^2$ và $\sqrt{A} > B \Leftrightarrow A > B^2$; điều kiện $A \geq 0$ đã nằm trong $A \geq B^2 \geq 0$.

(b), (c) If $B < 0$ every value of $\sqrt{A}$, which is $\geq 0 > B$, satisfies it, so only $A \geq 0$ is required. If $B \geq 0$ both sides are non-negative and squaring is an equivalence: $\sqrt{A} \geq B \Leftrightarrow A \geq B^2$ and $\sqrt{A} > B \Leftrightarrow A > B^2$; the condition $A \geq 0$ is already contained in $A \geq B^2 \geq 0$. ■

PHÂN TÍCH / ANALYSIS — Vế phải $x - 1$ đổi dấu, nên phải chia hai trường hợp theo dấu của nó đúng như Bổ đề 4.18 (b). Khi $x - 1 < 0$ chỉ cần điều kiện xác định. Khi $x - 1 \geq 0$ bình phương hai vế được và x^2 triệt tiêu, còn lại bất phương trình bậc nhất.

The right side $x - 1$ changes sign, so we must split on its sign exactly as in Lemma 4.18 (b). When $x - 1 < 0$ only the domain condition is needed. When $x - 1 \geq 0$ we may square, the x^2 terms cancel, and a linear inequality remains.

VÍ DỤ 4.14 (Xét dấu vế phải) / EXAMPLE 4.14 (Splitting on the sign of the right side)

— Giải bất phương trình $\sqrt{x^2 - x - 6} \geq x - 1$.

Solve the inequation $\sqrt{x^2 - x - 6} \geq x - 1$.

Lời giải. / Solution.

Áp dụng Bổ đề 4.18 (b) với $A = x^2 - x - 6, B = x - 1$. Tam thức $A = (x - 3)(x + 2)$ có hai nghiệm -2 và 3 , nên $A \geq 0$ khi $x \leq -2$ hoặc $x \geq 3$.

Apply Lemma 4.18 (b) with $A = x^2 - x - 6, B = x - 1$. The trinomial $A = (x - 3)(x + 2)$ has roots -2 and 3 , so $A \geq 0$ for $x \leq -2$ or $x \geq 3$.

Trường hợp 1: $x - 1 < 0$, tức $x < 1$, và $A \geq 0$. Giao với $x \leq -2$ hoặc $x \geq 3$ là $x \leq -2$.

Case 1: $x - 1 < 0$, that is $x < 1$, and $A \geq 0$. The intersection with $x \leq -2$ or $x \geq 3$ is $x \leq -2$.

Trường hợp 2: $x \geq 1$ và $x^2 - x - 6 \geq (x - 1)^2 = x^2 - 2x + 1$, tức $x \geq 7$. Giao với $x \geq 1$ là $x \geq 7$.

Case 2: $x \geq 1$ and $x^2 - x - 6 \geq (x - 1)^2 = x^2 - 2x + 1$, that is $x \geq 7$. The intersection with $x \geq 1$ is $x \geq 7$.

Vậy tập nghiệm là $(-\infty; -2] \cup [7; +\infty)$. Kiểm tra đầu mút: $x = 7$ cho $\sqrt{36} = 6 = 7 - 1$, đúng với dấu bằng.

Hence the solution set is $(-\infty, -2] \cup [7, +\infty)$. Endpoint check: $x = 7$ gives $\sqrt{36} = 6 = 7 - 1$, equality holds. ■

NHẬN XÉT / REMARK — Về hình học: với $x \leq -2$ đường thẳng $y = x - 1$ nằm dưới trục hoành, còn đường cong $y = \sqrt{x^2 - x - 6}$ không âm, nên đường cong nằm trên. Với $x \geq 7$ đường cong lại nằm trên đường thẳng, hai đường cắt nhau đúng tại $x = 7$. Trên $[3; 7)$, nơi đường cong xác định, đường thẳng nằm trên đường cong.

Geometrically: for $x \leq -2$ the line $y = x - 1$ lies below the x -axis while the curve $y = \sqrt{x^2 - x - 6}$ is non-negative, so the curve is above. For $x \geq 7$ the curve is again above the line, and they meet exactly at $x = 7$. On the part of $(-2, 7)$ where the curve is defined, namely $[3, 7)$, the line is above the curve.

PHẢI THUỘC / MEMORISE — $\sqrt{A} < B$: cần $A \geq 0, B > 0, A < B^2$. $\sqrt{A} > B$: hai trường hợp theo dấu B ; $B < 0$ chỉ cần $A \geq 0$.

$\sqrt{A} < B$: need $A \geq 0, B > 0, A < B^2$. $\sqrt{A} > B$: two cases by the sign of B ; for $B < 0$ only $A \geq 0$ is needed.

4.8. Bảng chiến lược — Strategy table

Dấu hiệu trong đề <i>Sign in the problem</i>	Công cụ nên thử <i>Tool to try</i>	Ví dụ <i>Example</i>
Vế phải của $\sqrt{A} = B$ có thể âm <i>The right side of $\sqrt{A} = B$ may be negative</i>	Nâng lũy thừa với điều kiện $B \geq 0$ (Bổ đề 4.7) <i>Square under the condition $B \geq 0$ (Lemma 4.7)</i>	Ví dụ 4.3 <i>Example 4.3</i>
Cùng một cụm $x^2 + 5x$ xuất hiện trong và ngoài căn <i>The same group $x^2 + 5x$ occurs inside and outside the root</i>	Đặt t bằng căn, giữ $t \geq 0$ <i>Let t be the root, keep $t \geq 0$</i>	Ví dụ 4.4 <i>Example 4.4</i>
Đoán được nghiệm; hiệu hai biểu thức trong căn chia hết cho $x - 1$ <i>A root can be guessed; the difference of radicands is divisible by $x - 1$</i>	Nhân liên hợp, tách $x - 1$, đánh giá thừa số còn lại <i>Conjugate, extract $x - 1$, estimate the remaining factor</i>	Ví dụ 4.5 <i>Example 4.5</i>
Tổng hai căn có tổng biểu thức trong căn là hằng số; vế phải là tam thức <i>Two roots whose radicands add to a constant; right side a quadratic</i>	Chặn hai vế, dấu bằng đồng thời <i>Bound both sides, simultaneous equality</i>	Ví dụ 4.6 <i>Example 4.6</i>

Dấu hiệu trong đề <i>Sign in the problem</i>	Công cụ nên thử <i>Tool to try</i>	Ví dụ <i>Example</i>
Hệ số đối xứng từ hai đầu <i>Coefficients symmetric from both ends</i>	Chia x^2 , đặt $t = x + 1/x$, kiểm tra $ t \geq 2$ <i>Divide by x^2, put $t = x + 1/x$, check that $t \geq 2$</i>	Ví dụ 4.7 <i>Example 4.7</i>
Hệ không đổi khi đổi x với y <i>System unchanged when x and y are swapped</i>	$S = x + y$, $P = xy$, điều kiện $S^2 \geq 4P$ <i>$S = x + y$, $P = xy$, condition $S^2 \geq 4P$</i>	Ví dụ 4.8 <i>Example 4.8</i>
Hai phương trình đổi chỗ cho nhau khi đổi x và y <i>The two equations exchange when x and y are swapped</i>	Trừ vế, nhân tử $x - y$ <i>Subtract, factor $x - y$</i>	Ví dụ 4.9 <i>Example 4.9</i>
Một phương trình thuần nhất bậc hai <i>One homogeneous quadratic equation</i>	Phân tích nhân tử, đặt $x = ky$ <i>Factor, put $x = ky$</i>	Ví dụ 4.10 <i>Example 4.10</i>
Hai vế cùng dạng $f(u)$ và $f(v)$ với f đồng biến <i>Both sides of the form $f(u)$ and $f(v)$ with f increasing</i>	$u = v$ (Định lý 4.15), rồi giải và thử lại <i>$u = v$ (Theorem 4.15), then solve and check</i>	Ví dụ 4.12 <i>Example 4.12</i>
Hệ vòng quanh $y = f(x)$, $z = f(y)$, $x = f(z)$ <i>Cyclic system $y = f(x)$, $z = f(y)$, $x = f(z)$</i>	$x = y = z$, giải $f(t) = t$ (Bổ đề 4.17) <i>$x = y = z$, solve $f(t) = t$ (Lemma 4.17)</i>	Ví dụ 4.13 <i>Example 4.13</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Tam thức bậc hai	Quadratic trinomial	$ax^2 + bx + c$ với $a \neq 0$ <i>$ax^2 + bx + c$ with $a \neq 0$</i>
Biệt thức	Discriminant	$\Delta = b^2 - 4ac$, quyết định số nghiệm <i>$\Delta = b^2 - 4ac$, decides the number of roots</i>
Parabol	Parabola	Đồ thị của tam thức bậc hai <i>The graph of a quadratic</i>
Đỉnh	Vertex	Điểm cực trị $(-b/(2a); -\Delta/(4a))$ <i>The extreme point $(-b/(2a), -\Delta/(4a))$</i>
Trục đối xứng	Axis of symmetry	Đường thẳng $x = -b/(2a)$ <i>The line $x = -b/(2a)$</i>
Nghiệm kép	Double root	Nghiệm của đa thức xuất hiện hai lần <i>A root counted twice</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Định lý Viète	Viète's theorem	Tổng và tích nghiệm theo hệ số <i>Sum and product of roots from the coefficients</i>
Điều kiện xác định	Domain of definition	Tập x để mọi biểu thức có nghĩa <i>The set of x where every expression is defined</i>
Nghiệm ngoại lai	Extraneous root	Nghiệm sinh ra khi biến đổi, không thỏa đề <i>A root created by a step that fails the original</i>
Phương trình hệ quả	Consequence equation	Mọi nghiệm của đề đều là nghiệm của nó <i>Every root of the original is a root of it</i>
Phương trình tương đương	Equivalent equation	Cùng tập nghiệm với đề <i>Same solution set as the original</i>
Biểu thức liên hợp	Conjugate expression	$\sqrt{A} + \sqrt{B}$ là liên hợp của $\sqrt{A} - \sqrt{B}$ <i>$\sqrt{A} + \sqrt{B}$ is the conjugate of $\sqrt{A} - \sqrt{B}$</i>
Ẩn phụ	Auxiliary unknown	Biến mới thay một cụm biểu thức <i>A new variable replacing a group of terms</i>
Phương trình hồi quy	Reciprocal equation	Hệ số đối xứng từ hai đầu <i>Coefficients symmetric from both ends</i>
Hệ đối xứng loại I	Symmetric system of type I	Không đổi khi hoán vị x và y <i>Unchanged when x and y are swapped</i>
Hệ đối xứng loại II	Symmetric system of type II	Hai phương trình đổi chỗ khi hoán vị <i>The two equations swap when x and y are swapped</i>
Hệ đẳng cấp	Homogeneous system	Có phương trình gồm các hạng tử cùng bậc <i>An equation whose terms all have the same degree</i>
Phép khử Gauss	Gaussian elimination	Biến đổi sơ cấp để khử dần ẩn <i>Elementary operations that eliminate unknowns step by step</i>
Hàm đồng biến	Increasing function	$u < v$ kéo theo $f(u) < f(v)$ <i>$u < v$ implies $f(u) < f(v)$</i>
Hàm nghịch biến	Decreasing function	$u < v$ kéo theo $f(u) > f(v)$ <i>$u < v$ implies $f(u) > f(v)$</i>
Hệ vòng quanh	Cyclic system	Mỗi biến là hàm của biến liền trước <i>Each variable is a function of the previous one</i>
Bất phương trình vô tỉ	Irrational inequation	Bất phương trình có ẩn dưới dấu căn <i>An inequation with the unknown under a root sign</i>

4.9. Bài tự luyện — Practice problems

Mức 1 — Học sinh giỏi cấp tỉnh — Level 1 — Provincial olympiad

Bài 4.1 / Problem 4.1 — Cho phương trình $x^2 - (m + 1)x + m - 2 = 0$ với nghiệm x_1, x_2 . Tìm m để $x_1^2 + x_2^2 = 10$.

Consider $x^2 - (m + 1)x + m - 2 = 0$ with roots x_1, x_2 . Find m such that $x_1^2 + x_2^2 = 10$.

Bài 4.2 / Problem 4.2 — Giải bất phương trình $\sqrt{x + 7} - \sqrt{x - 1} < 2$.

Solve the inequation $\sqrt{x + 7} - \sqrt{x - 1} < 2$.

Bài 4.3 / Problem 4.3 — Giải phương trình $(x + 1)(x + 2)(x + 4)(x + 5) = 40$.

Solve the equation $(x + 1)(x + 2)(x + 4)(x + 5) = 40$.

Bài 4.4 / Problem 4.4 — Giải phương trình $(x - 2)^3 + 2(x - 2) = (2x - 1)\sqrt{2x - 3}$.

Solve the equation $(x - 2)^3 + 2(x - 2) = (2x - 1)\sqrt{2x - 3}$.

Mức 2 — Học sinh giỏi quốc gia — Level 2 — National olympiad

Bài 4.5 / Problem 4.5 — Tìm tất cả giá trị m để hệ $x + y + xy = 5$, $xy(x + y) = m$ có nghiệm thực $(x; y)$.

Find all m for which the system $x + y + xy = 5$, $xy(x + y) = m$ has a real solution (x, y) .

Bài 4.6 / Problem 4.6 — Tìm m để phương trình $x^4 + x^3 - mx^2 + x + 1 = 0$ có nghiệm thực.

Find m such that $x^4 + x^3 - mx^2 + x + 1 = 0$ has a real root.

Bài 4.7 / Problem 4.7 — Giải hệ $x + y + z = 12$, $xy + yz + zx = 48$ trên $\mathbb{R}$.

Solve the system $x + y + z = 12$, $xy + yz + zx = 48$ over $\mathbb{R}$.

Bài 4.8 / Problem 4.8 — Biện luận theo m số nghiệm của hệ $x + y + z = 3$, $x + 2y + 4z = 7$, $x + 3y + mz = 9$.

Discuss, according to m , the solutions of $x + y + z = 3$, $x + 2y + 4z = 7$, $x + 3y + mz = 9$.

Mức 3 — Olympic quốc tế — Level 3 — International olympiad

Bài 4.9 / Problem 4.9 — Giải phương trình $\sqrt{x + 3 - 4\sqrt{x - 1}} + \sqrt{x + 8 - 6\sqrt{x - 1}} = 1$.

Solve the equation $\sqrt{x + 3 - 4\sqrt{x - 1}} + \sqrt{x + 8 - 6\sqrt{x - 1}} = 1$.

Bài 4.10 / Problem 4.10 — Tìm m để hệ $x^2 + y^2 = 2 + 2m$, $(x + y)^2 = 4$ có đúng hai nghiệm thực $(x; y)$.

Find m such that the system $x^2 + y^2 = 2 + 2m$, $(x + y)^2 = 4$ has exactly two real solutions (x, y) .

Bài 4.11 / Problem 4.11 — Tìm m để $x^2 - 2mx + m + 2 \geq 0$ với mọi $x \in [1; 3]$.

Find m such that $x^2 - 2mx + m + 2 \geq 0$ for all $x \in [1, 3]$.

Bài 4.12 / Problem 4.12 — Cho $f(x) = x^2 - m$. Tìm m để phương trình $f(f(x)) = x$ có đúng bốn nghiệm thực phân biệt, và với các m đó tính tổng bình phương bốn nghiệm theo m .

Let $f(x) = x^2 - m$. Find m such that the equation $ff(x) = x$ has exactly four distinct real roots, and for those m compute the sum of the squares of the four roots in terms of m .

4.10. Lời giải bài tự luyện — Solutions to practice problems

Bài 4.1 — Problem 4.1

Biệt thức $\Delta = (m + 1)^2 - 4(m - 2) = m^2 - 2m + 9 = (m - 1)^2 + 8 > 0$ với mọi m , nên phương trình luôn có hai nghiệm phân biệt.

The discriminant $\Delta = (m + 1)^2 - 4(m - 2) = m^2 - 2m + 9 = (m - 1)^2 + 8 > 0$ for every m , so there are always two distinct roots.

Theo Viète $S = x_1 + x_2 = m + 1$ và $P = x_1x_2 = m - 2$. Theo (4.3):

By Viète $S = x_1 + x_2 = m + 1$ and $P = x_1x_2 = m - 2$. By (4.3):

$$x_1^2 + x_2^2 = S^2 - 2P = (m + 1)^2 - 2(m - 2) = m^2 + 5$$

Điều kiện $m^2 + 5 = 10$ cho $m^2 = 5$. Vậy $m = \sqrt{5}$ hoặc $m = -\sqrt{5}$.

The condition $m^2 + 5 = 10$ gives $m^2 = 5$. Hence $m = \sqrt{5}$ or $m = -\sqrt{5}$. ■

Bài 4.2 — Problem 4.2

Điều kiện xác định: $x \geq 1$. Đặt $T = \sqrt{x + 7} + \sqrt{x - 1} > 0$. Theo (4.6), $\sqrt{x + 7} - \sqrt{x - 1} = 8/T$.

Domain: $x \geq 1$. Put $T = \sqrt{x + 7} + \sqrt{x - 1} > 0$. By (4.6), $\sqrt{x + 7} - \sqrt{x - 1} = 8/T$.

Bất phương trình tương đương $8/T < 2$, tức $T > 4$ (vì $T > 0$).

The inequation is equivalent to $8/T < 2$, that is $T > 4$ (because $T > 0$).

Hàm $g(x) = \sqrt{x + 7} + \sqrt{x - 1}$ đồng biến trên $[1; +\infty)$ theo Tính chất 4.16 (a), (b), (c). Vì $g(2) = 3 + 1 = 4$, theo Định lý 4.15 ta có $g(x) > 4$ khi và chỉ khi $x > 2$.

The function $g(x) = \sqrt{x + 7} + \sqrt{x - 1}$ is increasing on $[1, +\infty)$ by Property 4.16 (a), (b), (c). Since $g(2) = 3 + 1 = 4$, Theorem 4.15 gives $g(x) > 4$ if and only if $x > 2$.

Vậy tập nghiệm là $(2; +\infty)$. Kiểm tra $x = 3$: $\sqrt{10} - \sqrt{2}$ nhỏ hơn 2, còn tại $x = 2$ về trái bằng 2, không thỏa bất đẳng thức chặt.

Hence the solution set is $(2, +\infty)$. Check $x = 3$: $\sqrt{10} - \sqrt{2}$ is less than 2, while at $x = 2$ the left side equals 2, which fails the strict inequality. ■

Bài 4.3 — Problem 4.3

Ghép $(x + 1)(x + 5) = x^2 + 6x + 5$ và $(x + 2)(x + 4) = x^2 + 6x + 8$. Đặt $y = x^2 + 6x$, phương trình thành $(y + 5)(y + 8) = 40$, tức $y^2 + 13y = 0$, hay $y(y + 13) = 0$.

Pair $(x + 1)(x + 5) = x^2 + 6x + 5$ and $(x + 2)(x + 4) = x^2 + 6x + 8$. Put $y = x^2 + 6x$; the equation becomes $(y + 5)(y + 8) = 40$, that is $y^2 + 13y = 0$, or $y(y + 13) = 0$.

Với $y = 0$: $x^2 + 6x = 0$, $x = 0$ hoặc $x = -6$. Với $y = -13$: $x^2 + 6x + 13 = (x + 3)^2 + 4 > 0$ nên vô nghiệm thực.

For $y = 0$: $x^2 + 6x = 0$, $x = 0$ or $x = -6$. For $y = -13$: $x^2 + 6x + 13 = (x + 3)^2 + 4 > 0$, so there is no real solution.

Kiểm tra: $x = 0$ cho $1 \cdot 2 \cdot 4 \cdot 5 = 40$; $x = -6$ cho $(-5)(-4)(-2)(-1) = 40$. Vậy tập nghiệm là $\{0; -6\}$.

Check: $x = 0$ gives $1 \cdot 2 \cdot 4 \cdot 5 = 40$; $x = -6$ gives $(-5)(-4)(-2)(-1) = 40$. Hence the solution set is $\{0, -6\}$. ■

Bài 4.4 — Problem 4.4

Điều kiện: $x \geq 3/2$. Đặt $v = \sqrt{2x - 3} \geq 0$, khi đó $2x - 1 = v^2 + 2$ và vế phải bằng $(v^2 + 2)v = v^3 + 2v$.

Domain: $x \geq 3/2$. Put $v = \sqrt{2x - 3} \geq 0$; then $2x - 1 = v^2 + 2$ and the right side equals $(v^2 + 2)v = v^3 + 2v$.

Với $f(t) = t^3 + 2t$ đồng biến trên $\mathbb{R}$ (Tính chất 4.16 (c), $k = 2$), phương trình là $f(x - 2) = f(v)$, nên $x - 2 = v$ theo Định lý 4.15.

With $f(t) = t^3 + 2t$ increasing on $\mathbb{R}$ (Property 4.16 (c), $k = 2$), the equation is $f(x - 2) = f(v)$, so $x - 2 = v$ by Theorem 4.15.

Theo Bổ đề 4.7 (a): $x - 2 \geq 0$ và $(x - 2)^2 = 2x - 3$, tức $x \geq 2$ và $x^2 - 6x + 7 = 0$, nghiệm $x = 3 \pm \sqrt{2}$.

By Lemma 4.7 (a): $x - 2 \geq 0$ and $(x - 2)^2 = 2x - 3$, that is $x \geq 2$ and $x^2 - 6x + 7 = 0$, with roots $x = 3 \pm \sqrt{2}$.

Nghiệm $3 - \sqrt{2} < 2$ bị loại, nghiệm $3 + \sqrt{2} > 2$ thỏa. Kiểm tra: $x - 2 = 1 + \sqrt{2}$ và $2x - 3 = 3 + 2\sqrt{2} = (1 + \sqrt{2})^2$. Vậy phương trình có nghiệm duy nhất $x = 3 + \sqrt{2}$.

The root $3 - \sqrt{2} < 2$ is rejected, while $3 + \sqrt{2} > 2$ passes. Check: $x - 2 = 1 + \sqrt{2}$ and $2x - 3 = 3 + 2\sqrt{2} = (1 + \sqrt{2})^2$. Hence the equation has the single root $x = 3 + \sqrt{2}$. ■

Bài 4.5 — Problem 4.5

Đặt $S = x + y$, $P = xy$. Hệ thành $S + P = 5$ và $SP = m$. Theo Định lý 4.11, hệ có nghiệm thực khi và chỉ khi có $(S; P)$ thỏa hai phương trình đó cùng $S^2 \geq 4P$.

Put $S = x + y$, $P = xy$. The system becomes $S + P = 5$ and $SP = m$. By Theorem 4.11 it has a real solution if and only if some (S, P) satisfies both equations together with $S^2 \geq 4P$.

Từ $P = 5 - S$: $m = S(5 - S) = 25/4 - (S - 5/2)^2$, và điều kiện $S^2 \geq 4(5 - S)$, tức $S^2 + 4S - 20 \geq 0$. Tam thức này có nghiệm $S = -2 \pm 2\sqrt{6}$, nên điều kiện là $S \leq -2 - 2\sqrt{6}$ hoặc $S \geq s_0$ với $s_0 = -2 + 2\sqrt{6}$.

From $P = 5 - S$: $m = S(5 - S) = 25/4 - (S - 5/2)^2$, and the condition $S^2 \geq 4(5 - S)$ means $S^2 + 4S - 20 \geq 0$. This trinomial has roots $S = -2 \pm 2\sqrt{6}$, so the condition is $S \leq -2 - 2\sqrt{6}$ or $S \geq s_0$, where $s_0 = -2 + 2\sqrt{6}$.

Vì $s_0 > 5/2$ (do $2\sqrt{6} > 4,5$), hàm $m(S)$ giảm liên tục trên $[s_0; +\infty)$ và không bị chặn dưới, nên nhận mọi giá trị trong $(-\infty; m(s_0)]$. Tính $m(s_0) = 5s_0 - s_0^2 = (-10 + 10\sqrt{6}) - (28 - 8\sqrt{6}) = 18\sqrt{6} - 38$.

Since $s_0 > 5/2$ (as $2\sqrt{6} > 4.5$), the function $m(S)$ decreases continuously on $[s_0, +\infty)$ and is unbounded below, so it takes every value in $(-\infty, m(s_0)]$. Compute $m(s_0) = 5s_0 - s_0^2 = (-10 + 10\sqrt{6}) - (28 - 8\sqrt{6}) = 18\sqrt{6} - 38$.

Nhánh $S \leq -2 - 2\sqrt{6}$ cho $m(S) \leq m(-2 - 2\sqrt{6}) = -38 - 18\sqrt{6} < 0$, đã nằm trong khoảng trên. Vậy hệ có nghiệm thực khi và chỉ khi $m \leq 18\sqrt{6} - 38$.

The branch $S \leq -2 - 2\sqrt{6}$ gives $m(S) \leq m(-2 - 2\sqrt{6}) = -38 - 18\sqrt{6} < 0$, already inside that range. Hence the system has a real solution if and only if $m \leq 18\sqrt{6} - 38$. ■

Bài 4.6 — Problem 4.6

Các hệ số 1, 1, $-m$, 1, 1 đối xứng. Theo Định lý 4.10 với $a = 1$, $b = 1$, $c = -m$, phương trình có nghiệm thực khi và chỉ khi $t^2 + t - m - 2 = 0$ có nghiệm t với $|t| \geq 2$, tức $m = g(t)$ với $g(t) = t^2 + t - 2$.

The coefficients 1, 1, $-m$, 1, 1 are symmetric. By Theorem 4.10 with $a = 1$, $b = 1$, $c = -m$, the equation has a real root if and only if $t^2 + t - m - 2 = 0$ has a root t with $|t| \geq 2$, that is $m = g(t)$ with $g(t) = t^2 + t - 2$.

Với $t \geq 2$: $g(t) = (t + 1/2)^2 - 9/4$ tăng liên tục, $g(2) = 4$, không bị chặn trên, nên nhận mọi giá trị trong $[4; +\infty)$.

For $t \geq 2$: $g(t) = (t + 1/2)^2 - 9/4$ increases continuously, $g(2) = 4$, and is unbounded above, so it takes every value in $[4, +\infty)$.

Với $t \leq -2$: $t + 1/2 \leq -3/2$ nên $g(t)$ giảm khi t tăng, $g(-2) = 0$ và $g(t)$ không bị chặn trên khi t giảm, nên nhận mọi giá trị trong $[0; +\infty)$.

For $t \leq -2$: $t + 1/2 \leq -3/2$, so $g(t)$ decreases as t increases, $g(-2) = 0$ and $g(t)$ is unbounded above as t decreases, so it takes every value in $[0, +\infty)$.

Hợp hai tập là $[0; +\infty)$. Vậy phương trình có nghiệm thực khi và chỉ khi $m \geq 0$. Kiểm tra $m = 0$: $x = -1$ cho $1 - 1 + (-1) + 1 = 0$.

The union of the two sets is $[0, +\infty)$. Hence the equation has a real root if and only if $m \geq 0$. Check $m = 0$: $x = -1$ gives $1 - 1 - 1 + 1 = 0$. ■

Bài 4.7 — Problem 4.7

Bình phương tổng: $x^2 + y^2 + z^2 = 12^2 - 2 \cdot 48 = 48$.

Squaring the sum: $x^2 + y^2 + z^2 = 12^2 - 2 \cdot 48 = 48$.

Theo (4.9): $(x - y)^2 + (y - z)^2 + (z - x)^2 = 2 \cdot 48 - 2 \cdot 48 = 0$. Tổng ba số không âm bằng 0 nên cả ba bằng 0, tức $x = y = z$.

By (4.9): $(x - y)^2 + (y - z)^2 + (z - x)^2 = 2 \cdot 48 - 2 \cdot 48 = 0$. A sum of three non-negative numbers equal to 0 means all three vanish, that is $x = y = z$.

Từ $x + y + z = 12$ suy ra $3x = 12$ và $x = y = z = 4$. Kiểm tra: $4 + 4 + 4 = 12$ và $16 + 16 + 16 = 48$. Vậy nghiệm duy nhất là $(4; 4; 4)$.

From $x + y + z = 12$ we get $3x = 12$ and $x = y = z = 4$. Check: $4 + 4 + 4 = 12$ and $16 + 16 + 16 = 48$. Hence the unique solution is $(4, 4, 4)$. ■

Bài 4.8 — Problem 4.8

Ký hiệu ba phương trình là (E1), (E2), (E3). (E2) - (E1) cho $y + 3z = 4$. (E3) - (E1) cho $2y + (m - 1)z = 6$.

Call the equations (E1), (E2), (E3). (E2) - (E1) gives $y + 3z = 4$. (E3) - (E1) gives $2y + (m - 1)z = 6$.

Lấy $2y + (m - 1)z = 6$ trừ đi hai lần $y + 3z = 4$: $(m - 1 - 6)z = 6 - 8$, tức $(m - 7)z = -2$.

Subtracting twice $y + 3z = 4$ from $2y + (m - 1)z = 6$: $(m - 1 - 6)z = 6 - 8$, that is $(m - 7)z = -2$.

Nếu $m = 7$ thì $0 \cdot z = -2$, vô lý: hệ vô nghiệm.

If $m = 7$ then $0 \cdot z = -2$, absurd: the system has no solution.

Nếu $m \neq 7$ thì $z = 2/(7 - m)$; $y = 4 - 3z = (22 - 4m)/(7 - m)$; $x = 3 - y - z = (m - 3)/(7 - m)$. Theo Tính chất 4.13 các phép khử bảo toàn tập nghiệm, nên đây là nghiệm duy nhất.

If $m \neq 7$ then $z = 2/(7 - m)$; $y = 4 - 3z = (22 - 4m)/(7 - m)$; $x = 3 - y - z = (m - 3)/(7 - m)$.

By Property 4.13 the elimination steps preserve the solution set, so this is the unique solution.

Kiểm tra với $m = 0$: $(x; y; z) = (-3/7; 22/7; 2/7)$ cho $x + y + z = 3$, $x + 2y + 4z = (-3 + 44 + 8)/7 = 7$, $x + 3y = (-3 + 66)/7 = 9$. Vậy hệ vô nghiệm khi $m = 7$ và có nghiệm duy nhất khi $m \neq 7$.

Check with $m = 0$: $(x, y, z) = (-3/7, 22/7, 2/7)$ gives $x + y + z = 3$, $x + 2y + 4z = (-3 + 44 + 8)/7 = 7$, $x + 3y = (-3 + 66)/7 = 9$. Hence the system has no solution for $m = 7$ and a unique solution for $m \neq 7$. ■

Bài 4.9 — Problem 4.9

Điều kiện $x \geq 1$. Đặt $t = \sqrt{x - 1} \geq 0$, khi đó $x = t^2 + 1$. Biểu thức trong căn thứ nhất: $x + 3 - 4t = t^2 - 4t + 4 = (t - 2)^2$. Trong căn thứ hai: $x + 8 - 6t = t^2 - 6t + 9 = (t - 3)^2$.

Domain $x \geq 1$. Put $t = \sqrt{x - 1} \geq 0$, so $x = t^2 + 1$. The first radicand: $x + 3 - 4t = t^2 - 4t + 4 = (t - 2)^2$. The second: $x + 8 - 6t = t^2 - 6t + 9 = (t - 3)^2$.

Vì $\sqrt{u^2} = |u|$, phương trình thành $|t - 2| + |t - 3| = 1$.

Since $\sqrt{u^2} = |u|$, the equation becomes $|t - 2| + |t - 3| = 1$.

Theo bất đẳng thức tam giác, $|t - 2| + |3 - t| \geq |(t - 2) + (3 - t)| = 1$, dấu bằng khi và chỉ khi $(t - 2)$ và $(3 - t)$ cùng dấu hoặc một số bằng 0, tức $(t - 2)(3 - t) \geq 0$, hay $2 \leq t \leq 3$.

By the triangle inequality, $|t - 2| + |3 - t| \geq |(t - 2) + (3 - t)| = 1$, with equality if and only if -2 and $3 - t$ have the same sign or one of them is 0, that is $(t - 2)(3 - t) \geq 0$, or $2 \leq t \leq 3$.

Vậy $2 \leq \sqrt{x - 1} \leq 3$, tức $4 \leq x - 1 \leq 9$, hay $5 \leq x \leq 10$. Kiểm tra $x = 7$: $t = \sqrt{6}$; ở đây t nằm giữa 2 và 3, về trái là $(t - 2)$ hoặc $(2 - t)$ tùy dấu: $|\sqrt{6} - 2| + |\sqrt{6} - 3| = (\sqrt{6} - 2) + (3 - \sqrt{6}) = 1$. Vậy tập nghiệm là $[5; 10]$.

Hence $2 \leq \sqrt{x - 1} \leq 3$, that is $4 \leq x - 1 \leq 9$, or $5 \leq x \leq 10$. Check $x = 7$: $t = \sqrt{6}$ lies between 2 and 3, and $|\sqrt{6} - 2| + |\sqrt{6} - 3| = (\sqrt{6} - 2) + (3 - \sqrt{6}) = 1$. Hence the solution set is $[5, 10]$. ■

Bài 4.10 — Problem 4.10

Phương trình thứ hai cho $S = x + y = 2$ hoặc $S = -2$. Đặt $P = xy$; theo (4.3) phương trình thứ nhất là $S^2 - 2P = 2 + 2m$, tức $4 - 2P = 2 + 2m$, vậy $P = 1 - m$ với cả hai giá trị của S .

The second equation gives $S = x + y = 2$ or $S = -2$. Put $P = xy$; by (4.3) the first equation reads $S^2 - 2P = 2 + 2m$, that is $4 - 2P = 2 + 2m$, so $P = 1 - m$ for both values of S .

Theo Định lý 4.11, mỗi S cho nghiệm thực khi và chỉ khi $S^2 \geq 4P$, tức $4 \geq 4(1 - m)$, hay $m \geq 0$.

By Theorem 4.11 each S gives real solutions if and only if $S^2 \geq 4P$, that is $4 \geq 4(1 - m)$, or $m \geq 0$.

Nếu $m < 0$: hệ vô nghiệm. Nếu $m > 0$: $S^2 > 4P$, với mỗi S hai nghiệm X khác nhau nên có hai cặp $(x; y)$, $(y; x)$ khác nhau; tổng cộng 4 nghiệm. Nếu $m = 0$: $P = 1$, $S^2 = 4P$ nên $x = y = S/2$, ra $(1; 1)$ và $(-1; -1)$: đúng 2 nghiệm.

If $m < 0$: no solution. If $m > 0$: $S^2 > 4P$, for each S the two values X are distinct, giving two different pairs (x, y) , (y, x) ; four solutions in all. If $m = 0$: $P = 1$, $S^2 = 4P$, so $x = y = S/2$, giving $(1, 1)$ and $(-1, -1)$: exactly 2 solutions.

Vậy hệ có đúng hai nghiệm khi và chỉ khi $m = 0$.

Hence the system has exactly two solutions if and only if $m = 0$. ■

Bài 4.11 — Problem 4.11

Bất đẳng thức tương đương $m(2x - 1) \leq x^2 + 2$. Với $x \in [1; 3]$, $2x - 1 \geq 1 > 0$, nên nó tương đương $m \leq h(x)$, $h(x) = (x^2 + 2)/(2x - 1)$.

The inequality is equivalent to $m(2x - 1) \leq x^2 + 2$. For $x \in [1, 3]$, $2x - 1 \geq 1 > 0$, so it is equivalent to $m \leq h(x)$, where $h(x) = (x^2 + 2)/(2x - 1)$.

Ta có $h(x) \geq 2$ khi và chỉ khi $x^2 + 2 \geq 4x - 2$, tức $(x - 2)^2 \geq 0$, luôn đúng, dấu bằng tại $x = 2 \in [1; 3]$. Vậy giá trị nhỏ nhất của h trên $[1; 3]$ là 2.

We have $h(x) \geq 2$ if and only if $x^2 + 2 \geq 4x - 2$, that is $(x - 2)^2 \geq 0$, which always holds, with equality at $x = 2 \in [1, 3]$. So the minimum of h on $[1, 3]$ is 2.

Bất đẳng thức $m \leq h(x)$ đúng với mọi $x \in [1; 3]$ khi và chỉ khi m không vượt quá giá trị nhỏ nhất đó: $m \leq 2$. Kiểm tra $m = 2$: $x^2 - 4x + 4 = (x - 2)^2 \geq 0$. Vậy $m \leq 2$.

The inequality $m \leq h(x)$ holds for all $x \in [1, 3]$ if and only if m does not exceed that minimum: $m \leq 2$. Check $m = 2$: $x^2 - 4x + 4 = (x - 2)^2 \geq 0$. Hence $m \leq 2$. ■

Bài 4.12 — Problem 4.12

Ta có $f(f(x)) - x = (x^2 - m)^2 - m - x$. Nghiệm của $f(x) = x$, tức $x^2 - x - m = 0$, đương nhiên là nghiệm. Chia đa thức, ta kiểm tra phân tích:

We have $f(f(x)) - x = (x^2 - m)^2 - m - x$. Roots of $f(x) = x$, that is $x^2 - x - m = 0$, are certainly roots. Dividing, we check the factorisation:

$$(x^2 - m)^2 - m - x = (x^2 - x - m)(x^2 + x + 1 - m)$$

Khai triển vế phải: $x^4 + x^3 + (1 - m)x^2 - x^3 - x^2 - (1 - m)x - mx^2 - mx - m(1 - m) = x^4 - 2mx^2 - x + m^2 - m$, trùng với vế trái.

Expanding the right side: $x^4 + x^3 + (1 - m)x^2 - x^3 - x^2 - (1 - m)x - mx^2 - mx - m(1 - m) = x^4 - 2mx^2 - x + m^2 - m$, which equals the left side.

Tam thức $A = x^2 - x - m$ có $\Delta_A = 1 + 4m$; tam thức $B = x^2 + x + 1 - m$ có $\Delta_B = 1 - 4(1 - m) = 4m - 3$. Theo Định lý 4.3, A có hai nghiệm phân biệt khi $m > -1/4$ và B có hai nghiệm phân biệt khi $m > 3/4$.

The trinomial $A = x^2 - x - m$ has $\Delta_A = 1 + 4m$; $B = x^2 + x + 1 - m$ has $\Delta_B = 1 - 4(1 - m) = 4m - 3$. By Theorem 4.3, A has two distinct roots when $m > -1/4$ and B has two distinct roots when $m > 3/4$.

Nghiệm chung của A và B thỏa $A - B = (x^2 - x - m) - (x^2 + x + 1 - m) = -2x - 1 = 0$, nên $x = -1/2$; thế vào A: $1/4 + 1/2 - m = 0$, tức $m = 3/4$. Vậy với $m > 3/4$ hai tam thức không có nghiệm chung và bốn nghiệm đôi một khác nhau.

A common root satisfies $A - B = (x^2 - x - m) - (x^2 + x + 1 - m) = -2x - 1 = 0$, so $x = -1/2$; substituting into A: $1/4 + 1/2 - m = 0$, that is $m = 3/4$. So for $m > 3/4$ the two trinomials share no root and the four roots are pairwise distinct.

Với $m \leq 3/4$: nếu $-1/4 < m < 3/4$ thì A có 2 nghiệm, B vô nghiệm, được 2 nghiệm; nếu $m \leq -1/4$ thì chỉ còn nhiều nhất 1 nghiệm. Với $m = 3/4$ các nghiệm là $3/2$ và $-1/2$ (của A) cùng $-1/2$ kép (của B), tức 2 nghiệm phân biệt.

For $m \leq 3/4$: if $-1/4 < m < 3/4$ then A has 2 roots and B none, giving 2 roots; if $m \leq -1/4$ at most 1 root remains. For $m = 3/4$ the roots are $3/2$ and $-1/2$ (from A) and $-1/2$ double (from B), that is 2 distinct roots.

Vậy phương trình có đúng bốn nghiệm thực phân biệt khi và chỉ khi $m > 3/4$.

Hence the equation has exactly four distinct real roots if and only if $m > 3/4$.

Tổng bình phương: theo Viète và (4.3), hai nghiệm của A có tổng 1, tích $-m$ nên tổng bình phương $1 + 2m$; hai nghiệm của B có tổng -1 , tích $1 - m$ nên tổng bình phương $1 - 2(1 - m) = 2m - 1$. Cộng lại: $4m$.

Sum of squares: by Viète and (4.3), the roots of A have sum 1 and product $-m$, so sum of squares $1 + 2m$; the roots of B have sum -1 and product $1 - m$, so sum of squares $1 - 2(1 - m) = 2m - 1$. Adding: $4m$.

Kiểm tra $m = 1$: $A = x^2 - x - 1$ và $B = x^2 + x$, nghiệm $(1 \pm \sqrt{5})/2, 0, -1$; tổng bình phương $(3 + \sqrt{5})/2 + (3 - \sqrt{5})/2 + 0 + 1 = 4 = 4m$.

Check $m = 1$: $A = x^2 - x - 1$ and $B = x^2 + x$, with roots $(1 \pm \sqrt{5})/2, 0, -1$; sum of squares $(3 + \sqrt{5})/2 + (3 - \sqrt{5})/2 + 0 + 1 = 4 = 4m$. ■

Chương 5. Phương trình hàm, đa thức và dãy số — Chapter 5.

Functional equations, polynomials and sequences

Mục tiêu chương — Chapter objectives

- Giải phương trình hàm bằng phép thế, đơn ánh – toàn ánh, điểm bất động và hàm cộng tính Cauchy, luôn kèm bước thử lại.
Solve functional equations by substitution, injectivity and surjectivity, fixed points and Cauchy's additive equation, always with a final check.
- Dùng phép chia đa thức, định lý Bézout, công thức Viète và nội suy Lagrange để xử lý nghiệm và giá trị của đa thức.
Use polynomial division, Bézout's theorem, Vieta's formulas and Lagrange interpolation to handle roots and values of polynomials.
- Khai thác tính chất $(a - b) \mid P(a) - P(b)$ của đa thức hệ số nguyên để chứng minh bài số học.
Use the property $(a - b) \mid P(a) - P(b)$ of integer polynomials to prove number-theoretic statements.
- Tìm số hạng tổng quát của dãy truy hồi tuyến tính cấp 1, cấp 2 và nhận ra dãy tuần hoàn.
Find the general term of first- and second-order linear recurrences and recognise periodic sequences.
- Tính tổng bằng sai phân và chứng minh tính nguyên của dãy bằng bất biến.
Evaluate sums by telescoping and prove integrality of sequences with invariants.

5.1. Phương trình hàm và nguyên tắc hai pha — Functional equations and the two-phase principle

ĐỊNH NGHĨA 5.1 (Phương trình hàm) / DEFINITION 5.1 (Functional equation) —

Phương trình hàm là hệ thức chứa hàm chưa biết f , trong đó f xuất hiện tại những điểm phụ thuộc vào các biến, và hệ thức phải đúng với mọi giá trị của biến trong miền cho trước. Giải phương trình hàm là tìm mọi hàm $f: \mathbb{R} \rightarrow \mathbb{R}$ (hoặc trên miền khác nêu trong đề) thỏa hệ thức; mỗi hàm như vậy gọi là một nghiệm hàm.

A functional equation is a relation involving an unknown function f , evaluated at points that depend on the variables, which must hold for all values of the variables in a given domain. To solve it is to find every function $f: \mathbb{R} \rightarrow \mathbb{R}$ (or on another domain stated in the problem) satisfying the relation; each such function is a solution.

TÍNH CHẤT 5.2 / PROPERTY 5.2 — Nguyên tắc hai pha. Pha thứ nhất (điều kiện cần): giả sử f thỏa đề, dùng các phép thế để suy ra dạng của f . Pha thứ hai (điều kiện đủ): thế dạng tìm được vào đề và kiểm tra hệ thức đúng với mọi giá trị biến. Thiếu pha thứ hai thì lời giải chưa hoàn chỉnh, vì các phép thế chỉ khai thác một phần của hệ thức.

Two-phase principle. Phase one (necessary condition): assume f satisfies the equation and use substitutions to deduce its form. Phase two (sufficiency): substitute the form found into the equation and check that it holds for all values of the variables. Without phase two the solution is incomplete, because substitutions use only part of the relation.

Các phép thế thường dùng, theo thứ tự nên thử:

Substitutions that are usually worth trying, in this order:

- Đặt một biến bằng 0 hoặc 1 để tính $f(0)$, $f(1)$ hoặc đưa hệ thức về một biến.
Set a variable equal to 0 or 1 to find $f(0)$, $f(1)$ or to reduce the relation to one variable.
- Đặt hai biến bằng nhau ($y = x$) hoặc đối nhau ($y = -x$).
Set two variables equal ($y = x$) or opposite ($y = -x$).
- Hoán đổi vai trò hai biến; nếu vế trái đối xứng mà vế phải không đối xứng thì so sánh hai dạng của vế phải.
Swap the roles of two variables; if the left side is symmetric and the right is not, compare the two forms of the right side.
- Thay biến bằng một biểu thức làm lặp lại hệ thức (x thành $1 - x$, hay y thành $f(y)$).
Replace a variable by an expression that makes the relation recur (x by $1 - x$, or y by $f(y)$).
- Với miền $\mathbb{Z}$ hoặc $\mathbb{Z}^+$, đặt $n = 1$ để lập quan hệ giữa $f(m + 1)$ và $f(m)$, rồi quy nạp.
On $\mathbb{Z}$ or $\mathbb{Z}^+$, set $n = 1$ to relate $f(m + 1)$ to $f(m)$, then use induction.

VÍ DỤ 5.1 (Thế một biến bằng 0) / EXAMPLE 5.1 (Setting a variable to 0) — Tìm mọi hàm $f: \mathbb{R} \rightarrow \mathbb{R}$ thỏa $f(x + y) = f(x) + y(2x + y + 3)$ với mọi số thực x, y .
Find all functions $f: \mathbb{R} \rightarrow \mathbb{R}$ such that $f(x + y) = f(x) + y(2x + y + 3)$ for all real x, y .

Lời giải. / Solution.

1. Đặt $x = 0$: $f(y) = f(0) + y(y + 3)$ với mọi y . Gọi $c = f(0)$, ta có $f(y) = y^2 + 3y + c$.
Put $x = 0$: $f(y) = f(0) + y(y + 3)$ for all y . Writing $c = f(0)$, we get $f(y) = y^2 + 3y + c$.
2. Thử lại với $f(x) = x^2 + 3x + c$. Vế trái bằng $(x + y)^2 + 3(x + y) + c = x^2 + 2xy + y^2 + 3x + 3y + c$. Vế phải bằng $x^2 + 3x + c + 2xy + y^2 + 3y$. Hai vế bằng nhau với mọi x, y .
Check $f(x) = x^2 + 3x + c$. The left side is $(x + y)^2 + 3(x + y) + c = x^2 + 2xy + y^2 + 3x + 3y + c$. The right side is $x^2 + 3x + c + 2xy + y^2 + 3y$. The two sides agree for all x, y .

Vậy các nghiệm là $f(x) = x^2 + 3x + c$, với c là hằng số thực tùy ý.

Hence the solutions are $f(x) = x^2 + 3x + c$, where c is an arbitrary real constant. ■

PHÂN TÍCH / ANALYSIS — Hệ thức nối $f(x)$ với $f(1 - x)$. Phép đổi x thành $1 - x$ đưa $f(1 - x)$ về $f(x)$ và ngược lại, nên nếu viết hệ thức một lần nữa sau phép đổi ta có hai phương trình với đúng hai ẩn $f(x)$ và $f(1 - x)$. Bài toán trở thành giải hệ tuyến tính.
The relation links $f(x)$ with $f(1 - x)$. Replacing x by $1 - x$ swaps the two terms, so writing the relation again after the replacement gives two equations in exactly two unknowns, $f(x)$ and $f(1 - x)$. The problem becomes a linear system.

VÍ DỤ 5.2 (Hệ hai phương trình ẩn hàm) / EXAMPLE 5.2 (A system for two values of f) — Tìm mọi hàm $f: \mathbb{R} \rightarrow \mathbb{R}$ thỏa $2f(x) + f(1 - x) = x^2$ với mọi số thực x .
Find all functions $f: \mathbb{R} \rightarrow \mathbb{R}$ such that $2f(x) + f(1 - x) = x^2$ for all real x .

Lời giải. / Solution.

1. Thay x bởi $1 - x$: $2f(1 - x) + f(x) = (1 - x)^2$. Cùng với hệ thức đề cho ta có hệ hai phương trình ẩn $f(x)$, $f(1 - x)$.

Replace x by $1 - x$: $2f(1 - x) + f(x) = (1 - x)^2$. Together with the given relation this is a system in the unknowns $f(x)$, $f(1 - x)$.

2. Nhân phương trình đề cho với 2 rồi trừ phương trình vừa thu được: $3f(x) = 2x^2 - (1 - x)^2 = x^2 + 2x - 1$.

Multiply the given relation by 2 and subtract the new one: $3f(x) = 2x^2 - (1 - x)^2 = x^2 + 2x - 1$.

$$f(x) = (x^2 + 2x - 1)/3$$

3. Thử lại: $(1 - x)^2 + 2(1 - x) - 1 = x^2 - 4x + 2$, nên $2f(x) + f(1 - x) = (2x^2 + 4x - 2 + x^2 - 4x + 2)/3 = x^2$.

Check: $(1 - x)^2 + 2(1 - x) - 1 = x^2 - 4x + 2$, so $2f(x) + f(1 - x) = (2x^2 + 4x - 2 + x^2 - 4x + 2)/3 = x^2$.

Vậy có đúng một nghiệm $f(x) = (x^2 + 2x - 1)/3$.

Hence there is exactly one solution, $f(x) = (x^2 + 2x - 1)/3$. ■

VÍ DỤ 5.3 (Quy nạp hai chiều trên $\mathbb{Z}$) / EXAMPLE 5.3 (Two-sided induction on $\mathbb{Z}$) —

Tìm mọi hàm $f: \mathbb{Z} \rightarrow \mathbb{Z}$ thỏa $f(m + n) = f(m) + f(n) + mn$ với mọi số nguyên m, n .

Find all functions $f: \mathbb{Z} \rightarrow \mathbb{Z}$ such that $f(m + n) = f(m) + f(n) + mn$ for all integers m, n .

Lời giải. / Solution.

1. Đặt $m = n = 0$: $f(0) = 2f(0)$, nên $f(0) = 0$. Đặt $a = f(1)$, a là số nguyên.

Put $m = n = 0$: $f(0) = 2f(0)$, so $f(0) = 0$. Let $a = f(1)$, an integer.

2. Đặt $n = 1$: $f(m + 1) = f(m) + a + m$ với mọi số nguyên m (kể cả m âm).

Put $n = 1$: $f(m + 1) = f(m) + a + m$ for every integer m , negative values included.

3. Ta chứng minh $f(m) = am + m(m - 1)/2$ với mọi $m \in \mathbb{Z}$. Với $m \geq 0$, quy nạp: đúng tại $m = 0$; nếu đúng tại m thì $f(m + 1) = am + m(m - 1)/2 + a + m = a(m + 1) + m(m + 1)/2$.

We show $f(m) = am + m(m - 1)/2$ for all $m \in \mathbb{Z}$. For $m \geq 0$ use induction: it holds at $m = 0$; if it holds at m then $f(m + 1) = am + m(m - 1)/2 + a + m = a(m + 1) + m(m + 1)/2$.

4. Với $m \leq 0$, quy nạp lùi: nếu đúng tại $m + 1$ thì $f(m) = f(m + 1) - a - m = a(m + 1) + (m + 1)m/2 - a - m = am + m(m - 1)/2$.

For $m \leq 0$ use downward induction: if it holds at $m + 1$ then $f(m) = f(m + 1) - a - m = a(m + 1) + (m + 1)m/2 - a - m = am + m(m - 1)/2$.

5. Thử lại: $f(m) + f(n) + mn = a(m + n) + (m^2 - m + n^2 - n)/2 + mn = a(m + n) + (m + n)(m + n - 1)/2 = f(m + n)$. Giá trị $m(m - 1)/2$ là số nguyên nên f nhận giá trị nguyên.

Check: $f(m) + f(n) + mn = a(m + n) + (m^2 - m + n^2 - n)/2 + mn = a(m + n) + (m + n)(m + n - 1)/2 = f(m + n)$. Since $m(m - 1)/2$ is an integer, f takes integer values.

Vậy $f(n) = an + n(n - 1)/2$, với a là số nguyên tùy ý.

Hence $f(n) = an + n(n - 1)/2$, where a is an arbitrary integer. ■

NHẬN XÉT / REMARK — Trên $\mathbb{Z}$, một phương trình hàm thường quy về hiệu $f(m+1) - f(m)$. Phải xét cả chiều âm, vì phép quy nạp bắt đầu từ $f(0)$ chỉ phủ $m \geq 0$.

On $\mathbb{Z}$ a functional equation often reduces to the difference $f(m+1) - f(m)$. Both directions must be treated, since induction started at $f(0)$ covers only $m \geq 0$.

LỖI HAY GẶP / COMMON MISTAKE — Dừng ở bước suy ra dạng của f mà không thử lại. Dạng thu được từ các phép thế chỉ là điều kiện cần và có thể không thỏa đề.

Stopping once the form of f has been deduced, without checking. The form obtained from substitutions is only a necessary condition and may fail the equation.

LỖI HAY GẶP / COMMON MISTAKE — Chia hai vế cho $f(x)$ hoặc cho một biểu thức chứa x mà không xét trường hợp bằng 0. Phải tách riêng trường hợp đó.

Dividing both sides by $f(x)$, or by an expression in x , without treating the case where it is 0. That case must be handled separately.

5.2. Hàm cộng tính và phương trình Cauchy — Additive functions and Cauchy's equation

ĐỊNH NGHĨA 5.3 (Hàm cộng tính) / DEFINITION 5.3 (Additive function) — Hàm f gọi là cộng tính nếu $f(x+y) = f(x) + f(y)$ với mọi x, y thuộc miền xác định ($\mathbb{Z}$, $\mathbb{Q}$ hoặc $\mathbb{R}$). Hệ thức này gọi là phương trình Cauchy.

A function f is additive if $f(x+y) = f(x) + f(y)$ for all x, y in its domain ($\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$). The relation is called Cauchy's equation.

BỔ ĐỀ 5.4 / LEMMA 5.4 — Nếu f cộng tính thì $f(0) = 0$, $f(-x) = -f(x)$ và $f(nx) = nf(x)$ với mọi số nguyên n .

If f is additive then $f(0) = 0$, $f(-x) = -f(x)$ and $f(nx) = nf(x)$ for every integer n .

Chứng minh. / Proof.

Đặt $x = y = 0$: $f(0) = 2f(0)$, suy ra $f(0) = 0$. Đặt $y = -x$: $0 = f(0) = f(x) + f(-x)$, suy ra $f(-x) = -f(x)$.

Put $x = y = 0$: $f(0) = 2f(0)$, so $f(0) = 0$. Put $y = -x$: $0 = f(0) = f(x) + f(-x)$, so $f(-x) = -f(x)$.

Với $n \geq 0$, quy nạp theo n : $f(0 \cdot x) = 0$ và $f((n+1)x) = f(nx) + f(x) = (n+1)f(x)$. Với $n < 0$, $f(nx) = -f((-n)x) = -(-n)f(x) = nf(x)$.

For $n \geq 0$ use induction on n : $f(0 \cdot x) = 0$ and $f((n+1)x) = f(nx) + f(x) = (n+1)f(x)$. For $n < 0$, $f(nx) = -f((-n)x) = -(-n)f(x) = nf(x)$. ■

ĐỊNH LÝ 5.5 (Định lý Cauchy trên $\mathbb{Q}$) / THEOREM 5.5 (Cauchy's theorem on $\mathbb{Q}$) —

Nếu $f: \mathbb{Q} \rightarrow \mathbb{Q}$ cộng tính thì $f(x) = ax$ với mọi $x \in \mathbb{Q}$, trong đó $a = f(1)$. Phép chứng minh vẫn đúng khi f nhận giá trị thực.

If $f: \mathbb{Q} \rightarrow \mathbb{Q}$ is additive then $f(x) = ax$ for all $x \in \mathbb{Q}$, where $a = f(1)$. The proof is unchanged when f takes real values.

Chứng minh. / Proof.

Lấy $x = m/n$ với $m \in \mathbb{Z}$, $n \in \mathbb{Z}^+$. Theo Bổ đề 5.4, $nf(m/n) = f(n \cdot m/n) = f(m) = f(m \cdot 1) = mf(1)$.

Take $x = m/n$ with $m \in \mathbb{Z}$, $n \in \mathbb{Z}^+$. By Lemma 5.4, $nf(m/n) = f(n \cdot m/n) = f(m) = f(m \cdot 1) = mf(1)$.

$$f(m/n) = (m/n) \cdot f(1) = ax \quad (5.1)$$

Ngược lại, mọi hàm ax đều cộng tính.

Conversely every function ax is additive. ■

ĐỊNH LÝ 5.6 (Cauchy với điều kiện đơn điệu) / THEOREM 5.6 (Cauchy with monotonicity) — Nếu $f: \mathbb{R} \rightarrow \mathbb{R}$ cộng tính và đơn điệu tăng ($x \leq y \Rightarrow f(x) \leq f(y)$) thì $f(x) = ax$ với mọi $x \in \mathbb{R}$, trong đó $a = f(1) \geq 0$. Với hàm đơn điệu giảm, áp dụng kết quả cho $-f$.

If $f: \mathbb{R} \rightarrow \mathbb{R}$ is additive and nondecreasing ($x \leq y \Rightarrow f(x) \leq f(y)$) then $f(x) = ax$ for all $x \in \mathbb{R}$, where $a = f(1) \geq 0$. For a nonincreasing function apply the result to $-f$.

Chứng minh. / Proof.

Theo chứng minh của Định lý 5.5, $f(q) = aq$ với mọi $q \in \mathbb{Q}$, và $a = f(1) \geq f(0) = 0$ do tính đơn điệu.

By the proof of Theorem 5.5, $f(q) = aq$ for every $q \in \mathbb{Q}$, and $a = f(1) \geq f(0) = 0$ by monotonicity.

Với số thực x và số nguyên dương n , đặt $p = \lfloor nx \rfloor / n$ và $q = (\lfloor nx \rfloor + 1) / n$. Khi đó $p \leq x \leq q$ và $q - p = 1/n$. Do f đơn điệu tăng, $ap = f(p) \leq f(x) \leq f(q) = aq$.

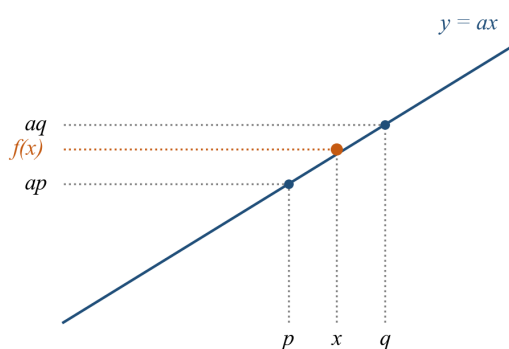
For a real x and a positive integer n put $p = \lfloor nx \rfloor / n$ and $q = (\lfloor nx \rfloor + 1) / n$. Then $p \leq x \leq q$ and $q - p = 1/n$. Since f is nondecreasing, $ap = f(p) \leq f(x) \leq f(q) = aq$.

Vì $a \geq 0$ nên cũng có $ap \leq ax \leq aq$. Hai số $f(x)$ và ax cùng nằm trong đoạn $[ap, aq]$ có độ dài a/n , do đó $|f(x) - ax| \leq a/n$ với mọi $n \in \mathbb{Z}^+$.

Since $a \geq 0$ we also have $ap \leq ax \leq aq$. The numbers $f(x)$ and ax lie in the interval $[ap, aq]$ of length a/n , so $|f(x) - ax| \leq a/n$ for every $n \in \mathbb{Z}^+$.

Cho n lớn tùy ý ta được $f(x) = ax$.

Letting n grow without bound gives $f(x) = ax$. ■



Hình 5.1. Hàm cộng tính đơn điệu bị kẹp giữa ap và aq tại mọi điểm x nằm giữa hai số hữu tỉ p và q

Figure 5.1. A monotone additive function is squeezed between ap and aq at every x lying between two rationals p and q

HỆ QUẢ 5.7 / COROLLARY 5.7 — Nếu $f: \mathbb{R} \rightarrow \mathbb{R}$ cộng tính và $f(x) \geq 0$ với mọi $x \geq 0$ thì $f(x) = ax$ với $a = f(1) \geq 0$.

If $f: \mathbb{R} \rightarrow \mathbb{R}$ is additive and $f(x) \geq 0$ for all $x \geq 0$ then $f(x) = ax$ with $a = f(1) \geq 0$.

Chứng minh. / Proof.

Nếu $x \leq y$ thì $f(y) - f(x) = f(y - x) \geq 0$, nên f đơn điệu tăng. Áp dụng Định lý 5.6.

If $x \leq y$ then $f(y) - f(x) = f(y - x) \geq 0$, so f is nondecreasing. Apply Theorem 5.6. ■

NHẬN XÉT / REMARK — Trên $\mathbb{R}$, nếu bỏ điều kiện đơn điệu (hoặc bị chặn trên một đoạn, hoặc liên tục) thì phương trình Cauchy còn những nghiệm không có dạng ax . Những nghiệm ấy xây bằng cơ sở Hamel nên không viết ra được tường minh; vì vậy đề thi luôn kèm điều kiện phụ hoặc đặt bài trên $\mathbb{Q}$.

On $\mathbb{R}$, without monotonicity (or boundedness on an interval, or continuity), Cauchy's equation has solutions not of the form ax . They are built from a Hamel basis and cannot be written explicitly, which is why problems add a side condition or work on $\mathbb{Q}$.

VÍ DỤ 5.4 (Cộng tính cùng dấu của bình phương) / EXAMPLE 5.4 (Additivity plus nonnegativity of squares) — Tìm mọi hàm $f: \mathbb{R} \rightarrow \mathbb{R}$ thỏa $f(x + y) = f(x) + f(y)$ và $f(x^2) = (f(x))^2$ với mọi số thực x, y .

Find all functions $f: \mathbb{R} \rightarrow \mathbb{R}$ such that $f(x + y) = f(x) + f(y)$ and $f(x^2) = (f(x))^2$ for all real x, y .

Lời giải. / Solution.

1. Với $x \geq 0$, viết $x = (\sqrt{x})^2$: $f(x) = (f(\sqrt{x}))^2 \geq 0$. Theo Hệ quả 5.7, $f(x) = ax$ với $a = f(1)$.

For $x \geq 0$ write $x = (\sqrt{x})^2$: $f(x) = (f(\sqrt{x}))^2 \geq 0$. By Corollary 5.7, $f(x) = ax$ with $a = f(1)$.

2. Thế vào điều kiện thứ hai: $ax^2 = a^2x^2$. Lấy $x = 1$ được $a = a^2$, tức $a = 0$ hoặc $a = 1$.

Substitute into the second condition: $ax^2 = a^2x^2$. Taking $x = 1$ gives $a = a^2$, that is $a = 0$ or $a = 1$.

3. Thử lại: $f(x) = 0$ và $f(x) = x$ đều cộng tính và thỏa $f(x^2) = (f(x))^2$.

Check: $f(x) = 0$ and $f(x) = x$ are both additive and satisfy $f(x^2) = (f(x))^2$.

Vậy $f(x) = 0$ với mọi x , hoặc $f(x) = x$ với mọi x .

Hence $f(x) = 0$ for all x , or $f(x) = x$ for all x . ■

PHÂN TÍCH / ANALYSIS — Về phải $f(x) + y$ chỉ chứa y ở dạng cộng. Nếu thay y bằng $f(y)$ và biết $f(f(y)) = y$ thì về phải thành $f(x) + f(y)$, đúng dạng Cauchy. Do đó cần chứng minh $f(f(y)) = y$, và công cụ để làm việc đó là tính đơn ánh.

On the right, y enters only additively. If y is replaced by $f(y)$ and $f(f(y)) = y$ is known, the right side becomes $f(x) + f(y)$, which is the Cauchy form. So the goal is $f(f(y)) = y$, and the tool for it is injectivity.

VÍ DỤ 5.5 (Đơn ánh rồi quy về Cauchy) / EXAMPLE 5.5 (Injectivity, then reduction to Cauchy) — Tìm mọi hàm $f: \mathbb{Q} \rightarrow \mathbb{Q}$ thỏa $f(x + f(y)) = f(x) + y$ với mọi $x, y \in \mathbb{Q}$.

Find all functions $f: \mathbb{Q} \rightarrow \mathbb{Q}$ such that $f(x + f(y)) = f(x) + y$ for all $x, y \in \mathbb{Q}$.

Lời giải. / Solution.

1. Đặt $c = f(0)$. Với $x = 0$: $f(f(y)) = c + y$. Nếu $f(u) = f(v)$ thì $c + u = f(f(u)) = f(f(v)) = c + v$, nên $u = v$: f đơn ánh.
Let $c = f(0)$. With $x = 0$: $f(f(y)) = c + y$. If $f(u) = f(v)$ then $c + u = f(f(u)) = f(f(v)) = c + v$, so $u = v$: f is injective.
2. Với $y = 0$: $f(x + c) = f(x)$. Do đơn ánh, $x + c = x$, tức $c = 0$. Vậy $f(f(y)) = y$.
With $y = 0$: $f(x + c) = f(x)$. By injectivity $x + c = x$, that is $c = 0$. Hence $f(f(y)) = y$.
3. Thay y bởi $f(y)$ trong hệ thức đề: $f(x + f(f(y))) = f(x) + f(y)$, tức $f(x + y) = f(x) + f(y)$.
Vậy f cộng tính.
Replace y by $f(y)$ in the given relation: $f(x + f(f(y))) = f(x) + f(y)$, that is $f(x + y) = f(x) + f(y)$. So f is additive.
4. Theo Định lý 5.5, $f(x) = ax$ với $a = f(1) \in \mathbb{Q}$. Khi đó $f(f(y)) = a^2y = y$, nên $a^2 = 1$, $a = 1$ hoặc $a = -1$.
By Theorem 5.5, $f(x) = ax$ with $a = f(1) \in \mathbb{Q}$. Then $f(f(y)) = a^2y = y$, so $a^2 = 1$, that is $a = 1$ or $a = -1$.
5. Thử lại: với $f(x) = x$, hai vế cùng bằng $x + y$. Với $f(x) = -x$, vế trái bằng $-(x - y) = -x + y$, vế phải bằng $-x + y$.
Check: for $f(x) = x$ both sides equal $x + y$. For $f(x) = -x$ the left side is $-(x - y) = -x + y$ and the right side is $-x + y$.

Vậy $f(x) = x$ hoặc $f(x) = -x$.

Hence $f(x) = x$ or $f(x) = -x$. ■

LỖI HAY GẶP / COMMON MISTAKE — Kết luận $f(x) = ax$ cho hàm cộng tính trên $\mathbb{R}$ mà không có điều kiện đơn điệu, bị chặn hay liên tục. Khẳng định này sai nếu thiếu điều kiện phụ; nếu đề không nêu thì phải tự chứng minh điều kiện ấy từ hệ thức.

Concluding $f(x) = ax$ for an additive function on $\mathbb{R}$ without monotonicity, boundedness or continuity. This is false without such a condition, and if the problem does not state one it must be derived from the relation.

PHẢI THUỘC / MEMORISE — f cộng tính trên $\mathbb{Q} \Rightarrow f(x) = f(1) \cdot x$. Trên $\mathbb{R}$ cần thêm đơn điệu: $f(x) \geq 0$ với $x \geq 0$ là đủ.

f additive on $\mathbb{Q} \Rightarrow f(x) = f(1) \cdot x$. On $\mathbb{R}$ add monotonicity: $f(x) \geq 0$ for $x \geq 0$ is enough.

5.3. Đơn ánh, toàn ánh và điểm bất động — Injectivity, surjectivity and fixed points

Hàm f đơn ánh nếu $f(u) = f(v) \Rightarrow u = v$, toàn ánh nếu mọi giá trị trong tập đích đều là $f(y)$ với y nào đó, song ánh nếu vừa đơn ánh vừa toàn ánh (Chương 1). Hai tính chất này cho phép bỏ f khỏi hệ thức (đơn ánh) và thay một giá trị tùy ý u bởi $f(y)$ (toàn ánh).

A function f is injective if $f(u) = f(v) \Rightarrow u = v$, surjective if every value in the target set equals $f(y)$ for some y , and bijective if both hold (Chapter 1). Injectivity lets us cancel f from a relation; surjectivity lets us replace an arbitrary value u by $f(y)$.

BỔ ĐỀ 5.8 / LEMMA 5.8 — Gọi $g(x) = f(f(x))$. Nếu g đơn ánh thì f đơn ánh. Nếu g toàn ánh thì f toàn ánh. Do đó nếu $f(f(x))$ là song ánh thì f là song ánh.

Let $g(x) = f(f(x))$. If g is injective then f is injective. If g is surjective then f is surjective. Hence if $f(f(x))$ is bijective then f is bijective.

Chứng minh. / Proof.

Giả sử $f(u) = f(v)$. Áp dụng f hai vế: $g(u) = g(v)$, nên $u = v$ do g đơn ánh. Vậy f đơn ánh.

Suppose $f(u) = f(v)$. Applying f to both sides, $g(u) = g(v)$, so $u = v$ because g is injective. Thus f is injective.

Giả sử g toàn ánh. Với mỗi giá trị w tồn tại x sao cho $w = g(x) = f(f(x))$, tức w là giá trị của f tại điểm $f(x)$. Vậy f toàn ánh.

Suppose g is surjective. For each value w there is x with $w = g(x) = f(f(x))$, so w is the value of f at the point $f(x)$. Thus f is surjective. ■

BỔ ĐỀ 5.9 / LEMMA 5.9 — Nếu $f: \mathbb{R} \rightarrow \mathbb{R}$ toàn ánh và $f(f(x)) = f(x)$ với mọi x thì $f(x) = x$ với mọi x .

If $f: \mathbb{R} \rightarrow \mathbb{R}$ is surjective and $f(f(x)) = f(x)$ for all x then $f(x) = x$ for all x .

Chứng minh. / Proof.

Lấy số thực tùy ý w . Do f toàn ánh, $w = f(t)$ với t nào đó. Khi đó $f(w) = f(f(t)) = f(t) = w$.

Take any real w . Since f is surjective, $w = f(t)$ for some t . Then $f(w) = f(f(t)) = f(t) = w$. ■

Bổ đề trên dùng điểm bất động, tức giá trị w thỏa $f(w) = w$. Khi hệ thức có dạng $f(f(x)) = g(x)$, hàm f giao hoán với g , nên f chuyển điểm bất động của g thành điểm bất động của g ; quan sát này được dùng ở bài tự luyện mức quốc tế.

The lemma uses fixed points, that is values w with $f(w) = w$. When a relation has the form $f(f(x)) = g(x)$, f commutes with g and therefore maps fixed points of g to fixed points of g ; the international-level practice problems use that observation.

PHÂN TÍCH / ANALYSIS — Vế phải chứa y^3 đứng riêng, và y^3 nhận mọi giá trị thực. Với $x = 0$ ta có $f(f(y)) = f(0) + y^3$, một song ánh, nên Bổ đề 5.8 cho f song ánh. Khi f toàn ánh, mọi số thực u đều bằng $f(y)$ với y nào đó, và $y^3 = f(f(y)) - f(0)$ viết lại được theo u . Hệ thức sẽ buộc f cộng tính, trong khi $f(f(y)) = y^3$ không cộng tính, nên hướng đúng là chứng minh vô nghiệm.

The term y^3 stands alone and takes every real value. With $x = 0$ we get $f(f(y)) = f(0) + y^3$, a bijection, so Lemma 5.8 makes f bijective. Once f is surjective every real u equals $f(y)$ for some y , and $y^3 = f(f(y)) - f(0)$ can be rewritten in terms of u . The relation will force f to be additive, while $f(f(y)) = y^3$ is not, so the right direction is to prove that no solution exists.

VÍ DỤ 5.6 (Đơn ánh, toàn ánh, mâu thuẫn) / EXAMPLE 5.6 (Injective, surjective, contradiction) — Chứng minh không tồn tại hàm $f: \mathbb{R} \rightarrow \mathbb{R}$ thỏa $f(x + f(y)) = f(x) + y^3$ với mọi số thực x, y .

Prove that there is no function $f: \mathbb{R} \rightarrow \mathbb{R}$ such that $f(x + f(y)) = f(x) + y^3$ for all real x, y .

Lời giải. / Solution.

- Giả sử f tồn tại. Đặt $c = f(0)$. Với $x = 0$: $f(f(y)) = c + y^3$. Ánh xạ y thành $c + y^3$ là song ánh trên $\mathbb{R}$, nên theo Bổ đề 5.8, f song ánh.

Suppose f exists and let $c = f(0)$. With $x = 0$: $f(f(y)) = c + y^3$. The map sending y to $c + y^3$ is a bijection of $\mathbb{R}$, so by Lemma 5.8 f is bijective.

2. Với $y = 0$: $f(x + c) = f(x)$. Do f đơn ánh, $x + c = x$, suy ra $c = 0$. Vậy $f(f(y)) = y^3$ và $f(x + f(y)) = f(x) + f(f(y))$.

With $y = 0$: $f(x + c) = f(x)$. Since f is injective, $x + c = x$, so $c = 0$. Hence $f(f(y)) = y^3$ and $f(x + f(y)) = f(x) + f(f(y))$.

3. Vì f toàn ánh, $u = f(y)$ chạy khắp $\mathbb{R}$, nên $f(x + u) = f(x) + f(u)$ với mọi x, u : f cộng tính. Theo Bổ đề 5.4, $f(nx) = nf(x)$.

Since f is surjective, $u = f(y)$ ranges over all of $\mathbb{R}$, so $f(x + u) = f(x) + f(u)$ for all x, u : f is additive. By Lemma 5.4, $f(nx) = nf(x)$.

4. Tính $f(f(2))$ theo hai cách. Một mặt, $f(f(2)) = 2^3 = 8$. Mặt khác, $f(2) = 2f(1)$, nên $f(f(2)) = f(2f(1)) = 2f(f(1)) = 2 \cdot 1^3 = 2$.

Compute $f(f(2))$ in two ways. On one hand $f(f(2)) = 2^3 = 8$. On the other, $f(2) = 2f(1)$, so $f(f(2)) = f(2f(1)) = 2f(f(1)) = 2 \cdot 1^3 = 2$.

Mâu thuẫn $8 = 2$. Vậy không tồn tại hàm f như đề yêu cầu.

The contradiction $8 = 2$ rules out every such function f . ■

NHẬN XÉT / REMARK — Một phương trình hàm có thể vô nghiệm; lời giải khi đó kết thúc bằng mâu thuẫn giữa hai số cụ thể. Với hệ thức $f(x + f(y)) = f(x) + y^2$ thì $f(f(y)) = y^2$ không âm, trong khi f toàn ánh phải nhận cả giá trị âm, cũng là mâu thuẫn.

A functional equation may have no solution, and the solution then ends in a contradiction between two concrete numbers. For $f(x + f(y)) = f(x) + y^2$ we get $f(f(y)) = y^2 \geq 0$, while a surjective f must take negative values too, again a contradiction.

PHÂN TÍCH / ANALYSIS — Hệ thức $f(f(n)) = n + 2$ áp dụng cho $f(n)$ cho ra $f(f(f(n))) = f(n) + 2$, và áp dụng f vào hai vế của hệ thức gốc cho $f(f(f(n))) = f(n + 2)$. Hai kết quả cho $f(n + 2) = f(n) + 2$, nên f được xác định bởi hai giá trị $f(1), f(2)$. Việc còn lại là một bài xét chẵn lẻ, và phải nhớ rằng tập giá trị là $\mathbb{Z}^+$ nên $f(2)$ có thể nhỏ hơn 2.

Applying $f(f(n)) = n + 2$ at the point $f(n)$ gives $f(f(f(n))) = f(n) + 2$, and applying f to both sides of the original gives $f(f(f(n))) = f(n + 2)$. Together, $f(n + 2) = f(n) + 2$, so f is determined by the two values $f(1), f(2)$. What remains is a parity analysis; note that the values lie in $\mathbb{Z}^+$, so $f(2)$ may be smaller than 2.

VÍ DỤ 5.7 (Quan hệ $f(n + 2) = f(n) + 2$ và chẵn lẻ) / EXAMPLE 5.7 (The relation $f(n + 2) = f(n) + 2$ and parity) — Tìm mọi hàm $f: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ thỏa $f(f(n)) = n + 2$ với mọi $n \in \mathbb{Z}^+$.

Find all functions $f: \mathbb{Z}^+ \rightarrow \mathbb{Z}^+$ such that $f(f(n)) = n + 2$ for all $n \in \mathbb{Z}^+$.

Lời giải. / Solution.

1. Áp dụng hệ thức tại $f(n)$: $f(f(f(n))) = f(n) + 2$. Áp dụng f vào hai vế của hệ thức gốc: $f(f(f(n))) = f(n + 2)$. Vậy $f(n + 2) = f(n) + 2$.

Apply the relation at $f(n)$: $f(f(f(n))) = f(n) + 2$. Apply f to both sides of the original relation: $f(f(f(n))) = f(n + 2)$. Hence $f(n + 2) = f(n) + 2$.

2. Đặt $a = f(1) - 1$ và $b = f(2) - 2$; ta có $a \geq 0$ và $b \geq -1$. Quy nạp theo bước nhảy 2 cho $f(n) = n + a$ khi n lẻ và $f(n) = n + b$ khi n chẵn.

Put $a = f(1) - 1$ and $b = f(2) - 2$; then $a \geq 0$ and $b \geq -1$. Induction in steps of 2 gives $f(n) = n + a$ for odd n and $f(n) = n + b$ for even n .

3. Lấy $n = 1$: $f(1 + a) = 3$. Nếu a chẵn thì $1 + a$ lẻ nên $f(1 + a) = 1 + 2a = 3$, $a = 1$, mâu thuẫn tính chẵn. Vậy a lẻ, $1 + a$ chẵn, $f(1 + a) = 1 + a + b = 3$, tức $a + b = 2$.

Take $n = 1$: $f(1 + a) = 3$. If a is even then $1 + a$ is odd, so $f(1 + a) = 1 + 2a = 3$ gives $a = 1$, contradicting parity. So a is odd, $1 + a$ is even, and $f(1 + a) = 1 + a + b = 3$, that is $a + b = 2$.

4. Lấy $n = 2$: $f(2 + b) = 4$. Nếu b chẵn thì $2 + b$ chẵn nên $2 + 2b = 4$, $b = 1$, mâu thuẫn tính chẵn. Vậy b lẻ, $2 + b$ lẻ, $2 + b + a = 4$, vẫn là $a + b = 2$.

Take $n = 2$: $f(2 + b) = 4$. If b is even then $2 + b$ is even, so $2 + 2b = 4$ gives $b = 1$, contradicting parity. So b is odd, $2 + b$ is odd, and $2 + b + a = 4$, again $a + b = 2$.

5. Với a, b lẻ, $a + b = 2$, $a \geq 0$, $b \geq -1$, chỉ còn $(a, b) = (1, 1)$ hoặc $(3, -1)$.

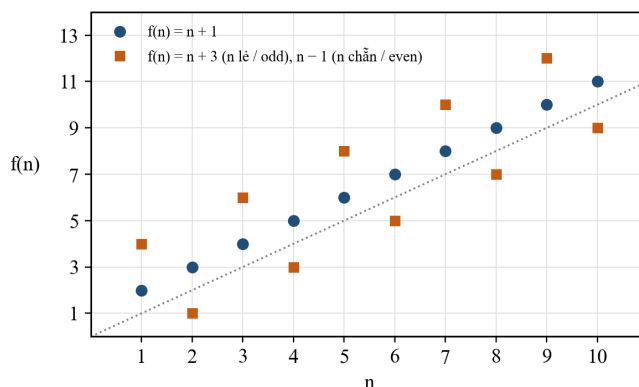
With a, b odd, $a + b = 2$, $a \geq 0$, $b \geq -1$, only $(a, b) = (1, 1)$ or $(3, -1)$ remain.

6. Thử lại. Với $(1, 1)$: $f(n) = n + 1$, $f(f(n)) = n + 2$. Với $(3, -1)$: $f(n) = n + 3$ khi n lẻ, $f(n) = n - 1$ khi n chẵn. Nếu n lẻ, $f(n) = n + 3$ chẵn, $f(f(n)) = n + 2$. Nếu n chẵn, $f(n) = n - 1$ lẻ và dương, $f(f(n)) = n - 1 + 3 = n + 2$.

Check. For $(1, 1)$: $f(n) = n + 1$ and $f(f(n)) = n + 2$. For $(3, -1)$: $f(n) = n + 3$ for odd n and $f(n) = n - 1$ for even n . If n is odd, $f(n) = n + 3$ is even and $f(f(n)) = n + 2$. If n is even, $f(n) = n - 1$ is odd and positive, and $f(f(n)) = n - 1 + 3 = n + 2$.

Vậy có đúng hai nghiệm: $f(n) = n + 1$; và $f(n) = n + 3$ với n lẻ, $f(n) = n - 1$ với n chẵn.

Hence there are exactly two solutions: $f(n) = n + 1$; and $f(n) = n + 3$ for odd n , $f(n) = n - 1$ for even n . ■



Hình 5.2. Đồ thị rời rạc của hai nghiệm trong Ví dụ 5.7 với n từ 1 đến 10

Figure 5.2. Discrete graphs of the two solutions of Example 5.7 for n from 1 to 10

NHẬN XÉT / REMARK — Nghiệm thứ hai khiến nhiều lời giải sai: nhìn hệ thức thấy ngay $f(n) = n + 1$ rồi dừng. Chỉ phép xét chẵn lẻ mới tách được hai nghiệm, và chỉ phép thử lại mới xác nhận nghiệm thứ hai hợp lệ, kể cả giá trị $f(2) = 1$.

The second solution defeats many attempts: $f(n) = n + 1$ is spotted at once and the search stops. Only the parity analysis separates the two, and only the check confirms that the second is valid, including the value $f(2) = 1$.

LỖI HAY GẶP / COMMON MISTAKE — Đoán nghiệm $f(n) = n + 1$ rồi tuyên bố duy nhất. Muốn kết luận duy nhất phải suy ra mọi giá trị $f(n)$ từ hệ thức; nêu ra một nghiệm là chưa đủ.

Guessing $f(n) = n + 1$ and declaring it unique. Uniqueness requires deriving every value $f(n)$ from the relation, not just exhibiting one solution.

LỖI HAY GẶP / COMMON MISTAKE — Thay biến bằng giá trị làm biểu thức ra ngoài miền, chẳng hạn dùng $f(0)$ hay $f(-1)$ khi f chỉ xác định trên $\mathbb{Z}^+$.

Substituting a value that leaves the domain, for instance using $f(0)$ or $f(-1)$ when f is defined only on $\mathbb{Z}^+$.

5.4. Đa thức: phép chia, định lý Bézout và nghiệm — Polynomials: division, Bézout's theorem and roots

ĐỊNH NGHĨA 5.10 (Đa thức) / DEFINITION 5.10 (Polynomial) — Đa thức một biến là biểu thức $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. Nếu $a_n \neq 0$ thì n là bậc của P (viết $\deg P = n$) và a_n là hệ số đầu. Số α gọi là nghiệm của P nếu $P(\alpha) = 0$. Ký hiệu $\mathbb{R}[x]$ là tập đa thức hệ số thực, $\mathbb{Z}[x]$ là tập đa thức hệ số nguyên.

A polynomial in one variable is an expression $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$. If $a_n \neq 0$ then n is the degree of P (written $\deg P = n$) and a_n is the leading coefficient. A number α is a root of P if $P(\alpha) = 0$. The sets of polynomials with real and with integer coefficients are denoted $\mathbb{R}[x]$ and $\mathbb{Z}[x]$.

ĐỊNH LÝ 5.11 (Phép chia có dư) / THEOREM 5.11 (Division with remainder) — Cho $A, B \in \mathbb{R}[x]$ với B khác đa thức không. Tồn tại duy nhất cặp đa thức Q, R sao cho $A = BQ + R$, trong đó R bằng 0 hoặc $\deg R < \deg B$. Q gọi là thương, R gọi là dư.

Let $A, B \in \mathbb{R}[x]$ with B not the zero polynomial. There is a unique pair of polynomials Q, R with $A = BQ + R$, where $R = 0$ or $\deg R < \deg B$. Q is the quotient and R the remainder.

Chứng minh. / Proof.

Duy nhất: nếu $BQ + R = BQ' + R'$ thì $B(Q - Q') = R' - R$. Nếu $Q \neq Q'$ thì vế trái có bậc không nhỏ hơn $\deg B$, còn vế phải có bậc nhỏ hơn $\deg B$ (hoặc bằng 0), vô lý. Vậy $Q = Q'$ và $R = R'$.

Uniqueness: if $BQ + R = BQ' + R'$ then $B(Q - Q') = R' - R$. If $Q \neq Q'$ the left side has degree at least $\deg B$ while the right has degree below $\deg B$ (or is zero), absurd. So $Q = Q'$ and $R = R'$.

Tồn tại: quy nạp theo $\deg A$. Nếu $A = 0$ hoặc $\deg A < \deg B$, lấy $Q = 0, R = A$. Nếu $\deg A = m \geq n = \deg B$, với a, b là hệ số đầu của A, B thì $A_1 = A - (a/b)x^{m-n}B$ có bậc nhỏ hơn m (hoặc bằng 0). Theo giả thiết quy nạp $A_1 = BQ_1 + R$, suy ra $A = B((a/b)x^{m-n} + Q_1) + R$.

Existence: induction on $\deg A$. If $A = 0$ or $\deg A < \deg B$ take $Q = 0, R = A$. If $\deg A = m \geq n = \deg B$, with a, b the leading coefficients of A, B , then $A_1 = A - (a/b)x^{m-n}B$ has degree below m (or is zero). By the induction hypothesis $A_1 = BQ_1 + R$, so $A = B((a/b)x^{m-n} + Q_1) + R$. ■

ĐỊNH LÝ 5.12 (Định lý Bézout) / THEOREM 5.12 (Bézout's theorem (remainder theorem)) — Dư của phép chia $P(x)$ cho $x - \alpha$ bằng $P(\alpha)$. Do đó α là nghiệm của P khi và chỉ khi $(x - \alpha)$ chia hết $P(x)$.

The remainder of $P(x)$ on division by $x - \alpha$ equals $P(\alpha)$. Hence α is a root of P if and only if $(x - \alpha)$ divides $P(x)$.

Chứng minh. / Proof.

Theo Định lý 5.11, $P(x) = (x - \alpha)Q(x) + r$ với r là hằng số (đư có bậc nhỏ hơn 1). Thay $x = \alpha$ được $r = P(\alpha)$.

By Theorem 5.11, $P(x) = (x - \alpha)Q(x) + r$ with r a constant (the remainder has degree below 1). Putting $x = \alpha$ gives $r = P(\alpha)$.

Đư bằng 0 khi và chỉ khi $P(\alpha) = 0$.

The remainder is 0 if and only if $P(\alpha) = 0$. ■

HỆ QUẢ 5.13 / COROLLARY 5.13 — (i) Đa thức khác không bậc n có không quá n nghiệm thực phân biệt. (ii) Hai đa thức có giá trị bằng nhau tại hơn $\max(\deg A, \deg B)$ điểm phân biệt thì đồng nhất bằng nhau, tức có cùng mọi hệ số. (iii) Đa thức bậc không quá n nhận cùng một giá trị tại $n + 1$ điểm phân biệt thì là hằng số.

(i) A nonzero polynomial of degree n has at most n distinct real roots. (ii) Two polynomials that agree at more than $\max(\deg A, \deg B)$ distinct points are identical, that is, have the same coefficients. (iii) A polynomial of degree at most n taking the same value at $n + 1$ distinct points is constant.

Chứng minh. / Proof.

(i) Quy nạp theo n . Với $n = 0$ đa thức là hằng số khác không, không có nghiệm. Với $n \geq 1$, nếu P không có nghiệm thì xong. Nếu α là nghiệm thì $P = (x - \alpha)Q$ (Định lý 5.12) với $\deg Q = n - 1$. Mọi nghiệm $\beta \neq \alpha$ của P thỏa $(\beta - \alpha)Q(\beta) = 0$ nên là nghiệm của Q , tối đa $n - 1$ nghiệm. Tổng cộng không quá n .

(i) Induction on n . For $n = 0$ the polynomial is a nonzero constant and has no roots. For $n \geq 1$, if P has no root we are done. If α is a root then $P = (x - \alpha)Q$ (Theorem 5.12) with $\deg Q = n - 1$. Every root $\beta \neq \alpha$ of P satisfies $(\beta - \alpha)Q(\beta) = 0$, so is a root of Q : at most $n - 1$ of them. In all, at most n .

(ii) $A - B$ triệt tiêu tại hơn $\max(\deg A, \deg B)$ điểm mà bậc của nó không vượt quá số đó, nên theo (i) $A - B$ là đa thức không. (iii) Áp dụng (ii) cho P và hằng số đó.

(ii) $A - B$ vanishes at more than $\max(\deg A, \deg B)$ points while its degree is at most that number, so by (i) $A - B$ is the zero polynomial. (iii) Apply (ii) to P and that constant. ■

ĐỊNH LÝ 5.14 (Định lý nghiệm hữu tỉ) / THEOREM 5.14 (Rational root theorem) —

Cho $P(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ với $a_n \neq 0$ và $a_0 \neq 0$. Nếu p/q (tối giản, $q > 0$) là nghiệm hữu tỉ của P thì $p \mid a_0$ và $q \mid a_n$.

Let $P(x) = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ with $a_n \neq 0$ and $a_0 \neq 0$. If p/q (in lowest terms, $q > 0$) is a rational root of P then $p \mid a_0$ and $q \mid a_n$.

Chứng minh. / Proof.

Nhân $P(p/q) = 0$ với q^n : $a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0$.

Multiply $P(p/q) = 0$ by q^n : $a_n p^n + a_{n-1} p^{n-1} q + \dots + a_1 p q^{n-1} + a_0 q^n = 0$.

Mọi số hạng trừ $a_0 q^n$ đều chia hết cho p , nên $p \mid a_0 q^n$. Vì $\text{ƯCLN}(p, q) = 1$ nên $p \mid a_0$. Tương tự mọi số hạng trừ $a_n p^n$ chia hết cho q , nên $q \mid a_n p^n$ và $q \mid a_n$.

Every term except $a_0 q^n$ is divisible by p , so $p \mid a_0 q^n$. Since $\gcd(p, q) = 1$, $p \mid a_0$. Similarly every term except $a_n p^n$ is divisible by q , so $q \mid a_n p^n$ and $q \mid a_n$. ■

ĐỊNH LÝ 5.15 (Định lý Viète tổng quát) / THEOREM 5.15 (Vieta's formulas) — Giả sử $P(x) = a_n x^n + \dots + a_0$ có n nghiệm $x_1, \dots, x_n$ kể cả bội, nghĩa là $P(x) = a_n(x - x_1)\dots(x - x_n)$. Gọi e_k là tổng các tích k nghiệm lấy từ n nghiệm ($e_1 = x_1 + \dots + x_n$, $e_2 = \sum x_i x_j$ với $i < j, \dots, e_n = x_1 \dots x_n$). Khi đó $e_k = (-1)^k \cdot a_{n-k}/a_n$ với $k = 1, \dots, n$.

Suppose $P(x) = a_n x^n + \dots + a_0$ has n roots $x_1, \dots, x_n$ counted with multiplicity, meaning $P(x) = a_n(x - x_1)\dots(x - x_n)$. Let e_k be the sum of all products of k roots chosen from the n ($e_1 = x_1 + \dots + x_n$, $e_2 = \sum x_i x_j$ over $i < j, \dots, e_n = x_1 \dots x_n$). Then $e_k = (-1)^k \cdot a_{n-k}/a_n$ for $k = 1, \dots, n$.

Chứng minh. / Proof.

Khai triển tích $(x - x_1)\dots(x - x_n)$: mỗi nhân tử cho x hoặc $-x_i$. Các số hạng chọn $-x_i$ ở đúng k nhân tử có dạng $(-1)^k x_{i_1} \dots x_{i_k} x^{n-k}$; cộng lại, hệ số của x^{n-k} là $(-1)^k e_k$.

Expand $(x - x_1)\dots(x - x_n)$: each factor contributes x or $-x_i$. The terms taking $-x_i$ from exactly k factors are $(-1)^k x_{i_1} \dots x_{i_k} x^{n-k}$; summing, the coefficient of x^{n-k} is $(-1)^k e_k$.

$$a_{n-k} = (-1)^k \cdot a_n \cdot e_k \quad (5.2)$$

So sánh với hệ số của P ta được kết luận. Định lý cơ bản của đại số bảo đảm đa thức bậc n có đủ n nghiệm phức kể cả bội; phát biểu trên chỉ dùng điều đó làm giả thiết.

Comparing with the coefficients of P gives the claim. The fundamental theorem of algebra guarantees n complex roots counted with multiplicity; the statement above uses this only as an assumption. ■

TÍNH CHẤT 5.16 / PROPERTY 5.16 — Cho $x^3 - px^2 + qx - r$ có ba nghiệm a, b, c ($p = a + b + c$, $q = ab + bc + ca$, $r = abc$). Khi đó $a^2 + b^2 + c^2 = p^2 - 2q$; $a^3 + b^3 + c^3 = p^3 - 3pq + 3r$; $1/a + 1/b + 1/c = q/r$; $1/a^2 + 1/b^2 + 1/c^2 = (q^2 - 2pr)/r^2$, với $r \neq 0$ ở hai công thức cuối.

Let $x^3 - px^2 + qx - r$ have three roots a, b, c ($p = a + b + c$, $q = ab + bc + ca$, $r = abc$). Then $a^2 + b^2 + c^2 = p^2 - 2q$; $a^3 + b^3 + c^3 = p^3 - 3pq + 3r$; $1/a + 1/b + 1/c = q/r$; $1/a^2 + 1/b^2 + 1/c^2 = (q^2 - 2pr)/r^2$, with $r \neq 0$ in the last two.

Chứng minh. / Proof.

Từ $(a + b + c)^2 = a^2 + b^2 + c^2 + 2q$ suy ra công thức thứ nhất. Mỗi nghiệm thỏa $t^3 = pt^2 - qt + r$; cộng ba đẳng thức: $a^3 + b^3 + c^3 = p(a^2 + b^2 + c^2) - qp + 3r = p(p^2 - 2q) - pq + 3r$.

$(a + b + c)^2 = a^2 + b^2 + c^2 + 2q$ gives the first formula. Each root satisfies $t^3 = pt^2 - qt + r$; adding the three: $a^3 + b^3 + c^3 = p(a^2 + b^2 + c^2) - qp + 3r = p(p^2 - 2q) - pq + 3r$.

Tiếp theo $1/a + 1/b + 1/c = (bc + ca + ab)/(abc) = q/r$. Và $1/a^2 + 1/b^2 + 1/c^2 = ((bc)^2 + (ca)^2 + (ab)^2)/r^2 = (q^2 - 2(ab \cdot bc + bc \cdot ca + ca \cdot ab))/r^2 = (q^2 - 2abc(a + b + c))/r^2 = (q^2 - 2pr)/r^2$.

Next, $1/a + 1/b + 1/c = (bc + ca + ab)/(abc) = q/r$. And $1/a^2 + 1/b^2 + 1/c^2 = ((bc)^2 + (ca)^2 + (ab)^2)/r^2 = (q^2 - 2(ab \cdot bc + bc \cdot ca + ca \cdot ab))/r^2 = (q^2 - 2abc(a + b + c))/r^2 = (q^2 - 2pr)/r^2$. ■

$$a^3 + b^3 + c^3 = p^3 - 3pq + 3r \quad (5.3)$$

VÍ DỤ 5.8 (Giá trị tại nghiệm của ước) / EXAMPLE 5.8 (Values at the roots of the divisor) — Tìm các số thực a, b để đa thức $P(x) = x^4 + ax^3 + bx - 12$ chia hết cho $x^2 + x - 2$, rồi tìm thương.

Find the real numbers a, b such that $P(x) = x^4 + ax^3 + bx - 12$ is divisible by $x^2 + x - 2$, and find the quotient.

Lời giải. / Solution.

1. Phân tích $x^2 + x - 2 = (x - 1)(x + 2)$. Nếu P chia hết cho tích này thì $P(1) = 0$ và $P(-2) = 0$ (Định lý 5.12).

Factor $x^2 + x - 2 = (x - 1)(x + 2)$. If P is divisible by this product then $P(1) = 0$ and $P(-2) = 0$ (Theorem 5.12).

2. $P(1) = 1 + a + b - 12 = 0$ cho $a + b = 11$. $P(-2) = 16 - 8a - 2b - 12 = 0$ cho $4a + b = 2$. Trừ hai phương trình: $3a = -9$, $a = -3$, $b = 14$.

$P(1) = 1 + a + b - 12 = 0$ gives $a + b = 11$. $P(-2) = 16 - 8a - 2b - 12 = 0$ gives $4a + b = 2$. Subtracting: $3a = -9$, so $a = -3$, $b = 14$.

3. Ngược lại với $a = -3$, $b = 14$: $P(x) = x^4 - 3x^3 + 14x - 12$ có $P(1) = 0$, nên $P = (x - 1)Q$; $P(-2) = 0$ cho $-3Q(-2) = 0$, nên $Q(-2) = 0$ và Q chia hết $x + 2$. Vậy P chia hết $(x - 1)(x + 2)$.

Conversely for $a = -3$, $b = 14$: $P(x) = x^4 - 3x^3 + 14x - 12$ has $P(1) = 0$, so $P = (x - 1)Q$; $P(-2) = 0$ gives $-3Q(-2) = 0$, so $Q(-2) = 0$ and $x + 2$ divides Q. Hence $(x - 1)(x + 2)$ divides P.

4. Chia đa thức: $x^4 - 3x^3 + 14x - 12 = (x^2 + x - 2)(x^2 - 4x + 6)$. Khai triển về phải để kiểm: $x^4 - 4x^3 + 6x^2 + x^3 - 4x^2 + 6x - 2x^2 + 8x - 12 = x^4 - 3x^3 + 0x^2 + 14x - 12$.

Polynomial division gives $x^4 - 3x^3 + 14x - 12 = (x^2 + x - 2)(x^2 - 4x + 6)$. Expanding the right side: $x^4 - 4x^3 + 6x^2 + x^3 - 4x^2 + 6x - 2x^2 + 8x - 12 = x^4 - 3x^3 + 0x^2 + 14x - 12$.

Vậy $a = -3$, $b = 14$ và thương là $x^2 - 4x + 6$.

Hence $a = -3$, $b = 14$ and the quotient is $x^2 - 4x + 6$. ■

NHẬN XÉT / REMARK — Cách khác là đồng nhất hệ số. Viết $P = (x^2 + x - 2)(x^2 + ux + v) = x^4 + (u + 1)x^3 + (v + u - 2)x^2 + (v - 2u)x - 2v$. So với $x^4 + ax^3 + 0x^2 + bx - 12$: $v = 6$, $v + u - 2 = 0$ cho $u = -4$, rồi $a = u + 1 = -3$ và $b = v - 2u = 14$. Cách này cho luôn thương, nhưng cần biết trước bậc của thương.

Another route is comparing coefficients. Write $P = (x^2 + x - 2)(x^2 + ux + v) = x^4 + (u + 1)x^3 + (v + u - 2)x^2 + (v - 2u)x - 2v$. Against $x^4 + ax^3 + 0x^2 + bx - 12$: $v = 6$, and $v + u - 2 = 0$ gives $u = -4$, then $a = u + 1 = -3$ and $b = v - 2u = 14$. This also yields the quotient, but the degree of the quotient must be known in advance.

LỖI HAY GẶP / COMMON MISTAKE — Nhầm dấu khi chia cho $x + 2$: dư là $P(-2)$, không phải $P(2)$. Muốn dùng Định lý Bézout phải viết ước dưới dạng $x - \alpha$.

Sign slip when dividing by $x + 2$: the remainder is $P(-2)$, not $P(2)$. To use Bézout's theorem the divisor must be written as $x - \alpha$.

LỖI HAY GẶP / COMMON MISTAKE — Kết luận chia hết cho tích $(x - 1)(x + 2)$ chỉ từ $P(1) = 0$ mà quên $P(-2) = 0$, hoặc ngược lại chỉ đòi hai điều kiện $P(1) = P(-2) = 0$ khi hai nghiệm trùng nhau. Với ước có nghiệm kép, chẳng hạn $(x - 1)^2$, điều kiện $P(1) = 0$ chưa đủ và phải chia hai lần.

Concluding divisibility by $(x - 1)(x + 2)$ from $P(1) = 0$ alone and forgetting $P(-2) = 0$, or asking for only $P(1) = P(-2) = 0$ when the two roots coincide. For a divisor with a double root, such as $(x - 1)^2$, the condition $P(1) = 0$ is not enough and the division must be done twice.

VÍ DỤ 5.9 (Nghiem hữu tỉ và hệ thức Viète) / EXAMPLE 5.9 (Rational roots and Vieta relations) — Cho $P(x) = x^3 - 5x^2 + 7x - 2$. (a) Tìm nghiệm hữu tỉ của P . (b) Gọi a, b, c là ba nghiệm của P ; tính $a^2 + b^2 + c^2$, $a^3 + b^3 + c^3$ và $1/a + 1/b + 1/c$.

Let $P(x) = x^3 - 5x^2 + 7x - 2$. (a) Find the rational roots of P . (b) Let a, b, c be the three roots of P ; compute $a^2 + b^2 + c^2$, $a^3 + b^3 + c^3$ and $1/a + 1/b + 1/c$.

Lời giải. / Solution.

1. (a) Hệ số đầu 1, hệ số tự do -2 , nên nghiệm hữu tỉ (nếu có) là số nguyên thuộc $\{\pm 1, \pm 2\}$ (Định lý 5.14). Ta có $P(1) = 1$, $P(-1) = -15$, $P(2) = 0$, $P(-2) = -44$. Vậy 2 là nghiệm hữu tỉ.

(a) The leading coefficient is 1 and the constant term -2 , so a rational root, if any, is an integer in $\{\pm 1, \pm 2\}$ (Theorem 5.14). We have $P(1) = 1$, $P(-1) = -15$, $P(2) = 0$, $P(-2) = -44$. So 2 is a rational root.

2. Chia cho $x - 2$: $P(x) = (x - 2)(x^2 - 3x + 1)$. Phương trình $x^2 - 3x + 1 = 0$ có biệt thức 5, hai nghiệm $(3 \pm \sqrt{5})/2$ vô tỉ. Vậy nghiệm hữu tỉ duy nhất là 2.

Dividing by $x - 2$: $P(x) = (x - 2)(x^2 - 3x + 1)$. The equation $x^2 - 3x + 1 = 0$ has discriminant 5 and irrational roots $(3 \pm \sqrt{5})/2$. So 2 is the only rational root.

3. (b) Với $p = 5$, $q = 7$, $r = 2$ (Tính chất 5.16): $a^2 + b^2 + c^2 = 25 - 14 = 11$.

(b) With $p = 5$, $q = 7$, $r = 2$ (Property 5.16): $a^2 + b^2 + c^2 = 25 - 14 = 11$.

4. $a^3 + b^3 + c^3 = 125 - 3 \cdot 5 \cdot 7 + 3 \cdot 2 = 125 - 105 + 6 = 26$ và $1/a + 1/b + 1/c = q/r = 7/2$.
 $a^3 + b^3 + c^3 = 125 - 3 \cdot 5 \cdot 7 + 3 \cdot 2 = 125 - 105 + 6 = 26$ and $1/a + 1/b + 1/c = q/r = 7/2$.

5. Kiểm tra trực tiếp với nghiệm 2 và $(3 \pm \sqrt{5})/2$: tổng bình phương $4 + 7 = 11$, tổng lập phương $8 + 18 = 26$.

Direct check with roots 2 and $(3 \pm \sqrt{5})/2$: sum of squares $4 + 7 = 11$, sum of cubes $8 + 18 = 26$.

Vậy $a^2 + b^2 + c^2 = 11$, $a^3 + b^3 + c^3 = 26$, $1/a + 1/b + 1/c = 7/2$.

Hence $a^2 + b^2 + c^2 = 11$, $a^3 + b^3 + c^3 = 26$, $1/a + 1/b + 1/c = 7/2$. ■

NHẬN XÉT / REMARK — Khi hệ số đầu khác 1, các nghiệm hữu tỉ p/q có p thuộc ước của a_0 và q thuộc ước của a_n . Với $6x^3 - 19x^2 - 26x + 24$, $p \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$ và $q \in \{1, 2, 3, 6\}$. Thử lần lượt cho ba nghiệm 4, $2/3$ và $-3/2$. Với $x^3 - 3x - 1$ các ứng viên ± 1 đều không phải nghiệm, nên đa thức không có nghiệm hữu tỉ.

When the leading coefficient is not 1, a rational root p/q has p dividing a_0 and q dividing a_n . For $6x^3 - 19x^2 - 26x + 24$, $p \in \{\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 8, \pm 12, \pm 24\}$ and $q \in \{1, 2, 3, 6\}$. Testing the candidates gives the three roots 4, $2/3$ and $-3/2$. For $x^3 - 3x - 1$ the candidates ± 1 are not roots, so the polynomial has no rational root.

PHẢI THUỘC / MEMORISE — Bézout: P chia $x - \alpha$ dư $P(\alpha)$. Viète bậc ba: $p = a + b + c$, $q = ab + bc + ca$, $r = abc$; $a^2 + b^2 + c^2 = p^2 - 2q$; $a^3 + b^3 + c^3 = p^3 - 3pq + 3r$.

Bézout: P divided by $x - \alpha$ leaves $P(\alpha)$. Cubic Vieta: $p = a + b + c$, $q = ab + bc + ca$, $r = abc$; $a^2 + b^2 + c^2 = p^2 - 2q$; $a^3 + b^3 + c^3 = p^3 - 3pq + 3r$.

LỖI HAY GẶP / COMMON MISTAKE — Cho rằng đa thức bậc n có đúng n nghiệm thực. Đa thức $x^2 + 1$ có bậc 2 mà không có nghiệm thực; Định lý Viète bậc n chỉ dùng được khi đã biết có đủ n nghiệm (thực hay phức).

Assuming a polynomial of degree n has exactly n real roots. The polynomial $x^2 + 1$ has degree 2 and no real root; Vieta's formulas of degree n apply only when n roots (real or complex) are known to exist.

5.5. Đa thức hệ số nguyên và nội suy Lagrange — Integer polynomials and Lagrange interpolation

ĐỊNH LÝ 5.17 (Tính chất hiệu của đa thức nguyên) / THEOREM 5.17 (Difference property of integer polynomials) — Nếu $P \in \mathbb{Z}[x]$ và a, b là hai số nguyên khác nhau thì $(a - b) \mid P(a) - P(b)$.

If $P \in \mathbb{Z}[x]$ and a, b are distinct integers then $(a - b) \mid P(a) - P(b)$.

Chứng minh. / Proof.

Viết $P(x) = \sum c_k x^k$ với $c_k \in \mathbb{Z}$. Khi đó $P(a) - P(b) = \sum c_k (a^k - b^k)$.

Write $P(x) = \sum c_k x^k$ with $c_k \in \mathbb{Z}$. Then $P(a) - P(b) = \sum c_k (a^k - b^k)$.

Mỗi hiệu $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \dots + b^{k-1})$ chia hết cho $a - b$, nên tổng cũng chia hết.

Each difference $a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \dots + b^{k-1})$ is divisible by $a - b$, hence so is the sum. ■

HỆ QUẢ 5.18 / COROLLARY 5.18 — Nếu $P \in \mathbb{Z}[x]$, s là số nguyên dương và $m \equiv n \pmod{s}$ thì $P(m) \equiv P(n) \pmod{s}$. Đặc biệt, giá trị $P(n)$ theo modulo s chỉ phụ thuộc vào $n \pmod{s}$.
If $P \in \mathbb{Z}[x]$, s is a positive integer and $m \equiv n \pmod{s}$ then $P(m) \equiv P(n) \pmod{s}$. In particular $P(n)$ modulo s depends only on $n \pmod{s}$.

Chứng minh. / Proof.

Nếu $m = n$ thì hiển nhiên. Nếu $m \neq n$ thì $s \mid m - n \mid P(m) - P(n)$ theo Định lý 5.17.

If $m = n$ this is trivial. If $m \neq n$ then $s \mid m - n \mid P(m) - P(n)$ by Theorem 5.17. ■

ĐỊNH LÝ 5.19 (Nội suy Lagrange) / THEOREM 5.19 (Lagrange interpolation) — Cho $n + 1$ số thực đôi một khác nhau $x_0, \dots, x_n$ và $n + 1$ số thực $y_0, \dots, y_n$. Tồn tại duy nhất đa thức P bậc không quá n thỏa $P(x_i) = y_i$ với mọi i , và nó cho bởi công thức nội suy Lagrange.
Given $n + 1$ distinct reals $x_0, \dots, x_n$ and any $n + 1$ reals $y_0, \dots, y_n$, there is exactly one polynomial P of degree at most n with $P(x_i) = y_i$ for all i , and it is given by the Lagrange interpolation formula.

Chứng minh. / Proof.

Đặt $L_i(x) = \prod (x - x_j)/(x_i - x_j)$ lấy theo mọi $j \neq i$. Mỗi L_i có bậc n , $L_i(x_i) = 1$ và $L_i(x_j) = 0$ với $j \neq i$. Do đó

Put $L_i(x) = \prod (x - x_j)/(x_i - x_j)$ over all $j \neq i$. Each L_i has degree n , $L_i(x_i) = 1$ and $L_i(x_j) = 0$ for $j \neq i$. Therefore

$$P(x) = y_0 L_0(x) + y_1 L_1(x) + \dots + y_n L_n(x) \quad (5.4)$$

có bậc không quá n và $P(x_i) = y_i$. Duy nhất: hai đa thức như vậy có hiệu bậc không quá n và triệt tiêu tại $n + 1$ điểm, nên bằng không theo Hệ quả 5.13.

has degree at most n and $P(x_i) = y_i$. Uniqueness: two such polynomials have a difference of degree at most n vanishing at $n + 1$ points, so it is zero by Corollary 5.13. ■

HỆ QUẢ 5.20 / COROLLARY 5.20 — Cho P là đa thức và $x_0, \dots, x_n$ đôi một khác nhau.

Dư của P khi chia cho $(x - x_0)\dots(x - x_n)$ là đa thức nội suy bậc không quá n qua các điểm $(x_i, P(x_i))$.

Let P be a polynomial and $x_0, \dots, x_n$ distinct. The remainder of P on division by $(x - x_0)\dots(x - x_n)$ is the interpolating polynomial of degree at most n through the points $(x_i, P(x_i))$.

Chứng minh. / Proof.

Viết $P = BQ + R$ với $B = (x - x_0)\dots(x - x_n)$ và $\deg R \leq n$. Tại mỗi x_i , $B(x_i) = 0$ nên $R(x_i) = P(x_i)$. Theo tính duy nhất của Định lý 5.19, R là đa thức nội suy.

Write $P = BQ + R$ with $B = (x - x_0)\dots(x - x_n)$ and $\deg R \leq n$. At each x_i , $B(x_i) = 0$ so $R(x_i) = P(x_i)$. By the uniqueness in Theorem 5.19, R is the interpolating polynomial. ■

PHÂN TÍCH / ANALYSIS — Ba số a, b, c khác nhau xoay vòng qua P . Tính chất hiệu cho ba quan hệ chia hết nối các hiệu $a - b, b - c, c - a$ theo vòng tròn; chia hết theo vòng tròn buộc ba hiệu có cùng giá trị tuyệt đối. Sau đó chỉ còn một xung đột về tổng.

The distinct numbers a, b, c cycle through P . The difference property gives three divisibility relations linking $a - b, b - c, c - a$ in a circle; divisibility around a circle forces the three differences to have the same absolute value. After that, only a conflict about their sum remains.

VÍ DỤ 5.10 (Tính chất hiệu và chia hết vòng tròn) / EXAMPLE 5.10 (Difference property and circular divisibility) — Có tồn tại hay không đa thức $P \in \mathbb{Z}[x]$ và ba số nguyên đôi một khác nhau a, b, c sao cho $P(a) = b, P(b) = c, P(c) = a$?

Do there exist a polynomial $P \in \mathbb{Z}[x]$ and three pairwise distinct integers a, b, c with $P(a) = b, P(b) = c, P(c) = a$?

Lời giải. / Solution.

- Giả sử có. Theo Định lý 5.17: $(a - b) \mid P(a) - P(b) = b - c$, $(b - c) \mid P(b) - P(c) = c - a$, $(c - a) \mid P(c) - P(a) = a - b$. Ba hiệu $a - b, b - c, c - a$ đều khác 0.

Suppose they exist. By Theorem 5.17: $(a - b) \mid P(a) - P(b) = b - c$, $(b - c) \mid P(b) - P(c) = c - a$, $(c - a) \mid P(c) - P(a) = a - b$. The three differences $a - b, b - c, c - a$ are all nonzero.

- Chia hết giữa các số khác 0 cho $|a - b| \leq |b - c| \leq |c - a| \leq |a - b|$. Vậy ba giá trị tuyệt đối bằng nhau, gọi chung là $t > 0$.

Divisibility between nonzero integers gives $|a - b| \leq |b - c| \leq |c - a| \leq |a - b|$. So the three absolute values are equal, say to $t > 0$.

- Mỗi hiệu bằng t hoặc $-t$. Giả sử có k hiệu bằng t ; tổng ba hiệu là $(a - b) + (b - c) + (c - a) = 0 = (k - (3 - k))t = (2k - 3)t$. Vì $2k - 3$ là số lẻ, nó khác 0, nên $(2k - 3)t \neq 0$.

Mâu thuẫn.

Each difference equals t or $-t$. If k of them equal t , the sum $(a - b) + (b - c) + (c - a) = 0$ equals $(k - (3 - k))t = (2k - 3)t$. Since $2k - 3$ is odd it is nonzero, so $(2k - 3)t \neq 0$.

Contradiction.

Vậy không tồn tại P và a, b, c như vậy.

Hence no such P, a, b, c exist. ■

NHẬN XÉT / REMARK — Kết quả vẫn đúng cho chu trình độ dài lẻ bất kỳ. Với chu trình độ dài 2 ($P(a) = b, P(b) = a$) thì lập luận không dùng được và có ví dụ: $P(x) = -x + (a + b)$ hoán đổi a và b .

The result extends to cycles of any odd length. For a cycle of length 2 ($P(a) = b, P(b) = a$) the argument fails and examples exist: $P(x) = -x + (a + b)$ swaps a and b .

VÍ DỤ 5.11 (Dư qua nội suy) / EXAMPLE 5.11 (Remainders by interpolation) — Đa thức P chia cho $x - 1$ dư 4, chia cho $x + 2$ dư 1, chia cho $x - 3$ dư -5 . Tìm dư của P khi chia cho $(x - 1)(x + 2)(x - 3)$.

A polynomial P leaves remainder 4 on division by $x - 1$, remainder 1 on division by $x + 2$ and remainder -5 on division by $x - 3$. Find the remainder of P on division by $(x - 1)(x + 2)(x - 3)$.

Lời giải. / Solution.

1. Theo Định lý 5.12: $P(1) = 4, P(-2) = 1, P(3) = -5$. Dư R cần tìm có bậc không quá 2 và $R(1) = 4, R(-2) = 1, R(3) = -5$ (Hệ quả 5.20).

By Theorem 5.12: $P(1) = 4, P(-2) = 1, P(3) = -5$. The required remainder R has degree at most 2 and $R(1) = 4, R(-2) = 1, R(3) = -5$ (Corollary 5.20).

2. Các mẫu số của L_i : tại $x = 1$: $(1 + 2)(1 - 3) = -6$; tại $x = -2$: $(-2 - 1)(-2 - 3) = 15$; tại $x = 3$: $(3 - 1)(3 + 2) = 10$.

The denominators of the L_i : at $x = 1$: $(1 + 2)(1 - 3) = -6$; at $x = -2$: $(-2 - 1)(-2 - 3) = 15$; at $x = 3$: $(3 - 1)(3 + 2) = 10$.

$$R(x) = 4 \cdot (x + 2)(x - 3) / (-6) + 1 \cdot (x - 1)(x - 3) / 15 + (-5) \cdot (x - 1)(x + 2) / 10$$

3. Quy đồng mẫu 30: $R(x) = [-20(x^2 - x - 6) + 2(x^2 - 4x + 3) - 15(x^2 + x - 2)] / 30 = (-33x^2 - 3x + 156) / 30$.

Over the common denominator 30: $R(x) = [-20(x^2 - x - 6) + 2(x^2 - 4x + 3) - 15(x^2 + x - 2)] / 30 = (-33x^2 - 3x + 156) / 30$.

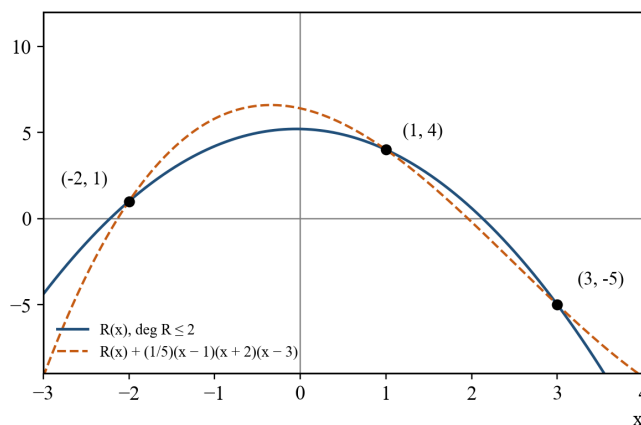
$$R(x) = (-11x^2 - x + 52) / 10$$

4. Kiểm tra: $R(1) = (-11 - 1 + 52) / 10 = 4$; $R(-2) = (-44 + 2 + 52) / 10 = 1$; $R(3) = (-99 - 3 + 52) / 10 = -5$.

Check: $R(1) = (-11 - 1 + 52) / 10 = 4$; $R(-2) = (-44 + 2 + 52) / 10 = 1$; $R(3) = (-99 - 3 + 52) / 10 = -5$.

Vậy dư là $R(x) = (-11x^2 - x + 52) / 10$.

Hence the remainder is $R(x) = (-11x^2 - x + 52) / 10$. ■



Hình 5.3. Đa thức bậc không quá 2 qua ba điểm cho trước (đường liền) và một đa thức bậc 3 qua cùng ba điểm (đường đứt)

Figure 5.3. The polynomial of degree at most 2 through three given points (solid) and a cubic through the same points (dashed)

LỖI HAY GẶP / COMMON MISTAKE — Cho rằng dư khi chia cho tích ba nhị thức là hằng số hoặc bậc nhất. Dư có bậc không quá 2; số điều kiện cần bằng số nghiệm của ước.
Assuming the remainder on division by a product of three linear factors is constant or linear. The remainder has degree at most 2; the number of conditions needed equals the number of roots of the divisor.

5.6. Dãy số truy hồi tuyến tính — Linear recurrence sequences

ĐỊNH NGHĨA 5.21 (Dãy truy hồi tuyến tính) / DEFINITION 5.21 (Linear recurrence)

— Dãy (a_n) gọi là truy hồi tuyến tính cấp 1 nếu $a_{n+1} = pa_n + q$ với các hằng số p, q , và cấp 2 nếu $a_{n+2} = pa_{n+1} + qa_n$. Với cấp 2, phương trình $r^2 = pr + q$ gọi là phương trình đặc trưng.

A sequence (a_n) is a first-order linear recurrence if $a_{n+1} = pa_n + q$ for constants p, q , and a second-order one if $a_{n+2} = pa_{n+1} + qa_n$. For the second order, the equation $r^2 = pr + q$ is the characteristic equation.

ĐỊNH LÝ 5.22 (Truy hồi cấp 1) / THEOREM 5.22 (First-order recurrence) — Cho $a_{n+1} = pa_n + q$ với $p \neq 1$. Đặt $c = q/(1 - p)$. Khi đó $a_n - c = p^{n-1}(a_1 - c)$ với mọi $n \geq 1$. Nếu $p = 1$ thì $a_n = a_1 + (n - 1)q$.

Let $a_{n+1} = pa_n + q$ with $p \neq 1$ and put $c = q/(1 - p)$. Then $a_n - c = p^{n-1}(a_1 - c)$ for all $n \geq 1$. If $p = 1$ then $a_n = a_1 + (n - 1)q$.

Chứng minh. / Proof.

Vì $c = pc + q$ nên $a_{n+1} - c = pa_n + q - pc - q = p(a_n - c)$. Vậy $(a_n - c)$ là cấp số nhân công bội p .

Since $c = pc + q$, we get $a_{n+1} - c = pa_n + q - pc - q = p(a_n - c)$. So $(a_n - c)$ is a geometric progression with ratio p .

$$a_n = c + p^{n-1}(a_1 - c) \quad (5.5)$$

Với $p = 1$, $a_{n+1} - a_n = q$ không đổi: cấp số cộng.

For $p = 1$, $a_{n+1} - a_n = q$ is constant: an arithmetic progression. ■

TÍNH CHẤT 5.23 / PROPERTY 5.23 — Với $a_{n+1} = pa_n + c \cdot s^n$ và $s \neq p$, dãy λs^n với $\lambda = c/(s - p)$ là một nghiệm riêng, và $a_n - \lambda s^n$ thỏa truy hồi thuần nhất $b_{n+1} = pb_n$.
For $a_{n+1} = pa_n + c \cdot s^n$ with $s \neq p$, the sequence λs^n with $\lambda = c/(s - p)$ is a particular solution, and $a_n - \lambda s^n$ satisfies the homogeneous recurrence $b_{n+1} = pb_n$.

Chứng minh. / Proof.

Thay λs^n vào: $\lambda s^{n+1} = p\lambda s^n + cs^n$ khi và chỉ khi $\lambda(s - p) = c$. Hiệu của hai nghiệm cùng truy hồi thì thỏa phần thuần nhất.

Substituting λs^n : $\lambda s^{n+1} = p\lambda s^n + cs^n$ if and only if $\lambda(s - p) = c$. The difference of two solutions of the same recurrence satisfies the homogeneous part. ■

ĐỊNH LÝ 5.24 (Truy hồi cấp 2) / THEOREM 5.24 (Second-order recurrence) — Cho $a_{n+2} = pa_{n+1} + qa_n$ ($n \geq 0$) với phương trình đặc trưng $r^2 = pr + q$. (i) Nếu có hai nghiệm thực phân biệt r_1, r_2 thì $a_n = Ar_1^n + Br_2^n$, trong đó $A = (a_1 - r_2a_0)/(r_1 - r_2)$ và $B = (r_1a_0 - a_1)/(r_1 - r_2)$. (ii) Nếu có nghiệm kép $r \neq 0$ thì $a_n = (A + Bn)r^n$, với $A = a_0$ và $B = (a_1 - ra_0)/r$.
Let $a_{n+2} = pa_{n+1} + qa_n$ ($n \geq 0$) with characteristic equation $r^2 = pr + q$. (i) If there are two distinct real roots r_1, r_2 then $a_n = Ar_1^n + Br_2^n$, where $A = (a_1 - r_2a_0)/(r_1 - r_2)$ and $B = (r_1a_0 - a_1)/(r_1 - r_2)$. (ii) If there is a double root $r \neq 0$ then $a_n = (A + Bn)r^n$, with $A = a_0$ and $B = (a_1 - ra_0)/r$.

Chứng minh. / Proof.

(i) Dãy r^n thỏa truy hồi vì $r^{n+2} = pr^{n+1} + qr^n$ khi $r^2 = pr + q$. Do truy hồi tuyến tính, $Ar_1^n + Br_2^n$ cũng thỏa. Với A, B như trên, tại $n = 0$ ta có $A + B = a_0$ và tại $n = 1$ có $Ar_1 + Br_2 = a_1$. Hai dãy cùng truy hồi và cùng hai số hạng đầu thì bằng nhau (quy nạp), nên đó là a_n .

(i) The sequence r^n satisfies the recurrence because $r^{n+2} = pr^{n+1} + qr^n$ when $r^2 = pr + q$. By linearity $Ar_1^n + Br_2^n$ satisfies it too. With A, B as above, $A + B = a_0$ at $n = 0$ and $Ar_1 + Br_2 = a_1$ at $n = 1$. Two sequences with the same recurrence and the same first two terms coincide (induction), so this is a_n .

(ii) Nghiệm kép nghĩa là $p = 2r, q = -r^2$. Với $n \cdot r^n$: $p(n+1)r^{n+1} + qnr^n = 2(n+1)r^{n+2} - nr^{n+2} = (n+2)r^{n+2}$. Vậy nr^n thỏa truy hồi. Chọn A, B để khớp $a_0 = A$ và $a_1 = (A+B)r$, rồi kết luận như trên.

(ii) A double root means $p = 2r, q = -r^2$. For $n \cdot r^n$: $p(n+1)r^{n+1} + qnr^n = 2(n+1)r^{n+2} - nr^{n+2} = (n+2)r^{n+2}$. So nr^n satisfies the recurrence. Choose A, B to match $a_0 = A$ and $a_1 = (A+B)r$, and conclude as before. ■

VÍ DỤ 5.12 (Nghiệm riêng và phương trình đặc trưng) / EXAMPLE 5.12 (Particular solution and characteristic equation) — (a) Cho $a_1 = 1$ và $a_{n+1} = 3a_n + 2^n$. Tìm a_n . (b) Cho $b_0 = 2, b_1 = 3$ và $b_{n+2} = 6b_{n+1} - 9b_n$. Tìm b_n .
(a) Let $a_1 = 1$ and $a_{n+1} = 3a_n + 2^n$. Find a_n . (b) Let $b_0 = 2, b_1 = 3$ and $b_{n+2} = 6b_{n+1} - 9b_n$. Find b_n .

Lời giải. / Solution.

1. (a) Theo Tính chất 5.23 với $p = 3, s = 2, c = 1$: $\lambda = 1/(2 - 3) = -1$. Đặt $u_n = a_n + 2^n$. Khi đó $u_{n+1} = 3a_n + 2^n + 2^{n+1} = 3a_n + 3 \cdot 2^n = 3u_n$.

(a) By Property 5.23 with $p = 3, s = 2, c = 1$: $\lambda = 1/(2 - 3) = -1$. Put $u_n = a_n + 2^n$. Then $u_{n+1} = 3a_n + 2^n + 2^{n+1} = 3a_n + 3 \cdot 2^n = 3u_n$.

2. $u_1 = 1 + 2 = 3$, nên $u_n = 3^n$ và $a_n = 3^n - 2^n$. Kiểm tra: $a_2 = 3 \cdot 1 + 2 = 5 = 9 - 4$; $a_3 = 3 \cdot 5 + 4 = 19 = 27 - 8$.

$u_1 = 1 + 2 = 3$, so $u_n = 3^n$ and $a_n = 3^n - 2^n$. Check: $a_2 = 3 \cdot 1 + 2 = 5 = 9 - 4$; $a_3 = 3 \cdot 5 + 4 = 19 = 27 - 8$.

3. (b) Phương trình đặc trưng $r^2 - 6r + 9 = 0$ có nghiệm kép $r = 3$. Theo Định lý 5.24(ii), $b_n = (A + Bn)3^n$ với $A = b_0 = 2$.

(b) The characteristic equation $r^2 - 6r + 9 = 0$ has the double root $r = 3$. By Theorem 5.24(ii), $b_n = (A + Bn)3^n$ with $A = b_0 = 2$.

4. $b_1 = (2 + B) \cdot 3 = 3$ cho $B = -1$. Vậy $b_n = (2 - n)3^n$. Kiểm tra: $b_2 = 6 \cdot 3 - 9 \cdot 2 = 0 = (2 - 2) \cdot 9$; $b_3 = 6 \cdot 0 - 9 \cdot 3 = -27 = (2 - 3) \cdot 27$.

$b_1 = (2 + B) \cdot 3 = 3$ gives $B = -1$. So $b_n = (2 - n)3^n$. Check: $b_2 = 6 \cdot 3 - 9 \cdot 2 = 0 = (2 - 2) \cdot 9$; $b_3 = 6 \cdot 0 - 9 \cdot 3 = -27 = (2 - 3) \cdot 27$.

Vậy $a_n = 3^n - 2^n$ và $b_n = (2 - n)3^n$.

Hence $a_n = 3^n - 2^n$ and $b_n = (2 - n)3^n$. ■

$$a_n = A \cdot r_1^n + B \cdot r_2^n \quad (5.6)$$

$$a_n = (A + B \cdot n) \cdot r^n \quad (5.7)$$

NHẬN XÉT / REMARK — Dãy Fibonacci $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$ có $r^2 = r + 1$, hai nghiệm $\varphi = (1 + \sqrt{5})/2$ và $\psi = (1 - \sqrt{5})/2$. Theo Định lý 5.24(i), $A = 1/\sqrt{5}, B = -1/\sqrt{5}$, nên $F_n = (\varphi^n - \psi^n)/\sqrt{5}$. Công thức chứa số vô tỉ nhưng cho giá trị nguyên với mọi n .

The Fibonacci sequence $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$ has $r^2 = r + 1$ with roots $\varphi = (1 + \sqrt{5})/2$ and $\psi = (1 - \sqrt{5})/2$. By Theorem 5.24(i), $A = 1/\sqrt{5}, B = -1/\sqrt{5}$, so $F_n = (\varphi^n - \psi^n)/\sqrt{5}$. The formula contains irrational numbers yet gives an integer for every n .

$$F_n = (\varphi^n - \psi^n)/\sqrt{5}, \quad \varphi = (1 + \sqrt{5})/2, \quad \psi = (1 - \sqrt{5})/2 \quad (5.8)$$

LỖI HAY GẶP / COMMON MISTAKE — Với nghiệm kép viết $a_n = Ar^n + Br^n = (A + B)r^n$: chỉ còn một hằng số tự do nên không khớp được hai số hạng đầu. Dạng đúng là $(A + Bn)r^n$.

For a double root writing $a_n = Ar^n + Br^n = (A + B)r^n$: only one free constant remains, so two initial terms cannot be matched. The correct form is $(A + Bn)r^n$.

PHẢI THUỘC / MEMORISE — Cấp 2: nghiệm phân biệt r_1, r_2 cho $a_n = Ar_1^n + Br_2^n$; nghiệm kép r cho $a_n = (A + Bn)r^n$; A, B tìm từ a_0, a_1 .

Second order: distinct roots r_1, r_2 give $a_n = Ar_1^n + Br_2^n$; a double root r gives $a_n = (A + Bn)r^n$; A, B come from a_0, a_1 .

5.7. Dãy tuần hoàn, tổng sai phân và dãy nguyên — Periodic sequences, telescoping sums and integer sequences

ĐỊNH NGHĨA 5.25 (Dãy tuần hoàn) / DEFINITION 5.25 (Periodic sequence) — Dãy (a_n) gọi là tuần hoàn với chu kỳ $T \geq 1$ (từ vị trí i) nếu $a_{n+T} = a_n$ với mọi $n \geq i$. Khi $i = 1$ dãy gọi là tuần hoàn thuần túy.

A sequence (a_n) is periodic with period $T \geq 1$ (from position i) if $a_{n+T} = a_n$ for all $n \geq i$. When $i = 1$ it is purely periodic.

BỔ ĐỀ 5.26 / LEMMA 5.26 — Giả sử mọi số hạng của dãy thuộc một tập hữu hạn X , và mỗi số hạng từ a_3 trở đi được xác định duy nhất bởi hai số hạng liền trước. Khi đó dãy tuần hoàn từ một vị trí nào đó.

Suppose every term of a sequence lies in a finite set X and each term from a_3 on is determined uniquely by the two terms before it. Then the sequence is periodic from some position on.

Chứng minh. / Proof.

Có không quá $|X|^2$ cặp (a_n, a_{n+1}) khác nhau. Xét $|X|^2 + 1$ cặp đầu tiên: theo nguyên lý Dirichlet có $i < j$ với $(a_i, a_{i+1}) = (a_j, a_{j+1})$.

There are at most $|X|^2$ distinct pairs (a_n, a_{n+1}) . Among the first $|X|^2 + 1$ pairs the pigeonhole principle gives $i < j$ with $(a_i, a_{i+1}) = (a_j, a_{j+1})$.

Vì mỗi số hạng được xác định bởi hai số hạng liền trước, quy nạp cho $a_{i+k} = a_{j+k}$ với mọi $k \geq 0$. Vậy dãy tuần hoàn từ vị trí i với chu kỳ $j - i$.

Since each term is determined by the two before it, induction gives $a_{i+k} = a_{j+k}$ for all $k \geq 0$. So the sequence is periodic from position i with period $j - i$. ■

NHẬN XÉT / REMARK — Áp dụng cho dãy Fibonacci lấy theo modulo m : các cặp $(F_n \bmod m, F_{n+1} \bmod m)$ chỉ có m^2 khả năng, nên dãy dư tuần hoàn. Với $m = 10$ chu kỳ là 60, vì thế chữ số tận cùng của F_n lặp lại sau mỗi 60 số hạng.

Applied to the Fibonacci sequence modulo m : the pairs $(F_n \bmod m, F_{n+1} \bmod m)$ have only m^2 possibilities, so the residue sequence is periodic. For $m = 10$ the period is 60, so the last digit of F_n repeats every 60 terms.

ĐỊNH LÝ 5.27 (Tổng sai phân (tổng thu gọn)) / THEOREM 5.27 (Telescoping sum) —

Với dãy bất kỳ (c_k) , $\sum_{k=1}^n (c_{k+1} - c_k) = c_{n+1} - c_1$.

For any sequence (c_k) , $\sum_{k=1}^n (c_{k+1} - c_k) = c_{n+1} - c_1$.

Chứng minh. / Proof.

Quy nạp theo n . Với $n = 1$ hai vế cùng bằng $c_2 - c_1$. Nếu đúng với n thì $\sum_{k=1}^{n+1} (c_{k+1} - c_k) = (c_{n+1} - c_1) + (c_{n+2} - c_{n+1}) = c_{n+2} - c_1$.

Induction on n . For $n = 1$ both sides equal $c_2 - c_1$. If true for n then $\sum_{k=1}^{n+1} (c_{k+1} - c_k) = (c_{n+1} - c_1) + (c_{n+2} - c_{n+1}) = c_{n+2} - c_1$. ■

HỆ QUẢ 5.28 / COROLLARY 5.28 — Với mọi $n \in \mathbb{Z}^+$: $1 + 2 + \dots + n = n(n+1)/2$ và $1^2 + 2^2 + \dots + n^2 = n(n+1)(2n+1)/6$.

For every $n \in \mathbb{Z}^+$: $1 + 2 + \dots + n = n(n+1)/2$ and $1^2 + 2^2 + \dots + n^2 = n(n+1)(2n+1)/6$.

Chứng minh. / Proof.

Áp dụng Định lý 5.27 cho $c_k = k^2$: $\sum (2k+1) = (n+1)^2 - 1$, tức $2(1 + \dots + n) + n = n^2 + 2n$, suy ra tổng đầu bằng $n(n+1)/2$.

Apply Theorem 5.27 with $c_k = k^2$: $\sum (2k+1) = (n+1)^2 - 1$, that is $2(1 + \dots + n) + n = n^2 + 2n$, which gives the first sum $n(n+1)/2$.

Với $c_k = k^3$: $\Sigma (3k^2 + 3k + 1) = (n + 1)^3 - 1$. Gọi S là tổng bình phương, ta có $3S = (n + 1)^3 - 1 - 3n(n + 1)/2 - n = (n + 1)[(n + 1)^2 - 1 - 3n/2] = (n + 1)(n^2 + n/2) = n(n + 1)(2n + 1)/2$.

With $c_k = k^3$: $\Sigma (3k^2 + 3k + 1) = (n + 1)^3 - 1$. Writing S for the sum of squares, $3S = (n + 1)^3 - 1 - 3n(n + 1)/2 - n = (n + 1)[(n + 1)^2 - 1 - 3n/2] = (n + 1)(n^2 + n/2) = n(n + 1)(2n + 1)/2$.

Chia cho 3 được công thức thứ hai.

Dividing by 3 gives the second formula. ■

$$1^2 + 2^2 + \dots + n^2 = n(n + 1)(2n + 1)/6 \quad (5.9)$$

VÍ DỤ 5.13 (Chu kỳ và tổng thu gọn) / EXAMPLE 5.13 (Period and telescoping) — (a)

Dãy (a_n) có $a_1 = x$, $a_2 = y$ và $a_{n+2} = a_{n+1} - a_n$. Tính tổng của 2026 số hạng đầu theo x, y . (b) Rút gọn $T_n = \Sigma_{k=1}^n 1/(k(k + 1)(k + 2))$.

(a) A sequence (a_n) has $a_1 = x$, $a_2 = y$ and $a_{n+2} = a_{n+1} - a_n$. Find the sum of its first 2026 terms in terms of x, y . (b) Simplify $T_n = \Sigma_{k=1}^n 1/(k(k + 1)(k + 2))$.

Lời giải. / Solution.

1. (a) Tính các số hạng đầu: $x, y, y - x, -x, -y, x - y, x, y, \dots$ Từ $a_7 = a_1$ và $a_8 = a_2$, theo truy hồi dãy tuần hoàn thuần túy chu kỳ 6.

(a) The first terms are $x, y, y - x, -x, -y, x - y, x, y, \dots$ Since $a_7 = a_1$ and $a_8 = a_2$, the recurrence makes the sequence purely periodic with period 6.

2. Tổng sáu số hạng liên tiếp: $x + y + (y - x) + (-x) + (-y) + (x - y) = 0$. Vì $2026 = 6 \cdot 337 + 4$, tổng cần tìm bằng tổng bốn số hạng đầu: $x + y + (y - x) - x = 2y - x$.

The sum of six consecutive terms is $x + y + (y - x) + (-x) + (-y) + (x - y) = 0$. Since $2026 = 6 \cdot 337 + 4$, the required sum equals the sum of the first four terms: $x + y + (y - x) - x = 2y - x$.

3. (b) Ta có $1/(k(k + 1)) - 1/((k + 1)(k + 2)) = ((k + 2) - k)/(k(k + 1)(k + 2)) = 2/(k(k + 1)(k + 2))$. Do đó $1/(k(k + 1)(k + 2)) = (1/2)(c_k - c_{k+1})$ với $c_k = 1/(k(k + 1))$.

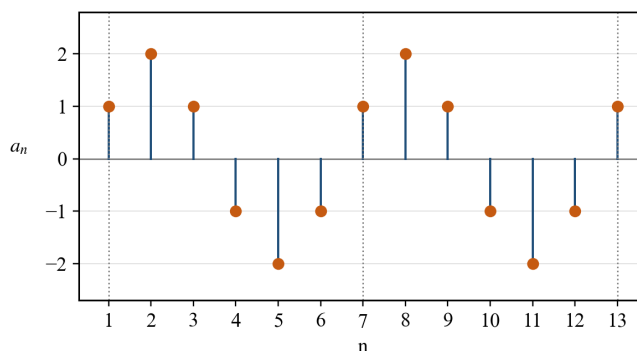
(b) We have $1/(k(k + 1)) - 1/((k + 1)(k + 2)) = ((k + 2) - k)/(k(k + 1)(k + 2)) = 2/(k(k + 1)(k + 2))$. Hence $1/(k(k + 1)(k + 2)) = (1/2)(c_k - c_{k+1})$ with $c_k = 1/(k(k + 1))$.

4. Theo Định lý 5.27, $T_n = (1/2)(c_1 - c_{n+1}) = (1/2)(1/2 - 1/((n + 1)(n + 2))) = 1/4 - 1/(2(n + 1)(n + 2))$. Với $n = 1$: $1/4 - 1/12 = 1/6 = 1/(1 \cdot 2 \cdot 3)$.

By Theorem 5.27, $T_n = (1/2)(c_1 - c_{n+1}) = (1/2)(1/2 - 1/((n + 1)(n + 2))) = 1/4 - 1/(2(n + 1)(n + 2))$. For $n = 1$: $1/4 - 1/12 = 1/6 = 1/(1 \cdot 2 \cdot 3)$.

Vậy (a) tổng bằng $2y - x$; (b) $T_n = 1/4 - 1/(2(n + 1)(n + 2))$.

Hence (a) the sum is $2y - x$; (b) $T_n = 1/4 - 1/(2(n + 1)(n + 2))$. ■



Hình 5.4. Dãy $a_{n+2} = a_{n+1} - a_n$ với $a_1 = 1, a_2 = 2$ lặp lại sau mỗi sáu số hạng

Figure 5.4. The sequence $a_{n+2} = a_{n+1} - a_n$ with $a_1 = 1, a_2 = 2$ repeats every six terms

PHÂN TÍCH / ANALYSIS — Hệ thức $a_{n+1}a_{n-1} = a_n^2 + 2$ chứa tích nên không tuyến tính, và chia cho a_{n-1} chưa cho tính nguyên. Hãy thử vài số hạng: 1, 1, 3, 11, 41, 153. Mỗi số bằng 4 lần số trước trừ số trước nữa ($11 = 4 \cdot 3 - 1$, $41 = 4 \cdot 11 - 3$), gợi ý một truy hồi tuyến tính. Ta dựng dãy tuyến tính đó, chứng minh nó thỏa hệ thức bằng một đại lượng bất biến, rồi suy ra hai dãy trùng nhau.

The relation $a_{n+1}a_{n-1} = a_n^2 + 2$ contains a product, so it is not linear, and dividing by a_{n-1} does not yet give integrality. Try a few terms: 1, 1, 3, 11, 41, 153. Each equals 4 times the previous term minus the one before ($11 = 4 \cdot 3 - 1$, $41 = 4 \cdot 11 - 3$), which suggests a linear recurrence. We build that linear sequence, prove it satisfies the relation using an invariant, and conclude that the two sequences coincide.

VÍ DỤ 5.14 (Dựng dãy tuyến tính và bất biến) / EXAMPLE 5.14 (Building a linear sequence and an invariant) — Dãy (a_n) có $a_0 = a_1 = 1$ và $a_{n+1}a_{n-1} = a_n^2 + 2$ với mọi $n \geq 1$. Chứng minh mọi a_n là số nguyên dương và $a_{n+1} = 4a_n - a_{n-1}$.

A sequence (a_n) has $a_0 = a_1 = 1$ and $a_{n+1}a_{n-1} = a_n^2 + 2$ for all $n \geq 1$. Prove that every a_n is a positive integer and $a_{n+1} = 4a_n - a_{n-1}$.

Lời giải. / Solution.

1. Định nghĩa dãy (b_n) bởi $b_0 = b_1 = 1$ và $b_{n+1} = 4b_n - b_{n-1}$. Ta có $b_2 = 3 > b_1 > 0$. Quy nạp: nếu $b_{n+1} > b_n > 0$ thì $b_{n+2} - b_{n+1} = 3b_{n+1} - b_n > 0$, nên mọi b_n là số nguyên dương và dãy tăng ngặt từ $n = 1$.
Define (b_n) by $b_0 = b_1 = 1$ and $b_{n+1} = 4b_n - b_{n-1}$. Then $b_2 = 3 > b_1 > 0$. By induction, if $b_{n+1} > b_n > 0$ then $b_{n+2} - b_{n+1} = 3b_{n+1} - b_n > 0$, so every b_n is a positive integer and the sequence increases strictly from $n = 1$.
2. Đặt $I_n = b_n^2 - 4b_nb_{n-1} + b_{n-1}^2$. Khi đó $I_{n+1} - I_n = (b_{n+1}^2 - b_{n-1}^2) - 4b_n(b_{n+1} - b_{n-1}) = (b_{n+1} - b_{n-1})(b_{n+1} + b_{n-1} - 4b_n) = 0$. Vậy $I_n = I_1 = 1 - 4 + 1 = -2$ với mọi $n \geq 1$.
Put $I_n = b_n^2 - 4b_nb_{n-1} + b_{n-1}^2$. Then $I_{n+1} - I_n = (b_{n+1}^2 - b_{n-1}^2) - 4b_n(b_{n+1} - b_{n-1}) = (b_{n+1} - b_{n-1})(b_{n+1} + b_{n-1} - 4b_n) = 0$. So $I_n = I_1 = 1 - 4 + 1 = -2$ for all $n \geq 1$.
3. Mặt khác $I_{n+1} = b_{n+1}(b_{n+1} - 4b_n) + b_n^2 = -b_{n+1}b_{n-1} + b_n^2$. Từ $I_{n+1} = -2$ suy ra $b_{n+1}b_{n-1} = b_n^2 + 2$ với mọi $n \geq 1$.
On the other hand $I_{n+1} = b_{n+1}(b_{n+1} - 4b_n) + b_n^2 = -b_{n+1}b_{n-1} + b_n^2$. From $I_{n+1} = -2$ we get $b_{n+1}b_{n-1} = b_n^2 + 2$ for all $n \geq 1$.

4. Dãy (b_n) có cùng hai số hạng đầu và cùng hệ thức với (a_n) ; hệ thức xác định $a_{n+1} = (a_n^2 + 2)/a_{n-1}$ duy nhất khi $a_{n-1} \neq 0$. Quy nạp cho $a_n = b_n$ với mọi n .

The sequence (b_n) has the same first two terms and satisfies the same relation as (a_n) ; the relation determines $a_{n+1} = (a_n^2 + 2)/a_{n-1}$ uniquely when $a_{n-1} \neq 0$. Induction gives $a_n = b_n$ for all n .

Vậy mọi a_n là số nguyên dương và $a_{n+1} = 4a_n - a_{n-1}$.

Hence every a_n is a positive integer and $a_{n+1} = 4a_n - a_{n-1}$. ■

NHẬN XÉT / REMARK — Cách tìm ra hằng số 4: trừ hai hệ thức $a_{n+1}a_{n-1} = a_n^2 + 2$ và $a_na_{n-2} = a_{n-1}^2 + 2$ được $a_{n-1}(a_{n+1} + a_{n-1}) = a_n(a_n + a_{n-2})$, tức $(a_{n+1} + a_{n-1})/a_n = (a_n + a_{n-2})/a_{n-1}$. Tỷ số này không đổi và bằng $(a_2 + a_0)/a_1 = 4$. Phép chia chỉ hợp lệ khi các số hạng khác 0, nên lời giải chặt phải chứng minh tính dương trước.

To discover the constant 4, subtract $a_{n+1}a_{n-1} = a_n^2 + 2$ and $a_na_{n-2} = a_{n-1}^2 + 2$ to get $a_{n-1}(a_{n+1} + a_{n-1}) = a_n(a_n + a_{n-2})$, that is $(a_{n+1} + a_{n-1})/a_n = (a_n + a_{n-2})/a_{n-1}$. This ratio is constant and equals $(a_2 + a_0)/a_1 = 4$. The division is valid only for nonzero terms, so a rigorous solution proves positivity first.

LỖI HAY GẶP / COMMON MISTAKE — Kết luận dãy nguyên từ vài số hạng đầu (1, 1, 3, 11, 41). Vài số hạng nguyên không chứng minh gì; phải có quy nạp hoặc bất biến cho mọi n .

Concluding that a sequence is integral from its first few terms (1, 1, 3, 11, 41). A few integer terms prove nothing; induction or an invariant for every n is required.

LỖI HAY GẶP / COMMON MISTAKE — Quy nạp thiếu bước cơ sở hoặc chỉ kiểm một số hạng khi truy hồi cần hai số hạng đầu. Truy hồi cấp 2 cần kiểm cả hai giá trị khởi đầu.

Induction with a missing base case, or only one starting term checked when the recurrence needs two. A second-order recurrence needs both starting values verified.

5.8. Bảng chiến lược và thuật ngữ — Strategy table and glossary

Dấu hiệu trong đề <i>Sign in the problem</i>	Công cụ nên thử <i>Tool to try</i>	Ví dụ <i>Example</i>
Hệ thức có $f(x + y)$ hoặc hai biến tự do <i>Relation with $f(x + y)$ or two free variables</i>	Đặt một biến bằng 0, 1; $y = x$; $y = -x$ <i>Set a variable to 0 or 1; $y = x$; $y = -x$</i>	Ví dụ 5.1 <i>Example 5.1</i>
Hệ thức chứa $f(x)$ và $f(1 - x)$ <i>Relation involving $f(x)$ and $f(1 - x)$</i>	Đổi x thành $1 - x$, giải hệ hai ẩn <i>Replace x by $1 - x$, solve the 2-unknown system</i>	Ví dụ 5.2 <i>Example 5.2</i>
Miền $\mathbb{Z}$ hoặc $\mathbb{Z}^+$ <i>Domain $\mathbb{Z}$ or $\mathbb{Z}^+$</i>	Quy nạp từ $f(n + 1) - f(n)$, xét cả chiều âm <i>Induction from $f(n + 1) - f(n)$, both directions</i>	Ví dụ 5.3 <i>Example 5.3</i>

Dấu hiệu trong đề <i>Sign in the problem</i>	Công cụ nên thử <i>Tool to try</i>	Ví dụ <i>Example</i>
$f(x + y) = f(x) + f(y)$ kèm đơn điệu hoặc dấu <i>$f(x + y) = f(x) + f(y)$ with monotonicity or sign</i>	Định lý Cauchy, đổi hàm để về cộng tính <i>Cauchy's theorem, shift to an additive function</i>	Ví dụ 5.4, 5.5 <i>Examples 5.4, 5.5</i>
Biến đứng riêng ở vế phải; $f(f(x))$ <i>A variable alone on the right; $f(f(x))$</i>	Chứng minh đơn ánh, toàn ánh; thay y bởi $f(y)$ <i>Prove injectivity, surjectivity; replace y by $f(y)$</i>	Ví dụ 5.6, 5.7 <i>Examples 5.6, 5.7</i>
Chia hết, dư, tìm hệ số, tổng lũy thừa các nghiệm <i>Divisibility, remainders, coefficients, power sums of roots</i>	Bézout, đồng nhất hệ số, Viète với p, q, r <i>Bézout, comparing coefficients, Vieta with p, q, r</i>	Ví dụ 5.8, 5.9 <i>Examples 5.8, 5.9</i>
Đa thức hệ số nguyên, $P(a)$, $P(b)$ <i>Integer polynomial, values $P(a), P(b)$</i>	$(a - b) \mid P(a) - P(b)$, đồng dư theo modulo <i>$(a - b) \mid P(a) - P(b)$, congruences</i>	Ví dụ 5.4 <i>Example 5.4</i>
Biết giá trị của đa thức tại vài điểm <i>Values of a polynomial at a few points</i>	Nội suy Lagrange, dư của phép chia <i>Lagrange interpolation, remainder of a division</i>	Ví dụ 5.11 <i>Example 5.11</i>
Dãy truy hồi, số hạng tổng quát <i>Recurrence, general term</i>	Phương trình đặc trưng, nghiệm riêng <i>Characteristic equation, particular solution</i>	Ví dụ 5.12 <i>Example 5.12</i>
Dãy lặp lại, tổng nhiều số hạng, tính nguyên <i>Repeating sequence, long sums, integrality</i>	Chu kỳ, tổng sai phân, bất biến <i>Period, telescoping, invariant</i>	Ví dụ 5.13, 5.14 <i>Examples 5.13, 5.14</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Phương trình hàm	Functional equation	Hệ thức chứa hàm chưa biết <i>A relation containing an unknown function</i>
Nghiệm hàm	Solution function	Hàm thỏa hệ thức trên cả miền <i>A function satisfying the relation on the whole domain</i>
Phép thế	Substitution	Gán biểu thức cho biến <i>Assigning an expression to a variable</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Thử lại	Verification	Kiểm hàm tìm được thỏa đề <i>Checking that the function found satisfies the equation</i>
Đơn ánh	Injective	$f(u) = f(v) \Rightarrow u = v$
Toàn ánh	Surjective	Mọi giá trị đích đều được nhận <i>Every target value is attained</i>
Song ánh	Bijjective	Vừa đơn ánh vừa toàn ánh <i>Both injective and surjective</i>
Điểm bất động	Fixed point	Giá trị w với $f(w) = w$ <i>A value w with $f(w) = w$</i>
Hàm cộng tính	Additive function	$f(x + y) = f(x) + f(y)$
Phương trình Cauchy	Cauchy's equation	Tên của hệ thức cộng tính <i>The name of the additive relation</i>
Hàm đơn điệu	Monotone function	Luôn tăng hoặc luôn giảm <i>Always nondecreasing or always nonincreasing</i>
Đa thức	Polynomial	Tổng các đơn thức một biến <i>A sum of monomials in one variable</i>
Bậc	Degree	Số mũ lớn nhất của biến <i>The largest exponent of the variable</i>
Hệ số đầu	Leading coefficient	Hệ số của số hạng bậc cao nhất <i>The coefficient of the highest-degree term</i>
Phép chia có dư	Division with remainder	$A = BQ + R$ với $\deg R < \deg B$ <i>$A = BQ + R$ with $\deg R < \deg B$</i>
Định lý Bézout	Remainder theorem	Dư khi chia cho $x - \alpha$ là $P(\alpha)$ <i>The remainder on division by $x - \alpha$ is $P(\alpha)$</i>
Nghiệm bội	Multiple root	Nghiệm lặp lại trong phân tích thành nhân tử <i>A root repeated in the factorisation</i>
Định lý Viète	Vieta's formulas	Liên hệ nghiệm và hệ số <i>Relations between roots and coefficients</i>
Nội suy Lagrange	Lagrange interpolation	Đa thức bậc thấp nhất qua các điểm cho trước <i>The least-degree polynomial through given points</i>
Đồng nhất hệ số	Comparing coefficients	Hai đa thức bằng nhau thì hệ số bằng nhau <i>Equal polynomials have equal coefficients</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Dãy truy hồi	Recurrence sequence	Số hạng cho bởi các số hạng trước <i>Terms given by earlier terms</i>
Phương trình đặc trưng	Characteristic equation	$r^2 = pr + q$ của truy hồi cấp 2 <i>$r^2 = pr + q$ for a second-order recurrence</i>
Nghiệm riêng	Particular solution	Một nghiệm cụ thể của truy hồi không thuần nhất <i>One specific solution of an inhomogeneous recurrence</i>
Dãy tuần hoàn	Periodic sequence	Dãy lặp lại sau T số hạng <i>A sequence repeating after T terms</i>
Tổng sai phân	Telescoping sum	Tổng mà các số hạng triệt tiêu nhau <i>A sum whose terms cancel in pairs</i>
Bất biến	Invariant	Đại lượng không đổi qua mỗi bước <i>A quantity unchanged at every step</i>

5.9. Bài tự luyện — Practice problems

Mức 1 — Học sinh giỏi cấp tỉnh — Level 1 — Provincial olympiad

Bài 5.1 / Problem 5.1 — Tìm mọi hàm $f: \mathbb{R} \rightarrow \mathbb{R}$ thỏa $f(x + y) = f(x) + y(3x^2 + 3xy + y^2 + 2)$ với mọi số thực x, y .

Find all functions $f: \mathbb{R} \rightarrow \mathbb{R}$ such that $f(x + y) = f(x) + y(3x^2 + 3xy + y^2 + 2)$ for all real x, y .

Bài 5.2 / Problem 5.2 — Tìm mọi hàm $f: \mathbb{R} \rightarrow \mathbb{R}$ thỏa $x \cdot f(x) + f(1 - x) = x^2 + 2$ với mọi số thực x .

Find all functions $f: \mathbb{R} \rightarrow \mathbb{R}$ such that $x \cdot f(x) + f(1 - x) = x^2 + 2$ for all real x .

Bài 5.3 / Problem 5.3 — Cho a, b, c là ba nghiệm của $x^3 - 7x^2 + 5x - 1 = 0$. Tính $a^2 + b^2 + c^2$, $a^3 + b^3 + c^3$ và $1/a^2 + 1/b^2 + 1/c^2$.

Let a, b, c be the three roots of $x^3 - 7x^2 + 5x - 1 = 0$. Compute $a^2 + b^2 + c^2$, $a^3 + b^3 + c^3$ and $1/a^2 + 1/b^2 + 1/c^2$.

Bài 5.4 / Problem 5.4 — dãy (a_n) có $a_1 = 1$ và $a_{n+1} = 2a_n + n$. Tìm công thức của a_n và tính a_{10} .

A sequence (a_n) has $a_1 = 1$ and $a_{n+1} = 2a_n + n$. Find a formula for a_n and compute a_{10} .

Mức 2 — Học sinh giỏi quốc gia — Level 2 — National olympiad

Bài 5.5 / Problem 5.5 — Tìm mọi hàm $f: \mathbb{R} \rightarrow \mathbb{R}$ đơn điệu tăng ($x \leq y \Rightarrow f(x) \leq f(y)$) thỏa $f(x + y) = f(x) + f(y) + 2$ với mọi x, y và $f(1) = 5$.

Find all nondecreasing functions $f: \mathbb{R} \rightarrow \mathbb{R}$ ($x \leq y \Rightarrow f(x) \leq f(y)$) such that $f(x + y) = f(x) + f(y) + 2$ for all x, y and $f(1) = 5$.

Bài 5.6 / Problem 5.6 — Tìm mọi hàm $f: \mathbb{R} \rightarrow \mathbb{R}$ thỏa $f(x) \cdot f(y) = f(x + y) + xy$ với mọi số thực x, y .

Find all functions $f: \mathbb{R} \rightarrow \mathbb{R}$ such that $f(x) \cdot f(y) = f(x + y) + xy$ for all real x, y .

Bài 5.7 / Problem 5.7 — Cho $P \in \mathbb{Z}[x]$ với $P(0) = 7, P(1) = 10, P(2) = 13$. Chứng minh P không có nghiệm nguyên.

Let $P \in \mathbb{Z}[x]$ with $P(0) = 7, P(1) = 10, P(2) = 13$. Prove that P has no integer root.

Bài 5.8 / Problem 5.8 — Tìm mọi đa thức P hệ số thực thỏa $P(x + 1) + P(x - 1) - 2P(x) = 2$ với mọi số thực x .

Find all polynomials P with real coefficients such that $P(x + 1) + P(x - 1) - 2P(x) = 2$ for all real x .

Mức 3 — Olympic quốc tế — Level 3 — International olympiad

Bài 5.9 / Problem 5.9 — Chứng minh không tồn tại hàm $f: \mathbb{R} \rightarrow \mathbb{R}$ thỏa $f(f(x)) = x^2 - 3$ với mọi số thực x .

Prove that there is no function $f: \mathbb{R} \rightarrow \mathbb{R}$ such that $f(f(x)) = x^2 - 3$ for all real x .

Bài 5.10 / Problem 5.10 — Cho $P \in \mathbb{Z}[x]$ sao cho phương trình $P(x) = 7$ có ít nhất bốn nghiệm nguyên phân biệt. (a) Chứng minh phương trình $P(x) = 10$ không có nghiệm nguyên. (b) Chỉ ra một đa thức P như vậy và một số nguyên m để $P(m) = 11$.

Let $P \in \mathbb{Z}[x]$ be such that the equation $P(x) = 7$ has at least four distinct integer roots. (a) Prove that the equation $P(x) = 10$ has no integer root. (b) Give such a polynomial P and an integer m with $P(m) = 11$.

Bài 5.11 / Problem 5.11 — Dãy (a_n) có $a_0 = 1, a_1 = 2$ và $a_{n+1}a_{n-1} = a_n^2 + 3$ với mọi $n \geq 1$. Chứng minh rằng (a) mọi a_n là số nguyên dương và $a_{n+1} = 4a_n - a_{n-1}$; (b) $a_n = ((2 + \sqrt{3})^n + (2 - \sqrt{3})^n)/2$; (c) $a_{2n} = 2a_n^2 - 1$.

A sequence (a_n) has $a_0 = 1, a_1 = 2$ and $a_{n+1}a_{n-1} = a_n^2 + 3$ for all $n \geq 1$. Prove that (a) every a_n is a positive integer and $a_{n+1} = 4a_n - a_{n-1}$; (b) $a_n = ((2 + \sqrt{3})^n + (2 - \sqrt{3})^n)/2$; (c) $a_{2n} = 2a_n^2 - 1$.

Bài 5.12 / Problem 5.12 — Tìm mọi hàm $f: \mathbb{Z} \rightarrow \mathbb{Z}$ thỏa $f(f(n)) = n$ với mọi $n \in \mathbb{Z}$ và $(m - n) \mid f(m) - f(n)$ với mọi số nguyên $m \neq n$.

Find all functions $f: \mathbb{Z} \rightarrow \mathbb{Z}$ such that $f(f(n)) = n$ for all $n \in \mathbb{Z}$ and $(m - n) \mid f(m) - f(n)$ for all integers $m \neq n$.

5.10. Lời giải bài tự luyện — Solutions to practice problems

Bài 5.1 — Problem 5.1

1. Đặt $x = 0$: $f(y) = f(0) + y(y^2 + 2) = y^3 + 2y + c$ với $c = f(0)$.

Put $x = 0$: $f(y) = f(0) + y(y^2 + 2) = y^3 + 2y + c$ with $c = f(0)$.

2. Thử lại với $f(x) = x^3 + 2x + c$. Vế trái trừ $f(x)$ là $(x + y)^3 - x^3 + 2y = 3x^2y + 3xy^2 + y^3 + 2y = y(3x^2 + 3xy + y^2 + 2)$, đúng bằng phần cộng thêm ở vế phải.

Check $f(x) = x^3 + 2x + c$. The left side minus $f(x)$ is $(x + y)^3 - x^3 + 2y = 3x^2y + 3xy^2 + y^3 + 2y = y(3x^2 + 3xy + y^2 + 2)$, exactly the extra term on the right.

Vậy $f(x) = x^3 + 2x + c$, với c là hằng số thực tùy ý.

Hence $f(x) = x^3 + 2x + c$, where c is an arbitrary real constant. ■

Bài 5.2 — Problem 5.2

1. Thay x bởi $1 - x$: $(1 - x)f(1 - x) + f(x) = (1 - x)^2 + 2 = x^2 - 2x + 3$.
Replace x by $1 - x$: $(1 - x)f(1 - x) + f(x) = (1 - x)^2 + 2 = x^2 - 2x + 3$.
2. Từ hệ thức đề, $f(1 - x) = x^2 + 2 - x \cdot f(x)$. Thế vào phương trình mới: $f(x) + (1 - x)(x^2 + 2 - x \cdot f(x)) = x^2 - 2x + 3$.
From the given relation, $f(1 - x) = x^2 + 2 - x \cdot f(x)$. Substituting in the new equation: $f(x) + (1 - x)(x^2 + 2 - x \cdot f(x)) = x^2 - 2x + 3$.
3. Gom $f(x)$: $f(x)(1 - x + x^2) = x^2 - 2x + 3 - (1 - x)(x^2 + 2) = x^3 + 1 = (x + 1)(x^2 - x + 1)$.
Collect $f(x)$: $f(x)(1 - x + x^2) = x^2 - 2x + 3 - (1 - x)(x^2 + 2) = x^3 + 1 = (x + 1)(x^2 - x + 1)$.
4. Vì $x^2 - x + 1 = (x - 1/2)^2 + 3/4 > 0$ với mọi x nên chia được: $f(x) = x + 1$.
Since $x^2 - x + 1 = (x - 1/2)^2 + 3/4 > 0$ for every x , we may divide: $f(x) = x + 1$.
5. Thử lại: $x(x + 1) + (2 - x) = x^2 + x + 2 - x = x^2 + 2$. Đúng.
Check: $x(x + 1) + (2 - x) = x^2 + x + 2 - x = x^2 + 2$. Correct.

Vậy có đúng một nghiệm $f(x) = x + 1$.

Hence there is exactly one solution, $f(x) = x + 1$. ■

Bài 5.3 — Problem 5.3

1. Theo định lý Viète: $p = a + b + c = 7$, $q = ab + bc + ca = 5$, $r = abc = 1$.
By Vieta's formulas: $p = a + b + c = 7$, $q = ab + bc + ca = 5$, $r = abc = 1$.
2. $a^2 + b^2 + c^2 = p^2 - 2q = 49 - 10 = 39$.
 $a^2 + b^2 + c^2 = p^2 - 2q = 49 - 10 = 39$.
3. $a^3 + b^3 + c^3 = p^3 - 3pq + 3r = 343 - 105 + 3 = 241$.
 $a^3 + b^3 + c^3 = p^3 - 3pq + 3r = 343 - 105 + 3 = 241$.
4. $1/a^2 + 1/b^2 + 1/c^2 = (q^2 - 2pr)/r^2 = (25 - 14)/1 = 11$. Mẫu $r = 1$ khác 0 nên công thức dùng được.
 $1/a^2 + 1/b^2 + 1/c^2 = (q^2 - 2pr)/r^2 = (25 - 14)/1 = 11$. The denominator $r = 1$ is nonzero, so the formula applies.

Vậy ba giá trị lần lượt là 39, 241 và 11.

Hence the three values are 39, 241 and 11. ■

Bài 5.4 — Problem 5.4

1. Tìm nghiệm riêng dạng $-n - 1$: $2(-n - 1) + n = -n - 2 = -(n + 1) - 1$. Đặt $b_n = a_n + n + 1$.
A particular solution of the form $-n - 1$: $2(-n - 1) + n = -n - 2 = -(n + 1) - 1$. Put $b_n = a_n + n + 1$.
2. Khi đó $b_{n+1} = a_{n+1} + n + 2 = 2a_n + 2n + 2 = 2b_n$, và $b_1 = 1 + 1 + 1 = 3$. Vậy $b_n = 3 \cdot 2^{n-1}$.
Then $b_{n+1} = a_{n+1} + n + 2 = 2a_n + 2n + 2 = 2b_n$, and $b_1 = 1 + 1 + 1 = 3$. So $b_n = 3 \cdot 2^{n-1}$.
3. Suy ra $a_n = 3 \cdot 2^{n-1} - n - 1$. Kiểm tra: $a_2 = 2 + 1 = 3 = 6 - 3$; $a_3 = 6 + 2 = 8 = 12 - 4$.
Hence $a_n = 3 \cdot 2^{n-1} - n - 1$. Check: $a_2 = 2 + 1 = 3 = 6 - 3$; $a_3 = 6 + 2 = 8 = 12 - 4$.

4. $a_{10} = 3 \cdot 2^9 - 11 = 1536 - 11 = 1525$.

$a_{10} = 3 \cdot 2^9 - 11 = 1536 - 11 = 1525$.

Vậy $a_n = 3 \cdot 2^{n-1} - n - 1$ và $a_{10} = 1525$.

Hence $a_n = 3 \cdot 2^{n-1} - n - 1$ and $a_{10} = 1525$. ■

Bài 5.5 — Problem 5.5

1. Đặt $g(x) = f(x) + 2$. Khi đó $g(x + y) = f(x + y) + 2 = f(x) + f(y) + 4 = g(x) + g(y)$: g cộng tính. Hơn nữa g đơn điệu tăng vì f đơn điệu tăng.

Put $g(x) = f(x) + 2$. Then $g(x + y) = f(x + y) + 2 = f(x) + f(y) + 4 = g(x) + g(y)$: g is additive. Moreover g is nondecreasing because f is.

2. Theo định lý Cauchy với điều kiện đơn điệu, $g(x) = ax$ với $a = g(1) = f(1) + 2 = 7$.

Vậy $f(x) = 7x - 2$.

By Cauchy's theorem with monotonicity, $g(x) = ax$ with $a = g(1) = f(1) + 2 = 7$. Hence $f(x) = 7x - 2$.

3. Thử lại: $f(x + y) = 7x + 7y - 2$; $f(x) + f(y) + 2 = 7x - 2 + 7y - 2 + 2 = 7x + 7y - 2$.

Hàm $7x - 2$ đơn điệu tăng và $f(1) = 5$.

Check: $f(x + y) = 7x + 7y - 2$; $f(x) + f(y) + 2 = 7x - 2 + 7y - 2 + 2 = 7x + 7y - 2$. The function $7x - 2$ is nondecreasing and $f(1) = 5$.

Vậy $f(x) = 7x - 2$.

Hence $f(x) = 7x - 2$. ■

Bài 5.6 — Problem 5.6

1. Đặt $y = 0$: $f(x) \cdot f(0) = f(x)$, tức $f(x)(f(0) - 1) = 0$ với mọi x . Nếu $f(0) \neq 1$ thì f đồng nhất bằng 0, nhưng khi đó $x = y = 1$ cho $0 = 0 + 1$, vô lý. Vậy $f(0) = 1$.

Put $y = 0$: $f(x) \cdot f(0) = f(x)$, that is $f(x)(f(0) - 1) = 0$ for all x . If $f(0) \neq 1$ then f is identically 0, but then $x = y = 1$ gives $0 = 0 + 1$, absurd. So $f(0) = 1$.

2. Đặt $a = f(1)$. Với $y = 1$: $a \cdot f(x) = f(x + 1) + x$, nên $f(x + 1) = a \cdot f(x) - x$. Với $x = 1$ suy ra $f(2) = a^2 - 1$.

Put $a = f(1)$. With $y = 1$: $a \cdot f(x) = f(x + 1) + x$, so $f(x + 1) = a \cdot f(x) - x$. With $x = 1$ this gives $f(2) = a^2 - 1$.

3. Với $y = 2$: $f(x) \cdot f(2) = f(x + 2) + 2x$, nên $f(x + 2) = (a^2 - 1)f(x) - 2x$.

With $y = 2$: $f(x) \cdot f(2) = f(x + 2) + 2x$, so $f(x + 2) = (a^2 - 1)f(x) - 2x$.

4. Áp dụng công thức $f(x + 1) = a \cdot f(x) - x$ hai lần: $f(x + 2) = a \cdot f(x + 1) - (x + 1) = a(a \cdot f(x) - x) - x - 1 = a^2 f(x) - (a + 1)x - 1$.

Applying the formula for $f(x + 1)$ twice: $f(x + 2) = a \cdot f(x + 1) - (x + 1) = a(a \cdot f(x) - x) - x - 1 = a^2 f(x) - (a + 1)x - 1$.

5. So hai biểu thức của $f(x + 2)$: $(a^2 - 1)f(x) - 2x = a^2 f(x) - (a + 1)x - 1$, suy ra $f(x) = (a + 1)x + 1 - 2x = (a - 1)x + 1$.

Comparing the two expressions for $f(x + 2)$: $(a^2 - 1)f(x) - 2x = a^2 f(x) - (a + 1)x - 1$, which gives $f(x) = (a + 1)x + 1 - 2x = (a - 1)x + 1$.

6. Thế vào đề: $((a - 1)x + 1)((a - 1)y + 1) = (a - 1)^2 xy + (a - 1)(x + y) + 1$ phải bằng $(a - 1)(x + y) + 1 + xy$. Vậy $(a - 1)^2 = 1$, tức $a = 0$ hoặc $a = 2$.

Substitute in the equation: $((a-1)x+1)((a-1)y+1) = (a-1)^2xy + (a-1)(x+y) + 1$ must equal $(a-1)(x+y) + 1 + xy$. So $(a-1)^2 = 1$, that is $a = 0$ or $a = 2$.

7. Với $a = 2$: $f(x) = x + 1$; $a = 0$: $f(x) = 1 - x$. Thử lại: $(x+1)(y+1) = xy + x + y + 1 = f(x+y) + xy$; $(1-x)(1-y) = 1 - x - y + xy = f(x+y) + xy$.
For $a = 2$: $f(x) = x + 1$; for $a = 0$: $f(x) = 1 - x$. Check: $(x+1)(y+1) = xy + x + y + 1 = f(x+y) + xy$; $(1-x)(1-y) = 1 - x - y + xy = f(x+y) + xy$.

Vậy $f(x) = x + 1$ hoặc $f(x) = 1 - x$.

Hence $f(x) = x + 1$ or $f(x) = 1 - x$. ■

Bài 5.7 — Problem 5.7

1. Mọi số nguyên n đồng dư theo modulo 3 với một trong 0, 1, 2. Theo tính chất đồng dư của đa thức nguyên, $P(n) \equiv P(r) \pmod{3}$ nếu $n \equiv r \pmod{3}$.

Every integer n is congruent modulo 3 to one of 0, 1, 2. By the congruence property of integer polynomials, $P(n) \equiv P(r) \pmod{3}$ when $n \equiv r \pmod{3}$.

2. Mặt khác $P(0) = 7 \equiv 1$, $P(1) = 10 \equiv 1$, $P(2) = 13 \equiv 1 \pmod{3}$. Vậy $P(n) \equiv 1 \pmod{3}$ với mọi số nguyên n .

Meanwhile $P(0) = 7 \equiv 1$, $P(1) = 10 \equiv 1$, $P(2) = 13 \equiv 1 \pmod{3}$. So $P(n) \equiv 1 \pmod{3}$ for every integer n .

Nếu $P(n) = 0$ thì $0 \equiv 1 \pmod{3}$, vô lý. Vậy P không có nghiệm nguyên.

If $P(n) = 0$ then $0 \equiv 1 \pmod{3}$, absurd. Hence P has no integer root. ■

Bài 5.8 — Problem 5.8

1. Vì $(x+1)^2 + (x-1)^2 - 2x^2 = 2$, đặt $Q(x) = P(x) - x^2$ thì $Q(x+1) + Q(x-1) - 2Q(x) = 0$.

Since $(x+1)^2 + (x-1)^2 - 2x^2 = 2$, putting $Q(x) = P(x) - x^2$ gives $Q(x+1) + Q(x-1) - 2Q(x) = 0$.

2. Đặt $D(x) = Q(x+1) - Q(x)$. Khi đó $D(x) - D(x-1) = Q(x+1) - 2Q(x) + Q(x-1) = 0$, tức $D(x) = D(x-1)$ với mọi x . Quy nạp: $D(n) = D(0)$ với mọi số nguyên $n \geq 0$.

Put $D(x) = Q(x+1) - Q(x)$. Then $D(x) - D(x-1) = Q(x+1) - 2Q(x) + Q(x-1) = 0$, that is $D(x) = D(x-1)$ for all x . Induction: $D(n) = D(0)$ for every integer $n \geq 0$.

3. Đa thức $D(x) - D(0)$ có vô số nghiệm 0, 1, 2, ... nên là đa thức không (đa thức khác không có hữu hạn nghiệm). Vậy $D(x) = b$ là hằng số.

The polynomial $D(x) - D(0)$ has infinitely many roots 0, 1, 2, ..., so it is the zero polynomial (a nonzero polynomial has finitely many roots). Hence $D(x) = b$ is constant.

4. Khi đó $Q(n+1) = Q(n) + b$, nên $Q(n) = Q(0) + bn$ với $n = 0, 1, 2, \dots$. Đa thức $Q(x) - bx - Q(0)$ có vô số nghiệm, nên $Q(x) = bx + c$ với $c = Q(0)$.

Then $Q(n+1) = Q(n) + b$, so $Q(n) = Q(0) + bn$ for $n = 0, 1, 2, \dots$. The polynomial $Q(x) - bx - Q(0)$ has infinitely many roots, so $Q(x) = bx + c$ with $c = Q(0)$.

5. Vậy $P(x) = x^2 + bx + c$. Thử lại: $(x+1)^2 + (x-1)^2 - 2x^2 + b(2x - 2x) + c(1 + 1 - 2) = 2$. Đúng với mọi b, c .

So $P(x) = x^2 + bx + c$. Check: $(x+1)^2 + (x-1)^2 - 2x^2 + b(2x - 2x) + c(1 + 1 - 2) = 2$. True for all b, c .

Vậy $P(x) = x^2 + bx + c$, với b, c là hằng số thực tùy ý.

Hence $P(x) = x^2 + bx + c$, where b, c are arbitrary real constants. ■

Bài 5.9 — Problem 5.9

1. Giả sử f tồn tại và đặt $g(x) = x^2 - 3$. Tính $f(f(f(x)))$ theo hai cách: $f(g(x)) = f(f(f(x)))$ và $g(f(x)) = f(f(f(x)))$. Vậy $f(g(x)) = g(f(x))$: f giao hoán với g , và do đó giao hoán với $g \circ g$.

Suppose f exists and put $g(x) = x^2 - 3$. Compute $f(f(f(x)))$ in two ways: $f(g(x)) = f(f(f(x)))$ and $g(f(x)) = f(f(f(x)))$. So $f(g(x)) = g(f(x))$: f commutes with g , and hence with $g \circ g$.

2. Nghiệm của $g(g(x)) = x$: $(x^2 - 3)^2 - 3 = x$ tương đương $x^4 - 6x^2 - x + 6 = 0$, tức $(x^2 - x - 3)(x + 2)(x - 1) = 0$. Điểm bất động của g ($g(x) = x$) là hai nghiệm p, q của $x^2 - x - 3 = 0$ ($p, q = (1 \pm \sqrt{13})/2$). Ngoài ra $g(1) = -2$ và $g(-2) = 1$.

The solutions of $g(g(x)) = x$: $(x^2 - 3)^2 - 3 = x$ is equivalent to $x^4 - 6x^2 - x + 6 = 0$, that is $(x^2 - x - 3)(x + 2)(x - 1) = 0$. The fixed points of g ($g(x) = x$) are the two roots p, q of $x^2 - x - 3 = 0$ ($p, q = (1 \pm \sqrt{13})/2$). Also $g(1) = -2$ and $g(-2) = 1$.

3. Xét $f(1)$. Vì $g(g(1)) = 1$ và f giao hoán với $g \circ g$ nên $g(g(f(1))) = f(g(g(1))) = f(1)$. Vậy $f(1)$ là nghiệm của $g(g(x)) = x$, tức $f(1) \in \{p, q, 1, -2\}$. Ngoài ra $f(f(1)) = g(1) = -2$.

Consider $f(1)$. Since $g(g(1)) = 1$ and f commutes with $g \circ g$, $g(g(f(1))) = f(g(g(1))) = f(1)$. So $f(1)$ is a solution of $g(g(x)) = x$, that is $f(1) \in \{p, q, 1, -2\}$. Also $f(f(1)) = g(1) = -2$.

4. Trường hợp $f(1) = 1$: $f(f(1)) = 1 \neq -2$, vô lý. Trường hợp $f(1) = -2$: $f(-2) = f(f(1)) = -2$, nên $f(f(-2)) = -2$, nhưng $g(-2) = 1 \neq -2$, vô lý.

Case $f(1) = 1$: $f(f(1)) = 1 \neq -2$, absurd. Case $f(1) = -2$: $f(-2) = f(f(1)) = -2$, so $f(f(-2)) = -2$, but $g(-2) = 1 \neq -2$, absurd.

5. Trường hợp $f(1) = p$: $f(p) = f(f(1)) = -2$. Nhưng p là điểm bất động của g nên $g(f(p)) = f(g(p)) = f(p)$, tức $f(p)$ cũng là điểm bất động của g , thuộc $\{p, q\}$, không bằng -2 . Vô lý. Trường hợp $f(1) = q$ xử lý giống hệt.

Case $f(1) = p$: $f(p) = f(f(1)) = -2$. But p is a fixed point of g , so $g(f(p)) = f(g(p)) = f(p)$, meaning $f(p)$ is also a fixed point of g , lying in $\{p, q\}$, not equal to -2 . Absurd. Case $f(1) = q$ is identical.

Mọi trường hợp đều mâu thuẫn. Vậy không tồn tại hàm f như đề yêu cầu.

Every case is contradictory. Hence no such function f exists. ■

Bài 5.10 — Problem 5.10

1. (a) Gọi a_1, a_2, a_3, a_4 là bốn nghiệm nguyên phân biệt của $P(x) - 7$. Chia liên tiếp cho các nhị thức monic $x - a_i$ (hệ số nguyên): $P(x) - 7 = (x - a_1)(x - a_2)(x - a_3)(x - a_4)Q(x)$ với $Q \in \mathbb{Z}[x]$. Mỗi lần chia, nghiệm a_j khác a_i vẫn là nghiệm của thương vì $(a_j - a_i) \neq 0$.

(a) Let a_1, a_2, a_3, a_4 be four distinct integer roots of $P(x) - 7$. Dividing successively by the monic binomials $x - a_i$ (integer coefficients): $P(x) - 7 = (x - a_1)(x - a_2)(x - a_3)(x - a_4)Q(x)$ with $Q \in \mathbb{Z}[x]$. At each division a root $a_j \neq a_i$ remains a root of the quotient because $a_j - a_i \neq 0$.

2. Giả sử $P(m) = 10$ với m nguyên. Khi đó $(m - a_1)(m - a_2)(m - a_3)(m - a_4)Q(m) = 3$. Bốn số $m - a_i$ là các số nguyên đôi một khác nhau và đều là ước của 3, tức thuộc $\{1,$

$-1, 3, -3\}$.

Suppose $P(m) = 10$ for an integer m . Then $(m - a_1)(m - a_2)(m - a_3)(m - a_4)Q(m) = 3$. The four numbers $m - a_i$ are pairwise distinct integers and all divide 3, so they lie in $\{1, -1, 3, -3\}$.

3. Bốn số khác nhau trong tập bốn phần tử nên chúng đúng là 1, -1, 3, -3, với tích 9.

Khi đó $9 \cdot Q(m) = 3$, nghĩa là $9 \mid 3$, vô lý. Vậy $P(x) = 10$ không có nghiệm nguyên.

Four distinct numbers from a four-element set are exactly 1, -1, 3, -3, with product 9. Then $9 \cdot Q(m) = 3$, so $9 \mid 3$, absurd. Hence $P(x) = 10$ has no integer root.

4. (b) Lấy $P(x) = 7 + (x^2 - 1)(x^2 - 4) = x^4 - 5x^2 + 11$. Phương trình $P(x) = 7$ có bốn nghiệm nguyên $\pm 1, \pm 2$, và $P(0) = 11$. Vậy $m = 0$.

(b) Take $P(x) = 7 + (x^2 - 1)(x^2 - 4) = x^4 - 5x^2 + 11$. The equation $P(x) = 7$ has the four integer roots $\pm 1, \pm 2$, and $P(0) = 11$. So $m = 0$.

Vậy (a) $P(x) = 10$ vô nghiệm nguyên; (b) $P(x) = x^4 - 5x^2 + 11$ với $m = 0$.

Hence (a) $P(x) = 10$ has no integer root; (b) $P(x) = x^4 - 5x^2 + 11$ with $m = 0$. ■

Bài 5.11 — Problem 5.11

1. (a) Định nghĩa $b_0 = 1, b_1 = 2, b_{n+1} = 4b_n - b_{n-1}$. Ta có $b_2 = 7 > b_1 > 0$. Nếu $b_{n+1} > b_n > 0$ thì $b_{n+2} - b_{n+1} = 3b_{n+1} - b_n > 0$, nên mọi b_n là số nguyên dương.

(a) Define $b_0 = 1, b_1 = 2, b_{n+1} = 4b_n - b_{n-1}$. Then $b_2 = 7 > b_1 > 0$. If $b_{n+1} > b_n > 0$ then $b_{n+2} - b_{n+1} = 3b_{n+1} - b_n > 0$, so every b_n is a positive integer.

2. Đặt $I_n = b_n^2 - 4b_nb_{n-1} + b_{n-1}^2$. Vì $I_{n+1} - I_n = (b_{n+1} - b_{n-1})(b_{n+1} + b_{n-1} - 4b_n) = 0$ nên $I_n = I_1 = 4 - 8 + 1 = -3$.

Put $I_n = b_n^2 - 4b_nb_{n-1} + b_{n-1}^2$. Since $I_{n+1} - I_n = (b_{n+1} - b_{n-1})(b_{n+1} + b_{n-1} - 4b_n) = 0$, $I_n = I_1 = 4 - 8 + 1 = -3$.

3. Mặt khác $I_{n+1} = b_{n+1}(b_{n+1} - 4b_n) + b_n^2 = -b_{n+1}b_{n-1} + b_n^2$. Do $I_{n+1} = -3$ nên $b_{n+1}b_{n-1} = b_n^2 + 3$. Dãy (b_n) thỏa cùng hệ thức và cùng hai số hạng đầu với (a_n) , mà hệ thức xác định a_{n+1} duy nhất vì $a_{n-1} \neq 0$. Vậy $a_n = b_n$ với mọi n , và (a) đúng.

Also $I_{n+1} = b_{n+1}(b_{n+1} - 4b_n) + b_n^2 = -b_{n+1}b_{n-1} + b_n^2$. Since $I_{n+1} = -3$, $b_{n+1}b_{n-1} = b_n^2 + 3$. The sequence (b_n) satisfies the same relation and has the same first two terms as (a_n) , and the relation determines a_{n+1} uniquely since $a_{n-1} \neq 0$. So $a_n = b_n$ for all n , and (a) holds.

4. (b) Phương trình đặc trưng $r^2 - 4r + 1 = 0$ có nghiệm $u = 2 + \sqrt{3}$ và $v = 2 - \sqrt{3}$, phân biệt. Theo định lý truy hồi cấp 2: $a_n = Au^n + Bv^n$, $A + B = 1$ và $Au + Bv = 2$. Ta có $2(A + B) + \sqrt{3}(A - B) = 2$, nên $\sqrt{3}(A - B) = 0$, $A = B = 1/2$. Vậy $a_n = (u^n + v^n)/2$.

(b) The characteristic equation $r^2 - 4r + 1 = 0$ has the distinct roots $u = 2 + \sqrt{3}$ and $v = 2 - \sqrt{3}$. By the second-order recurrence theorem $a_n = Au^n + Bv^n$, with $A + B = 1$ and $Au + Bv = 2$. Now $2(A + B) + \sqrt{3}(A - B) = 2$, so $\sqrt{3}(A - B) = 0$ and $A = B = 1/2$. Hence $a_n = (u^n + v^n)/2$.

5. (c) Vì $uv = (2 + \sqrt{3})(2 - \sqrt{3}) = 1$, $(u^n + v^n)^2 = u^{2n} + v^{2n} + 2$. Do đó $a_{2n} = (u^{2n} + v^{2n})/2 = ((2a_n)^2 - 2)/2 = 2a_n^2 - 1$. Kiểm tra: $a_2 = 7 = 2 \cdot 4 - 1$.

(c) Since $uv = (2 + \sqrt{3})(2 - \sqrt{3}) = 1$, $(u^n + v^n)^2 = u^{2n} + v^{2n} + 2$. Hence $a_{2n} = (u^{2n} + v^{2n})/2 = ((2a_n)^2 - 2)/2 = 2a_n^2 - 1$. Check: $a_2 = 7 = 2 \cdot 4 - 1$.

Vậy cả ba khẳng định (a), (b), (c) đều đúng.

Hence all three statements (a), (b), (c) hold. ■

Bài 5.12 — Problem 5.12

1. Từ $f(f(n)) = n$, f là song ánh; đặc biệt $f(m) \neq f(n)$ khi $m \neq n$.
From $f(f(n)) = n$, f is a bijection; in particular $f(m) \neq f(n)$ when $m \neq n$.
2. Áp dụng điều kiện chia hết cho hai số khác nhau $f(m), f(n)$: $(f(m) - f(n)) \mid f(f(m)) - f(f(n)) = m - n$. Đồng thời $(m - n) \mid f(m) - f(n)$. Hai số nguyên khác 0 chia hết cho nhau thì có giá trị tuyệt đối bằng nhau: $|f(m) - f(n)| = |m - n|$.
Apply the divisibility condition to the distinct numbers $f(m), f(n)$: $(f(m) - f(n)) \mid f(f(m)) - f(f(n)) = m - n$. Also $(m - n) \mid f(m) - f(n)$. Two nonzero integers dividing each other have equal absolute values: $|f(m) - f(n)| = |m - n|$.
3. Với $m = n + 1$: $\varepsilon_n = f(n + 1) - f(n)$ bằng 1 hoặc -1 . Nếu ε_n và ε_{n+1} trái dấu thì $f(n + 2) = f(n)$, mâu thuẫn tính đơn ánh. Vậy mọi ε_n bằng một dấu chung ε , và $f(n) = \varepsilon n + c$ với $c = f(0)$.
With $m = n + 1$: $\varepsilon_n = f(n + 1) - f(n)$ equals 1 or -1 . If ε_n and ε_{n+1} have opposite signs then $f(n + 2) = f(n)$, contradicting injectivity. So all ε_n share one sign ε , and $f(n) = \varepsilon n + c$ with $c = f(0)$.
4. Nếu $\varepsilon = 1$: $f(f(n)) = n + 2c = n$ suy ra $c = 0$, $f(n) = n$. Nếu $\varepsilon = -1$: $f(f(n)) = -(c - n) + c = n$ với mọi c .
If $\varepsilon = 1$: $f(f(n)) = n + 2c = n$ gives $c = 0$, so $f(n) = n$. If $\varepsilon = -1$: $f(f(n)) = -(c - n) + c = n$ for every c .
5. Thử lại: với $f(n) = n$ hoặc $f(n) = c - n$, hiệu $f(m) - f(n)$ bằng $m - n$ hoặc $-(m - n)$, chia hết cho $m - n$.
Check: for $f(n) = n$ or $f(n) = c - n$, the difference $f(m) - f(n)$ equals $m - n$ or $-(m - n)$, divisible by $m - n$.

Vậy $f(n) = n$, hoặc $f(n) = c - n$ với c là số nguyên tùy ý.

Hence $f(n) = n$, or $f(n) = c - n$ with c an arbitrary integer. ■

Chương 6. Chia hết, ước chung lớn nhất và số nguyên tố — Chapter 6. Divisibility, gcd and primes

Mục tiêu chương — Chapter objectives

- Chạy thuật toán Euclid, viết ƯCLN dưới dạng $ax + by$ và giải phương trình nghiệm nguyên $ax + by = c$.
Run the Euclidean algorithm, write the gcd in the form $ax + by$ and solve the integer equation $ax + by = c$.
- Dùng định lý cơ bản của số học và số mũ p -adic v_p để tính ƯCLN, BCNN, số ước, tổng ước và $v_p(n!)$.
Use the fundamental theorem of arithmetic and the p -adic valuation v_p to compute the gcd, lcm, number of divisors, sum of divisors and $v_p(n!)$.
- Loại số chính phương bằng dư của phép chia cho 3, 4, 8 và bằng phép xuống thang vô hạn.
Rule out perfect squares by remainders modulo 3, 4 and 8 and by infinite descent.
- Phân tích $a^n - b^n$, $a^n + b^n$ và $a^4 + 4b^4$ để chứng minh chia hết hoặc chỉ ra hợp số.
Factorise $a^n - b^n$, $a^n + b^n$ and $a^4 + 4b^4$ to prove divisibility or exhibit composite numbers.

6.1. Chia hết và phép chia có dư — Divisibility and division with remainder

ĐỊNH NGHĨA 6.1 (Chia hết) / DEFINITION 6.1 (Divisibility) — Cho $a, b \in \mathbb{Z}$, $a \neq 0$. Ta nói a chia hết b , viết $a \mid b$, nếu tồn tại $k \in \mathbb{Z}$ sao cho $b = ak$. Khi đó a là ước của b và b là bội của a . Viết $a \nmid b$ khi a không chia hết b .

Let $a, b \in \mathbb{Z}$ with $a \neq 0$. We say that a divides b , written $a \mid b$, if there is $k \in \mathbb{Z}$ with $b = ak$. Then a is a divisor of b and b is a multiple of a . We write $a \nmid b$ when a does not divide b .

TÍNH CHẤT 6.2 (Tính chất cơ bản của chia hết) / PROPERTY 6.2 (Basic properties of divisibility) — Với $a \neq 0$ và $b, c, x, y \in \mathbb{Z}$: (i) $a \mid b$ và $b \mid c \Rightarrow a \mid c$; (ii) $a \mid b$ và $a \mid c \Rightarrow a \mid (bx + cy)$; (iii) $b \neq 0$ và $a \mid b \Rightarrow |a| \leq |b|$; (iv) $a \mid b$ và $b \mid a \Rightarrow |a| = |b|$.

For $a \neq 0$ and $b, c, x, y \in \mathbb{Z}$: (i) $a \mid b$ and $b \mid c \Rightarrow a \mid c$; (ii) $a \mid b$ and $a \mid c \Rightarrow a \mid (bx + cy)$; (iii) $b \neq 0$ and $a \mid b \Rightarrow |a| \leq |b|$; (iv) $a \mid b$ and $b \mid a \Rightarrow |a| = |b|$.

Chứng minh. / Proof.

(i) Viết $b = ak$ và $c = bl$. Khi đó $c = a(kl)$.

(i) Write $b = ak$ and $c = bl$. Then $c = a(kl)$.

(ii) Viết $b = ak$ và $c = al$. Khi đó $bx + cy = a(kx + ly)$.

(ii) Write $b = ak$ and $c = al$. Then $bx + cy = a(kx + ly)$.

(iii) Viết $b = ak$. Vì $b \neq 0$ nên $k \neq 0$, do đó $|k| \geq 1$ và $|b| = |a| \cdot |k| \geq |a|$.

(iii) Write $b = ak$. Since $b \neq 0$ we have $k \neq 0$, so $|k| \geq 1$ and $|b| = |a| \cdot |k| \geq |a|$.

(iv) Cả hai số khác 0. Áp dụng (iii) hai lần: $|a| \leq |b|$ và $|b| \leq |a|$.

(iv) Both numbers are non-zero. Applying (iii) twice gives $|a| \leq |b|$ and $|b| \leq |a|$. ■

ĐỊNH LÝ 6.3 (Phép chia có dư) / THEOREM 6.3 (Division with remainder) — Cho $a \in \mathbb{Z}$ và $b \in \mathbb{Z}^+$. Tồn tại duy nhất cặp $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ sao cho $a = bq + r$ và $0 \leq r < b$. Ta gọi q là thương, r là số dư của a khi chia cho b .

Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^+$. There is exactly one pair $(q, r) \in \mathbb{Z} \times \mathbb{Z}$ with $a = bq + r$ and $0 \leq r < b$. We call q the quotient and r the remainder of a on division by b .

$$a = bq + r, \quad 0 \leq r < b \quad (6.1)$$

Chứng minh. / Proof.

Tồn tại. Tập $S = \{a - bk : k \in \mathbb{Z}, a - bk \geq 0\}$ khác rỗng, vì với $k = -|a|$ ta có $a + b|a| \geq a + |a| \geq 0$. Theo nguyên lý sắp thứ tự tốt, S có phần tử nhỏ nhất $r = a - bq$. Nếu $r \geq b$ thì $r - b = a - b(q + 1)$ thuộc S và nhỏ hơn r , mâu thuẫn. Vậy $0 \leq r < b$.

Existence. The set $S = \{a - bk : k \in \mathbb{Z}, a - bk \geq 0\}$ is non-empty, because $k = -|a|$ gives $a + b|a| \geq a + |a| \geq 0$. By the well-ordering principle S has a least element $r = a - bq$. If $r \geq b$ then $r - b = a - b(q + 1)$ lies in S and is smaller than r , a contradiction. Hence $0 \leq r < b$.

Duy nhất. Giả sử $a = bq + r = bq' + r'$ với $0 \leq r, r' < b$. Khi đó $b(q - q') = r' - r$ và $|r' - r| < b$. Số $r' - r$ là bội của b có giá trị tuyệt đối nhỏ hơn b nên bằng 0 (Tính chất 6.2(iii)). Suy ra $r = r'$ và $q = q'$.

Uniqueness. Suppose $a = bq + r = bq' + r'$ with $0 \leq r, r' < b$. Then $b(q - q') = r' - r$ and $|r' - r| < b$. So $r' - r$ is a multiple of b of absolute value less than b , hence 0 (Property 6.2(iii)). Therefore $r = r'$ and $q = q'$. ■

PHẢI THUỘC / MEMORISE — Mọi bài chia hết bắt đầu từ $a = bq + r$ với $0 \leq r < b$. Dư r chỉ có b khả năng: đó là lý do xét dư theo từng trường hợp luôn hữu hạn.

Every divisibility argument starts from $a = bq + r$ with $0 \leq r < b$. There are only b possible remainders, which is why a case check by remainders is always finite.

VÍ DỤ 6.1 (Hạ bậc bằng phép chia đa thức) / EXAMPLE 6.1 (Reducing the degree by polynomial division) — Tìm tất cả số nguyên dương n sao cho $n + 5$ là ước của $n^2 + 7$.

Find all positive integers n such that $n + 5$ divides $n^2 + 7$.

Lời giải. / Solution.

1. Ta có $n^2 + 7 = (n + 5)(n - 5) + 32$. Nếu $(n + 5) \mid (n^2 + 7)$ thì $(n + 5) \mid (n^2 + 7) - (n + 5)(n - 5) = 32$ theo Tính chất 6.2(ii). Ngược lại, nếu $(n + 5) \mid 32$ thì $(n + 5) \mid (n^2 + 7)$ cũng theo (ii). Vậy điều kiện tương đương với $(n + 5) \mid 32$.

We have $n^2 + 7 = (n + 5)(n - 5) + 32$. If $(n + 5) \mid (n^2 + 7)$ then $(n + 5) \mid (n^2 + 7) - (n + 5)(n - 5) = 32$ by Property 6.2(ii). Conversely, if $(n + 5) \mid 32$ then $(n + 5) \mid (n^2 + 7)$, again by (ii). So the condition is equivalent to $(n + 5) \mid 32$.

2. Ước dương của 32 là 1, 2, 4, 8, 16, 32. Vì $n \geq 1$ nên $n + 5 \geq 6$, còn lại $n + 5 \in \{8, 16, 32\}$, tức $n \in \{3, 11, 27\}$.

The positive divisors of 32 are 1, 2, 4, 8, 16, 32. Since $n \geq 1$ we have $n + 5 \geq 6$, which leaves $n + 5 \in \{8, 16, 32\}$, that is $n \in \{3, 11, 27\}$.

3. Kiểm tra: $3^2 + 7 = 16 = 2 \cdot 8$; $11^2 + 7 = 128 = 8 \cdot 16$; $27^2 + 7 = 736 = 23 \cdot 32$.

Check: $3^2 + 7 = 16 = 2 \cdot 8$; $11^2 + 7 = 128 = 8 \cdot 16$; $27^2 + 7 = 736 = 23 \cdot 32$.

Vậy $n \in \{3, 11, 27\}$.

Hence $n \in \{3, 11, 27\}$. ■

NHẬN XÉT / REMARK — Cách làm của Ví dụ 6.1 dùng cho mọi bài dạng $(an + b) \mid P(n)$ với P là đa thức hệ số nguyên: nhân P với lũy thừa thích hợp của a để chia được cho $an + b$, phần dư là hằng số, rồi liệt kê ước của hằng số đó. Nhân thêm lũy thừa của a có thể thêm nghiệm ngoại lai, nên phải kiểm lại từng nghiệm hoặc dùng bổ đề Euclid (Mục 6.3).

The method of Example 6.1 works for every problem of the form $(an + b) \mid P(n)$ with P an integer polynomial: multiply P by a suitable power of a so that division by $an + b$ is possible, the remainder is a constant, and list the divisors of that constant. The extra factor of a can introduce spurious solutions, so check each candidate or use Euclid's lemma (Section 6.3).

LỖI HAY GẶP / COMMON MISTAKE — Kết luận $a \mid bc \Rightarrow a \mid b$ hoặc $a \mid c$ với a bất kỳ. Phản ví dụ: $6 \mid 3 \cdot 4$ nhưng $6 \nmid 3$ và $6 \nmid 4$. Mệnh đề chỉ đúng khi a nguyên tố (Hệ quả 6.14) hoặc khi $\gcd(a, b) = 1$ (Bổ đề 6.9).

Concluding $a \mid bc \Rightarrow a \mid b$ or $a \mid c$ for an arbitrary a . Counterexample: $6 \mid 3 \cdot 4$ but $6 \nmid 3$ and $6 \nmid 4$. The statement holds only when a is prime (Corollary 6.14) or when $\gcd(a, b) = 1$ (Lemma 6.9).

6.2. Ước chung lớn nhất, bội chung nhỏ nhất và thuật toán Euclid — Greatest common divisor, least common multiple and the Euclidean algorithm

ĐỊNH NGHĨA 6.4 (Ước chung lớn nhất, bội chung nhỏ nhất) / DEFINITION 6.4

(Greatest common divisor, least common multiple) — Cho $a, b \in \mathbb{Z}$ không đồng thời bằng 0. Ước chung lớn nhất $\gcd(a, b)$ là số nguyên dương lớn nhất chia hết cả a lẫn b . Với $a, b \neq 0$, bội chung nhỏ nhất $\text{lcm}(a, b)$ là số nguyên dương nhỏ nhất mà cả a và b cùng chia hết. Hai số a, b gọi là nguyên tố cùng nhau nếu $\gcd(a, b) = 1$. Quy ước $\gcd(a, 0) = |a|$.

Let $a, b \in \mathbb{Z}$, not both zero. The greatest common divisor $\gcd(a, b)$ is the largest positive integer dividing both a and b . For $a, b \neq 0$ the least common multiple $\text{lcm}(a, b)$ is the smallest positive integer divisible by both a and b . The integers a, b are coprime if $\gcd(a, b) = 1$. By convention $\gcd(a, 0) = |a|$.

BỔ ĐỀ 6.5 / LEMMA 6.5 — Cho $a, b, q \in \mathbb{Z}$ với a, b không đồng thời bằng 0. Hai cặp (a, b) và $(b, a - bq)$ có cùng tập ước chung, do đó $\gcd(a, b) = \gcd(b, a - bq)$.

Let $a, b, q \in \mathbb{Z}$ with a, b not both zero. The pairs (a, b) and $(b, a - bq)$ have the same set of common divisors, hence $\gcd(a, b) = \gcd(b, a - bq)$.

Chứng minh. / Proof.

Nếu $d \mid a$ và $d \mid b$ thì $d \mid a - bq$ theo Tính chất 6.2(ii). Ngược lại nếu $d \mid b$ và $d \mid a - bq$ thì $d \mid (a - bq) + bq = a$. Hai tập ước chung trùng nhau nên phần tử lớn nhất của chúng bằng nhau.

If $d \mid a$ and $d \mid b$ then $d \mid a - bq$ by Property 6.2(ii). Conversely, if $d \mid b$ and $d \mid a - bq$ then $d \mid (a - bq) + bq = a$. The two sets of common divisors coincide, so their greatest elements are equal.

■

ĐỊNH LÝ 6.6 (Thuật toán Euclid) / THEOREM 6.6 (Euclidean algorithm)

— Cho $a, b \in \mathbb{Z}^+$. Đặt $r_0 = a, r_1 = b$ và với $k \geq 1$ chia r_{k-1} cho r_k : $r_{k-1} = r_k q_k + r_{k+1}$, $0 \leq r_{k+1} < r_k$. Quá trình dừng sau hữu hạn bước tại dư $r_{n+1} = 0$ và r_n , dư khác 0 cuối cùng, bằng $\gcd(a, b)$.

Let $a, b \in \mathbb{Z}^+$. Put $r_0 = a, r_1 = b$ and for $k \geq 1$ divide r_{k-1} by r_k : $r_{k-1} = r_k q_k + r_{k+1}$, $0 \leq r_{k+1} < r_k$. The process stops after finitely many steps at $r_{n+1} = 0$, and r_n , the last non-zero remainder, equals $\gcd(a, b)$.

$$\gcd(a, b) = \gcd(b, r), \quad a = bq + r \quad (6.2)$$

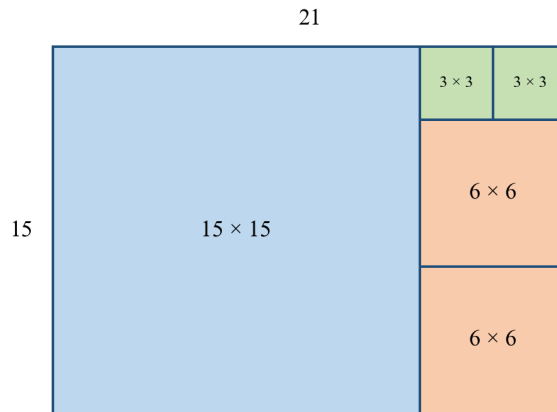
Chứng minh. / Proof.

Các dư $r_1 > r_2 > \dots$ là dãy số nguyên không âm giảm ngặt nên sau hữu hạn bước xuất hiện $r_{n+1} = 0$.

The remainders $r_1 > r_2 > \dots$ form a strictly decreasing sequence of non-negative integers, so $r_{n+1} = 0$ occurs after finitely many steps.

Theo Bổ đề 6.5 với $q = q_k$ ta có $\gcd(r_{k-1}, r_k) = \gcd(r_k, r_{k+1})$ ở mỗi bước. Nói các đẳng thức: $\gcd(a, b) = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0) = r_n$.

By Lemma 6.5 with $q = q_k$ we get $\gcd(r_{k-1}, r_k) = \gcd(r_k, r_{k+1})$ at every step. Chaining these: $\gcd(a, b) = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0) = r_n$. ■



Hình 6.1. Thuật toán Euclid cho 21 và 15: cắt hình chữ nhật 21×15 bằng hình vuông lớn nhất còn lại, cạnh 15, rồi 6, rồi 3. Cạnh nhỏ nhất, 3, là $\gcd(21, 15)$.

Figure 6.1. The Euclidean algorithm for 21 and 15: cut the 21×15 rectangle by the largest remaining square, of side 15, then 6, then 3. The smallest side, 3, is $\gcd(21, 15)$.

NHẬN XÉT / REMARK — Từ r_1 trở đi, sau hai bước liên tiếp số dư giảm quá một nửa: $r_{k+2} < r_k/2$ với $k \geq 1$. Thật vậy, nếu $r_{k+1} \leq r_k/2$ thì $r_{k+2} < r_{k+1} \leq r_k/2$; nếu $r_{k+1} > r_k/2$ thì $q_{k+1} = 1$ và $r_{k+2} = r_k - r_{k+1} < r_k/2$. Vì vậy số phép chia chỉ cỡ $2\log_2 b$, và thuật toán Euclid chạy nhanh ngay cả với số hàng trăm chữ số.

From r_1 on, after two consecutive steps the remainder falls by more than half: $r_{k+2} < r_k/2$ for $k \geq 1$. Indeed, if $r_{k+1} \leq r_k/2$ then $r_{k+2} < r_{k+1} \leq r_k/2$; if $r_{k+1} > r_k/2$ then $q_{k+1} = 1$ and $r_{k+2} = r_k - r_{k+1} < r_k/2$. So the number of divisions is only about $2\log_2 b$, and the Euclidean algorithm runs fast even for numbers with hundreds of digits.

PHÂN TÍCH / ANALYSIS — Muốn tìm biểu diễn $91 = 1547x + 1001y$, chạy thuật toán Euclid xuôi để tìm UCLN, rồi thay ngược từng dư bằng hai số đứng trước nó. Mỗi dư luôn là tổ hợp nguyên của hai số trước, nên cuối cùng ra tổ hợp nguyên của 1547 và 1001.

To find a representation $91 = 1547x + 1001y$, run the Euclidean algorithm forwards to find the gcd, then substitute backwards, replacing each remainder by the two numbers before it. Each remainder is an integer combination of the two previous ones, so in the end it is an integer combination of 1547 and 1001.

VÍ DỤ 6.2 (Euclid xuôi, thay ngược) / EXAMPLE 6.2 (Euclid forwards, back-substitution) — Tính $\gcd(1547, 1001)$ và tìm các số nguyên x, y sao cho $1547x + 1001y = \gcd(1547, 1001)$.

Compute $\gcd(1547, 1001)$ and find integers x, y with $1547x + 1001y = \gcd(1547, 1001)$.

Lời giải. / Solution.

Chạy thuật toán Euclid:

Run the Euclidean algorithm:

$$1547 = 1 \cdot 1001 + 546$$

$$1001 = 1 \cdot 546 + 455$$

$$546 = 1 \cdot 455 + 91$$

$$455 = 5 \cdot 91 + 0$$

Dư khác 0 cuối cùng là 91, nên $\gcd(1547, 1001) = 91$. Thay ngược từ dòng ba:

The last non-zero remainder is 91, so $\gcd(1547, 1001) = 91$. Substituting backwards from the third line:

$$91 = 546 - 455 = 546 - (1001 - 546) = 2 \cdot 546 - 1001$$

$$91 = 2(1547 - 1001) - 1001 = 2 \cdot 1547 - 3 \cdot 1001$$

Kiểm tra: $2 \cdot 1547 - 3 \cdot 1001 = 3094 - 3003 = 91$. Vậy $\gcd(1547, 1001) = 91$ và $(x, y) = (2, -3)$ là một nghiệm.

Check: $2 \cdot 1547 - 3 \cdot 1001 = 3094 - 3003 = 91$. Hence $\gcd(1547, 1001) = 91$ and $(x, y) = (2, -3)$ is a solution. ■

PHÂN TÍCH / ANALYSIS — Thuật toán Euclid trên cặp (m, n) trừ dần n khỏi m . Hỏi khi trừ n khỏi m thì $\gcd(2^m - 1, 2^n - 1)$ có đổi không? Viết $2^m - 1 = 2^n(2^{m-n} - 1) + (2^n - 1)$: đây là dạng $a = bq + r$ của Bổ đề 6.5, chỉ khác là nhân thêm 2^n , mà 2^n nguyên tố cùng nhau với mọi ước lẻ.

The Euclidean algorithm on the pair (m, n) repeatedly subtracts n from m . Does $\gcd(2^m - 1, 2^n - 1)$ change when n is subtracted from m ? Write $2^m - 1 = 2^n(2^{m-n} - 1) + (2^n - 1)$: this is the shape $a = bq + r$ of Lemma 6.5, with the extra factor 2^n , which is coprime to every odd divisor.

VÍ DỤ 6.3 (Euclid trên số mũ) / EXAMPLE 6.3 (Euclid on the exponents) — Chứng minh rằng với mọi $m, n \in \mathbb{Z}^+$ ta có $\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m, n)} - 1$.

Prove that for all $m, n \in \mathbb{Z}^+$ we have $\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m, n)} - 1$.

Lời giải. / Solution.

1. Đặt $g(m, n) = \gcd(2^m - 1, 2^n - 1)$. Với $m > n$ có $2^m - 1 = 2^n(2^{m-n} - 1) + (2^n - 1)$.

Put $g(m, n) = \gcd(2^m - 1, 2^n - 1)$. For $m > n$ we have $2^m - 1 = 2^n(2^{m-n} - 1) + (2^n - 1)$.

2. Gọi e là ước chung của $2^m - 1$ và $2^n - 1$. Khi đó e lẻ, nên $\gcd(e, 2^n) = 1$. Từ $e \mid 2^n(2^{m-n} - 1)$ suy ra $e \mid 2^{m-n} - 1$ theo bổ đề Euclid. Ngược lại, mọi ước chung của $2^{m-n} - 1$ và $2^n - 1$ chia hết $2^m - 1$ theo đẳng thức trên. Hai cặp có cùng ước chung: $g(m, n) = g(m - n, n)$.

Let e be a common divisor of $2^m - 1$ and $2^n - 1$. Then e is odd, so $\gcd(e, 2^n) = 1$. From $e \mid 2^n(2^{m-n} - 1)$ we get $e \mid 2^{m-n} - 1$ by Euclid's lemma. Conversely, every common divisor of $2^{m-n} - 1$ and $2^n - 1$ divides $2^m - 1$ by the identity above. The two pairs have the same common divisors: $g(m, n) = g(m - n, n)$.

3. Quy nạp theo $m + n$. Nếu $m = n$ thì $g(n, n) = 2^n - 1 = 2^{\gcd(n, n)} - 1$. Nếu $m > n$ thì $g(m, n) = g(m - n, n) = 2^{\gcd(m-n, n)} - 1$ theo giả thiết quy nạp, và $\gcd(m - n, n) = \gcd(m, n)$ theo Bổ đề 6.5. Trường hợp $m < n$ đối xứng.

Induct on $m + n$. If $m = n$ then $g(n, n) = 2^n - 1 = 2^{\gcd(n, n)} - 1$. If $m > n$ then $g(m, n) = g(m - n, n) = 2^{\gcd(m-n, n)} - 1$ by the induction hypothesis, and $\gcd(m - n, n) = \gcd(m, n)$ by Lemma 6.5. The case $m < n$ is symmetric.

Vậy $\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m, n)} - 1$. Chẳng hạn $\gcd(2^{60} - 1, 2^{84} - 1) = 2^{12} - 1 = 4095$.

Hence $\gcd(2^m - 1, 2^n - 1) = 2^{\gcd(m, n)} - 1$. For instance $\gcd(2^{60} - 1, 2^{84} - 1) = 2^{12} - 1 = 4095$.



NHẬN XÉT / REMARK — Kết quả của Ví dụ 6.3 mở rộng cho $a^m - 1$ với mọi cơ số $a \geq 2$: $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m, n)} - 1$. Chứng minh y hệt, thay 2 bằng a ; chỉ cần để ý ước chung e của $a^n - 1$ nguyên tố cùng nhau với a . Bài 6.11 xử lý hiệu $a^n - b^n$ với hai cơ số nguyên tố cùng nhau.

The result of Example 6.3 extends to $a^m - 1$ for every base $a \geq 2$: $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m, n)} - 1$. The proof is identical with 2 replaced by a ; one only notes that a common divisor e of $a^n - 1$ is coprime to a . Problem 6.11 treats the difference $a^n - b^n$ for two coprime bases.

6.3. Định lý Bézout và bổ đề Euclid — Bézout's theorem and Euclid's lemma

ĐỊNH LÝ 6.7 (Định lý Bézout) / THEOREM 6.7 (Bézout's theorem) — Cho $a, b \in \mathbb{Z}$ không đồng thời bằng 0 và $g = \gcd(a, b)$. Khi đó tồn tại $x, y \in \mathbb{Z}$ sao cho $ax + by = g$. Hơn nữa, tập các số có dạng $ax + by$ ($x, y \in \mathbb{Z}$) chính là tập các bội của g .

Let $a, b \in \mathbb{Z}$ be not both zero and $g = \gcd(a, b)$. Then there are $x, y \in \mathbb{Z}$ with $ax + by = g$. Moreover, the set of numbers of the form $ax + by$ ($x, y \in \mathbb{Z}$) is exactly the set of multiples of g .

$$ax + by = \gcd(a, b) \quad (6.3)$$

Chứng minh. / Proof.

Gọi S là tập các số nguyên dương có dạng $ax + by$. S khác rỗng vì $a \cdot a + b \cdot b > 0$. Gọi d là phần tử nhỏ nhất của S , $d = ax_0 + by_0$.

Let S be the set of positive integers of the form $ax + by$. It is non-empty because $a \cdot a + b \cdot b > 0$. Let d be its least element, $d = ax_0 + by_0$.

Chia a cho d : $a = dq + r$, $0 \leq r < d$. Khi đó $r = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)$ cũng có dạng $ax + by$. Vì $r < d$ và d là nhỏ nhất trong S nên $r \notin S$, tức $r = 0$. Vậy $d \mid a$; lý luận tương tự cho $d \mid b$. Do đó d là ước chung, $d \leq g$.

Divide a by d : $a = dq + r$, $0 \leq r < d$. Then $r = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)$ also has the form $ax + by$. Since $r < d$ and d is least in S , $r \notin S$, so $r = 0$. Thus $d \mid a$, and the same argument gives $d \mid b$. So d is a common divisor and $d \leq g$.

Mặt khác $g \mid a$ và $g \mid b$ nên $g \mid ax_0 + by_0 = d$, suy ra $g \leq d$. Vậy $d = g$.

On the other hand $g \mid a$ and $g \mid b$ give $g \mid ax_0 + by_0 = d$, so $g \leq d$. Hence $d = g$.

Với bội kg bất kỳ: $kg = a(kx_0) + b(ky_0)$. Ngược lại mọi số $ax + by$ đều chia hết cho g theo Tính chất 6.2(ii).

For any multiple kg : $kg = a(kx_0) + b(ky_0)$. Conversely every number $ax + by$ is divisible by g by Property 6.2(ii). ■

HỆ QUẢ 6.8 / COROLLARY 6.8 — $\gcd(a, b) = 1$ khi và chỉ khi tồn tại $x, y \in \mathbb{Z}$ sao cho $ax + by = 1$.
 $\gcd(a, b) = 1$ if and only if there are $x, y \in \mathbb{Z}$ with $ax + by = 1$.

Chứng minh. / Proof.

Chiều thuận là Định lý Bézout với $g = 1$. Chiều đảo: nếu $ax + by = 1$ thì mọi ước chung của a và b chia hết 1, nên $\gcd(a, b) = 1$.

The forward direction is Bézout's theorem with $g = 1$. Conversely, if $ax + by = 1$ then every common divisor of a and b divides 1, so $\gcd(a, b) = 1$. ■

BỔ ĐỀ 6.9 (Bổ đề Euclid) / LEMMA 6.9 (Euclid's lemma) — Nếu $a \mid bc$ và $\gcd(a, b) = 1$ thì $a \mid c$.
 If $a \mid bc$ and $\gcd(a, b) = 1$ then $a \mid c$.

Chứng minh. / Proof.

Theo Hệ quả 6.8 có x, y với $ax + by = 1$. Nhân với c : $c = acx + bcy$. Cả hai số hạng chia hết cho a , nên $a \mid c$.

By Corollary 6.8 there are x, y with $ax + by = 1$. Multiplying by c : $c = acx + bcy$. Both terms are divisible by a , so $a \mid c$. ■

TÍNH CHẤT 6.10 (Tính chất của nguyên tố cùng nhau) / PROPERTY 6.10 (Properties of coprime integers) — (i) Nếu $\gcd(a, b) = \gcd(a, c) = 1$ thì $\gcd(a, bc) = 1$. (ii) Nếu $a \mid c$, $b \mid c$ và $\gcd(a, b) = 1$ thì $ab \mid c$. (iii) Với $k \in \mathbb{Z}^+$: $\gcd(ka, kb) = k \cdot \gcd(a, b)$.
 (i) If $\gcd(a, b) = \gcd(a, c) = 1$ then $\gcd(a, bc) = 1$. (ii) If $a \mid c$, $b \mid c$ and $\gcd(a, b) = 1$ then $ab \mid c$. (iii) For $k \in \mathbb{Z}^+$: $\gcd(ka, kb) = k \cdot \gcd(a, b)$.

Chứng minh. / Proof.

(i) Có $ax + by = 1$ và $au + cv = 1$. Nhân hai đẳng thức:

(i) We have $ax + by = 1$ and $au + cv = 1$. Multiplying the two identities:

$$1 = (ax + by)(au + cv) = a(axu + xcv + byu) + bc \cdot yv$$

Theo Hệ quả 6.8, $\gcd(a, bc) = 1$.

By Corollary 6.8, $\gcd(a, bc) = 1$.

(ii) Viết $c = ak$. Vì $b \mid ak$ và $\gcd(b, a) = 1$ nên $b \mid k$ theo Bổ đề 6.9, tức $k = bl$ và $c = abl$.

(ii) Write $c = ak$. Since $b \mid ak$ and $\gcd(b, a) = 1$, Lemma 6.9 gives $b \mid k$, so $k = bl$ and $c = abl$.

(iii) Gọi $g = \gcd(a, b)$ và $ax + by = g$. Khi đó $(ka)x + (kb)y = kg$, nên mọi ước chung của ka và kb chia hết kg . Mặt khác kg là một ước chung của ka và kb . Vậy $\gcd(ka, kb) = kg$.

(iii) Let $g = \gcd(a, b)$ and $ax + by = g$. Then $(ka)x + (kb)y = kg$, so every common divisor of ka and kb divides kg . On the other hand kg is a common divisor of ka and kb . Hence $\gcd(ka, kb) = kg$. ■

ĐỊNH LÝ 6.11 (Tích ƯCLN và BCNN) / THEOREM 6.11 (Product of gcd and lcm) —

Với $a, b \in \mathbb{Z}^+$: $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.

For $a, b \in \mathbb{Z}^+$: $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$.

$$\gcd(a, b) \cdot \text{lcm}(a, b) = ab \quad (6.4)$$

Chứng minh. / Proof.

Đặt $g = \gcd(a, b)$, $a = ga'$, $b = gb'$. Theo Tính chất 6.10(iii), $g = \gcd(ga', gb') = g \cdot \gcd(a', b')$, nên $\gcd(a', b') = 1$. Đặt $m = ga'b'$. Đây là bội chung của a và b .

Put $g = \gcd(a, b)$, $a = ga'$, $b = gb'$. By Property 6.10(iii), $g = \gcd(ga', gb') = g \cdot \gcd(a', b')$, so $\gcd(a', b') = 1$. Put $m = ga'b'$. This is a common multiple of a and b .

Giả sử c là bội chung dương bất kỳ, $c = ak = ga'k$. Từ $b \mid c$ có $gb' \mid ga'k$, tức $b' \mid a'k$. Vì $\gcd(a', b') = 1$ nên $b' \mid k$ theo Bổ đề 6.9; viết $k = b'l$ thì $c = ga'b'l = ml$. Vậy mọi bội chung là bội của m , nên m là bội chung nhỏ nhất: $\text{lcm}(a, b) = ga'b'$.

Let c be any positive common multiple, $c = ak = ga'k$. From $b \mid c$ we get $gb' \mid ga'k$, that is $b' \mid a'k$. Since $\gcd(a', b') = 1$, Lemma 6.9 gives $b' \mid k$; writing $k = b'l$ we get $c = ga'b'l = ml$. So every common multiple is a multiple of m , hence m is the least one: $\text{lcm}(a, b) = ga'b'$.

Do đó $\gcd(a, b) \cdot \text{lcm}(a, b) = g \cdot ga'b' = (ga')(gb') = ab$.

Therefore $\gcd(a, b) \cdot \text{lcm}(a, b) = g \cdot ga'b' = (ga')(gb') = ab$. ■

ĐỊNH LÝ 6.12 (Phương trình nghiệm nguyên bậc nhất hai ẩn) / THEOREM 6.12

(Linear Diophantine equation in two unknowns) — Cho $a, b, c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, $g = \gcd(a, b)$. Phương trình $ax + by = c$ có nghiệm nguyên khi và chỉ khi $g \mid c$. Khi đó, nếu (x_0, y_0) là một nghiệm, mọi nghiệm nguyên có dạng $x = x_0 + (b/g)t$, $y = y_0 - (a/g)t$ với $t \in \mathbb{Z}$.

Let $a, b, c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, $g = \gcd(a, b)$. The equation $ax + by = c$ has an integer solution if and only if $g \mid c$. In that case, if (x_0, y_0) is one solution, every integer solution has the form $x = x_0 + (b/g)t$, $y = y_0 - (a/g)t$ with $t \in \mathbb{Z}$.

$$x = x_0 + (b/g)t, \quad y = y_0 - (a/g)t, \quad t \in \mathbb{Z} \quad (6.5)$$

Chứng minh. / Proof.

Điều kiện cần: $g \mid a$ và $g \mid b$ nên $g \mid ax + by = c$. Điều kiện đủ: nếu $c = gk$ và $ax_1 + by_1 = g$ (Bézout) thì (kx_1, ky_1) là nghiệm.

Necessity: $g \mid a$ and $g \mid b$ give $g \mid ax + by = c$. Sufficiency: if $c = gk$ and $ax_1 + by_1 = g$ (Bézout) then (kx_1, ky_1) is a solution.

Cho (x, y) là nghiệm bất kỳ. Trừ $ax + by = c$ cho $ax_0 + by_0 = c$ được $a(x - x_0) = -b(y - y_0)$; chia cho g :

Let (x, y) be any solution. Subtracting $ax_0 + by_0 = c$ from $ax + by = c$ gives $a(x - x_0) = -b(y - y_0)$; dividing by g :

$$(a/g)(x - x_0) = -(b/g)(y - y_0)$$

Vì $\gcd(a/g, b/g) = 1$ (Tính chất 6.10(iii)) nên $(b/g) \mid (x - x_0)$ theo Bổ đề 6.9, tức $x - x_0 = (b/g)t$. Thế vào được $y - y_0 = -(a/g)t$. Ngược lại mọi cặp như vậy đều là nghiệm.

Since $\gcd(a/g, b/g) = 1$ (Property 6.10(iii)), Lemma 6.9 gives $(b/g) \mid (x - x_0)$, that is $x - x_0 = (b/g)t$. Substituting gives $y - y_0 = -(a/g)t$. Conversely every such pair is a solution. ■

VÍ DỤ 6.4 (Nghiệm tổng quát và đếm theo tham số t) / EXAMPLE 6.4 (General solution and counting by the parameter t) — Có bao nhiêu cặp số nguyên dương (x, y) thỏa $7x + 11y = 400$?

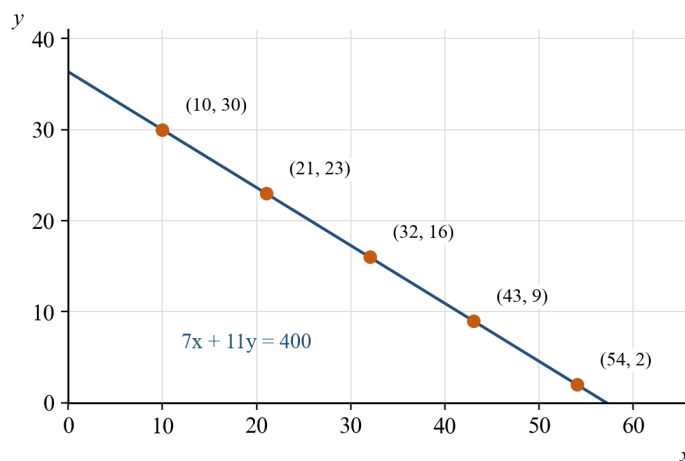
How many pairs of positive integers (x, y) satisfy $7x + 11y = 400$?

Lời giải. / Solution.

- $\gcd(7, 11) = 1$ chia hết 400 nên phương trình có nghiệm nguyên. Thử $y = 1, 2, \dots$:
 $400 - 11 \cdot 2 = 378 = 7 \cdot 54$, nên $(x_0, y_0) = (54, 2)$ là một nghiệm.
 $\gcd(7, 11) = 1$ divides 400, so integer solutions exist. Trying $y = 1, 2, \dots$: $400 - 11 \cdot 2 = 378 = 7 \cdot 54$, so $(x_0, y_0) = (54, 2)$ is a solution.
- Theo (6.5), nghiệm tổng quát là $x = 54 - 11t, y = 2 + 7t, t \in \mathbb{Z}$.
By (6.5) the general solution is $x = 54 - 11t, y = 2 + 7t, t \in \mathbb{Z}$.
- $x > 0 \Leftrightarrow t \leq 4$ (với $t = 4$ được $x = 10$, với $t = 5$ được $x = -1$). $y > 0 \Leftrightarrow t \geq 0$ (với $t = -1$ được $y = -5$).
 $x > 0 \Leftrightarrow t \leq 4$ ($t = 4$ gives $x = 10$, $t = 5$ gives $x = -1$). $y > 0 \Leftrightarrow t \geq 0$ ($t = -1$ gives $y = -5$).
- Vậy $t \in \{0, 1, 2, 3, 4\}$, ứng với các nghiệm $(54, 2), (43, 9), (32, 16), (21, 23), (10, 30)$.
So $t \in \{0, 1, 2, 3, 4\}$, giving the solutions $(54, 2), (43, 9), (32, 16), (21, 23), (10, 30)$.

Vậy có 5 cặp.

Hence there are 5 pairs. ■



Hình 6.2. Các nghiệm nguyên dương của $7x + 11y = 400$ là các điểm nguyên trên đoạn thẳng nằm trong góc phần tư thứ nhất; hai điểm kề nhau cách nhau 11 theo x và 7 theo y .

Figure 6.2. The positive integer solutions of $7x + 11y = 400$ are the lattice points on the segment in the first quadrant; neighbouring points differ by 11 in x and 7 in y .

NHẬN XÉT / REMARK — Đếm nghiệm không âm hoặc dương của $ax + by = c$ luôn đi theo ba bước của Ví dụ 6.4: một nghiệm riêng, nghiệm tổng quát theo t , rồi đổi hai bất đẳng thức $x > 0$, $y > 0$ thành một khoảng của t . Số nghiệm là số số nguyên trong khoảng đó; độ dài khoảng bằng $c/(ab)$ khi $\gcd(a, b) = 1$.

Counting non-negative or positive solutions of $ax + by = c$ always follows the three steps of Example 6.4: one particular solution, the general solution in t , then turning the two inequalities $x > 0$, $y > 0$ into an interval for t . The number of solutions is the number of integers in that interval; its length is $c/(ab)$ when $\gcd(a, b) = 1$.

VÍ DỤ 6.5 (Chia hết từng thừa số nguyên tố) / EXAMPLE 6.5 (Divisibility prime by prime) — Chứng minh rằng $n^5 - n$ chia hết cho 30 với mọi số nguyên n .

Prove that $n^5 - n$ is divisible by 30 for every integer n .

Lời giải. / Solution.

1. Phân tích $n^5 - n = n(n^4 - 1) = n(n - 1)(n + 1)(n^2 + 1)$.
Factorise $n^5 - n = n(n^4 - 1) = n(n - 1)(n + 1)(n^2 + 1)$.
2. Trong ba số nguyên liên tiếp $n - 1$, n , $n + 1$ có một số chia hết cho 3 và có ít nhất một số chẵn. Vậy 2 và 3 đều chia hết tích.
Among the three consecutive integers $n - 1$, n , $n + 1$ one is divisible by 3 and at least one is even. So both 2 and 3 divide the product.
3. Xét dư của n khi chia cho 5. Dư 0, 1, 4: một trong các số n , $n - 1$, $n + 1$ chia hết cho 5. Dư 2: $n = 5k + 2$ và $n^2 + 1 = 25k^2 + 20k + 5$ chia hết cho 5. Dư 3: $n = 5k + 3$ và $n^2 + 1 = 25k^2 + 30k + 10$ chia hết cho 5.
Consider the remainder of n on division by 5. Remainders 0, 1, 4: one of n , $n - 1$, $n + 1$ is divisible by 5. Remainder 2: $n = 5k + 2$ and $n^2 + 1 = 25k^2 + 20k + 5$ is divisible by 5. Remainder 3: $n = 5k + 3$ and $n^2 + 1 = 25k^2 + 30k + 10$ is divisible by 5.
4. Các số 2, 3, 5 đôi một nguyên tố cùng nhau. Áp dụng Tính chất 6.10(ii) hai lần: $2 \cdot 3 = 6$ chia hết tích, rồi $\gcd(6, 5) = 1$ nên $6 \cdot 5 = 30$ chia hết tích.

The numbers 2, 3, 5 are pairwise coprime. Applying Property 6.10(ii) twice: $2 \cdot 3 = 6$ divides the product, and since $\gcd(6, 5) = 1$, so does $6 \cdot 5 = 30$.

Vậy $30 \mid n^5 - n$ với mọi $n \in \mathbb{Z}$.

Hence $30 \mid n^5 - n$ for every $n \in \mathbb{Z}$. ■

PHÂN TÍCH / ANALYSIS — Tổng $a^2 + b^2$ không chia hết trực tiếp cho $a + b$, nhưng $a^2 + b^2 = (a + b)^2 - 2ab$. Mọi ước chung của $a + b$ và $a^2 + b^2$ phải chia hết $2ab$, nên bài toán quy về việc $a + b$ có nguyên tố cùng nhau với ab hay không. Kết quả UCLN chỉ có thể là 1 hoặc 2.
The sum $a^2 + b^2$ is not directly divisible by $a + b$, but $a^2 + b^2 = (a + b)^2 - 2ab$. Every common divisor of $a + b$ and $a^2 + b^2$ must divide $2ab$, so the problem reduces to whether $a + b$ is coprime to ab . The gcd can only be 1 or 2.

VÍ DỤ 6.6 (Quy về nguyên tố cùng nhau) / EXAMPLE 6.6 (Reducing to coprimality) — Cho $a, b \in \mathbb{Z}^+$ nguyên tố cùng nhau. Chứng minh $\gcd(a + b, a^2 + b^2) \in \{1, 2\}$ và cả hai giá trị đều xảy ra.

Let $a, b \in \mathbb{Z}^+$ be coprime. Prove that $\gcd(a + b, a^2 + b^2) \in \{1, 2\}$ and that both values occur.

Lời giải. / Solution.

1. Theo Bổ đề 6.5, $\gcd(a + b, a) = \gcd(a, b) = 1$ và $\gcd(a + b, b) = \gcd(b, a) = 1$. Theo Tính chất 6.10(i), $\gcd(a + b, ab) = 1$.
By Lemma 6.5, $\gcd(a + b, a) = \gcd(a, b) = 1$ and $\gcd(a + b, b) = \gcd(b, a) = 1$. By Property 6.10(i), $\gcd(a + b, ab) = 1$.
2. Đặt $e = \gcd(a + b, a^2 + b^2)$. Vì $e \mid a + b$ nên $e \mid (a + b)^2$ và $e \mid (a + b)^2 - (a^2 + b^2) = 2ab$.
Put $e = \gcd(a + b, a^2 + b^2)$. Since $e \mid a + b$ we have $e \mid (a + b)^2$, hence $e \mid (a + b)^2 - (a^2 + b^2) = 2ab$.
3. e là ước của $a + b$ nên $\gcd(e, ab)$ chia hết $\gcd(a + b, ab) = 1$. Do đó $\gcd(e, ab) = 1$ và từ $e \mid 2ab$ suy ra $e \mid 2$ theo Bổ đề 6.9. Vậy $e \in \{1, 2\}$.
Since e divides $a + b$, $\gcd(e, ab)$ divides $\gcd(a + b, ab) = 1$. So $\gcd(e, ab) = 1$ and $e \mid 2ab$ gives $e \mid 2$ by Lemma 6.9. Hence $e \in \{1, 2\}$.
4. Hai giá trị đều xảy ra: $(a, b) = (1, 2)$ cho $\gcd(3, 5) = 1$; $(a, b) = (1, 3)$ cho $\gcd(4, 10) = 2$.
Both values occur: $(a, b) = (1, 2)$ gives $\gcd(3, 5) = 1$; $(a, b) = (1, 3)$ gives $\gcd(4, 10) = 2$.

Vậy $\gcd(a + b, a^2 + b^2) \in \{1, 2\}$, và cả 1 lẫn 2 đều đạt được.

Hence $\gcd(a + b, a^2 + b^2) \in \{1, 2\}$, and both 1 and 2 are attained. ■

LỖI HAY GẶP / COMMON MISTAKE — Giải $ax + by = c$ khi chưa kiểm $\gcd(a, b) \mid c$, hoặc dừng ở một nghiệm riêng trong khi đề hỏi mọi nghiệm hay số nghiệm dương. Ví dụ $6x + 9y = 100$ vô nghiệm nguyên vì $\gcd(6, 9) = 3 \nmid 100$.

Solving $ax + by = c$ without first checking $\gcd(a, b) \mid c$, or stopping at one particular solution when the problem asks for all solutions or the number of positive ones. For example $6x + 9y = 100$ has no integer solution because $\gcd(6, 9) = 3 \nmid 100$.

LỖI HAY GẶP / COMMON MISTAKE — Dừng thuật toán Euclid ở dư đầu tiên thay vì dư khác 0 cuối cùng, hoặc quên nhân dấu khi thay ngược. Luôn kiểm lại bằng cách tính $ax + by$.

Stopping the Euclidean algorithm at the first remainder instead of the last non-zero one, or losing a sign during back-substitution. Always verify by computing $ax + by$.

PHẢI THUỘC / MEMORISE — $\gcd(a, b) = \gcd(b, a - bq)$; $ax + by = \gcd(a, b)$; $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$; $ax + by = c$ có nghiệm nguyên $\Leftrightarrow \gcd(a, b) \mid c$.
 $\gcd(a, b) = \gcd(b, a - bq)$; $ax + by = \gcd(a, b)$; $\gcd(a, b) \cdot \text{lcm}(a, b) = ab$; $ax + by = c$ has an integer solution $\Leftrightarrow \gcd(a, b) \mid c$.

6.4. Số nguyên tố và định lý cơ bản của số học — *Primes and the fundamental theorem of arithmetic*

ĐỊNH NGHĨA 6.13 (Số nguyên tố) / DEFINITION 6.13 (Prime number) — Số nguyên $p > 1$ là số nguyên tố nếu ước dương duy nhất của nó là 1 và p . Số nguyên $n > 1$ không nguyên tố gọi là hợp số.

An integer $p > 1$ is prime if its only positive divisors are 1 and p . An integer $n > 1$ that is not prime is composite.

HỆ QUẢ 6.14 (Bổ đề Euclid cho số nguyên tố) / COROLLARY 6.14 (Euclid's lemma for primes) — Nếu p nguyên tố và $p \mid ab$ thì $p \mid a$ hoặc $p \mid b$. Tổng quát, nếu $p \mid a_1 a_2 \dots a_k$ thì $p \mid a_i$ với một chỉ số i nào đó.

If p is prime and $p \mid ab$ then $p \mid a$ or $p \mid b$. More generally, if $p \mid a_1 a_2 \dots a_k$ then $p \mid a_i$ for some index i .

Chứng minh. / *Proof.*

Giả sử $p \nmid a$. Ước dương của p chỉ là 1 và p , và p không chia hết a , nên $\gcd(p, a) = 1$. Theo Bổ đề 6.9, $p \mid b$. Trường hợp k thừa số suy ra bằng quy nạp theo k : $p \mid (a_1 \dots a_{k-1}) \cdot a_k$ thì $p \mid a_k$ hoặc $p \mid a_1 \dots a_{k-1}$.

Suppose $p \nmid a$. The positive divisors of p are only 1 and p , and p does not divide a , so $\gcd(p, a) = 1$. By Lemma 6.9, $p \mid b$. The case of k factors follows by induction on k : $p \mid (a_1 \dots a_{k-1}) \cdot a_k$ gives $p \mid a_k$ or $p \mid a_1 \dots a_{k-1}$. ■

ĐỊNH LÝ 6.15 (Định lý cơ bản của số học) / THEOREM 6.15 (Fundamental theorem of arithmetic) — Mọi số nguyên $n > 1$ phân tích được thành tích các số nguyên tố, và sự phân tích đó là duy nhất nếu không kể thứ tự các thừa số.

Every integer $n > 1$ can be written as a product of primes, and this factorisation is unique up to the order of the factors.

Chứng minh. / *Proof.*

Sự tồn tại, quy nạp mạnh theo n . Nếu n nguyên tố thì n là tích một thừa số. Nếu n là hợp số thì $n = ab$ với $1 < a, b < n$; theo giả thiết quy nạp a và b là tích các số nguyên tố, nên n cũng vậy.

Existence, by strong induction on n . If n is prime it is a product of one prime. If n is composite then $n = ab$ with $1 < a, b < n$; by the induction hypothesis a and b are products of primes, hence so is n .

Tính duy nhất, quy nạp mạnh theo n . Giả sử $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ là hai cách phân tích. Vì $p_1 \mid q_1 \dots q_s$ nên theo Hệ quả 6.14, $p_1 \mid q_j$ với một j ; q_j nguyên tố và $p_1 > 1$ nên $p_1 =$

q_j . Đánh số lại để $j = 1$ và giản ước: $n/p_1 = p_2 \dots p_r = q_2 \dots q_s$. Nếu $n/p_1 = 1$ thì $r = s = 1$; ngược lại $1 < n/p_1 < n$ và hai cách phân tích này trùng nhau theo giả thiết quy nạp.

Uniqueness, by strong induction on n . Suppose $n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s$ are two factorisations. Since $p_1 \mid q_1 \dots q_s$, Corollary 6.14 gives $p_1 \mid q_j$ for some j ; as q_j is prime and $p_1 > 1$, we get $p_1 = q_j$. Renumber so that $j = 1$ and cancel: $n/p_1 = p_2 \dots p_r = q_2 \dots q_s$. If $n/p_1 = 1$ then $r = s = 1$; otherwise $1 < n/p_1 < n$ and the two factorisations agree by the induction hypothesis. ■

TÍNH CHẤT 6.16 (Ước nguyên tố nhỏ) / PROPERTY 6.16 (Small prime divisor) — Hợp số n có một ước nguyên tố p thỏa $p \leq \sqrt{n}$. Do đó nếu $n > 1$ không chia hết cho số nguyên tố nào không vượt quá $\sqrt{n}$ thì n nguyên tố.

A composite number n has a prime divisor p with $p \leq \sqrt{n}$. Hence if $n > 1$ is divisible by no prime not exceeding $\sqrt{n}$ then n is prime.

Chứng minh. / Proof.

Viết $n = ab$ với $1 < a \leq b$. Khi đó $a^2 \leq ab = n$ nên $a \leq \sqrt{n}$. Ước nguyên tố p của a (tồn tại theo định lý cơ bản) thỏa $p \leq a \leq \sqrt{n}$ và $p \mid n$.

Write $n = ab$ with $1 < a \leq b$. Then $a^2 \leq ab = n$ so $a \leq \sqrt{n}$. A prime divisor p of a (it exists by the fundamental theorem) satisfies $p \leq a \leq \sqrt{n}$ and $p \mid n$. ■

ĐỊNH LÝ 6.17 (Euclid: vô hạn số nguyên tố) / THEOREM 6.17 (Euclid: infinitude of primes) — Có vô hạn số nguyên tố.

There are infinitely many primes.

Chứng minh. / Proof.

Giả sử chỉ có các số nguyên tố $p_1, \dots, p_m$. Đặt $N = p_1 \dots p_m + 1 > 1$. N có một ước nguyên tố q ; q là một trong các p_i , nên $q \mid p_1 \dots p_m$ và $q \mid N$, suy ra $q \mid 1$, vô lý.

Suppose the only primes are $p_1, \dots, p_m$. Put $N = p_1 \dots p_m + 1 > 1$. N has a prime divisor q ; q is one of the p_i , so $q \mid p_1 \dots p_m$ and $q \mid N$, giving $q \mid 1$, absurd. ■

ĐỊNH LÝ 6.18 (Số nguyên tố dạng $4k + 3$) / THEOREM 6.18 (Primes of the form $4k + 3$) — Có vô hạn số nguyên tố dạng $4k + 3$.

There are infinitely many primes of the form $4k + 3$.

Chứng minh. / Proof.

Giả sử các số nguyên tố dạng $4k + 3$ chỉ là $p_1 = 3, p_2, \dots, p_m$. Đặt $P = p_1 \dots p_m$ và $N = 4P - 1 = 4(P - 1) + 3$. Khi đó N lẻ và N chia 4 dư 3.

Suppose the primes of the form $4k + 3$ are only $p_1 = 3, p_2, \dots, p_m$. Put $P = p_1 \dots p_m$ and $N = 4P - 1 = 4(P - 1) + 3$. Then N is odd and leaves remainder 3 on division by 4.

Mọi ước nguyên tố của N đều lẻ, nên dạng $4k + 1$ hoặc $4k + 3$. Tích hai số dạng $4k + 1$ cũng có dạng $4k + 1$ vì $(4a + 1)(4b + 1) = 4(4ab + a + b) + 1$. Nếu mọi ước nguyên tố của N có dạng $4k + 1$ thì N có dạng $4k + 1$, mâu thuẫn. Vậy N có ước nguyên tố q dạng $4k + 3$.

Every prime divisor of N is odd, hence of the form $4k + 1$ or $4k + 3$. A product of two numbers of the form $4k + 1$ has the form $4k + 1$, since $(4a + 1)(4b + 1) = 4(4ab + a + b) + 1$. If all prime

divisors of N had the form $4k + 1$, N would too, a contradiction. So N has a prime divisor q of the form $4k + 3$.

Nếu $q = p_i$ thì $q \mid 4P$ và $q \mid N = 4P - 1$, nên $q \mid 1$, vô lý. Vậy q là số nguyên tố dạng $4k + 3$ nằm ngoài danh sách.

If $q = p_i$ then $q \mid 4P$ and $q \mid N = 4P - 1$, so $q \mid 1$, absurd. So q is a prime of the form $4k + 3$ outside the list. ■

NHẬN XÉT / REMARK — Cách lập $N = 4P - 1$ dùng được cho dạng $6k + 5$ ($N = 6P - 1$) nhưng không cho dạng $4k + 1$: ước nguyên tố của $N = 4P + 1$ có thể đều dạng $4k + 3$ (hai số dạng $4k + 3$ nhân lại cho dạng $4k + 1$), nên không ép được một ước nguyên tố mới dạng $4k + 1$. Với dạng $4k + 1$ cần thêm một kết quả về ước nguyên tố của $x^2 + 1$, thuộc chương Đồng dư và các định lý Fermat, Euler, Wilson (Chương 7).

The construction $N = 4P - 1$ also works for the form $6k + 5$ ($N = 6P - 1$) but not for $4k + 1$: the prime divisors of $N = 4P + 1$ may all have the form $4k + 3$ (two numbers of the form $4k + 3$ multiply to the form $4k + 1$), so no new prime of the form $4k + 1$ is forced. The form $4k + 1$ needs a further fact about prime divisors of $x^2 + 1$, which belongs to the chapter on congruences and the theorems of Fermat, Euler and Wilson (Chapter 7).

PHÂN TÍCH / ANALYSIS — Ba số p , $2p + 1$, $4p + 1$ khi chia cho 3 có dư phụ thuộc vào dư của p . Một số lớn hơn 3 mà chia hết cho 3 là hợp số, nên chỉ cần tìm dư của p làm một trong hai số sau chia hết cho 3.

The three numbers p , $2p + 1$, $4p + 1$ have remainders on division by 3 that depend on the remainder of p . A number greater than 3 that is divisible by 3 is composite, so it suffices to find the remainders of p that make one of the last two numbers divisible by 3.

VÍ DỤ 6.7 (Xét dư khi chia cho số nguyên tố nhỏ) / EXAMPLE 6.7 (Remainders modulo a small prime) — Tìm tất cả số nguyên tố p sao cho $2p + 1$ và $4p + 1$ cũng là số nguyên tố.

Find all primes p such that $2p + 1$ and $4p + 1$ are also prime.

Lời giải. / Solution.

1. Viết $p = 3k$, $3k + 1$ hoặc $3k + 2$.

Write $p = 3k$, $3k + 1$ or $3k + 2$.

2. Nếu $p = 3k + 1$ thì $2p + 1 = 6k + 3 = 3(2k + 1)$. Vì $p \geq 2$ nên $2p + 1 \geq 5 > 3$, do đó $2p + 1$ là hợp số. Loại.

If $p = 3k + 1$ then $2p + 1 = 6k + 3 = 3(2k + 1)$. Since $p \geq 2$ we have $2p + 1 \geq 5 > 3$, so $2p + 1$ is composite. Rejected.

3. Nếu $p = 3k + 2$ thì $4p + 1 = 12k + 9 = 3(4k + 3) \geq 9$, là hợp số. Loại.

If $p = 3k + 2$ then $4p + 1 = 12k + 9 = 3(4k + 3) \geq 9$, which is composite. Rejected.

4. Còn $p = 3k$: p nguyên tố nên $p = 3$. Khi đó $2p + 1 = 7$ và $4p + 1 = 13$ đều nguyên tố.

Only $p = 3k$ remains: p is prime so $p = 3$. Then $2p + 1 = 7$ and $4p + 1 = 13$ are both prime.

Vậy $p = 3$.

Hence $p = 3$. ■

LỖI HAY GẶP / COMMON MISTAKE — Khẳng định một số là nguyên tố chỉ vì thử vài số nguyên tố nhỏ, hoặc quên rằng 1 không phải nguyên tố và 2 là số nguyên tố chẵn duy nhất. Bài về số nguyên tố luôn phải xét riêng $p = 2$ và $p = 3$.

Declaring a number prime because a few small primes fail to divide it, or forgetting that 1 is not prime and 2 is the only even prime. Problems about primes always need $p = 2$ and $p = 3$ checked separately.

6.5. Số mũ p-adic và công thức Legendre — The p-adic valuation and Legendre's formula

ĐỊNH NGHĨA 6.19 (Số mũ p-adic) / DEFINITION 6.19 (p-adic valuation) — Cho p nguyên tố và $n \in \mathbb{Z}^+$. Số mũ p-adic $v_p(n)$ là số mũ lớn nhất $k \geq 0$ sao cho $p^k \mid n$. Theo định lý cơ bản của số học, $v_p(n)$ là số mũ của p trong sự phân tích n ra thừa số nguyên tố.

Let p be prime and $n \in \mathbb{Z}^+$. The p-adic valuation $v_p(n)$ is the largest $k \geq 0$ with $p^k \mid n$. By the fundamental theorem of arithmetic, $v_p(n)$ is the exponent of p in the prime factorisation of n .

TÍNH CHẤT 6.20 (Tính chất của số mũ p-adic) / PROPERTY 6.20 (Properties of the p-adic valuation) — Với $a, b \in \mathbb{Z}^+$ và p nguyên tố: (i) $v_p(ab) = v_p(a) + v_p(b)$; (ii) $a \mid b$ khi và chỉ khi $v_p(a) \leq v_p(b)$ với mọi số nguyên tố p ; (iii) $v_p(\gcd(a, b)) = \min(v_p(a), v_p(b))$ và $v_p(\text{lcm}(a, b)) = \max(v_p(a), v_p(b))$; (iv) $v_p(a + b) \geq \min(v_p(a), v_p(b))$, và dấu bằng xảy ra khi $v_p(a) \neq v_p(b)$.

For $a, b \in \mathbb{Z}^+$ and p prime: (i) $v_p(ab) = v_p(a) + v_p(b)$; (ii) $a \mid b$ if and only if $v_p(a) \leq v_p(b)$ for every prime p ; (iii) $v_p(\gcd(a, b)) = \min(v_p(a), v_p(b))$ and $v_p(\text{lcm}(a, b)) = \max(v_p(a), v_p(b))$; (iv) $v_p(a + b) \geq \min(v_p(a), v_p(b))$, with equality when $v_p(a) \neq v_p(b)$.

Chứng minh. / Proof.

(i) Nhân hai sự phân tích ra thừa số nguyên tố; số mũ của p cộng lại.

(i) Multiply the two prime factorisations; the exponents of p add.

(ii) Nếu $b = ac$ thì $v_p(b) = v_p(a) + v_p(c) \geq v_p(a)$. Ngược lại, nếu $v_p(a) \leq v_p(b)$ với mọi p thì $b/a = \prod p^{k(p)}$ với $k(p) = v_p(b) - v_p(a) \geq 0$ là số nguyên.

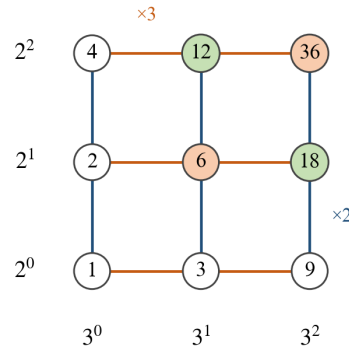
(ii) If $b = ac$ then $v_p(b) = v_p(a) + v_p(c) \geq v_p(a)$. Conversely, if $v_p(a) \leq v_p(b)$ for all p then $b/a = \prod p^{k(p)}$ with $k(p) = v_p(b) - v_p(a) \geq 0$ is an integer.

(iii) Theo (ii), ước chung d của a và b có $v_p(d) \leq \min(v_p(a), v_p(b))$ với mọi p . Số $\prod p^{m(p)}$, với $m(p) = \min(v_p(a), v_p(b))$, là một ước chung và chia hết mọi ước chung nên là ước chung lớn nhất. Lý luận với max cho bội chung nhỏ nhất.

(iii) By (ii), a common divisor d of a and b has $v_p(d) \leq \min(v_p(a), v_p(b))$ for every p . The number $\prod p^{m(p)}$, with $m(p) = \min(v_p(a), v_p(b))$, is a common divisor and is divisible by every common divisor, so it is the greatest. The same argument with max gives the least common multiple.

(iv) Đặt $m = \min(v_p(a), v_p(b))$. Khi đó $p^m \mid a$ và $p^m \mid b$ nên $p^m \mid a + b$. Nếu $v_p(a) = m < v_p(b)$ thì $a = p^m a'$ với $p \nmid a'$ và $b = p^{m+1} b'$, suy ra $a + b = p^m(a' + pb')$ mà $a' + pb'$ không chia hết cho p . Vậy $v_p(a + b) = m$.

(iv) Put $m = \min(v_p(a), v_p(b))$. Then $p^m \mid a$ and $p^m \mid b$ so $p^m \mid a + b$. If $v_p(a) = m < v_p(b)$ then $a = p^m a'$ with $p \nmid a'$ and $b = p^{m+1} b'$, so $a + b = p^m(a' + pb')$ and $a' + pb'$ is not divisible by p . Hence $v_p(a + b) = m$. ■



Hình 6.3. Các ước của 36 xếp theo số mũ của 2 (hàng) và của 3 (cột). Ô xanh: 12 và 18. Ô cam: $\text{UCLN}(12, 18) = 6$ lấy số mũ nhỏ hơn ở mỗi tọa độ, $\text{BCNN}(12, 18) = 36$ lấy số mũ lớn hơn.

Figure 6.3. The divisors of 36 arranged by the exponent of 2 (rows) and of 3 (columns). Green: 12 and 18. Orange: $\text{gcd}(12, 18) = 6$ takes the smaller exponent in each coordinate, $\text{lcm}(12, 18) = 36$ takes the larger.

ĐỊNH LÝ 6.21 (Công thức Legendre) / THEOREM 6.21 (Legendre's formula) — Cho p nguyên tố và $n \in \mathbb{Z}^+$. Khi đó $v_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \dots$ (tổng hữu hạn, các số hạng bằng 0 khi $p^k > n$).

Let p be prime and $n \in \mathbb{Z}^+$. Then $v_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \dots$ (a finite sum: terms vanish once $p^k > n$).

$$v_p(n!) = \lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \dots \quad (6.6)$$

Chứng minh. / Proof.

Theo Tính chất 6.20(i), $v_p(n!) = v_p(1) + v_p(2) + \dots + v_p(n)$. Số $v_p(m)$ bằng số các $k \geq 1$ sao cho $p^k \mid m$.

By Property 6.20(i), $v_p(n!) = v_p(1) + v_p(2) + \dots + v_p(n)$. The number $v_p(m)$ equals the number of $k \geq 1$ with $p^k \mid m$.

Đếm theo k thay vì theo m : với k cố định, trong $1, 2, \dots, n$ có đúng $\lfloor n/p^k \rfloor$ số chia hết cho p^k . Cộng theo $k \geq 1$ được công thức.

Count by k instead of by m : for fixed k , exactly $\lfloor n/p^k \rfloor$ of the numbers $1, 2, \dots, n$ are divisible by p^k . Summing over $k \geq 1$ gives the formula. ■

HỆ QUẢ 6.22 (Công thức Legendre qua tổng chữ số) / COROLLARY 6.22 (Legendre's formula via digit sum) — Gọi $s_p(n)$ là tổng các chữ số của n trong hệ cơ số p . Khi đó $v_p(n!) = (n - s_p(n))/(p - 1)$.

Let $s_p(n)$ be the sum of the digits of n in base p . Then $v_p(n!) = (n - s_p(n))/(p - 1)$.

$$v_p(n!) = (n - s_p(n))/(p - 1) \quad (6.7)$$

Chứng minh. / Proof.

Viết $n = a_0 + a_1p + \dots + a_mp^m$ với $0 \leq a_i < p$. Phần nguyên $\lfloor n/p^k \rfloor = a_k + a_{k+1}p + \dots + a_mp^{m-k}$, vì các chữ số thấp hơn cộng lại nhỏ hơn p^k .

Write $n = a_0 + a_1p + \dots + a_mp^m$ with $0 \leq a_i < p$. Then $[n/p^k] = a_k + a_{k+1}p + \dots + a_mp^{m-k}$, because the lower digits add up to less than p^k .

Cộng theo $k = 1, \dots, m$: mỗi chữ số a_i xuất hiện với hệ số $p^{i-1} + \dots + p + 1 = (p^i - 1)/(p - 1)$. Vậy $v_p(n!) = \sum a_i(p^i - 1)/(p - 1) = (n - \sum a_i)/(p - 1)$.

Sum over $k = 1, \dots, m$: each digit a_i appears with coefficient $p^{i-1} + \dots + p + 1 = (p^i - 1)/(p - 1)$. Hence $v_p(n!) = \sum a_i(p^i - 1)/(p - 1) = (n - \sum a_i)/(p - 1)$. ■

VÍ DỤ 6.8 (Đếm thừa số 5) / EXAMPLE 6.8 (Counting factors of 5) — (a) 2468! tận cùng bằng bao nhiêu chữ số 0? (b) Tìm số nguyên dương n nhỏ nhất sao cho 10^{25} chia hết $n!$.
(a) How many zeros does 2468! end with? (b) Find the least positive integer n such that 10^{25} divides $n!$.

Lời giải. / Solution.

- Số chữ số 0 tận cùng là số mũ lớn nhất k với $10^k \mid 2468!$, tức $\min(v_2(2468!), v_5(2468!))$. Theo (6.6), $v_2(2468!) \geq \lfloor 2468/2 \rfloor = 1234$.
The number of trailing zeros is the largest k with $10^k \mid 2468!$, that is $\min(v_2(2468!), v_5(2468!))$. By (6.6), $v_2(2468!) \geq \lfloor 2468/2 \rfloor = 1234$.

$$v_5(2468!) = 493 + 98 + 19 + 3 = 613$$

- Vì $613 < 1234$ nên 2468! tận cùng bằng đúng 613 chữ số 0.
Since $613 < 1234$, 2468! ends with exactly 613 zeros.
- (b) Cần $v_5(n!) \geq 25$ và $v_2(n!) \geq 25$. Hàm $v_5(n!)$ không giảm theo n . Ta có $v_5(104!) = 20 + 4 = 24 < 25$ và $v_5(105!) = 21 + 4 = 25$.
(b) We need $v_5(n!) \geq 25$ and $v_2(n!) \geq 25$. The function $v_5(n!)$ is non-decreasing in n . We have $v_5(104!) = 20 + 4 = 24 < 25$ and $v_5(105!) = 21 + 4 = 25$.
- Với $n = 105$: $v_2(105!) \geq \lfloor 105/2 \rfloor = 52 \geq 25$, nên $10^{25} \mid 105!$. Với $n \leq 104$ thì $v_5(n!) \leq 24$.
For $n = 105$: $v_2(105!) \geq \lfloor 105/2 \rfloor = 52 \geq 25$, so $10^{25} \mid 105!$. For $n \leq 104$ we have $v_5(n!) \leq 24$.

Vậy (a) 613 chữ số 0; (b) $n = 105$.

Hence (a) 613 zeros; (b) $n = 105$. ■

NHẬN XÉT / REMARK — Chỉ cần đếm thừa số 5 vì $v_2(n!) \geq v_5(n!)$ với mọi n : $\lfloor n/2^k \rfloor \geq \lfloor n/5^k \rfloor$ ở từng số hạng của (6.6). Nếu hỏi về số $12 = 2^2 \cdot 3$ thì phải so cả hai: $12^k \mid n!$ khi $2k \leq v_2(n!)$ và $k \leq v_3(n!)$.
Only the factors of 5 need counting because $v_2(n!) \geq v_5(n!)$ for all n : $\lfloor n/2^k \rfloor \geq \lfloor n/5^k \rfloor$ term by term in (6.6). For a number such as $12 = 2^2 \cdot 3$ both counts matter: $12^k \mid n!$ when $2k \leq v_2(n!)$ and $k \leq v_3(n!)$.

PHÂN TÍCH / ANALYSIS — Điều kiện $2^{n-1} \mid n!$ nghĩa là $v_2(n!) \geq n - 1$. Với $p = 2$, công thức (6.7) cho $v_2(n!) = n - s_2(n)$, trong đó $s_2(n)$ là số chữ số 1 của n trong hệ nhị phân. Bất đẳng thức $n - s_2(n) \geq n - 1$ chỉ còn là một điều kiện đếm chữ số.
The condition $2^{n-1} \mid n!$ means $v_2(n!) \geq n - 1$. For $p = 2$, formula (6.7) gives $v_2(n!) = n - s_2(n)$, where $s_2(n)$ is the number of digits 1 of n in binary. The inequality $n - s_2(n) \geq n - 1$ becomes a condition on counting digits.

VÍ DỤ 6.9 (Tổng chữ số nhị phân) / EXAMPLE 6.9 (Binary digit sum) — Tìm tất cả số nguyên dương n sao cho 2^{n-1} chia hết $n!$.
Find all positive integers n such that 2^{n-1} divides $n!$.

Lời giải. / Solution.

1. Theo (6.7) với $p = 2$: $v_2(n!) = n - s_2(n)$, với $s_2(n)$ là số chữ số 1 trong biểu diễn nhị phân của n .

By (6.7) with $p = 2$: $v_2(n!) = n - s_2(n)$, where $s_2(n)$ is the number of digits 1 in the binary representation of n .

2. $2^{n-1} \mid n! \Leftrightarrow v_2(n!) \geq n - 1 \Leftrightarrow n - s_2(n) \geq n - 1 \Leftrightarrow s_2(n) \leq 1$.

$2^{n-1} \mid n! \Leftrightarrow v_2(n!) \geq n - 1 \Leftrightarrow n - s_2(n) \geq n - 1 \Leftrightarrow s_2(n) \leq 1$.

3. Vì $n \geq 1$ nên $s_2(n) \geq 1$. Do đó điều kiện là $s_2(n) = 1$, tức n là lũy thừa của 2.

Since $n \geq 1$ we have $s_2(n) \geq 1$. So the condition is $s_2(n) = 1$, that is n is a power of 2.

Vậy $n \in \{1, 2, 4, 8, 16, \dots\}$, tức $n = 2^j$ với $j \in \mathbb{N}$.

Hence $n \in \{1, 2, 4, 8, 16, \dots\}$, that is $n = 2^j$ with $j \in \mathbb{N}$. ■

LỖI HAY GẶP / COMMON MISTAKE — Công thức Legendre dừng sớm: chỉ lấy $[n/p]$ và bỏ $[n/p^2]$, $[n/p^3]$, Ví dụ $v_5(100!) = 20 + 4 = 24$, không phải 20.

Stopping Legendre's formula early: taking only $[n/p]$ and dropping $[n/p^2]$, $[n/p^3]$, For example $v_5(100!) = 20 + 4 = 24$, not 20.

6.6. Số ước, tổng ước và số hoàn hảo — Number of divisors, sum of divisors and perfect numbers

ĐỊNH NGHĨA 6.23 (Số ước, tổng ước, số hoàn hảo) / DEFINITION 6.23 (Divisor count, divisor sum, perfect number) — Với $n \in \mathbb{Z}^+$, $\tau(n)$ là số ước dương của n và $\sigma(n)$ là tổng các ước dương của n . Số n gọi là hoàn hảo nếu $\sigma(n) = 2n$, tức n bằng tổng các ước dương nhỏ hơn n .

For $n \in \mathbb{Z}^+$, $\tau(n)$ is the number of positive divisors of n and $\sigma(n)$ is their sum. The number n is perfect if $\sigma(n) = 2n$, that is n equals the sum of its positive divisors smaller than n .

ĐỊNH LÝ 6.24 (Công thức τ và σ) / THEOREM 6.24 (The formulas for τ and σ) — Cho $n = \prod p^{e(p)}$ là dạng chính tắc của n (tích lấy theo các số nguyên tố $p \mid n$, $e(p) = v_p(n)$). Khi đó $\tau(n) = \prod (e(p) + 1)$ và $\sigma(n) = \prod (p^{e(p)+1} - 1)/(p - 1)$.

Let $n = \prod p^{e(p)}$ be the canonical form of n (the product runs over primes $p \mid n$, with $e(p) = v_p(n)$). Then $\tau(n) = \prod (e(p) + 1)$ and $\sigma(n) = \prod (p^{e(p)+1} - 1)/(p - 1)$.

$$\tau(n) = \prod (e(p) + 1) \quad (6.8)$$

$$\sigma(n) = \prod (p^{e(p)+1} - 1)/(p - 1) \quad (6.9)$$

Chứng minh. / Proof.

Theo Tính chất 6.20(ii), $d \mid n$ khi và chỉ khi $d = \prod p^{b(p)}$ với $0 \leq b(p) \leq e(p)$ (một số nguyên tố không chia hết n không thể chia hết d). Theo tính duy nhất của định lý cơ bản, các bộ số mũ khác nhau cho các ước khác nhau. Mỗi p có $e(p) + 1$ lựa chọn $b(p)$, nên có $\prod (e(p) + 1)$ ước.

By Property 6.20(ii), $d \mid n$ if and only if $d = \prod p^{b(p)}$ with $0 \leq b(p) \leq e(p)$ (a prime that does not divide n cannot divide d). By the uniqueness in the fundamental theorem, different exponent choices give different divisors. Each p has $e(p) + 1$ choices for $b(p)$, so there are $\prod (e(p) + 1)$ divisors.

Khai triển tích $\prod (1 + p + p^2 + \dots + p^{e(p)})$ bằng phép phân phối: mỗi số hạng là một ước d của n , xuất hiện đúng một lần. Vậy tích bằng $\sigma(n)$. Tổng cấp số nhân $1 + p + \dots + p^{e(p)} = (p^{e(p)+1} - 1)/(p - 1)$.

Expand $\prod (1 + p + p^2 + \dots + p^{e(p)})$ by distributivity: each term is a divisor d of n , appearing exactly once. So the product equals $\sigma(n)$. The geometric sum is $1 + p + \dots + p^{e(p)} = (p^{e(p)+1} - 1)/(p - 1)$. ■

NHẬN XÉT / REMARK — Với $n = 360 = 2^3 \cdot 3^2 \cdot 5$: $\tau(360) = 4 \cdot 3 \cdot 2 = 24$ và $\sigma(360) = 15 \cdot 13 \cdot 6 = 1170$. Công thức (6.8) và (6.9) cho thấy τ , σ nhân tính: $\tau(mn) = \tau(m)\tau(n)$, $\sigma(mn) = \sigma(m)\sigma(n)$ khi $\gcd(m, n) = 1$. Ghép mỗi ước d với n/d , tích mọi ước của n bằng $n^{\tau(n)/2}$: với 360 là 360^{12} .
For $n = 360 = 2^3 \cdot 3^2 \cdot 5$: $\tau(360) = 4 \cdot 3 \cdot 2 = 24$ and $\sigma(360) = 15 \cdot 13 \cdot 6 = 1170$. Formulas (6.8) and (6.9) show that τ and σ are multiplicative: $\tau(mn) = \tau(m)\tau(n)$, $\sigma(mn) = \sigma(m)\sigma(n)$ when $\gcd(m, n) = 1$. Pairing each divisor d with n/d , the product of all divisors of n is $n^{\tau(n)/2}$: for 360 it is 360^{12} .

HỆ QUẢ 6.25 / COROLLARY 6.25 — $\tau(n)$ lẻ khi và chỉ khi n là số chính phương.
 $\tau(n)$ is odd if and only if n is a perfect square.

Chứng minh. / Proof.

Theo (6.8), $\tau(n)$ lẻ khi và chỉ khi mọi $e(p) + 1$ lẻ, tức mọi $e(p)$ chẵn. Điều này tương đương $n = (\prod p^{e(p)/2})^2$; ngược lại số chính phương m^2 có $v_p(m^2) = 2v_p(m)$ chẵn.

By (6.8), $\tau(n)$ is odd if and only if every $e(p) + 1$ is odd, that is every $e(p)$ is even. This is equivalent to $n = (\prod p^{e(p)/2})^2$; conversely a square m^2 has $v_p(m^2) = 2v_p(m)$, which is even. ■

ĐỊNH LÝ 6.26 (Euclid–Euler: số hoàn hảo chẵn) / THEOREM 6.26 (Euclid–Euler: even perfect numbers) — Số chẵn n là hoàn hảo khi và chỉ khi $n = 2^{k-1}(2^k - 1)$ với $2^k - 1$ là số nguyên tố.

An even number n is perfect if and only if $n = 2^{k-1}(2^k - 1)$ with $2^k - 1$ prime.

Chứng minh. / Proof.

Điều kiện đủ. Đặt $M = 2^k - 1$ nguyên tố; $k \geq 2$ vì $M > 1$, nên M lẻ. Theo (6.9) $\sigma(2^{k-1}) = 2^k - 1 = M$ và $\sigma(M) = M + 1 = 2^k$. σ nhân tính, nên $\sigma(n) = M \cdot 2^k = 2n$.

Sufficiency. Put $M = 2^k - 1$, prime; $k \geq 2$ because $M > 1$, so M is odd. By (6.9) $\sigma(2^{k-1}) = 2^k - 1 = M$ and $\sigma(M) = M + 1 = 2^k$. Since σ is multiplicative, $\sigma(n) = M \cdot 2^k = 2n$.

Điều kiện cần. Viết $n = 2^a m$ với $a \geq 1$ và m lẻ. Từ $\sigma(n) = 2n$ ta có $(2^{a+1} - 1)\sigma(m) = 2^{a+1}m$. Hai số $2^{a+1} - 1$ và 2^{a+1} nguyên tố cùng nhau, nên $2^{a+1} - 1$ chia hết m theo Bổ đề 6.9: $m = (2^{a+1} - 1)c$. Thế vào, $\sigma(m) = 2^{a+1}c$.

Necessity. Write $n = 2^a m$ with $a \geq 1$ and m odd. From $\sigma(n) = 2n$ we get $(2^{a+1} - 1)\sigma(m) = 2^{a+1}m$. The numbers $2^{a+1} - 1$ and 2^{a+1} are coprime, so $2^{a+1} - 1$ divides m by Lemma 6.9: $m = (2^{a+1} - 1)c$. Substituting, $\sigma(m) = 2^{a+1}c$.

Nếu $c > 1$ thì 1, c , m là ba ước phân biệt của m ($c \neq m$ vì $2^{a+1} - 1 \geq 3$), nên $\sigma(m) \geq 1 + c + m = 1 + c + (2^{a+1} - 1)c = 1 + 2^{a+1}c > \sigma(m)$, vô lý. Vậy $c = 1$.

If $c > 1$ then 1, c , m are three distinct divisors of m ($c \neq m$ since $2^{a+1} - 1 \geq 3$), so $\sigma(m) \geq 1 + c + m = 1 + c + (2^{a+1} - 1)c = 1 + 2^{a+1}c > \sigma(m)$, absurd. Hence $c = 1$.

Với $c = 1$: $m = 2^{a+1} - 1 > 1$ và $\sigma(m) = 2^{a+1} = m + 1$. Tổng các ước của m chỉ là $1 + m$ nên m chỉ có hai ước 1 và m , tức m nguyên tố. Đặt $k = a + 1$ ta được $n = 2^{k-1}(2^k - 1)$.

With $c = 1$: $m = 2^{a+1} - 1 > 1$ and $\sigma(m) = 2^{a+1} = m + 1$. The divisors of m sum to just $1 + m$, so m has only the divisors 1 and m , that is m is prime. Putting $k = a + 1$ gives $n = 2^{k-1}(2^k - 1)$. ■

k	Số Mersenne <i>Mersenne number</i>	Số hoàn hảo chẵn <i>Even perfect number</i>
2	3	6
3	7	28
4	$15 = 3 \cdot 5$	không có <i>none</i>
5	31	496
7	127	8128
13	8191	33.550.336 <i>33,550,336</i>

PHÂN TÍCH / ANALYSIS — Số ước chỉ phụ thuộc vào bộ số mũ, còn độ lớn của n phụ thuộc cả vào việc đặt số mũ nào lên số nguyên tố nào. Hai việc tách rời: trước hết liệt kê các cách viết $48 = (e_1 + 1)(e_2 + 1) \dots$, rồi dồn số mũ lớn vào số nguyên tố nhỏ để n bé nhất.

The number of divisors depends only on the multiset of exponents, whereas the size of n also depends on which exponent sits on which prime. The two tasks separate: first list the ways to write $48 = (e_1 + 1)(e_2 + 1) \dots$, then put the large exponents on the small primes to make n least.

VÍ DỤ 6.10 (Số mũ giảm dần trên các số nguyên tố nhỏ) / EXAMPLE 6.10 (Decreasing exponents on the smallest primes) — Tìm số nguyên dương nhỏ nhất có đúng 48 ước dương.

Find the least positive integer with exactly 48 positive divisors.

Lời giải. / Solution.

- Theo (6.8), $n = \prod p^{e(p)}$ có 48 ước khi $\prod (e(p) + 1) = 48$. Với bộ số mũ cho trước, n nhỏ nhất khi số mũ giảm dần theo thứ tự số nguyên tố 2, 3, 5, 7, 11, ...: nếu $p < q$ và $x < y$ thì $p^y q^x / (p^x q^y) = (p/q)^{y-x} < 1$, nên đổi chỗ hai số mũ cho số nhỏ hơn.

By (6.8), $n = \prod p^{e(p)}$ has 48 divisors when $\prod (e(p) + 1) = 48$. For a given multiset of exponents, n is least when the exponents decrease along the primes 2, 3, 5, 7, 11, ...: if $p < q$ and $x < y$ then $p^y q^x / (p^x q^y) = (p/q)^{y-x} < 1$, so swapping the two exponents gives a smaller number.

- Các cách viết 48 thành tích không tăng các thừa số lớn hơn 1 (mỗi thừa số là $e + 1$), kèm giá trị n nhỏ nhất tương ứng: (48) và (24, 2) cho $n \geq 2^{23} > 2520$; (16, 3): $2^{15} \cdot 3^2 =$

294912; (12, 4): $2^{11} \cdot 3^3 = 55296$; (8, 6): $2^7 \cdot 3^5 = 31104$; (12, 2, 2): $2^{11} \cdot 3 \cdot 5 = 30720$; (8, 3, 2): $2^7 \cdot 3^2 \cdot 5 = 5760$; (6, 4, 2): $2^5 \cdot 3^3 \cdot 5 = 4320$; (4, 4, 3): $2^3 \cdot 3^3 \cdot 5^2 = 5400$; (6, 2, 2, 2): $2^5 \cdot 3 \cdot 5 \cdot 7 = 3360$; (4, 3, 2, 2): $2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$; (3, 2, 2, 2, 2): $2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 4620$.

The ways to write 48 as a non-increasing product of factors greater than 1 (each factor is $e + 1$), with the corresponding least n : (48) and (24, 2) give $n \geq 2^{23} > 2520$; (16, 3): $2^{15} \cdot 3^2 = 294,912$; (12, 4): $2^{11} \cdot 3^3 = 55,296$; (8, 6): $2^7 \cdot 3^5 = 31,104$; (12, 2, 2): $2^{11} \cdot 3 \cdot 5 = 30,720$; (8, 3, 2): $2^7 \cdot 3^2 \cdot 5 = 5,760$; (6, 4, 2): $2^5 \cdot 3^3 \cdot 5 = 4,320$; (4, 4, 3): $2^3 \cdot 3^3 \cdot 5^2 = 5,400$; (6, 2, 2, 2): $2^5 \cdot 3 \cdot 5 \cdot 7 = 3,360$; (4, 3, 2, 2): $2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2,520$; (3, 2, 2, 2, 2): $2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 4,620$.

3. Giá trị nhỏ nhất trong mười hai trường hợp là $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$, và $\tau(2520) = 4 \cdot 3 \cdot 2 \cdot 2 = 48$.

The least of the twelve values is $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$, and $\tau(2520) = 4 \cdot 3 \cdot 2 \cdot 2 = 48$.

Vậy số cần tìm là 2520.

Hence the required number is 2520. ■

NHẬN XÉT / REMARK — Các thừa số của 48 có thể trùng nhau, nên phải liệt kê cả những cách có thừa số lặp, ví dụ (12, 2, 2) và (4, 4, 3). Một cách kiểm tra đủ: $48 = 2^4 \cdot 3$ có 12 cách viết thành tích không tăng các thừa số lớn hơn 1, đúng bằng 12 trường hợp ở trên.

The factors of 48 may repeat, so partitions with repeated factors, such as (12, 2, 2) and (4, 4, 3), must be listed as well. A check on completeness: $48 = 2^4 \cdot 3$ has 12 ways to be written as a non-increasing product of factors greater than 1, matching the 12 cases above.

LỖI HAY GẶP / COMMON MISTAKE — Tính số ước bằng tổng thay vì tích, hoặc quên cộng 1 vào số mũ: $\tau(2^3 \cdot 3^2) = (3 + 1)(2 + 1) = 12$, không phải $3 + 2 = 5$ hay $3 \cdot 2 = 6$. Số ước luôn gồm cả 1 và n .

Computing the number of divisors by a sum instead of a product, or forgetting to add 1 to each exponent: $\tau(2^3 \cdot 3^2) = (3 + 1)(2 + 1) = 12$, not $3 + 2 = 5$ or $3 \cdot 2 = 6$. The divisors always include 1 and n .

6.7. Số chính phương và phép thử bằng số dư — Perfect squares and tests by remainders

TÍNH CHẤT 6.27 (Dư của bình phương) / PROPERTY 6.27 (Remainders of squares) — Ký hiệu $a \equiv b \pmod{m}$ nghĩa là $m \mid a - b$. Với mọi $n \in \mathbb{Z}$: $n^2 \equiv 0$ hoặc $1 \pmod{3}$; $n^2 \equiv 0$ hoặc $1 \pmod{4}$; $n^2 \equiv 0, 1$ hoặc $4 \pmod{5}$; $n^2 \equiv 0, 1$ hoặc $4 \pmod{8}$. Nếu n lẻ thì $n^2 \equiv 1 \pmod{8}$.

The notation $a \equiv b \pmod{m}$ means $m \mid a - b$. For every $n \in \mathbb{Z}$: $n^2 \equiv 0$ or $1 \pmod{3}$; $n^2 \equiv 0$ or $1 \pmod{4}$; $n^2 \equiv 0, 1$ or $4 \pmod{5}$; $n^2 \equiv 0, 1$ or $4 \pmod{8}$. If n is odd then $n^2 \equiv 1 \pmod{8}$.

Chứng minh. / Proof.

Với số chia m , viết $n = mk + r$ và $n^2 = m(mk^2 + 2kr) + r^2$, nên n^2 có cùng dư với r^2 . Chỉ cần xét r trong hệ dư đủ. Mod 3: $r \in \{0, \pm 1\}$, $r^2 \in \{0, 1\}$. Mod 4: $r \in \{0, \pm 1, 2\}$, $r^2 \in \{0, 1, 4\}$ và $4 \equiv 0$. Mod 5: $r \in \{0, \pm 1, \pm 2\}$, $r^2 \in \{0, 1, 4\}$. Mod 8: $r \in \{0, \pm 1, \pm 2, \pm 3, 4\}$, $r^2 \in \{0, 1, 4, 9, 16\}$ với $9 \equiv 1$ và $16 \equiv 0$. Số lẻ có $r \in \{\pm 1, \pm 3\}$, $r^2 \in \{1, 9\} \equiv 1$.

For divisor m , write $n = mk + r$, so $n^2 = m(mk^2 + 2kr) + r^2$ and n^2 has the same remainder as r^2 . It suffices to run r through a complete residue system. Mod 3: $r \in \{0, \pm 1\}$, $r^2 \in \{0, 1\}$. Mod 4: $r \in \{0, \pm 1, 2\}$, $r^2 \in \{0, 1, 4\}$ and $4 \equiv 0$. Mod 5: $r \in \{0, \pm 1, \pm 2\}$, $r^2 \in \{0, 1, 4\}$. Mod 8: $r \in \{0, \pm 1, \pm 2, \pm 3, 4\}$, $r^2 \in \{0, 1, 4, 9, 16\}$ with $9 \equiv 1$ and $16 \equiv 0$. Odd n has $r \in \{\pm 1, \pm 3\}$, $r^2 \in \{1, 9\} \equiv 1$.

$\pm 3, 4\}$, $r^2 \in \{0, 1, 4, 9, 16\}$ with $9 \equiv 1$ and $16 \equiv 0$. An odd number has $r \in \{\pm 1, \pm 3\}$, $r^2 \in \{1, 9\} \equiv 1$. ■

Modulo Modulus	Dư có thể có của n^2 Possible remainders of n^2	Số không thể là chính phương nếu dư là A number cannot be a square if its remainder is
3	0, 1	2
4	0, 1	2, 3
5	0, 1, 4	2, 3
8	0, 1, 4	2, 3, 5, 6, 7

BỔ ĐỀ 6.28 (Tích nguyên tố cùng nhau là chính phương) / LEMMA 6.28 (Coprime product that is a square) — Nếu $a, b \in \mathbb{Z}^+$, $\gcd(a, b) = 1$ và ab là số chính phương thì a và b đều là số chính phương.

If $a, b \in \mathbb{Z}^+$, $\gcd(a, b) = 1$ and ab is a perfect square, then a and b are both perfect squares.

Chứng minh. / Proof.

Với mỗi số nguyên tố p , $v_p(a) + v_p(b) = v_p(ab)$ chẵn. Vì $\gcd(a, b) = 1$ nên p không chia hết đồng thời cả hai, tức một trong hai số $v_p(a)$, $v_p(b)$ bằng 0; số còn lại phải chẵn. Mọi số mũ trong dạng chính tắc của a và b đều chẵn, nên a và b là số chính phương.

For each prime p , $v_p(a) + v_p(b) = v_p(ab)$ is even. Since $\gcd(a, b) = 1$, p cannot divide both, so one of $v_p(a)$, $v_p(b)$ is 0 and the other must be even. Every exponent in the canonical forms of a and b is even, so a and b are perfect squares. ■

NHẬN XÉT / REMARK — Cách kẹp: nếu $n^2 < m < (n+1)^2$ thì m không là số chính phương, vì không có số nguyên nào nằm giữa n và $n+1$. Với Ví dụ 6.12 có thể kẹp $n^2 + 20n$ giữa $(n+9)^2$ và $(n+10)^2$: $n^2 + 20n > (n+9)^2$ khi $n \geq 41$, nên chỉ còn phải thử $n \leq 40$. Ví dụ này được giải bằng phân tích nhân tử, nhanh hơn và không cần thử.

Squeezing: if $n^2 < m < (n+1)^2$ then m is not a perfect square, since no integer lies strictly between n and $n+1$. In Example 6.12 one can squeeze $n^2 + 20n$ between $(n+9)^2$ and $(n+10)^2$: $n^2 + 20n > (n+9)^2$ when $n \geq 41$, so only $n \leq 40$ remains to be tried. The example is solved by factorising instead, which is quicker and needs no trials.

VÍ DỤ 6.11 (Loại bằng dư mod 8) / EXAMPLE 6.11 (Elimination by remainders mod 8)

— Tìm tất cả cặp số nguyên tố (p, q) thỏa $p^2 - 2q^2 = 1$.

Find all pairs of primes (p, q) with $p^2 - 2q^2 = 1$.

Lời giải. / Solution.

1. Giả sử q lẻ. Theo Tính chất 6.27, $q^2 \equiv 1 \pmod{8}$, nên $p^2 = 2q^2 + 1 \equiv 3 \pmod{8}$.

Suppose q is odd. By Property 6.27, $q^2 \equiv 1 \pmod{8}$, so $p^2 = 2q^2 + 1 \equiv 3 \pmod{8}$.

2. Nhưng bình phương chỉ có dư 0, 1 hoặc 4 khi chia cho 8 (Tính chất 6.27). Mâu thuẫn, nên q chẵn, tức $q = 2$.

But squares leave remainder 0, 1 or 4 on division by 8 (Property 6.27). Contradiction, so q is even, that is $q = 2$.

3. Với $q = 2$: $p^2 = 9$ nên $p = 3$, nguyên tố.

For $q = 2$: $p^2 = 9$, so $p = 3$, which is prime.

Vậy $(p, q) = (3, 2)$.

Hence $(p, q) = (3, 2)$. ■

VÍ DỤ 6.12 (Hiệu hai bình phương bằng hằng số) / EXAMPLE 6.12 (Difference of two squares equal to a constant) — Tìm tất cả số nguyên dương n sao cho $n^2 + 20n$ là số chính phương.

Find all positive integers n such that $n^2 + 20n$ is a perfect square.

Lời giải. / Solution.

1. Giả sử $n^2 + 20n = m^2$ với $m \geq 0$. Khi đó $(n + 10)^2 - m^2 = 100$, tức $(n + 10 - m)(n + 10 + m) = 100$.

Suppose $n^2 + 20n = m^2$ with $m \geq 0$. Then $(n + 10)^2 - m^2 = 100$, that is $(n + 10 - m)(n + 10 + m) = 100$.

2. Đặt $u = n + 10 - m$, $v = n + 10 + m$. Khi đó $uv = 100$, $v \geq u$, $v > 0$ nên $u > 0$. Tổng $u + v = 2(n + 10)$ chẵn, nên u, v cùng tính chẵn lẻ; vì uv chẵn nên cả hai chẵn: $u = 2u'$, $v = 2v'$, $u'v' = 25$.

Put $u = n + 10 - m$, $v = n + 10 + m$. Then $uv = 100$, $v \geq u$, $v > 0$ so $u > 0$. The sum $u + v = 2(n + 10)$ is even, so u and v have the same parity; since uv is even, both are even: $u = 2u'$, $v = 2v'$, $u'v' = 25$.

3. Với $u' \leq v'$: $(u', v') \in \{(1, 25), (5, 5)\}$. Trường hợp $(1, 25)$: $u + v = 52$ nên $n + 10 = 26$, $n = 16$ và $m = (v - u)/2 = 24$. Trường hợp $(5, 5)$: $n + 10 = 10$, $n = 0$, loại.

With $u' \leq v'$: $(u', v') \in \{(1, 25), (5, 5)\}$. Case $(1, 25)$: $u + v = 52$ so $n + 10 = 26$, $n = 16$ and $m = (v - u)/2 = 24$. Case $(5, 5)$: $n + 10 = 10$, $n = 0$, rejected.

4. Kiểm tra: $16^2 + 20 \cdot 16 = 256 + 320 = 576 = 24^2$.

Check: $16^2 + 20 \cdot 16 = 256 + 320 = 576 = 24^2$.

Vậy $n = 16$.

Hence $n = 16$. ■

PHÂN TÍCH / ANALYSIS — Bình phương chia 3 chỉ dư 0 hoặc 1, nên $x^2 + y^2$ chia hết cho 3 chỉ khi cả x, y chia hết 3. Khi đó $9 \mid 3z^2$, suy ra $3 \mid z$, và nghiệm (x, y, z) sinh ra nghiệm $(x/3, y/3, z/3)$ nhỏ hơn. Chọn nghiệm nhỏ nhất rồi chỉ ra nghiệm nhỏ hơn thì mâu thuẫn: phép xuống thang vô hạn.

A square leaves remainder 0 or 1 on division by 3, so $x^2 + y^2$ is divisible by 3 only if both x and y are. Then $9 \mid 3z^2$, hence $3 \mid z$, and a solution (x, y, z) yields a smaller solution $(x/3, y/3, z/3)$. Choose a least solution and exhibit a smaller one for a contradiction: infinite descent.

VÍ DỤ 6.13 (Xuống thang vô hạn) / EXAMPLE 6.13 (Infinite descent) — Chứng minh rằng phương trình $x^2 + y^2 = 3z^2$ chỉ có nghiệm nguyên $(x, y, z) = (0, 0, 0)$.

Prove that the equation $x^2 + y^2 = 3z^2$ has no integer solution other than $(x, y, z) = (0, 0, 0)$.

Lời giải. / Solution.

- Giả sử có nghiệm khác $(0, 0, 0)$. Nếu $z = 0$ thì $x^2 + y^2 = 0$ nên $x = y = 0$; vậy $z \neq 0$.
Chọn nghiệm (x, y, z) với $|z|$ nhỏ nhất, $|z| \geq 1$.
Suppose there is a solution other than $(0, 0, 0)$. If $z = 0$ then $x^2 + y^2 = 0$, so $x = y = 0$; hence $z \neq 0$. Choose a solution (x, y, z) with $|z|$ least, $|z| \geq 1$.
- Có $3 \mid x^2 + y^2$. Theo Tính chất 6.27, x^2 và y^2 mỗi số có dư 0 hoặc 1 khi chia cho 3. Tổng hai dư là 0, 1 hoặc 2 và chỉ bằng 0 (chia hết cho 3) khi cả hai dư 0. Vậy $3 \mid x$ và $3 \mid y$.
We have $3 \mid x^2 + y^2$. By Property 6.27, each of x^2 and y^2 has remainder 0 or 1 modulo 3. The sum of the two remainders is 0, 1 or 2, and it is divisible by 3 only when both are 0. So $3 \mid x$ and $3 \mid y$.
- Viết $x = 3a$, $y = 3b$. Khi đó $9(a^2 + b^2) = 3z^2$, nên $z^2 = 3(a^2 + b^2)$. Vậy $3 \mid z^2$ và $3 \mid z$ theo Hệ quả 6.14; viết $z = 3c$ thì $9c^2 = 3(a^2 + b^2)$, tức $a^2 + b^2 = 3c^2$.
Write $x = 3a$, $y = 3b$. Then $9(a^2 + b^2) = 3z^2$, so $z^2 = 3(a^2 + b^2)$. Thus $3 \mid z^2$ and $3 \mid z$ by Corollary 6.14; writing $z = 3c$ gives $9c^2 = 3(a^2 + b^2)$, that is $a^2 + b^2 = 3c^2$.
- Cặp (a, b, c) là nghiệm với $|c| = |z|/3 < |z|$, mâu thuẫn với tính nhỏ nhất của $|z|$.
The triple (a, b, c) is a solution with $|c| = |z|/3 < |z|$, contradicting the minimality of $|z|$.

Vậy chỉ có nghiệm $(0, 0, 0)$.

Hence the only solution is $(0, 0, 0)$. ■

LỖI HAY GẶP / COMMON MISTAKE — Dùng dư làm điều kiện đủ. Số dư 0 hoặc 1 khi chia cho 4 chỉ là điều kiện cần của số chính phương: 5 chia 4 dư 1 mà không là số chính phương. Phép thử bằng dư chỉ loại được những số không phải chính phương.

Using remainders as a sufficient condition. Remainder 0 or 1 modulo 4 is only necessary for a perfect square: 5 leaves remainder 1 on division by 4 but is not a square. Remainder tests can only rule numbers out.

6.8. Hằng đẳng thức và tính chia hết của $a^n \pm b^n$ — Identities and divisibility of $a^n \pm b^n$

ĐỊNH LÝ 6.29 (Hiệu và tổng lũy thừa) / THEOREM 6.29 (Difference and sum of powers) — Với $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}^+$: $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$. Do đó $(a - b) \mid (a^n - b^n)$. Nếu n lẻ thì $a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \dots - ab^{n-2} + b^{n-1})$, nên $(a + b) \mid (a^n + b^n)$.

For $a, b \in \mathbb{Z}$, $n \in \mathbb{Z}^+$: $a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1})$. Hence $(a - b) \mid (a^n - b^n)$. If n is odd then $a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \dots - ab^{n-2} + b^{n-1})$, so $(a + b) \mid (a^n + b^n)$.

$$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \dots + ab^{n-2} + b^{n-1}) \quad (6.10)$$

Chứng minh. / Proof.

Nhân $(a - b)$ với tổng: các số hạng $a^{n-k}b^k$ và $a^{n-1-k}b^{k+1}$ triệt tiêu từng đôi liên tiếp, chỉ còn $a^n - b^n$. Với n lẻ, thay b bằng $-b$ trong (6.10) và dùng $(-b)^n = -b^n$: $a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \dots + b^{n-1})$.

Multiply $(a - b)$ by the sum: the terms $a^{n-k}b^k$ and $a^{n-1-k}b^{k+1}$ cancel in consecutive pairs, leaving $a^n - b^n$. For odd n , replace b by $-b$ in (6.10) and use $(-b)^n = -b^n$: $a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \dots + b^{n-1})$. ■

HỆ QUẢ 6.30 (Số Mersenne và số Fermat) / COROLLARY 6.30 (Mersenne and Fermat numbers) — Cho $a \geq 2$. (i) Nếu $m \mid n$ thì $(a^m - 1) \mid (a^n - 1)$. (ii) Nếu $n \geq 2$ và $a^n - 1$ nguyên tố thì $a = 2$ và n nguyên tố. (iii) Nếu $2^n + 1$ nguyên tố thì $n = 2^j$ với $j \in \mathbb{N}$.

Let $a \geq 2$. (i) If $m \mid n$ then $(a^m - 1) \mid (a^n - 1)$. (ii) If $n \geq 2$ and $a^n - 1$ is prime then $a = 2$ and n is prime. (iii) If $2^n + 1$ is prime then $n = 2^j$ with $j \in \mathbb{N}$.

Chứng minh. / Proof.

(i) Viết $n = mk$, $x = a^m$. Theo Định lý 6.29, $(x - 1) \mid (x^k - 1)$, tức $(a^m - 1) \mid (a^n - 1)$.

(i) Write $n = mk$, $x = a^m$. By Theorem 6.29, $(x - 1) \mid (x^k - 1)$, that is $(a^m - 1) \mid (a^n - 1)$.

(ii) $(a - 1) \mid (a^n - 1)$ và $1 \leq a - 1 < a^n - 1$ (vì $n \geq 2$). Nếu $a^n - 1$ nguyên tố thì $a - 1 = 1$, tức $a = 2$. Nếu $n = mk$ với $1 < m < n$ thì $1 < 2^m - 1 < 2^n - 1$ và $(2^m - 1) \mid (2^n - 1)$, nên $2^n - 1$ là hợp số. Vậy n nguyên tố.

(ii) $(a - 1) \mid (a^n - 1)$ and $1 \leq a - 1 < a^n - 1$ (as $n \geq 2$). If $a^n - 1$ is prime then $a - 1 = 1$, so $a = 2$. If $n = mk$ with $1 < m < n$ then $1 < 2^m - 1 < 2^n - 1$ and $(2^m - 1) \mid (2^n - 1)$, so $2^n - 1$ is composite. Hence n is prime.

(iii) Nếu n có ước lẻ $d > 1$, viết $n = dk$. Vì d lẻ, $(2^k + 1) \mid ((2^k)^d + 1) = 2^n + 1$ và $1 < 2^k + 1 < 2^n + 1$, nên $2^n + 1$ là hợp số. Vậy n không có ước lẻ lớn hơn 1, tức $n = 2^j$.

(iii) If n has an odd divisor $d > 1$, write $n = dk$. Since d is odd, $(2^k + 1) \mid ((2^k)^d + 1) = 2^n + 1$ and $1 < 2^k + 1 < 2^n + 1$, so $2^n + 1$ is composite. Hence n has no odd divisor greater than 1, that is $n = 2^j$. ■

TÍNH CHẤT 6.31 (Hằng đẳng thức Sophie Germain) / PROPERTY 6.31 (Sophie Germain identity) — Với mọi a, b : $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab) = ((a + b)^2 + b^2)((a - b)^2 + b^2)$.

For all a, b : $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab) = ((a + b)^2 + b^2)((a - b)^2 + b^2)$.

$$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab) \quad (6.11)$$

Chứng minh. / Proof.

Thêm bớt $4a^2b^2$: $a^4 + 4b^4 = (a^2 + 2b^2)^2 - 4a^2b^2 = (a^2 + 2b^2 - 2ab)(a^2 + 2b^2 + 2ab)$. Ngoài ra $a^2 + 2b^2 + 2ab = (a + b)^2 + b^2$ và $a^2 + 2b^2 - 2ab = (a - b)^2 + b^2$.

Add and subtract $4a^2b^2$: $a^4 + 4b^4 = (a^2 + 2b^2)^2 - 4a^2b^2 = (a^2 + 2b^2 - 2ab)(a^2 + 2b^2 + 2ab)$. Also $a^2 + 2b^2 + 2ab = (a + b)^2 + b^2$ and $a^2 + 2b^2 - 2ab = (a - b)^2 + b^2$. ■

PHÂN TÍCH / ANALYSIS — Biến n của $n^4 + 4^n$ xuất hiện ở cả cơ số lẫn số mũ, nên thử vài n nhỏ trước: $n = 1$ cho 5 nguyên tố, $n = 2$ cho 32. Khi n lẻ, $n = 2k + 1$, ta có $4^n = 4 \cdot (2^k)^4$, đúng dạng $a^4 + 4b^4$ với $b = 2^k$. Hằng đẳng thức (6.11) sẽ tách biểu thức thành hai thừa số.

The variable n in $n^4 + 4^n$ appears in both a base and an exponent, so try small n first: $n = 1$ gives the prime 5, $n = 2$ gives 32. For odd $n = 2k + 1$ we have $4^n = 4 \cdot (2^k)^4$, exactly the shape $a^4 + 4b^4$ with $b = 2^k$. Identity (6.11) splits the expression into two factors.

VÍ DỤ 6.14 (Hằng đẳng thức Sophie Germain) / EXAMPLE 6.14 (The Sophie Germain identity) — Tìm tất cả số nguyên dương n sao cho $n^4 + 4^n$ là số nguyên tố.
Find all positive integers n such that $n^4 + 4^n$ is prime.

Lời giải. / Solution.

1. Nếu n chẵn thì $n^4 + 4^n$ chẵn và lớn hơn 2, nên là hợp số.
If n is even then $n^4 + 4^n$ is even and greater than 2, hence composite.
2. Nếu $n = 2k + 1$ lẻ, đặt $b = 2^k$. Khi đó $4^n = 4 \cdot 4^{2k} = 4b^4$. Theo (6.11): $n^4 + 4b^4 = ((n + b)^2 + b^2)((n - b)^2 + b^2)$.
If $n = 2k + 1$ is odd, put $b = 2^k$. Then $4^n = 4 \cdot 4^{2k} = 4b^4$. By (6.11): $n^4 + 4b^4 = ((n + b)^2 + b^2)((n - b)^2 + b^2)$.
3. Cả hai thừa số là số nguyên dương và thừa số lớn hơn thừa số nhỏ. Nếu $k \geq 1$ thì $b \geq 2$ nên $(n - b)^2 + b^2 \geq 4 > 1$, và tích hai số lớn hơn 1 là hợp số.
Both factors are positive integers and the first is larger than the second. If $k \geq 1$ then $b \geq 2$, so $(n - b)^2 + b^2 \geq 4 > 1$, and a product of two integers greater than 1 is composite.
4. Còn $k = 0$, tức $n = 1$: $1^4 + 4^1 = 5$ là số nguyên tố.
Only $k = 0$ remains, that is $n = 1$: $1^4 + 4^1 = 5$ is prime.

Vậy $n = 1$.

Hence $n = 1$. ■

NHẬN XÉT / REMARK — Cùng kỹ thuật cho $n^4 + n^2 + 1 = (n^2 + n + 1)(n^2 - n + 1)$: với $n \geq 2$ cả hai thừa số lớn hơn 1 nên tích là hợp số, chỉ $n = 1$ cho số nguyên tố 3. Khi biểu thức dạng $a^4 + 4b^4$ bị ngụy trang bằng lũy thừa của 2, hãy viết $4^n = 4 \cdot (2^k)^4$ để nhận ra nó.
The same technique handles $n^4 + n^2 + 1 = (n^2 + n + 1)(n^2 - n + 1)$: for $n \geq 2$ both factors exceed 1, so the product is composite and only $n = 1$ gives the prime 3. When an expression of the form $a^4 + 4b^4$ is disguised by powers of 2, write $4^n = 4 \cdot (2^k)^4$ to recognise it.

PHẢI THUỘC / MEMORISE — $v_p(n!) = \sum [n/p^k]$; $\tau(n) = \prod (e(p) + 1)$; $\sigma(n) = \prod (p^{e(p)+1} - 1)/(p - 1)$; số hoàn hảo chẵn $= 2^{k-1}(2^k - 1)$ với $2^k - 1$ nguyên tố; $n^2 \equiv 0, 1 \pmod{3}$, $\pmod{4}$; $n^2 \equiv 0, 1, 4 \pmod{8}$; $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$.
 $v_p(n!) = \sum [n/p^k]$; $\tau(n) = \prod (e(p) + 1)$; $\sigma(n) = \prod (p^{e(p)+1} - 1)/(p - 1)$; even perfect numbers $= 2^{k-1}(2^k - 1)$ with $2^k - 1$ prime; $n^2 \equiv 0, 1 \pmod{3}$, $\pmod{4}$; $n^2 \equiv 0, 1, 4 \pmod{8}$; $a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$.

Bảng chiến lược — Strategy table

Dấu hiệu trong đề <i>Sign in the problem</i>	Công cụ nên thử <i>Tool to try</i>	Ví dụ <i>Example</i>
$(an + b)$ chia hết một đa thức theo n <i>$(an + b)$ divides a polynomial in n</i>	Chia đa thức, quy về ước của một hằng số <i>Polynomial division, reduce to divisors of a constant</i>	Ví dụ 6.1 <i>Example 6.1</i>

Dấu hiệu trong đề <i>Sign in the problem</i>	Công cụ nên thử <i>Tool to try</i>	Ví dụ <i>Example</i>
$ax + by = c$, đếm nghiệm nguyên dương <i>$ax + by = c$, count positive integer solutions</i>	Bézout, nghiệm tổng quát (6.5), khoảng của t <i>Bézout, general solution (6.5), interval for t</i>	Ví dụ 6.4 <i>Example 6.4</i>
ƯCLN của hai biểu thức cùng dạng, chứa số mũ m, n <i>gcd of two expressions of the same shape with exponents m, n</i>	Euclid trên số mũ, $a^m - b^m$ <i>Euclid on the exponents, $a^m - b^m$</i>	Ví dụ 6.3 <i>Example 6.3</i>
Tích hai nhân tử bằng hằng số, hiệu hai bình phương <i>Product of two factors equal to a constant, difference of squares</i>	Phân tích nhân tử, liệt kê cặp ước cùng tính chẵn lẻ <i>Factorise, list divisor pairs of equal parity</i>	Ví dụ 6.12 <i>Example 6.12</i>
Nhiều biểu thức cùng phải là số nguyên tố <i>Several expressions all required to be prime</i>	Xét dư khi chia cho 2, 3 <i>Remainders modulo 2 and 3</i>	Ví dụ 6.7 <i>Example 6.7</i>
$n!$, tích liên tiếp, số chữ số 0 tận cùng <i>$n!$, products of consecutive integers, trailing zeros</i>	Công thức Legendre, tổng chữ số cơ số p <i>Legendre's formula, base-p digit sum</i>	Ví dụ 6.8, 6.9 <i>Examples 6.8, 6.9</i>
Đếm ước, số có đúng k ước, tổng ước <i>Counting divisors, exactly k divisors, sum of divisors</i>	Dạng chính tắc, τ, σ , số mũ giảm dần <i>Canonical form, τ, σ, decreasing exponents</i>	Ví dụ 6.10 <i>Example 6.10</i>
Phương trình không có nghiệm, số chính phương <i>Equation with no solution, perfect squares</i>	Dư mod 3, 4, 8; xuống thang vô hạn <i>Remainders mod 3, 4, 8; infinite descent</i>	Ví dụ 6.11, 6.13 <i>Examples 6.11, 6.13</i>
$a^4 + 4b^4$, $a^n \pm b^n$, biểu thức có số mũ lẻ <i>$a^4 + 4b^4$, $a^n \pm b^n$, odd exponents</i>	Hằng đẳng thức, $(a - b) \mid a^n - b^n$ <i>Identities, $(a - b) \mid a^n - b^n$</i>	Ví dụ 6.14 <i>Example 6.14</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Chia hết	Divisibility	$a \mid b$ khi $b = ak$ với k nguyên <i>$a \mid b$ when $b = ak$ for an integer k</i>
Ước, bội	Divisor, multiple	a là ước của b , b là bội của a <i>a is a divisor of b, b is a multiple of a</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Phép chia có dư	Division with remainder	$a = bq + r, 0 \leq r < b$
Thương, số dư	Quotient, remainder	q và r trong phép chia có dư <i>q and r in the division with remainder</i>
Ước chung lớn nhất (ƯCLN)	Greatest common divisor (gcd)	Ước chung dương lớn nhất của hai số <i>Largest positive common divisor of two integers</i>
Bội chung nhỏ nhất (BCNN)	Least common multiple (lcm)	Bội chung dương nhỏ nhất của hai số <i>Smallest positive common multiple of two integers</i>
Nguyên tố cùng nhau	Coprime	ƯCLN bằng 1 <i>The gcd equals 1</i>
Thuật toán Euclid	Euclidean algorithm	Chia liên tiếp để tìm ƯCLN <i>Repeated division to find the gcd</i>
Đồng nhất thức Bézout	Bézout's identity	$ax + by = \gcd(a, b)$ có nghiệm nguyên <i>$ax + by = \gcd(a, b)$ has an integer solution</i>
Bổ đề Euclid	Euclid's lemma	$a \mid bc$ và $\gcd(a, b) = 1 \Rightarrow a \mid c$ <i>$a \mid bc$ and $\gcd(a, b) = 1 \Rightarrow a \mid c$</i>
Số nguyên tố	Prime number	Số nguyên lớn hơn 1 chỉ có ước 1 và chính nó <i>Integer greater than 1 whose only positive divisors are 1 and itself</i>
Hợp số	Composite number	Số nguyên lớn hơn 1 không nguyên tố <i>Integer greater than 1 that is not prime</i>
Định lý cơ bản của số học	Fundamental theorem of arithmetic	Phân tích ra nguyên tố tồn tại và duy nhất <i>Prime factorisation exists and is unique</i>
Dạng chính tắc	Canonical form	$n = \prod p^{e(p)}$
Số mũ p-adic	p-adic valuation	$v_p(n)$: số mũ lớn nhất của p chia hết n <i>$v_p(n)$: greatest exponent of p dividing n</i>
Công thức Legendre	Legendre's formula	$v_p(n!) = \sum \lfloor n/p^k \rfloor$
Hàm số ước τ	Divisor-count function τ	$\tau(n)$: số ước dương của n <i>$\tau(n)$: number of positive divisors of n</i>
Hàm tổng ước σ	Divisor-sum function σ	$\sigma(n)$: tổng các ước dương của n <i>$\sigma(n)$: sum of positive divisors of n</i>
Số hoàn hảo	Perfect number	$\sigma(n) = 2n$
Số Mersenne	Mersenne number	Số có dạng $2^k - 1$ <i>A number of the form $2^k - 1$</i>

Thuật ngữ <i>Term (Vietnamese)</i>	Tiếng Anh <i>English</i>	Giải thích ngắn <i>Short definition</i>
Số chính phương	Perfect square	Bình phương của một số nguyên <i>Square of an integer</i>
Xuống thang vô hạn	Infinite descent	Từ một nghiệm dựng nghiệm nhỏ hơn để suy ra mâu thuẫn <i>Building a smaller solution from a given one to reach a contradiction</i>
Nghiệm riêng, nghiệm tổng quát	Particular solution, general solution	Một nghiệm cụ thể; công thức cho mọi nghiệm <i>One specific solution; a formula for all solutions</i>
Hằng đẳng thức Sophie Germain	Sophie Germain identity	$a^4 + 4b^4 = (a^2 + 2b^2 + 2ab)(a^2 + 2b^2 - 2ab)$

6.9. Bài tự luyện — Practice problems

Mức 1 — Học sinh giỏi cấp tỉnh — Level 1 — Provincial olympiad

Bài 6.1 / Problem 6.1 — Tìm tất cả số nguyên dương n sao cho $3n + 1$ là ước của $n^2 + 10$.
Find all positive integers n such that $3n + 1$ divides $n^2 + 10$.

Bài 6.2 / Problem 6.2 — Tìm tất cả cặp số nguyên dương (a, b) sao cho $\text{lcm}(a, b) - \text{gcd}(a, b) = 2(a + b)$.
Find all pairs of positive integers (a, b) such that $\text{lcm}(a, b) - \text{gcd}(a, b) = 2(a + b)$.

Bài 6.3 / Problem 6.3 — Tìm số nguyên k lớn nhất sao cho 12^k chia hết $100!$.
Find the largest integer k such that 12^k divides $100!$.

Bài 6.4 / Problem 6.4 — Tính số ước dương của $10!$, số ước dương của $10!$ là số chính phương, và số ước dương lẻ của $10!$.
Find the number of positive divisors of $10!$, the number of those that are perfect squares, and the number of odd positive divisors of $10!$.

Mức 2 — Học sinh giỏi quốc gia — Level 2 — National olympiad

Bài 6.5 / Problem 6.5 — Chứng minh rằng với mọi $n \in \mathbb{Z}^+$, $\text{gcd}(n! + 1, (n + 1)! + 1) = 1$.
Prove that for every $n \in \mathbb{Z}^+$, $\text{gcd}(n! + 1, (n + 1)! + 1) = 1$.

Bài 6.6 / Problem 6.6 — Chứng minh rằng 65 là số nguyên dương lớn nhất không viết được dưới dạng $7x + 12y$ với x, y là các số nguyên không âm.
Prove that 65 is the largest positive integer that cannot be written as $7x + 12y$ with x, y non-negative integers.

Bài 6.7 / Problem 6.7 — Chứng minh rằng mọi số hoàn hảo chẵn có chữ số tận cùng là 6 hoặc 8.
Prove that every even perfect number ends in the digit 6 or 8.

Bài 6.8 / Problem 6.8 — Với mỗi $n \in \mathbb{Z}^+$, gọi $z(n)$ là số chữ số 0 tận cùng của $n!$. Có bao nhiêu số nguyên dương $k \leq 1000$ không bằng $z(n)$ với bất kỳ n nào?

For $n \in \mathbb{Z}^+$ let $z(n)$ be the number of trailing zeros of $n!$. How many positive integers $k \leq 1000$ are not equal to $z(n)$ for any n ?

Mức 3 — Olympic quốc tế — Level 3 — International olympiad

Bài 6.9 / Problem 6.9 — Với $n \in \mathbb{Z}^+$, chứng minh $\sum \tau(d)^3 = (\sum \tau(d))^2$, trong đó cả hai tổng chạy trên mọi ước dương d của n .

For $n \in \mathbb{Z}^+$ prove that $\sum \tau(d)^3 = (\sum \tau(d))^2$, where both sums run over all positive divisors d of n .

Bài 6.10 / Problem 6.10 — Chứng minh rằng với mọi $n \in \mathbb{Z}^+$, số $1/(n+1) + 1/(n+2) + \dots + 1/(2n)$ không là số nguyên.

Prove that for every $n \in \mathbb{Z}^+$ the number $1/(n+1) + 1/(n+2) + \dots + 1/(2n)$ is not an integer.

Bài 6.11 / Problem 6.11 — Chứng minh rằng với mọi $m, n \in \mathbb{Z}^+$: $\gcd(3^m - 2^m, 3^n - 2^n) = 3^{\gcd(m, n)} - 2^{\gcd(m, n)}$.

Prove that for all $m, n \in \mathbb{Z}^+$: $\gcd(3^m - 2^m, 3^n - 2^n) = 3^{\gcd(m, n)} - 2^{\gcd(m, n)}$.

Bài 6.12 / Problem 6.12 — Cho $a, b \in \mathbb{Z}^+$ nguyên tố cùng nhau và $n \in \mathbb{N}$. Chứng minh số cặp $(x, y) \in \mathbb{N} \times \mathbb{N}$ thỏa $ax + by = n$ bằng $\lfloor n/(ab) \rfloor$ hoặc $\lfloor n/(ab) \rfloor + 1$.

Let $a, b \in \mathbb{Z}^+$ be coprime and $n \in \mathbb{N}$. Prove that the number of pairs $(x, y) \in \mathbb{N} \times \mathbb{N}$ with $ax + by = n$ equals $\lfloor n/(ab) \rfloor$ or $\lfloor n/(ab) \rfloor + 1$.

6.10. Lời giải bài tự luyện — Solutions to practice problems

Bài 6.1 — Problem 6.1

1. Nếu $(3n+1) \mid (n^2+10)$ thì $(3n+1) \mid 9(n^2+10)$. Ta có:

If $(3n+1) \mid (n^2+10)$ then $(3n+1) \mid 9(n^2+10)$. We have:

$$9(n^2+10) = (3n+1)(3n-1) + 91$$

2. Suy ra $(3n+1) \mid 91 = 7 \cdot 13$. Ước dương của 91 là 1, 7, 13, 91; vì $3n+1 \geq 4$ nên $3n+1 \in \{7, 13, 91\}$, tức $n \in \{2, 4, 30\}$.

Hence $(3n+1) \mid 91 = 7 \cdot 13$. The positive divisors of 91 are 1, 7, 13, 91; since $3n+1 \geq 4$ we get $3n+1 \in \{7, 13, 91\}$, that is $n \in \{2, 4, 30\}$.

3. Ngược lại, nếu $(3n+1) \mid 91$ thì $(3n+1) \mid 9(n^2+10)$. Vì $3n+1$ chia 3 dư 1 nên $\gcd(3n+1, 9) = 1$, và $(3n+1) \mid (n^2+10)$ theo Bổ đề 6.9. Kiểm tra: $2^2+10=14=2 \cdot 7$; $4^2+10=26=2 \cdot 13$; $30^2+10=910=10 \cdot 91$.

Conversely, if $(3n+1) \mid 91$ then $(3n+1) \mid 9(n^2+10)$. Since $3n+1$ leaves remainder 1 modulo 3, $\gcd(3n+1, 9) = 1$, and $(3n+1) \mid (n^2+10)$ by Lemma 6.9. Check: $2^2+10=14=2 \cdot 7$; $4^2+10=26=2 \cdot 13$; $30^2+10=910=10 \cdot 91$.

Vậy $n \in \{2, 4, 30\}$.

Hence $n \in \{2, 4, 30\}$. ■

Bài 6.2 — Problem 6.2

1. Đặt $g = \gcd(a, b)$, $a = gx$, $b = gy$ với $\gcd(x, y) = 1$. Theo Định lý 6.11, $\text{lcm}(a, b) = ab/g = gxy$.

Put $g = \gcd(a, b)$, $a = gx$, $b = gy$ with $\gcd(x, y) = 1$. By Theorem 6.11, $\text{lcm}(a, b) = ab/g = gxy$.

2. Phương trình trở thành $g(xy - 1) = 2g(x + y)$, tức $xy - 1 = 2x + 2y$, hay:

The equation becomes $g(xy - 1) = 2g(x + y)$, that is $xy - 1 = 2x + 2y$, or:

$$(x - 2)(y - 2) = 5$$

3. Vì $5 = 1 \cdot 5 = 5 \cdot 1 = (-1)(-5) = (-5)(-1)$: $(x - 2, y - 2) = (1, 5)$ hoặc $(5, 1)$ cho $(x, y) = (3, 7)$ hoặc $(7, 3)$; $(-1, -5)$ cho $(1, -3)$ và $(-5, -1)$ cho $(-3, 1)$ đều có số âm, loại.

Since $5 = 1 \cdot 5 = 5 \cdot 1 = (-1)(-5) = (-5)(-1)$: $(x - 2, y - 2) = (1, 5)$ or $(5, 1)$ gives $(x, y) = (3, 7)$ or $(7, 3)$; $(-1, -5)$ gives $(1, -3)$ and $(-5, -1)$ gives $(-3, 1)$, both containing a negative number, rejected.

4. Các cặp $(3, 7)$ và $(7, 3)$ nguyên tố cùng nhau, nên hợp lệ với mọi $g \in \mathbb{Z}^+$. Kiểm tra: $(a, b) = (6, 14)$ có $\text{lcm} = 42$, $\gcd = 2$ và $42 - 2 = 40 = 2 \cdot 20$.

The pairs $(3, 7)$ and $(7, 3)$ are coprime, so they are valid for every $g \in \mathbb{Z}^+$. Check: $(a, b) = (6, 14)$ has $\text{lcm} = 42$, $\gcd = 2$ and $42 - 2 = 40 = 2 \cdot 20$.

Vậy $(a, b) = (3g, 7g)$ hoặc $(7g, 3g)$ với $g \in \mathbb{Z}^+$ bất kỳ.

Hence $(a, b) = (3g, 7g)$ or $(7g, 3g)$ with $g \in \mathbb{Z}^+$ arbitrary. ■

Bài 6.3 — Problem 6.3

1. $12 = 2^2 \cdot 3$ nên $12^k \mid 100!$ khi và chỉ khi $2k \leq v_2(100!)$ và $k \leq v_3(100!)$.

Since $12 = 2^2 \cdot 3$, $12^k \mid 100!$ if and only if $2k \leq v_2(100!)$ and $k \leq v_3(100!)$.

$$v_2(100!) = 50 + 25 + 12 + 6 + 3 + 1 = 97$$

$$v_3(100!) = 33 + 11 + 3 + 1 = 48$$

2. Điều kiện thứ nhất cho $k \leq \lfloor 97/2 \rfloor = 48$, điều kiện thứ hai cho $k \leq 48$. Vậy k lớn nhất là 48.

The first condition gives $k \leq \lfloor 97/2 \rfloor = 48$, the second gives $k \leq 48$. So the largest k is 48.

Vậy $k = 48$.

Hence $k = 48$. ■

Bài 6.4 — Problem 6.4

1. Theo Định lý 6.21: $v_2(10!) = 5 + 2 + 1 = 8$, $v_3(10!) = 3 + 1 = 4$, $v_5(10!) = 2$, $v_7(10!) = 1$. Vậy $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$.

By Theorem 6.21: $v_2(10!) = 5 + 2 + 1 = 8$, $v_3(10!) = 3 + 1 = 4$, $v_5(10!) = 2$, $v_7(10!) = 1$. So $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$.

2. Theo (6.8): $\tau(10!) = 9 \cdot 5 \cdot 3 \cdot 2 = 270$.

By (6.8): $\tau(10!) = 9 \cdot 5 \cdot 3 \cdot 2 = 270$.

3. Một ước $d = 2^{b_2} \cdot 3^{b_3} \cdot 5^{b_5} \cdot 7^{b_7}$ là số chính phương khi mọi số mũ chẵn. Số mũ của 2 chọn trong $\{0, 2, 4, 6, 8\}$ (5 cách), của 3 trong $\{0, 2, 4\}$ (3 cách), của 5 trong $\{0, 2\}$ (2 cách), của 7 chỉ là 0 (1 cách): $5 \cdot 3 \cdot 2 \cdot 1 = 30$.

A divisor $d = 2^{b_2} \cdot 3^{b_3} \cdot 5^{b_5} \cdot 7^{b_7}$ is a perfect square when all exponents are even. The exponent of 2 is chosen from $\{0, 2, 4, 6, 8\}$ (5 ways), of 3 from $\{0, 2, 4\}$ (3 ways), of 5 from $\{0, 2\}$ (2 ways), of 7 only 0 (1 way): $5 \cdot 3 \cdot 2 \cdot 1 = 30$.

4. Ước lẻ là ước có số mũ của 2 bằng 0, còn lại 3, 5, 7 tự do: $5 \cdot 3 \cdot 2 = 30$.

An odd divisor has exponent 0 for the prime 2, with the exponents of 3, 5, 7 free: $5 \cdot 3 \cdot 2 = 30$.

Vậy 270 ước, trong đó 30 ước chính phương và 30 ước lẻ.

Hence there are 270 divisors, of which 30 are perfect squares and 30 are odd. ■

Bài 6.5 — Problem 6.5

1. Đặt $e = \gcd(n! + 1, (n + 1)! + 1)$. Vì $e \mid n! + 1$ nên $e \mid (n + 1)(n! + 1) = (n + 1)! + n + 1$.

Put $e = \gcd(n! + 1, (n + 1)! + 1)$. Since $e \mid n! + 1$ we have $e \mid (n + 1)(n! + 1) = (n + 1)! + n + 1$.

2. Trừ đi $(n + 1)! + 1$, vôn chia hết cho e : $e \mid (n + 1)! + n + 1 - ((n + 1)! + 1) = n$.

Subtracting $(n + 1)! + 1$, which e divides: $e \mid (n + 1)! + n + 1 - ((n + 1)! + 1) = n$.

3. Vì $n \mid n!$ nên $e \mid n!$. Kết hợp $e \mid n! + 1$, ta có $e \mid (n! + 1) - n! = 1$, tức $e = 1$.

Since $n \mid n!$ we get $e \mid n!$. Together with $e \mid n! + 1$ this gives $e \mid (n! + 1) - n! = 1$, that is $e = 1$.

Vậy $\gcd(n! + 1, (n + 1)! + 1) = 1$.

Hence $\gcd(n! + 1, (n + 1)! + 1) = 1$. ■

Bài 6.6 — Problem 6.6

1. 65 không biểu diễn được. Ta có $7 \cdot (-1) + 12 \cdot 6 = 65$ nên theo (6.5) mọi nghiệm nguyên của $7x + 12y = 65$ là $x = -1 + 12t$, $y = 6 - 7t$. Để $x \geq 0$ cần $t \geq 1$, khi đó $y = 6 - 7t \leq -1 < 0$. Vậy không có nghiệm không âm.

65 is not representable. Since $7 \cdot (-1) + 12 \cdot 6 = 65$, by (6.5) every integer solution of $7x + 12y = 65$ is $x = -1 + 12t$, $y = 6 - 7t$. For $x \geq 0$ we need $t \geq 1$, and then $y = 6 - 7t \leq -1 < 0$. So there is no non-negative solution.

2. Mọi $n \geq 66$ đều biểu diễn được. Các số $12 \cdot 0, 12 \cdot 1, \dots, 12 \cdot 6$ có dư đôi một khác nhau khi chia cho 7: nếu $12y \equiv 12y' \pmod{7}$ thì $7 \mid 12(y - y')$ nên $7 \mid y - y'$ theo Bổ đề 6.9, với $|y - y'| \leq 6$ suy ra $y = y'$. Bảy dư khác nhau phải là cả bảy dư $0, 1, \dots, 6$, nên tồn tại $y \in \{0, 1, \dots, 6\}$ với $12y \equiv n \pmod{7}$.

Every $n \geq 66$ is representable. The numbers $12 \cdot 0, 12 \cdot 1, \dots, 12 \cdot 6$ have pairwise different remainders modulo 7: if $12y \equiv 12y' \pmod{7}$ then $7 \mid 12(y - y')$ so $7 \mid y - y'$ by Lemma 6.9, and $|y - y'| \leq 6$ forces $y = y'$. Seven different remainders must be all of $0, 1, \dots, 6$, so there is $y \in \{0, 1, \dots, 6\}$ with $12y \equiv n \pmod{7}$.

3. Với y đó, $n - 12y$ chia hết cho 7 và $n - 12y \geq 66 - 72 = -6 > -7$. Bội của 7 lớn hơn -7 thì không âm, nên $x = (n - 12y)/7$ là số nguyên không âm và $n = 7x + 12y$.

For that y , $n - 12y$ is divisible by 7 and $n - 12y \geq 66 - 72 = -6 > -7$. A multiple of 7 greater than -7 is non-negative, so $x = (n - 12y)/7$ is a non-negative integer and $n = 7x + 12y$.

Vậy số lớn nhất không biểu diễn được là 65.

Hence the largest non-representable integer is 65. ■

Bài 6.7 — Problem 6.7

1. Theo Định lý 6.26, $n = 2^{k-1}(2^k - 1)$ với $2^k - 1$ nguyên tố. Theo Hệ quả 6.30(ii), nếu $k \geq 2$ thì k nguyên tố ($k \geq 2$ vì $2^k - 1 > 1$). Do đó $k = 2$ hoặc k lẻ.

By Theorem 6.26, $n = 2^{k-1}(2^k - 1)$ with $2^k - 1$ prime. By Corollary 6.30(ii), k is prime ($k \geq 2$ since $2^k - 1 > 1$). So $k = 2$ or k is odd.

2. $k = 2$: $n = 6$. $k = 3$: $n = 28$. Còn lại $k \geq 5$ lẻ, $k = 4m + 1$ hoặc $4m + 3$ với $m \geq 1$. Vì $16 \equiv 6 \pmod{10}$ và $6 \cdot 6 = 36 \equiv 6 \pmod{10}$ nên $16^m \equiv 6 \pmod{10}$.

$k = 2$: $n = 6$. $k = 3$: $n = 28$. Otherwise $k \geq 5$ is odd, $k = 4m + 1$ or $4m + 3$ with $m \geq 1$. Since $16 \equiv 6 \pmod{10}$ and $6 \cdot 6 = 36 \equiv 6 \pmod{10}$, we have $16^m \equiv 6 \pmod{10}$.

3. $k = 4m + 1$: $2^{k-1} = 16^m \equiv 6$ và $2^k - 1 = 2 \cdot 16^m - 1 \equiv 12 - 1 \equiv 1 \pmod{10}$, nên $n \equiv 6 \cdot 1 = 6 \pmod{10}$.

$k = 4m + 1$: $2^{k-1} = 16^m \equiv 6$ and $2^k - 1 = 2 \cdot 16^m - 1 \equiv 12 - 1 \equiv 1 \pmod{10}$, so $n \equiv 6 \cdot 1 = 6 \pmod{10}$.

4. $k = 4m + 3$: $2^{k-1} = 4 \cdot 16^m \equiv 4$ và $2^k - 1 = 8 \cdot 16^m - 1 \equiv 48 - 1 \equiv 7 \pmod{10}$, nên $n \equiv 4 \cdot 7 = 28 \equiv 8 \pmod{10}$.

$k = 4m + 3$: $2^{k-1} = 4 \cdot 16^m \equiv 4$ and $2^k - 1 = 8 \cdot 16^m - 1 \equiv 48 - 1 \equiv 7 \pmod{10}$, so $n \equiv 4 \cdot 7 = 28 \equiv 8 \pmod{10}$.

Vậy chữ số tận cùng của mọi số hoàn hảo chẵn là 6 hoặc 8.

Hence the last digit of every even perfect number is 6 or 8. ■

Bài 6.8 — Problem 6.8

1. Như Ví dụ 6.8, $z(n) = v_5(n!)$, không giảm theo n . Khi n tăng từ $5m - 1$ lên $5m$, z tăng thêm $v_5(5m) \geq 1$; khi n không chia hết cho 5, $z(n) = z(n - 1)$. Vậy mọi giá trị của $z(n)$ với $n \geq 5$ là $z(5m)$, $m \geq 1$.

As in Example 6.8, $z(n) = v_5(n!)$, which is non-decreasing in n . When n increases from $5m - 1$ to $5m$, z grows by $v_5(5m) \geq 1$; when $5 \nmid n$, $z(n) = z(n - 1)$. So every value of $z(n)$ with $n \geq 5$ is $z(5m)$ for some $m \geq 1$.

2. Dãy $z(5)$, $z(10)$, $z(15)$, ... tăng ngặt. Theo (6.6), $z(4005) = 801 + 160 + 32 + 6 + 1 = 1000$ và $z(4010) = 802 + 160 + 32 + 6 + 1 = 1001$. Vậy các giá trị $z(5m)$ thuộc $[1, 1000]$ ứng với $m = 1, 2, \dots, 801$: đúng 801 giá trị phân biệt.

The sequence $z(5), z(10), z(15), \dots$ is strictly increasing. By (6.6), $z(4005) = 801 + 160 + 32 + 6 + 1 = 1000$ and $z(4010) = 802 + 160 + 32 + 6 + 1 = 1001$. So the values $z(5m)$ lying in $[1, 1000]$ correspond to $m = 1, 2, \dots, 801$: exactly 801 distinct values.

3. Số nguyên dương $k \leq 1000$ không đạt được là $1000 - 801 = 199$.

The number of positive integers $k \leq 1000$ that are not attained is $1000 - 801 = 199$.

Vậy có 199 số.

Hence there are 199 such numbers. ■

Bài 6.9 — Problem 6.9

1. Bổ trợ: $\sum_{j=1}^m j^3 = (m(m+1)/2)^2$. Quy nạp: $m = 1$ đúng; nếu đúng với m thì $(m(m+1)/2)^2 + (m+1)^3 = (m+1)^2(m^2/4 + m + 1) = ((m+1)(m+2)/2)^2$.

Lemma: $\sum_{j=1}^m j^3 = (m(m+1)/2)^2$. Induction: $m = 1$ holds; if it holds for m then $(m(m+1)/2)^2 + (m+1)^3 = (m+1)^2(m^2/4 + m + 1) = ((m+1)(m+2)/2)^2$.

2. Với $n = 1$ cả hai vế bằng 1. Với $n > 1$ viết $n = \prod p^{e(p)}$. Mỗi ước dương d của n là $d = \prod p^{b(p)}$ với $0 \leq b(p) \leq e(p)$, các bộ $(b(p))$ khác nhau cho ước khác nhau, và $\tau(d) = \prod$

$(b(p) + 1)$ theo (6.8).

For $n = 1$ both sides equal 1. For $n > 1$ write $n = \prod p^{e(p)}$. Every positive divisor d of n is $d = \prod p^{b(p)}$ with $0 \leq b(p) \leq e(p)$, different tuples $(b(p))$ give different divisors, and $\tau(d) = \prod (b(p) + 1)$ by (6.8).

3. Phân phối tích qua tổng: $\sum_d \tau(d)^r = \sum_{(b(p))} \prod (b(p) + 1)^r = \prod_p \sum_{b=0}^{e(p)} (b + 1)^r$, với $r = 1$ và $r = 3$.

Distributing the product over the sum: $\sum_d \tau(d)^r = \sum_{(b(p))} \prod (b(p) + 1)^r = \prod_p \sum_{b=0}^{e(p)} (b + 1)^r$, for $r = 1$ and $r = 3$.

4. Theo bổ trợ với $m = e(p) + 1$: $\sum_{b=0}^{e(p)} (b + 1)^3 = (\sum_{b=0}^{e(p)} (b + 1))^2$. Lấy tích theo p :
By the lemma with $m = e(p) + 1$: $\sum_{b=0}^{e(p)} (b + 1)^3 = (\sum_{b=0}^{e(p)} (b + 1))^2$. Taking the product over p :

$$\sum_{d|n} \tau(d)^3 = \prod_p (\sum_{b=0}^{e(p)} (b + 1))^2 = (\prod_p \sum_{b=0}^{e(p)} (b + 1))^2 = (\sum_{d|n} \tau(d))^2$$

Vậy $\sum \tau(d)^3 = (\sum \tau(d))^2$.

Hence $\sum \tau(d)^3 = (\sum \tau(d))^2$. ■

Bài 6.10 — Problem 6.10

1. Gọi a là số nguyên thỏa $2^a \leq 2n < 2^{a+1}$; $a \geq 1$. Trong khoảng $n < k \leq 2n$ chỉ có đúng một số chia hết cho 2^a , đó là 2^a : thật vậy $2^{a+1} > 2n$ nên $2^a > n$, $2^a \leq 2n$, và mọi bội khác của 2^a là $\geq 2^{a+1} > 2n$.

Let a be the integer with $2^a \leq 2n < 2^{a+1}$; then $a \geq 1$. In the range $n < k \leq 2n$ exactly one number is divisible by 2^a , namely 2^a : indeed $2^{a+1} > 2n$ gives $2^a > n$, also $2^a \leq 2n$, and every other multiple of 2^a is $\geq 2^{a+1} > 2n$.

2. Với mỗi k khác trong khoảng đó, viết $k = 2^f w$ với w lẻ; khi đó $f \leq a - 1$. Đặt W là tích các phần lẻ w đó (W lẻ, $W = 1$ nếu không có k nào khác). Khi đó $2^{a-1}W$ chia hết cho mọi $k \neq 2^a$ trong khoảng.

For each other k in the range write $k = 2^f w$ with w odd; then $f \leq a - 1$. Let W be the product of these odd parts w (W is odd, $W = 1$ if there are no other k). Then $2^{a-1}W$ is divisible by every $k \neq 2^a$ in the range.

3. Gọi S là tổng. Khi đó $2^{a-1}W \cdot S = 2^{a-1}W/2^a + (\text{tổng các số nguyên}) = W/2 + (\text{số nguyên})$. Vì W lẻ, $W/2$ không nguyên, nên $2^{a-1}W \cdot S$ không nguyên.

Let S be the sum. Then $2^{a-1}W \cdot S = 2^{a-1}W/2^a + (\text{a sum of integers}) = W/2 + (\text{an integer})$. Since W is odd, $W/2$ is not an integer, so $2^{a-1}W \cdot S$ is not an integer.

4. Nếu S là số nguyên thì $2^{a-1}W \cdot S$ là số nguyên ($a \geq 1$), mâu thuẫn.

If S were an integer then $2^{a-1}W \cdot S$ would be an integer ($a \geq 1$), a contradiction.

Vậy tổng đã cho không là số nguyên với mọi $n \geq 1$.

Hence the given sum is not an integer for any $n \geq 1$. ■

Bài 6.11 — Problem 6.11

1. Đặt $A_k = 3^k - 2^k$, quy ước $A_0 = 0$. Với $k \geq 1$, A_k là số lẻ (lẻ trừ chẵn). Giả sử $m \geq n$ và chia $m = qn + r$, $0 \leq r < n$.

Put $A_k = 3^k - 2^k$, with $A_0 = 0$. For $k \geq 1$, A_k is odd (odd minus even). Assume $m \geq n$ and divide $m = qn + r$, $0 \leq r < n$.

2. Ta có đẳng thức:

We have the identity:

$$A_m = 3^r(3^{qn} - 2^{qn}) + 2^{qn}(3^r - 2^r) = 3^r(3^{qn} - 2^{qn}) + 2^{qn}A_r$$

3. Theo Định lý 6.29 với $a = 3^n$, $b = 2^n$: $A_n \mid 3^{qn} - 2^{qn}$. Vậy $A_m = A_n \cdot K + 2^{qn}A_r$ với K nguyên.

By Theorem 6.29 with $a = 3^n$, $b = 2^n$: $A_n \mid 3^{qn} - 2^{qn}$. So $A_m = A_n \cdot K + 2^{qn}A_r$ with K an integer.

4. Gọi e là ước chung của A_m và A_n . Khi đó $e \mid 2^{qn}A_r$. Vì $e \mid A_n$ lẻ nên e lẻ, $\gcd(e, 2^{qn}) = 1$, và $e \mid A_r$ theo Bổ đề 6.9. Ngược lại mọi ước chung của A_n và A_r chia hết A_m . Vậy $\gcd(A_m, A_n) = \gcd(A_n, A_r)$ (với $\gcd(A_n, A_0) = A_n$).

Let e be a common divisor of A_m and A_n . Then $e \mid 2^{qn}A_r$. Since $e \mid A_n$, which is odd, e is odd, $\gcd(e, 2^{qn}) = 1$, and $e \mid A_r$ by Lemma 6.9. Conversely every common divisor of A_n and A_r divides A_m . So $\gcd(A_m, A_n) = \gcd(A_n, A_r)$ (with $\gcd(A_n, A_0) = A_n$).

5. Quy nạp mạnh theo n , với phát biểu $\gcd(A_m, A_n) = A_{\gcd(m, n)}$ cho mọi $m \geq n$. Nếu $r = 0$ thì $n \mid m$ và $\gcd(A_m, A_n) = A_n = A_{\gcd(m, n)}$. Nếu $r > 0$ thì $\gcd(A_m, A_n) = \gcd(A_n, A_r) = A_{\gcd(n, r)}$ theo giả thiết quy nạp ($r < n$), và $\gcd(n, r) = \gcd(m, n)$ theo Bổ đề 6.5. Trường hợp $m < n$ suy ra do tính đối xứng.

Strong induction on n , with the statement $\gcd(A_m, A_n) = A_{\gcd(m, n)}$ for all $m \geq n$. If $r = 0$ then $n \mid m$ and $\gcd(A_m, A_n) = A_n = A_{\gcd(m, n)}$. If $r > 0$ then $\gcd(A_m, A_n) = \gcd(A_n, A_r) = A_{\gcd(n, r)}$ by the induction hypothesis ($r < n$), and $\gcd(n, r) = \gcd(m, n)$ by Lemma 6.5. The case $m < n$ follows by symmetry.

Vậy $\gcd(3^m - 2^m, 3^n - 2^n) = 3^{\gcd(m, n)} - 2^{\gcd(m, n)}$.

Hence $\gcd(3^m - 2^m, 3^n - 2^n) = 3^{\gcd(m, n)} - 2^{\gcd(m, n)}$. ■

Bài 6.12 — Problem 6.12

1. Vì $\gcd(a, b) = 1$, phương trình $ax + by = n$ có nghiệm nguyên (x_0, y_0) theo Định lý 6.12, và theo (6.5) mọi nghiệm nguyên là $x = x_0 + bt$, $y = y_0 - at$, $t \in \mathbb{Z}$.

Since $\gcd(a, b) = 1$, the equation $ax + by = n$ has an integer solution (x_0, y_0) by Theorem 6.12, and by (6.5) every integer solution is $x = x_0 + bt$, $y = y_0 - at$, $t \in \mathbb{Z}$.

2. Điều kiện $x \geq 0$, $y \geq 0$ tương đương $-x_0/b \leq t \leq y_0/a$. Khoảng này có độ dài:

The conditions $x \geq 0$, $y \geq 0$ are equivalent to $-x_0/b \leq t \leq y_0/a$. This interval has length:

$$L = y_0/a + x_0/b = (ax_0 + by_0)/(ab) = n/(ab)$$

3. Đặt $\alpha = -x_0/b$, $t_0 = \lceil \alpha \rceil$ và $\delta = t_0 - \alpha$, $0 \leq \delta < 1$. Các số nguyên trong $[\alpha, \alpha + L]$ là $t_0, t_0 + 1, \dots, t_0 + j$ với j lớn nhất thỏa $t_0 + j \leq \alpha + L$, tức $j = \lfloor L - \delta \rfloor$. Số nghiệm là $\lfloor L - \delta \rfloor + 1$ (bằng 0 nếu $\lfloor L - \delta \rfloor = -1$).

Put $\alpha = -x_0/b$, $t_0 = \lceil \alpha \rceil$ and $\delta = t_0 - \alpha$, $0 \leq \delta < 1$. The integers in $[\alpha, \alpha + L]$ are $t_0, t_0 + 1, \dots, t_0 + j$ with j largest such that $t_0 + j \leq \alpha + L$, that is $j = \lfloor L - \delta \rfloor$. The number of solutions is $\lfloor L - \delta \rfloor + 1$ (it is 0 if $\lfloor L - \delta \rfloor = -1$).

4. Gọi $k = \lfloor L \rfloor$, $L = k + \theta$ với $0 \leq \theta < 1$. Vì $L - 1 < L - \delta \leq L$ nên $k - 1 \leq \lfloor L - \delta \rfloor \leq k$ ($L - \delta > L - 1 \geq k - 1$ và $L - \delta \leq L < k + 1$). Do đó số nghiệm là k hoặc $k + 1$.

Let $k = \lfloor L \rfloor$, $L = k + \theta$ with $0 \leq \theta < 1$. Since $L - 1 < L - \delta \leq L$ we get $k - 1 \leq \lfloor L - \delta \rfloor \leq k$ ($L - \delta > L - 1 \geq k - 1$ and $L - \delta \leq L < k + 1$). Hence the number of solutions is k or $k + 1$.

Vậy số nghiệm bằng $\lfloor n/(ab) \rfloor$ hoặc $\lfloor n/(ab) \rfloor + 1$.

Hence the number of solutions is $\lfloor n/(ab) \rfloor$ or $\lfloor n/(ab) \rfloor + 1$. ■

Chương 7. Đồng dư và các định lý Fermat, Euler, Wilson — Chapter 7. Congruences; Fermat, Euler and Wilson theorems

Mục tiêu chương — Chapter objectives

- Tính và biến đổi đồng dư thành thạo: nghịch đảo modulo m , phương trình đồng dư bậc nhất, hệ đồng dư theo định lý số dư Trung Hoa.
Compute with congruences fluently: inverses modulo m , linear congruences and systems solved by the Chinese remainder theorem.
- Chứng minh và dùng các định lý Fermat nhỏ, Euler, Wilson, kèm công thức tính $\varphi(n)$.
Prove and apply Fermat's little theorem, Euler's theorem and Wilson's theorem, together with the formula for $\varphi(n)$.
- Dùng cấp của một số modulo n để suy ra ràng buộc về ước nguyên tố của $a^n - 1$ và $a^n + 1$.
Use the order of a number modulo n to constrain the prime divisors of $a^n - 1$ and $a^n + 1$.
- Nhận biết khi nào -1 là thặng dư bình phương modulo p và dùng điều đó trong chứng minh về số nguyên tố dạng $4k + 1$.
Decide when -1 is a quadratic residue modulo p and use it to prove statements about primes of the form $4k + 1$.
- Áp dụng bổ đề nâng số mũ (LTE) với p lẻ, tìm chữ số tận cùng và số dư của lũy thừa tầng.
Apply the lifting-the-exponent lemma (LTE) for odd p , and find last digits and remainders of tower powers.

7.1. Đồng dư và các tính chất cơ bản — Congruences and their basic properties

Từ đây trở đi m là số nguyên dương, UCLN của a và b viết $\gcd(a, b)$, $C(n, k)$ là số tổ hợp chập k của n phần tử (SGK viết C_n^k).

Throughout, m is a positive integer, $\gcd(a, b)$ is the greatest common divisor, and $C(n, k)$ is the number of k -element subsets of an n -element set (the textbook writes C_n^k).

ĐỊNH NGHĨA 7.1 (Đồng dư) / DEFINITION 7.1 (congruence) — Hai số nguyên a, b gọi là đồng dư modulo m , viết $a \equiv b \pmod{m}$, nếu $m \mid a - b$, tức là a và b có cùng số dư khi chia cho m .

Integers a and b are congruent modulo m , written $a \equiv b \pmod{m}$, if $m \mid a - b$; equivalently a and b leave the same remainder on division by m .

TÍNH CHẤT 7.2 (Phép toán trên đồng dư) / PROPERTY 7.2 (arithmetic of congruences) — Nếu $a \equiv b$ và $c \equiv e \pmod{m}$ thì: (i) $a + c \equiv b + e$; (ii) $a - c \equiv b - e$; (iii) $ac \equiv be$; (iv) $a^n \equiv b^n$ với mọi $n \in \mathbb{Z}^+$ (đều theo modulo m). Quan hệ $\equiv$ có tính phản xạ, đối xứng, bắc cầu.

If $a \equiv b$ and $c \equiv e \pmod{m}$ then, all modulo m : (i) $a + c \equiv b + e$; (ii) $a - c \equiv b - e$; (iii) $ac \equiv be$; (iv) $a^n \equiv b^n$ for every $n \in \mathbb{Z}^+$. The relation $\equiv$ is reflexive, symmetric and transitive.

Chứng minh. / Proof.

Đặt $a - b = mu$ và $c - e = mv$ với $u, v \in \mathbb{Z}$. Khi đó $(a + c) - (b + e) = m(u + v)$ và $(a - c) - (b - e) = m(u - v)$, nên (i), (ii) đúng.

Write $a - b = mu$ and $c - e = mv$ with $u, v \in \mathbb{Z}$. Then $(a + c) - (b + e) = m(u + v)$ and $(a - c) - (b - e) = m(u - v)$, which gives (i) and (ii).

$$ac - be = a(c - e) + e(a - b) = m(av + eu)$$

Vậy $m \mid ac - be$, tức (iii). Áp dụng (iii) liên tiếp $n - 1$ lần cho $a \equiv b$ ta được (iv). Ba tính chất của quan hệ suy ra từ $m \mid 0$, $m \mid -(a - b)$ và $m \mid (a - b) + (b - c)$.

So $m \mid ac - be$, which is (iii). Applying (iii) $n - 1$ times to $a \equiv b$ gives (iv). The three properties of the relation follow from $m \mid 0$, $m \mid -(a - b)$ and $m \mid (a - b) + (b - c)$. ■

Phép chia không được dùng tùy tiện: $6 \equiv 15 \pmod{9}$ nhưng $2 \not\equiv 5 \pmod{9}$. Điều kiện đúng cho trong hệ quả sau.

Division cannot be used freely: $6 \equiv 15 \pmod{9}$ but $2 \not\equiv 5 \pmod{9}$. The correct condition is given in the next corollary.

HỆ QUẢ 7.3 (Rút gọn hai vế) / COROLLARY 7.3 (cancellation) — Nếu $ac \equiv bc \pmod{m}$ và $\gcd(c, m) = g$ thì $a \equiv b \pmod{m/g}$. Đặc biệt, nếu $\gcd(c, m) = 1$ thì $a \equiv b \pmod{m}$.
If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = g$ then $a \equiv b \pmod{m/g}$. In particular, if $\gcd(c, m) = 1$ then $a \equiv b \pmod{m}$.

Chứng minh. / Proof.

Từ $m \mid c(a - b)$, chia cho g : $(m/g) \mid (c/g)(a - b)$. Vì $\gcd(m/g, c/g) = 1$ nên $(m/g) \mid a - b$ theo bổ đề Euclid (Chương 6).

From $m \mid c(a - b)$, divide by g : $(m/g) \mid (c/g)(a - b)$. Since $\gcd(m/g, c/g) = 1$, Euclid's lemma (Chapter 6) gives $(m/g) \mid a - b$. ■

$$a \equiv b \pmod{m} \Rightarrow f(a) \equiv f(b) \pmod{m} \text{ với mọi đa thức } f \text{ hệ số nguyên} \quad (7.1)$$

PHÂN TÍCH / ANALYSIS — Hai biểu thức $3^{2n+2} = 9 \cdot 9^n$ và $2^{6n+1} = 2 \cdot 64^n$ có cơ số khác nhau. Modulo 11 ta có $64 \equiv 9$, nên cả hai thành bội của 9^n . Đề bài chia hết cho 11 gợi ý thử đưa cơ số về cùng một số dư.

The terms $3^{2n+2} = 9 \cdot 9^n$ and $2^{6n+1} = 2 \cdot 64^n$ have different bases. Modulo 11 we have $64 \equiv 9$, so both become multiples of 9^n . Divisibility by 11 suggests reducing the bases to a common residue.

VÍ DỤ 7.1 (Đưa về cùng số dư) / EXAMPLE 7.1 (Common residue) — Chứng minh rằng với mọi $n \in \mathbb{Z}^+$ số $3^{2n+2} + 2^{6n+1}$ chia hết cho 11.

Prove that $3^{2n+2} + 2^{6n+1}$ is divisible by 11 for every $n \in \mathbb{Z}^+$.

Lời giải. / Solution.

1. Viết $3^{2n+2} = 9 \cdot 9^n$ và $2^{6n+1} = 2 \cdot 64^n$.

Write $3^{2n+2} = 9 \cdot 9^n$ and $2^{6n+1} = 2 \cdot 64^n$.

2. Vì $64 - 9 = 55$ chia hết cho 11 nên $64 \equiv 9 \pmod{11}$, suy ra $64^n \equiv 9^n \pmod{11}$ theo tính chất (iv).

Since $64 - 9 = 55$ is divisible by 11, $64 \equiv 9 \pmod{11}$, hence $64^n \equiv 9^n \pmod{11}$ by property (iv).

$$3^{2n+2} + 2^{6n+1} \equiv 9 \cdot 9^n + 2 \cdot 9^n = 11 \cdot 9^n \equiv 0 \pmod{11}$$

Vậy $11 \mid 3^{2n+2} + 2^{6n+1}$ với mọi $n \in \mathbb{Z}^+$.

Hence $11 \mid 3^{2n+2} + 2^{6n+1}$ for every $n \in \mathbb{Z}^+$. ■

VÍ DỤ 7.2 (Chặn bằng đồng dư) / EXAMPLE 7.2 (Obstruction by a modulus) — Chứng minh phương trình $x^3 + y^3 + z^3 = 2029$ không có nghiệm nguyên.
Prove that $x^3 + y^3 + z^3 = 2029$ has no integer solutions.

Lời giải. / Solution.

1. Lập phương modulo 9. Mỗi số nguyên có dạng $3k$ hoặc $3k \pm 1$. Nếu $x = 3k$ thì $x^3 = 27k^3 \equiv 0$. Nếu $x = 3k \pm 1$ thì $x^3 = 27k^3 \pm 27k^2 + 9k \pm 1 \equiv \pm 1 \pmod{9}$.
Cubes modulo 9. Every integer has the form $3k$ or $3k \pm 1$. If $x = 3k$ then $x^3 = 27k^3 \equiv 0$. If $x = 3k \pm 1$ then $x^3 = 27k^3 \pm 27k^2 + 9k \pm 1 \equiv \pm 1 \pmod{9}$.
2. Vậy mỗi lập phương đồng dư với $-1, 0$ hoặc 1 modulo 9, nên tổng ba lập phương đồng dư với một số trong $\{-3, -2, \dots, 3\}$. Các số này modulo 9 cho các dư 6, 7, 8, 0, 1, 2, 3; không có dư 4 và 5.
So each cube is congruent to $-1, 0$ or 1 modulo 9, hence a sum of three cubes is congruent to one of $-3, -2, \dots, 3$. Modulo 9 these give the residues 6, 7, 8, 0, 1, 2, 3; the residues 4 and 5 never occur.
3. Mà $2029 = 9 \cdot 225 + 4 \equiv 4 \pmod{9}$. Vậy phương trình vô nghiệm nguyên.
But $2029 = 9 \cdot 225 + 4 \equiv 4 \pmod{9}$. Hence the equation has no integer solution. ■

NHẬN XÉT / REMARK — Modulo 9 chặn được mọi số có dạng $9k + 4$ và $9k + 5$ trong tổng ba lập phương. Chọn modulus để tập các dư của vế trái nhỏ: bình phương modulo 4 hoặc 8, lập phương modulo 7 hoặc 9, lũy thừa bốn modulo 16.
Modulo 9 rules out every number of the form $9k + 4$ and $9k + 5$ as a sum of three cubes. Choose the modulus so that the set of residues of the left side is small: squares modulo 4 or 8, cubes modulo 7 or 9, fourth powers modulo 16.

LỖI HAY GẶP / COMMON MISTAKE — Rút gọn thừa số chung hai vế đồng dư mà không kiểm $\gcd(c, m) = 1$: từ $6 \equiv 15 \pmod{9}$ suy ra $2 \equiv 5$ là sai. Phải chia luôn cả modulus, như Hệ quả 7.3.
Cancelling a common factor from a congruence without checking $\gcd(c, m) = 1$: from $6 \equiv 15 \pmod{9}$ concluding $2 \equiv 5$ is false. The modulus must be divided too, as in Corollary 7.3.

7.2. Nghịch đảo modulo m và phương trình đồng dư bậc nhất — Inverses modulo m and linear congruences

ĐỊNH NGHĨA 7.4 (Nghịch đảo modulo m) / DEFINITION 7.4 (modular inverse) — Số nguyên a' gọi là nghịch đảo của a modulo m nếu $aa' \equiv 1 \pmod{m}$. Khi đó ta viết $a' \equiv a^{-1} \pmod{m}$.
An integer a' is an inverse of a modulo m if $aa' \equiv 1 \pmod{m}$. We then write $a' \equiv a^{-1} \pmod{m}$.

ĐỊNH LÝ 7.5 (Tồn tại nghịch đảo) / THEOREM 7.5 (existence of inverses) — Số a có nghịch đảo modulo m khi và chỉ khi $\gcd(a, m) = 1$. Nghịch đảo nếu có là duy nhất modulo m .
The number a has an inverse modulo m if and only if $\gcd(a, m) = 1$. An inverse, when it exists, is unique modulo m .

Chứng minh. / Proof.

Nếu $aa' \equiv 1$ thì $aa' + mt = 1$ với $t \in \mathbb{Z}$ nào đó, nên mọi ước chung của a và m chia hết 1: $\gcd(a, m) = 1$.

If $aa' \equiv 1$ then $aa' + mt = 1$ for some $t \in \mathbb{Z}$, so every common divisor of a and m divides 1: $\gcd(a, m) = 1$.

Ngược lại, nếu $\gcd(a, m) = 1$ thì theo định lý Bézout (Chương 6) tồn tại $u, v \in \mathbb{Z}$ với $au + mv = 1$; khi đó $au \equiv 1$ và u là nghịch đảo.

Conversely, if $\gcd(a, m) = 1$ then by Bézout's theorem (Chapter 6) there are $u, v \in \mathbb{Z}$ with $au + mv = 1$; hence $au \equiv 1$ and u is an inverse.

Nếu u và u' đều là nghịch đảo thì $u \equiv u(au') = (ua)u' \equiv u' \pmod{m}$.

If u and u' are both inverses then $u \equiv u(au') = (ua)u' \equiv u' \pmod{m}$. ■

ĐỊNH LÝ 7.6 (Đồng dư bậc nhất) / THEOREM 7.6 (linear congruence) — Cho $a, b, m \in \mathbb{Z}$, $m \geq 1$ và $g = \gcd(a, m)$. Phương trình $ax \equiv b \pmod{m}$ có nghiệm khi và chỉ khi $g \mid b$. Khi đó nó có đúng g nghiệm modulo m , và các nghiệm này đồng dư với nhau modulo m/g .
Let $a, b, m \in \mathbb{Z}$, $m \geq 1$ and $g = \gcd(a, m)$. The congruence $ax \equiv b \pmod{m}$ is solvable if and only if $g \mid b$. In that case it has exactly g solutions modulo m , and they are congruent to each other modulo m/g .

Chứng minh. / Proof.

Phương trình tương đương $ax - b = mk$ với $k \in \mathbb{Z}$, tức $ax - mk = b$. Vế trái chia hết cho g nên cần $g \mid b$.

The congruence is equivalent to $ax - b = mk$ for some $k \in \mathbb{Z}$, that is $ax - mk = b$. The left side is divisible by g , so $g \mid b$ is necessary.

Giả sử $g \mid b$. Đặt $a = ga_1$, $b = gb_1$, $m = gm_1$ với $\gcd(a_1, m_1) = 1$. Phương trình tương đương $a_1x \equiv b_1 \pmod{m_1}$ (chia cả hai vế và modulus cho g).

Assume $g \mid b$ and write $a = ga_1$, $b = gb_1$, $m = gm_1$ with $\gcd(a_1, m_1) = 1$. The congruence is equivalent to $a_1x \equiv b_1 \pmod{m_1}$ (divide both sides and the modulus by g).

Theo Định lý 7.5, a_1 có nghịch đảo u modulo m_1 , nên $x \equiv ub_1 \pmod{m_1}$ là toàn bộ nghiệm. Trong một hệ thặng dư đầy đủ modulo $m = gm_1$ có đúng g số thuộc lớp này, ví dụ $x_0, x_0 + m_1, \dots, x_0 + (g-1)m_1$.

By Theorem 7.5, a_1 has an inverse u modulo m_1 , so $x \equiv ub_1 \pmod{m_1}$ describes all solutions. A complete residue system modulo $m = gm_1$ contains exactly g numbers of this class, for example $x_0, x_0 + m_1, \dots, x_0 + (g-1)m_1$. ■

PHÂN TÍCH / ANALYSIS — Hệ số 28 và modulus 70 có ước chung 14, nên không thể nhân với nghịch đảo ngay. Việc đầu tiên là tính $g = \gcd(28, 70)$ rồi xem g có chia hết vế phải 42 không, sau đó rút gọn theo chứng minh của Định lý 7.6.

The coefficient 28 and the modulus 70 share the factor 14, so we cannot multiply by an inverse straight away. First compute $g = \gcd(28, 70)$, check that g divides the right side 42, then reduce as in the proof of Theorem 7.6.

VÍ DỤ 7.3 (Đồng dư bậc nhất có ước chung) / EXAMPLE 7.3 (Linear congruence with common factor) — Giải phương trình đồng dư $28x \equiv 42 \pmod{70}$ và tìm nghịch đảo của 17 modulo 120.

Solve the congruence $28x \equiv 42 \pmod{70}$ and find the inverse of 17 modulo 120.

Lời giải. / Solution.

1. $g = \gcd(28, 70) = 14$ và $14 \mid 42$ ($42 = 14 \cdot 3$), nên phương trình có nghiệm. Chia cả hai vế và modulus cho 14: $2x \equiv 3 \pmod{5}$.
 $g = \gcd(28, 70) = 14$ and $14 \mid 42$ ($42 = 14 \cdot 3$), so solutions exist. Divide both sides and the modulus by 14: $2x \equiv 3 \pmod{5}$.
2. Nghịch đảo của 2 modulo 5 là 3 (vì $2 \cdot 3 = 6 \equiv 1$). Nhân hai vế với 3: $x \equiv 9 \equiv 4 \pmod{5}$.
The inverse of 2 modulo 5 is 3 (since $2 \cdot 3 = 6 \equiv 1$). Multiply by 3: $x \equiv 9 \equiv 4 \pmod{5}$.
3. Vậy nghiệm là $x = 4 + 5t$, $t \in \mathbb{Z}$. Modulo 70 có đúng 14 nghiệm: $x \equiv 4, 9, 14, \dots, 69 \pmod{70}$.
So the solutions are $x = 4 + 5t$, $t \in \mathbb{Z}$. Modulo 70 there are exactly 14 solutions: $x \equiv 4, 9, 14, \dots, 69 \pmod{70}$.
4. Với 17 modulo 120: thuật toán Euclid cho $120 = 7 \cdot 17 + 1$. Do đó $1 = 120 - 7 \cdot 17$, tức $17 \cdot (-7) \equiv 1 \pmod{120}$. Nghịch đảo của 17 là $-7 \equiv 113 \pmod{120}$; kiểm lại $17 \cdot 113 = 1921 = 16 \cdot 120 + 1$.
For 17 modulo 120: Euclid's algorithm gives $120 = 7 \cdot 17 + 1$. Hence $1 = 120 - 7 \cdot 17$, i.e. $17 \cdot (-7) \equiv 1 \pmod{120}$. The inverse of 17 is $-7 \equiv 113 \pmod{120}$; check: $17 \cdot 113 = 1921 = 16 \cdot 120 + 1$. ■

NHẬN XÉT / REMARK — Số nghiệm modulo m bằng g , có thể lớn hơn 1. Khi $g = 1$ phương trình có nghiệm duy nhất $x \equiv a^{-1}b \pmod{m}$; khi $g > 1$ phải rút gọn trước rồi mới nhân nghịch đảo.

The number of solutions modulo m is g , which can exceed 1. For $g = 1$ there is a unique solution $x \equiv a^{-1}b \pmod{m}$; for $g > 1$ one must reduce first and only then multiply by an inverse.

NHẬN XÉT / REMARK — Cách tìm nghịch đảo khi modulus lớn: chạy thuật toán Euclid rồi thay ngược. Với 37 modulo 101: $101 = 2 \cdot 37 + 27$, $37 = 1 \cdot 27 + 10$, $27 = 2 \cdot 10 + 7$, $10 = 1 \cdot 7 + 3$, $7 = 2 \cdot 3 + 1$. Thay ngược: $1 = 7 - 2 \cdot 3 = 3 \cdot 7 - 2 \cdot 10 = 3 \cdot 27 - 8 \cdot 10 = 11 \cdot 27 - 8 \cdot 37 = 11 \cdot 101 - 30 \cdot 37$. Vậy $37 \cdot (-30) \equiv 1 \pmod{101}$, nghịch đảo của 37 là $-30 \equiv 71$; kiểm lại $37 \cdot 71 = 2627 = 26 \cdot 101 + 1$.

Finding an inverse for a large modulus: run Euclid's algorithm and substitute back. For 37 modulo 101: $101 = 2 \cdot 37 + 27$, $37 = 1 \cdot 27 + 10$, $27 = 2 \cdot 10 + 7$, $10 = 1 \cdot 7 + 3$, $7 = 2 \cdot 3 + 1$. Back-substitution: $1 = 7 - 2 \cdot 3 = 3 \cdot 7 - 2 \cdot 10 = 3 \cdot 27 - 8 \cdot 10 = 11 \cdot 27 - 8 \cdot 37 = 11 \cdot 101 - 30 \cdot 37$. So $37 \cdot (-30) \equiv 1 \pmod{101}$; the inverse of 37 is $-30 \equiv 71$; check: $37 \cdot 71 = 2627 = 26 \cdot 101 + 1$.

7.3. Định lý số dư Trung Hoa — The Chinese remainder theorem

ĐỊNH LÝ 7.7 (Định lý số dư Trung Hoa) / THEOREM 7.7 (Chinese remainder theorem)

— Cho $m_1, m_2, \dots, m_k$ là các số nguyên dương đôi một nguyên tố cùng nhau, $M = m_1 m_2 \dots m_k$ và $a_1, \dots, a_k$ là các số nguyên bất kỳ. Khi đó hệ $x \equiv a_1 \pmod{m_1}, \dots, x \equiv a_k \pmod{m_k}$ có nghiệm, và nghiệm duy nhất modulo M .

Let $m_1, m_2, \dots, m_k$ be pairwise coprime positive integers, $M = m_1 m_2 \dots m_k$, and let $a_1, \dots, a_k$ be arbitrary integers. Then the system $x \equiv a_1 \pmod{m_1}, \dots, x \equiv a_k \pmod{m_k}$ has a solution, and the solution is unique modulo M .

Chứng minh. / Proof.

Tồn tại. Đặt $M_i = M/m_i$. Vì các m_j đôi một nguyên tố cùng nhau nên $\gcd(M_i, m_i) = 1$, theo Định lý 7.5 có y_i với $M_i y_i \equiv 1 \pmod{m_i}$. Xét

Existence. Put $M_i = M/m_i$. Since the m_j are pairwise coprime, $\gcd(M_i, m_i) = 1$, so by Theorem 7.5 there is y_i with $M_i y_i \equiv 1 \pmod{m_i}$. Consider

$$x_0 = a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_k M_k y_k \quad (7.2)$$

Với $j \neq i$ ta có $m_i \mid M_j$ nên số hạng thứ j đồng dư 0 modulo m_i ; số hạng thứ i đồng dư $a_i \cdot 1$. Vậy $x_0 \equiv a_i \pmod{m_i}$ với mọi i .

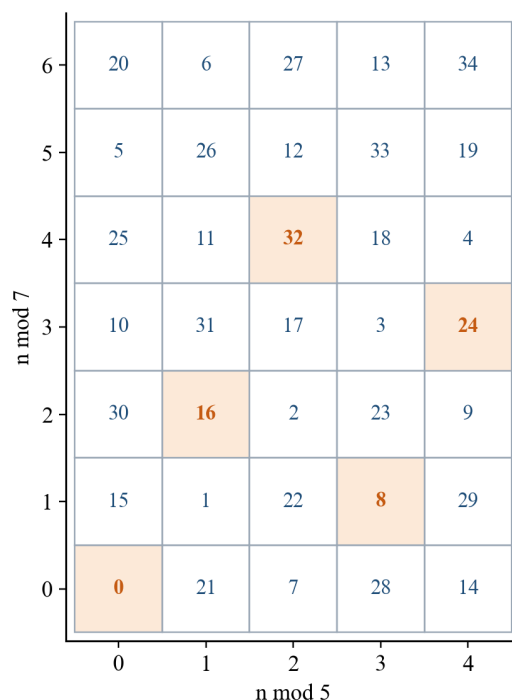
For $j \neq i$ we have $m_i \mid M_j$, so the j -th term is $\equiv 0 \pmod{m_i}$, while the i -th term is $\equiv a_i \cdot 1$. Hence $x_0 \equiv a_i \pmod{m_i}$ for every i .

Duy nhất. Nếu x và x' cùng là nghiệm thì $m_i \mid x - x'$ với mọi i . Các m_i đôi một nguyên tố cùng nhau nên tích M cũng chia hết $x - x'$ (Chương 6), tức $x \equiv x' \pmod{M}$.

Uniqueness. If x and x' are both solutions then $m_i \mid x - x'$ for every i . The m_i are pairwise coprime, so their product M also divides $x - x'$ (Chapter 6), i.e. $x \equiv x' \pmod{M}$. ■

Hệ quả thực hành: giải một đồng dư modulo $M = m_1 \dots m_k$ bằng cách giải riêng từng modulo m_i rồi ghép. Số nghiệm modulo M bằng tích số nghiệm modulo từng m_i .

In practice: solve a congruence modulo $M = m_1 \dots m_k$ by solving it separately modulo each m_i and gluing the answers. The number of solutions modulo M is the product of the numbers of solutions modulo the m_i .



Hình 7.1. Mỗi số n từ 0 đến 34 chiếm đúng một ô $(n \bmod 5, n \bmod 7)$ của lưới 5×7 ; các số 0, 8, 16, 24, 32 tô màu: mỗi lần cộng 8 là nhảy 3 ô sang phải (modulo 5) và 1 ô lên trên (modulo 7).

Figure 7.1. Each n from 0 to 34 occupies exactly one cell $(n \bmod 5, n \bmod 7)$ of the 5×7 grid; the numbers 0, 8, 16, 24, 32 are shaded: each step of $+8$ moves 3 cells right (modulo 5) and 1 cell up (modulo 7).

PHÂN TÍCH / ANALYSIS — Ba modulus 5, 7, 9 đôi một nguyên tố cùng nhau, nên hệ có nghiệm duy nhất modulo 315. Thay vì dùng công thức (7.2) với ba nghịch đảo, ghép lần lượt từng phương trình: nghiệm của phương trình đầu có dạng $3 + 5a$, thế vào phương trình sau. *The moduli 5, 7, 9 are pairwise coprime, so the system has a unique solution modulo 315. Instead of formula (7.2) with three inverses, glue the equations one at a time: solutions of the first have the form $3 + 5a$, which is substituted into the next one.*

VÍ DỤ 7.4 (Ghép từng phương trình) / EXAMPLE 7.4 (Gluing equations one at a time) — Tìm số nguyên dương nhỏ nhất x thỏa mãn $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{7}$, $x \equiv 5 \pmod{9}$. *Find the smallest positive integer x with $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{7}$, $x \equiv 5 \pmod{9}$.*

Lời giải. / Solution.

1. Từ $x \equiv 3 \pmod{5}$ viết $x = 3 + 5a$. Thế vào phương trình thứ hai: $3 + 5a \equiv 4 \pmod{7}$, tức $5a \equiv 1 \pmod{7}$. Vì $5 \cdot 3 = 15 \equiv 1$ nên $a \equiv 3 \pmod{7}$, $a = 3 + 7b$.
From $x \equiv 3 \pmod{5}$ write $x = 3 + 5a$. Substituting into the second equation: $3 + 5a \equiv 4 \pmod{7}$, i.e. $5a \equiv 1 \pmod{7}$. Since $5 \cdot 3 = 15 \equiv 1$, $a \equiv 3 \pmod{7}$, so $a = 3 + 7b$.
2. Khi đó $x = 18 + 35b$. Phương trình thứ ba: $18 + 35b \equiv 5 \pmod{9}$. Vì $18 \equiv 0$ và $35 \equiv -1 \pmod{9}$ nên $-b \equiv 5$, $b \equiv -5 \equiv 4 \pmod{9}$.
Then $x = 18 + 35b$. The third equation: $18 + 35b \equiv 5 \pmod{9}$. Since $18 \equiv 0$ and $35 \equiv -1 \pmod{9}$, we get $-b \equiv 5$, so $b \equiv -5 \equiv 4 \pmod{9}$.

3. Với $b = 4$ ta được $x = 18 + 140 = 158$. Theo Định lý 7.7 mọi nghiệm là $x \equiv 158 \pmod{315}$. Kiểm lại: $158 = 5 \cdot 31 + 3 = 7 \cdot 22 + 4 = 9 \cdot 17 + 5$.

With $b = 4$ we get $x = 18 + 140 = 158$. By Theorem 7.7 all solutions are $x \equiv 158 \pmod{315}$.

Check: $158 = 5 \cdot 31 + 3 = 7 \cdot 22 + 4 = 9 \cdot 17 + 5$.

Vậy số nhỏ nhất là 158.

Hence the smallest positive solution is 158. ■

PHÂN TÍCH / ANALYSIS — Cần bốn số liên tiếp, mỗi số chia hết cho một số chính phương lớn hơn 1. Ý tưởng: gán cho số thứ i một bình phương p_i^2 của số nguyên tố p_i khác nhau; yêu cầu $n + i$ chia hết p_i^2 là một hệ đồng dư mà các modulus nguyên tố cùng nhau, nên CRT cho nghiệm.

We need four consecutive numbers, each divisible by a square greater than 1. Idea: assign to the i -th number the square p_i^2 of a different prime p_i ; requiring $p_i^2 \mid n + i$ is a system of congruences with coprime moduli, so the CRT supplies a solution.

VÍ DỤ 7.5 (CRT dựng dãy số) / EXAMPLE 7.5 (Building runs with the CRT) — Chứng minh với mọi $k \in \mathbb{Z}^+$ tồn tại k số nguyên dương liên tiếp, mỗi số chia hết cho một số chính phương lớn hơn 1. Tìm cụ thể bốn số như vậy.

Prove that for every $k \in \mathbb{Z}^+$ there are k consecutive positive integers, each divisible by a square greater than 1. Find four such numbers explicitly.

Lời giải. / Solution.

1. Lấy k số nguyên tố phân biệt $p_1, \dots, p_k$. Xét hệ $n \equiv -(i - 1) \pmod{p_i^2}$, $i = 1, \dots, k$. Các p_i^2 đôi một nguyên tố cùng nhau nên theo Định lý 7.7 hệ có nghiệm n dương.

Take k distinct primes $p_1, \dots, p_k$. Consider the system $n \equiv -(i - 1) \pmod{p_i^2}$, $i = 1, \dots, k$. The p_i^2 are pairwise coprime, so by Theorem 7.7 the system has a positive solution n .

2. Với nghiệm đó $p_i^2 \mid n + i - 1$ với mỗi i , nên k số $n, n + 1, \dots, n + k - 1$ thỏa yêu cầu.

For such n we have $p_i^2 \mid n + i - 1$ for each i , so the k numbers $n, n + 1, \dots, n + k - 1$ satisfy the requirement.

3. Với $k = 4$ chọn các số nguyên tố 2, 3, 5, 7: $n \equiv 0 \pmod{4}$, $n \equiv 8 \pmod{9}$, $n \equiv 23 \pmod{25}$, $n \equiv 46 \pmod{49}$. Giải bằng cách ghép như Ví dụ 7.4 được $n \equiv 29348 \pmod{44100}$.

For $k = 4$ choose the primes 2, 3, 5, 7: $n \equiv 0 \pmod{4}$, $n \equiv 8 \pmod{9}$, $n \equiv 23 \pmod{25}$, $n \equiv 46 \pmod{49}$. Gluing as in Example 7.4 gives $n \equiv 29348 \pmod{44100}$.

4. Kiểm lại bằng phép chia: $29348 = 4 \cdot 7337$, $29349 = 9 \cdot 3261$, $29350 = 25 \cdot 1174$, $29351 = 49 \cdot 599$.

Check by division: $29348 = 4 \cdot 7337$, $29349 = 9 \cdot 3261$, $29350 = 25 \cdot 1174$, $29351 = 49 \cdot 599$.

Vậy bốn số 29348, 29349, 29350, 29351 liên tiếp và lần lượt chia hết cho 4, 9, 25, 49.

Hence 29348, 29349, 29350, 29351 are consecutive and divisible by 4, 9, 25, 49 respectively. ■

NHẬN XÉT / REMARK — CRT cho modulus không nguyên tố cùng nhau. Hệ $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ có nghiệm khi và chỉ khi $\gcd(m, n) \mid a - b$, và khi đó nghiệm duy nhất modulo BCNN(m, n). Chứng minh: đặt $g = \gcd(m, n)$; nghiệm của phương trình đầu là $x = a + mt$; thế vào phương trình sau được $mt \equiv b - a \pmod{n}$, giải được khi và chỉ khi $g \mid b - a$

(Định lý 7.6). Khi giải được, t xác định duy nhất modulo n/g nên $x = a + mt$ xác định duy nhất modulo $m \cdot (n/g) = \text{BCNN}(m, n)$.

CRT for non-coprime moduli. The system $x \equiv a \pmod{m}$, $x \equiv b \pmod{n}$ is solvable if and only if $\gcd(m, n) \mid a - b$, and then the solution is unique modulo $\text{lcm}(m, n)$. Proof: put $g = \gcd(m, n)$; the solutions of the first equation are $x = a + mt$; substituting into the second gives $mt \equiv b - a \pmod{n}$, solvable iff $g \mid b - a$ (Theorem 7.6). When solvable, t is unique modulo n/g , so $x = a + mt$ is unique modulo $m \cdot (n/g) = \text{lcm}(m, n)$.

$$x \equiv a \pmod{m}, x \equiv b \pmod{n} \Leftrightarrow \gcd(m, n) \mid a - b, x \equiv x_0 \pmod{\text{lcm}(m, n)}$$

Ví dụ: $x \equiv 3 \pmod{4}$ và $x \equiv 1 \pmod{6}$ có $\gcd(4, 6) = 2 \mid 3 - 1 = 2$, nên có nghiệm duy nhất modulo 12, đó là $x \equiv 7$. Còn $x \equiv 1 \pmod{4}$ và $x \equiv 2 \pmod{6}$ vô nghiệm vì $2 \nmid 1$.

Example: $x \equiv 3 \pmod{4}$ and $x \equiv 1 \pmod{6}$ have $\gcd(4, 6) = 2 \mid 3 - 1 = 2$, so there is a unique solution modulo 12, namely $x \equiv 7$. By contrast $x \equiv 1 \pmod{4}$ and $x \equiv 2 \pmod{6}$ has no solution because $2 \nmid 1$.

LỖI HAY GẶP / COMMON MISTAKE — Ghép hệ đồng dư bằng công thức (7.2) khi các modulus không đôi một nguyên tố cùng nhau. Phải kiểm $\gcd(m_i, m_j) = 1$, hoặc ghép từng cặp một theo nhận xét về CRT tổng quát. Hệ $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{6}$ vô nghiệm dù cả hai phương trình đều giải được riêng.

Gluing congruences with formula (7.2) when the moduli are not pairwise coprime. Check $\gcd(m_i, m_j) = 1$, or glue pair by pair as in the remark on the general CRT. The system $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{6}$ has no solution although each equation is solvable alone.

7.4. Hàm φ , các định lý Euler, Fermat và Wilson — The function φ and the theorems of Euler, Fermat and Wilson

ĐỊNH NGHĨA 7.8 (Hệ thặng dư) / DEFINITION 7.8 (residue system) — Hệ thặng dư đầy đủ modulo m là tập m số nguyên đôi một không đồng dư modulo m (mỗi lớp dư có đúng một đại diện), ví dụ $\{0, 1, \dots, m-1\}$. Hệ thặng dư thu gọn modulo m là tập các số nguyên nguyên tố cùng nhau với m , đôi một không đồng dư, và mọi số nguyên tố cùng nhau với m đều đồng dư với một số trong tập.

A complete residue system modulo m is a set of m integers, pairwise incongruent modulo m (one representative of each residue class), for example $\{0, 1, \dots, m-1\}$. A reduced residue system modulo m is a set of pairwise incongruent integers coprime to m such that every integer coprime to m is congruent to one of them.

ĐỊNH NGHĨA 7.9 (Hàm Euler) / DEFINITION 7.9 (Euler's totient function) — Hàm Euler $\varphi(m)$ là số các số nguyên k với $1 \leq k \leq m$ và $\gcd(k, m) = 1$; đó cũng là số phần tử của một hệ thặng dư thu gọn modulo m .

Euler's totient function $\varphi(m)$ is the number of integers k with $1 \leq k \leq m$ and $\gcd(k, m) = 1$; it is also the size of any reduced residue system modulo m .

TÍNH CHẤT 7.10 (Nhân với số nguyên tố cùng nhau) / PROPERTY 7.10 (multiplying by a coprime number) — Cho $\gcd(a, m) = 1$. Nếu $\{r_1, \dots, r_s\}$ là hệ thặng dư thu gọn modulo m thì $\{ar_1, \dots, ar_s\}$ cũng là hệ thặng dư thu gọn modulo m . Nếu $\{r_1, \dots, r_m\}$ là hệ đầy đủ thì $\{ar_1 + b, \dots, ar_m + b\}$ cũng là hệ đầy đủ với mọi $b \in \mathbb{Z}$.

Let $\gcd(a, m) = 1$. If $\{r_1, \dots, r_s\}$ is a reduced residue system modulo m then so is $\{ar_1, \dots, ar_s\}$. If $\{r_1, \dots, r_m\}$ is a complete system then so is $\{ar_1 + b, \dots, ar_m + b\}$ for every $b \in \mathbb{Z}$.

Chứng minh. / Proof.

Mỗi ar_i nguyên tố cùng nhau với m vì $\gcd(a, m) = \gcd(r_i, m) = 1$. Giả sử $ar_i \equiv ar_j \pmod{m}$; do $\gcd(a, m) = 1$, Hệ quả 7.3 cho $r_i \equiv r_j$, tức $i = j$. Vậy s số ar_i đôi một không đồng dư; vì có đúng $s = \varphi(m)$ lớp dư nguyên tố cùng nhau với m nên chúng đại diện cho tất cả các lớp đó.

Each ar_i is coprime to m because $\gcd(a, m) = \gcd(r_i, m) = 1$. If $ar_i \equiv ar_j \pmod{m}$ then, as $\gcd(a, m) = 1$, Corollary 7.3 gives $r_i \equiv r_j$, i.e. $i = j$. So the s numbers ar_i are pairwise incongruent; since there are exactly $s = \varphi(m)$ residue classes coprime to m , they represent all of them.

Với hệ đầy đủ: $ar_i + b \equiv ar_j + b$ suy ra $ar_i \equiv ar_j$, rồi $r_i \equiv r_j$, nên m số này đôi một không đồng dư, tức đủ m lớp.

For a complete system: $ar_i + b \equiv ar_j + b$ gives $ar_i \equiv ar_j$ and then $r_i \equiv r_j$, so the m numbers are pairwise incongruent, hence they fill all m classes. ■

ĐỊNH LÝ 7.11 (Công thức tính φ) / THEOREM 7.11 (formula for φ) — (i) Với p nguyên tố và $k \geq 1$: $\varphi(p^k) = p^k - p^{k-1}$. (ii) Nếu $\gcd(m, n) = 1$ thì $\varphi(mn) = \varphi(m)\varphi(n)$. (iii) Nếu $n = p_1^{k_1} \dots p_r^{k_r}$ là phân tích ra thừa số nguyên tố thì
(i) For a prime p and $k \geq 1$: $\varphi(p^k) = p^k - p^{k-1}$. (ii) If $\gcd(m, n) = 1$ then $\varphi(mn) = \varphi(m)\varphi(n)$. (iii) If $n = p_1^{k_1} \dots p_r^{k_r}$ is the prime factorisation then

$$\varphi(n) = n(1 - 1/p_1)(1 - 1/p_2) \dots (1 - 1/p_r) \quad (7.3)$$

Chứng minh. / Proof.

(i) Trong p^k số $1, \dots, p^k$ chỉ các bội của p không nguyên tố cùng nhau với p^k ; có p^{k-1} bội, nên $\varphi(p^k) = p^k - p^{k-1}$.

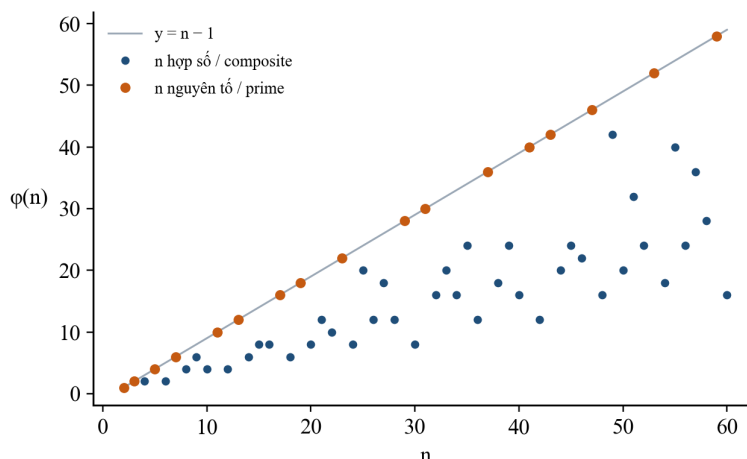
(i) Among the p^k numbers $1, \dots, p^k$ only the multiples of p fail to be coprime to p^k ; there are p^{k-1} of them, so $\varphi(p^k) = p^k - p^{k-1}$.

(ii) Theo CRT (Định lý 7.7), ánh xạ $x \mapsto (x \bmod m, x \bmod n)$ là song ánh giữa các lớp dư modulo mn và các cặp (lớp modulo m , lớp modulo n). Số x nguyên tố cùng nhau với mn khi và chỉ khi nó nguyên tố cùng nhau với cả m và n , tức khi và chỉ khi cả hai thành phần của cặp nguyên tố cùng nhau với modulus tương ứng. Đếm hai bên cho $\varphi(mn) = \varphi(m)\varphi(n)$.

(ii) By the CRT (Theorem 7.7), the map $x \mapsto (x \bmod m, x \bmod n)$ is a bijection between residue classes modulo mn and pairs (class modulo m , class modulo n). A number x is coprime to mn exactly when it is coprime to both m and n , that is, when both components of the pair are coprime to their moduli. Counting both sides gives $\varphi(mn) = \varphi(m)\varphi(n)$.

(iii) Các $p_i^{k_i}$ đôi một nguyên tố cùng nhau, nên theo (ii) và (i): $\varphi(n) = \prod (p_i^{k_i} - p_i^{k_i-1}) = \prod p_i^{k_i}(1 - 1/p_i) = n \prod (1 - 1/p_i)$.

(iii) The $p_i^{k_i}$ are pairwise coprime, so by (ii) and (i): $\varphi(n) = \prod (p_i^{k_i} - p_i^{k_i-1}) = \prod p_i^{k_i}(1 - 1/p_i) = n \prod (1 - 1/p_i)$. ■



Hình 7.2. Đồ thị $\varphi(n)$ với $2 \leq n \leq 60$: các số nguyên tố nằm trên đường $y = n - 1$, số hợp số nằm thấp hơn hẳn.

Figure 7.2. Graph of $\varphi(n)$ for $2 \leq n \leq 60$: primes lie on the line $y = n - 1$, composite numbers lie well below it.

ĐỊNH LÝ 7.12 (Định lý Euler) / THEOREM 7.12 (Euler's theorem) — Nếu $\gcd(a, m) = 1$ thì $a^{\varphi(m)} \equiv 1 \pmod{m}$.
If $\gcd(a, m) = 1$ then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Chứng minh. / Proof.

Gọi $\{r_1, \dots, r_s\}$, $s = \varphi(m)$, là hệ thặng dư thu gọn modulo m . Theo Tính chất 7.10, $\{ar_1, \dots, ar_s\}$ cũng là hệ thặng dư thu gọn, nên các số ar_i là một hoán vị của r_i xét modulo m . Nhân tất cả:

Let $\{r_1, \dots, r_s\}$, $s = \varphi(m)$, be a reduced residue system modulo m . By Property 7.10, $\{ar_1, \dots, ar_s\}$ is also a reduced residue system, so the ar_i are a permutation of the r_i modulo m . Multiplying them all:

$$a^s \cdot r_1 r_2 \dots r_s \equiv r_1 r_2 \dots r_s \pmod{m}$$

Tích $r_1 \dots r_s$ nguyên tố cùng nhau với m nên rút gọn được (Hệ quả 7.3): $a^s \equiv 1 \pmod{m}$.

The product $r_1 \dots r_s$ is coprime to m , so it can be cancelled (Corollary 7.3): $a^s \equiv 1 \pmod{m}$. ■

$$\gcd(a, m) = 1 \Rightarrow a^{\varphi(m)} \equiv 1 \pmod{m} \quad (7.4)$$

HỆ QUẢ 7.13 (Định lý Fermat nhỏ) / COROLLARY 7.13 (Fermat's little theorem) — Định lý Fermat nhỏ. Nếu p nguyên tố thì $a^p \equiv a \pmod{p}$ với mọi $a \in \mathbb{Z}$; và nếu $p \nmid a$ thì $a^{p-1} \equiv 1 \pmod{p}$.
Fermat's little theorem. If p is prime then $a^p \equiv a \pmod{p}$ for every $a \in \mathbb{Z}$; and if $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$.

Chứng minh. / Proof.

Nếu $p \nmid a$ thì $\gcd(a, p) = 1$ và $\varphi(p) = p - 1$, nên Định lý Euler cho $a^{p-1} \equiv 1$. Nhân hai vế với a được $a^p \equiv a$. Nếu $p \mid a$ thì cả hai vế a^p và a đồng dư 0 modulo p .

If $p \nmid a$ then $\gcd(a, p) = 1$ and $\phi(p) = p - 1$, so Euler's theorem gives $a^{p-1} \equiv 1$. Multiplying by a yields $a^p \equiv a$. If $p \mid a$ then both a^p and a are $\equiv 0$ modulo p . ■

$$a^p \equiv a \pmod{p} \text{ với mọi } a \in \mathbb{Z}, p \text{ nguyên tố} \quad (7.5)$$

NHẬN XÉT / REMARK — Chiều đảo của Fermat nhỏ sai. Số $341 = 11 \cdot 31$ là hợp số nhưng $2^{10} = 1024 = 3 \cdot 341 + 1 \equiv 1 \pmod{341}$, nên $2^{340} = (2^{10})^{34} \equiv 1 \pmod{341}$. Vì vậy $a^{n-1} \equiv 1 \pmod{n}$ không đủ để kết luận n nguyên tố; Định lý Wilson cho điều kiện cần và đủ, nhưng khó tính. *The converse of Fermat's little theorem is false. The number $341 = 11 \cdot 31$ is composite, yet $2^{10} = 1024 = 3 \cdot 341 + 1 \equiv 1 \pmod{341}$, so $2^{340} = (2^{10})^{34} \equiv 1 \pmod{341}$. Hence $a^{n-1} \equiv 1 \pmod{n}$ does not prove that n is prime; Wilson's theorem gives an exact criterion but is hard to evaluate.*

PHẢI THUỘC / MEMORISE — $\phi(n) = n \prod (1 - 1/p)$ theo các ước nguyên tố p của n . $\gcd(a, m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \pmod{m}$. p nguyên tố $\Rightarrow a^p \equiv a \pmod{p}$. Muốn đổi a^N thành lũy thừa nhỏ hơn: lấy N modulo $\phi(m)$ (khi $\gcd(a, m) = 1$).
 $\phi(n) = n \prod (1 - 1/p)$ over the prime divisors p of n . $\gcd(a, m) = 1 \Rightarrow a^{\phi(m)} \equiv 1 \pmod{m}$. p prime $\Rightarrow a^p \equiv a \pmod{p}$. To shrink a^N : reduce N modulo $\phi(m)$ (when $\gcd(a, m) = 1$).

PHÂN TÍCH / ANALYSIS — Muốn tính 3^{1000} modulo 77 mà 1000 lớn. Vì $77 = 7 \cdot 11$ và $\gcd(3, 77) = 1$, Định lý Euler cho $3^{\phi(77)} \equiv 1$ với $\phi(77) = 6 \cdot 10 = 60$. Do $1000 = 60 \cdot 16 + 40$, chỉ cần tính 3^{40} .
We want 3^{1000} modulo 77 with 1000 large. Since $77 = 7 \cdot 11$ and $\gcd(3, 77) = 1$, Euler's theorem gives $3^{\phi(77)} \equiv 1$ with $\phi(77) = 6 \cdot 10 = 60$. As $1000 = 60 \cdot 16 + 40$, it suffices to compute 3^{40} .

VÍ DỤ 7.6 (Hạ số mũ bằng ϕ) / EXAMPLE 7.6 (Reducing the exponent by ϕ) — Tính số dư của 3^{1000} khi chia cho 77.
Find the remainder of 3^{1000} on division by 77.

Lời giải. / Solution.

- $\phi(77) = \phi(7)\phi(11) = 6 \cdot 10 = 60$, và $\gcd(3, 77) = 1$ nên $3^{60} \equiv 1 \pmod{77}$. Vì $1000 = 60 \cdot 16 + 40$ nên $3^{1000} \equiv 3^{40} \pmod{77}$.
 $\phi(77) = \phi(7)\phi(11) = 6 \cdot 10 = 60$, and $\gcd(3, 77) = 1$, so $3^{60} \equiv 1 \pmod{77}$. Since $1000 = 60 \cdot 16 + 40$, $3^{1000} \equiv 3^{40} \pmod{77}$.
- $3^4 = 81 \equiv 4 \pmod{77}$, nên $3^{40} = (3^4)^{10} \equiv 4^{10} = 2^{20} \pmod{77}$.
 $3^4 = 81 \equiv 4 \pmod{77}$, so $3^{40} = (3^4)^{10} \equiv 4^{10} = 2^{20} \pmod{77}$.
- $2^{10} = 1024 = 77 \cdot 13 + 23 \equiv 23$, nên $2^{20} \equiv 23^2 = 529 = 77 \cdot 6 + 67 \equiv 67 \pmod{77}$.
 $2^{10} = 1024 = 77 \cdot 13 + 23 \equiv 23$, so $2^{20} \equiv 23^2 = 529 = 77 \cdot 6 + 67 \equiv 67 \pmod{77}$.

Vậy số dư là 67.

Hence the remainder is 67. ■

PHÂN TÍCH / ANALYSIS — Số $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37$ là tích các số nguyên tố p mà $p - 1$ là ước của 36. Với mỗi p như vậy Fermat cho $n^{p-1} \equiv 1$ khi $p \nmid n$, nên $n^{36} = (n^{p-1})^{36/(p-1)} \equiv 1$.
The number $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37$ is the product of the primes p for which $p - 1$ divides 36. For each such p Fermat gives $n^{p-1} \equiv 1$ when $p \nmid n$, hence $n^{36} = (n^{p-1})^{36/(p-1)} \equiv 1$.

VÍ DỤ 7.7 (Fermat cho nhiều số nguyên tố) / EXAMPLE 7.7 (Fermat for several primes)

— Chứng minh rằng với mọi $n \in \mathbb{Z}$ số $n^{37} - n$ chia hết cho $1.919.190 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37$.

Prove that $n^{37} - n$ is divisible by $1,919,190 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37$ for every $n \in \mathbb{Z}$.

Lời giải. / Solution.

1. Các ước 2, 3, 5, 7, 13, 19, 37 là các số nguyên tố đôi một khác nhau, nên chỉ cần chứng minh từng số nguyên tố p trong đó chia hết $n^{37} - n$.

The factors 2, 3, 5, 7, 13, 19, 37 are distinct primes, so it suffices to show that each of them divides $n^{37} - n$.

2. Nếu $p \mid n$ thì $p \mid n^{37} - n$ vì cả hai số n^{37} và n chia hết cho p . Nếu $p \nmid n$ thì $n^{p-1} \equiv 1 \pmod{p}$ theo Fermat. Với mỗi p trong danh sách, $p - 1$ lần lượt là 1, 2, 4, 6, 12, 18, 36, đều là ước của 36.

If $p \mid n$ then $p \mid n^{37} - n$ since both n^{37} and n are divisible by p . If $p \nmid n$ then $n^{p-1} \equiv 1 \pmod{p}$ by Fermat. For the primes in the list, $p - 1$ equals 1, 2, 4, 6, 12, 18, 36, all divisors of 36.

3. Do đó $n^{36} = (n^{p-1})^{36/(p-1)} \equiv 1 \pmod{p}$, suy ra $n^{37} \equiv n \pmod{p}$.

Hence $n^{36} = (n^{p-1})^{36/(p-1)} \equiv 1 \pmod{p}$, so $n^{37} \equiv n \pmod{p}$.

Vì 7 số nguyên tố đôi một khác nhau, tích của chúng chia hết $n^{37} - n$.

Since the seven primes are distinct, their product divides $n^{37} - n$. ■

NHẬN XÉT / REMARK — Tổng quát: $n^{k+1} - n$ chia hết cho tích mọi số nguyên tố p mà $(p - 1) \mid k$. Với $k = 36$ tích đó là 1.919.190 và đó cũng là ƯCLN của mọi số $n^{37} - n$ (kiểm bằng máy với $n \leq 5000$; chứng minh tính lớn nhất cần căn nguyên thủy nên không trình bày ở đây).
In general $n^{k+1} - n$ is divisible by the product of all primes p with $(p - 1) \mid k$. For $k = 36$ this product is 1,919,190, and it is also the gcd of all the numbers $n^{37} - n$ (checked by computer for $n \leq 5000$; proving maximality needs primitive roots and is not done here).

NHẬN XÉT / REMARK — Đẳng thức Gauss: $\sum \varphi(d) = n$, tổng lấy theo mọi ước dương d của n . Chứng minh: chia các số 1, ..., n theo $g = \gcd(k, n)$. Số k có $\gcd(k, n) = n/d$ khi và chỉ khi $k = (n/d) \cdot u$ với $1 \leq u \leq d$ và $\gcd(u, d) = 1$, nên có đúng $\varphi(d)$ số như vậy. Cộng theo mọi $d \mid n$ được n . Ví dụ $n = 12$: $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$.
Gauss's identity: $\sum \varphi(d) = n$, summed over all positive divisors d of n . Proof: sort the numbers 1, ..., n by $g = \gcd(k, n)$. We have $\gcd(k, n) = n/d$ exactly when $k = (n/d) \cdot u$ with $1 \leq u \leq d$ and $\gcd(u, d) = 1$, so there are exactly $\varphi(d)$ such k . Summing over $d \mid n$ gives n . Example $n = 12$: $\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 1 + 1 + 2 + 2 + 2 + 4 = 12$.

LỖI HAY GẶP / COMMON MISTAKE — Áp dụng Định lý Euler khi $\gcd(a, m) \neq 1$, chẳng hạn viết $6^{\varphi(9)} \equiv 1 \pmod{9}$. Thực tế $6^6 \equiv 0 \pmod{9}$. Luôn kiểm $\gcd(a, m) = 1$ trước khi dùng.

Applying Euler's theorem when $\gcd(a, m) \neq 1$, for example writing $6^{\varphi(9)} \equiv 1 \pmod{9}$. In fact $6^6 \equiv 0 \pmod{9}$. Always check $\gcd(a, m) = 1$ first.

LỖI HAY GẶP / COMMON MISTAKE — Dùng Fermat với modulus hợp số: $a^{m-1} \equiv 1 \pmod{m}$ sai khi $m = 4$, $a = 3$, vì $3^3 = 27 \equiv 3 \pmod{4}$. Định lý Fermat nhỏ chỉ dành cho modulus nguyên tố.

Using Fermat with a composite modulus: $a^{m-1} \equiv 1 \pmod{m}$ fails for $m = 4$, $a = 3$, since $3^3 = 27 \equiv 3 \pmod{4}$. Fermat's little theorem is for prime moduli only.

ĐỊNH LÝ 7.14 (Định lý Wilson) / THEOREM 7.14 (Wilson's theorem) — Định lý Wilson. Số nguyên $p \geq 2$ là số nguyên tố khi và chỉ khi $(p-1)! \equiv -1 \pmod{p}$.
Wilson's theorem. An integer $p \geq 2$ is prime if and only if $(p-1)! \equiv -1 \pmod{p}$.

Chứng minh. / Proof.

Giả sử p hợp số. Khi đó p có ước d với $1 < d < p$, và $d \mid (p-1)!$. Nếu $(p-1)! \equiv -1 \pmod{p}$ thì $d \mid (p-1)! + 1$, kết hợp với $d \mid (p-1)!$ được $d \mid 1$, vô lý. Vậy $(p-1)! \not\equiv -1$.

Suppose p is composite. Then p has a divisor d with $1 < d < p$, and $d \mid (p-1)!$. If $(p-1)! \equiv -1 \pmod{p}$ then $d \mid (p-1)! + 1$, together with $d \mid (p-1)!$ this gives $d \mid 1$, a contradiction. So $(p-1)! \not\equiv -1$.

Giả sử p nguyên tố. Với $p = 2$ và $p = 3$ kiểm trực tiếp: $1! = 1 \equiv -1 \pmod{2}$ và $2! = 2 \equiv -1 \pmod{3}$. Với $p \geq 5$, mỗi $k \in \{1, \dots, p-1\}$ có nghịch đảo $k' \in \{1, \dots, p-1\}$ duy nhất modulo p (Định lý 7.5).

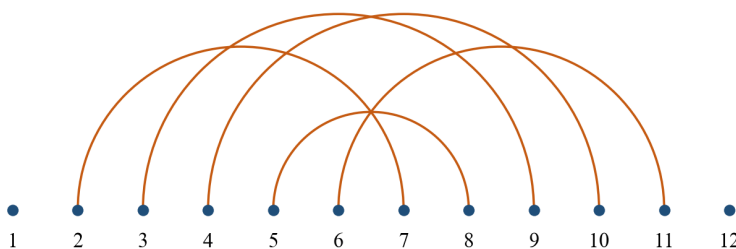
Suppose p is prime. For $p = 2$ and $p = 3$ check directly: $1! = 1 \equiv -1 \pmod{2}$ and $2! = 2 \equiv -1 \pmod{3}$. For $p \geq 5$, each $k \in \{1, \dots, p-1\}$ has a unique inverse $k' \in \{1, \dots, p-1\}$ modulo p (Theorem 7.5).

Ta có $k' = k$ khi và chỉ khi $k^2 \equiv 1$, tức $p \mid (k-1)(k+1)$, tức $k = 1$ hoặc $k = p-1$. Các số $2, 3, \dots, p-2$ còn lại ghép thành cặp $\{k, k'\}$ với $k \neq k'$, mỗi cặp có tích $\equiv 1$. Do đó

We have $k' = k$ exactly when $k^2 \equiv 1$, i.e. $p \mid (k-1)(k+1)$, i.e. $k = 1$ or $k = p-1$. The remaining numbers $2, 3, \dots, p-2$ split into pairs $\{k, k'\}$ with $k \neq k'$, each with product $\equiv 1$. Therefore

$$(p-1)! = 1 \cdot (p-1) \cdot (2 \cdot 3 \cdots (p-2)) \equiv 1 \cdot (-1) \cdot 1 = -1 \pmod{p}$$

■



Hình 7.3. Với $p = 13$, mỗi số k trong $\{1, \dots, 12\}$ nối với nghịch đảo của nó modulo 13: các cung nối các cặp $\{2, 7\}$, $\{3, 9\}$, $\{4, 10\}$, $\{5, 8\}$, $\{6, 11\}$; hai số 1 và 12 là nghịch đảo của chính mình.

Figure 7.3. For $p = 13$, each k in $\{1, \dots, 12\}$ is joined to its inverse modulo 13: the arcs join the pairs $\{2, 7\}$, $\{3, 9\}$, $\{4, 10\}$, $\{5, 8\}$, $\{6, 11\}$; the numbers 1 and 12 are their own inverses.

HỆ QUẢ 7.15 (Căn bậc hai của $(p-1)!$) / COROLLARY 7.15 (square root of $(p-1)!$)

— Với p nguyên tố lẻ: $((p-1)/2!)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.

For an odd prime p : $((p-1)/2!)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$.

Chứng minh. / Proof.

Đặt $h = (p - 1)/2$. Với $1 \leq j \leq h$ có $p - j \equiv -j \pmod{p}$, nên các số $h + 1, \dots, p - 1$ (là $p - h, \dots, p - 1$) đồng dư lần lượt với $-h, \dots, -1$. Do đó

Put $h = (p - 1)/2$. For $1 \leq j \leq h$ we have $p - j \equiv -j \pmod{p}$, so the numbers $h + 1, \dots, p - 1$ (that is $p - h, \dots, p - 1$) are congruent to $-h, \dots, -1$. Hence

$$(p - 1)! = (1 \cdot 2 \cdot \dots \cdot h) \cdot ((h + 1) \cdot \dots \cdot (p - 1)) \equiv (h!) \cdot (-1)^h \cdot (h!) = (-1)^h (h!)^2$$

Theo Định lý Wilson về trái $\equiv -1$. Nhân hai vế của $-1 \equiv (-1)^h (h!)^2$ với $(-1)^h$ ta được $(h!)^2 \equiv -(-1)^h = (-1)^{h+1}$, và $h + 1 = (p + 1)/2$.

By Wilson's theorem the left side is $\equiv -1$. Multiplying $-1 \equiv (-1)^h (h!)^2$ by $(-1)^h$ gives $(h!)^2 \equiv -(-1)^h = (-1)^{h+1}$, and $h + 1 = (p + 1)/2$. ■

PHÂN TÍCH / ANALYSIS — Có $22! \equiv -1 \pmod{23}$ theo Wilson, nhưng cần $20!$. Hai thừa số thiếu là 21 và 22, mà $21 \equiv -2$ và $22 \equiv -1 \pmod{23}$. Thay chúng vào, $22!$ thành bội của $20!$ với hệ số nhỏ.

Wilson gives $22! \equiv -1 \pmod{23}$, but we need $20!$. The missing factors are 21 and 22, and $21 \equiv -2, 22 \equiv -1 \pmod{23}$. Substituting them turns $22!$ into a small multiple of $20!$.

VÍ DỤ 7.8 (Wilson với thừa số thiếu) / EXAMPLE 7.8 (Wilson with missing factors) — Tính số dư của $20!$ khi chia cho 23.

Find the remainder of $20!$ on division by 23.

Lời giải. / Solution.

- 23 nguyên tố nên $22! \equiv -1 \pmod{23}$ theo Định lý Wilson.
23 is prime, so $22! \equiv -1 \pmod{23}$ by Wilson's theorem.
- Mặt khác $22! = 22 \cdot 21 \cdot 20! \equiv (-1)(-2) \cdot 20! = 2 \cdot 20! \pmod{23}$. Do đó $2 \cdot 20! \equiv -1 \equiv 22 \pmod{23}$.
Also $22! = 22 \cdot 21 \cdot 20! \equiv (-1)(-2) \cdot 20! = 2 \cdot 20! \pmod{23}$. Hence $2 \cdot 20! \equiv -1 \equiv 22 \pmod{23}$.
- Vì $\gcd(2, 23) = 1$, rút gọn thừa số 2: $20! \equiv 11 \pmod{23}$.
Since $\gcd(2, 23) = 1$, cancel the factor 2: $20! \equiv 11 \pmod{23}$.

Vậy số dư là 11.

Hence the remainder is 11. ■

NHẬN XÉT / REMARK — Tổng quát, $(p - 1 - k)! \cdot k! \equiv (-1)^{k+1} \pmod{p}$ với $0 \leq k \leq p - 1$. Ví dụ 7.8 là trường hợp $p = 23, k = 2$: $20! \cdot 2! \equiv -1$, tức $20! \equiv -1 \cdot 2^{-1} = -12 \equiv 11$. Với $p \equiv 1 \pmod{4}$ nghiệm của $x^2 \equiv -1$ là $x \equiv \pm((p - 1)/2)!$, ví dụ $p = 29$ cho $x \equiv \pm 14! \equiv \pm 12$ vì $12^2 = 144 = 5 \cdot 29 - 1$.

In general $(p - 1 - k)! \cdot k! \equiv (-1)^{k+1} \pmod{p}$ for $0 \leq k \leq p - 1$. Example 7.8 is the case $p = 23, k = 2$: $20! \cdot 2! \equiv -1$, so $20! \equiv -1 \cdot 2^{-1} = -12 \equiv 11$. For $p \equiv 1 \pmod{4}$ the solutions of $x^2 \equiv -1$ are $x \equiv \pm((p - 1)/2)!$; for $p = 29$ this gives $x \equiv \pm 14! \equiv \pm 12$ because $12^2 = 144 = 5 \cdot 29 - 1$.

LỖI HAY GẶP / COMMON MISTAKE — Dùng Wilson để kiểm tra tính nguyên tố của số lớn: $(p - 1)!$ quá lớn để tính, nên định lý đúng nhưng không thực dụng. Trong bài thi dùng Wilson để rút gọn tích, không dùng làm phép thử số nguyên tố.

Using Wilson as a primality test for large numbers: $(p-1)!$ is far too large to evaluate, so the theorem is correct but impractical. In contests use Wilson to simplify products, not as a primality test.

7.5. Cấp của một số modulo n — The order of a number modulo n

ĐỊNH NGHĨA 7.16 (Cấp của một số) / DEFINITION 7.16 (multiplicative order) — Cho $\gcd(a, n) = 1$. Cấp của a modulo n , ký hiệu $\text{ord}_n(a)$, là số nguyên dương d nhỏ nhất sao cho $a^d \equiv 1 \pmod{n}$. Theo Định lý Euler số d như vậy tồn tại và $d \leq \varphi(n)$.

Let $\gcd(a, n) = 1$. The order of a modulo n , written $\text{ord}_n(a)$, is the least positive integer d with $a^d \equiv 1 \pmod{n}$. By Euler's theorem such d exists and $d \leq \varphi(n)$.

ĐỊNH LÝ 7.17 (Tính chất đặc trưng của cấp) / THEOREM 7.17 (characterisation of the order) — Cho $\gcd(a, n) = 1$ và $d = \text{ord}_n(a)$. Với mọi số nguyên $k \geq 0$: $a^k \equiv 1 \pmod{n}$ khi và chỉ khi $d \mid k$.

Let $\gcd(a, n) = 1$ and $d = \text{ord}_n(a)$. For every integer $k \geq 0$: $a^k \equiv 1 \pmod{n}$ if and only if $d \mid k$.

Chứng minh. / Proof.

Nếu $k = dq$ thì $a^k = (a^d)^q \equiv 1$. Ngược lại, giả sử $a^k \equiv 1$. Chia $k = dq + r$ với $0 \leq r < d$. Khi đó $1 \equiv a^k = (a^d)^q a^r \equiv a^r \pmod{n}$.

If $k = dq$ then $a^k = (a^d)^q \equiv 1$. Conversely, assume $a^k \equiv 1$ and divide $k = dq + r$ with $0 \leq r < d$. Then $1 \equiv a^k = (a^d)^q a^r \equiv a^r \pmod{n}$.

Vì d là số nguyên dương nhỏ nhất có $a^d \equiv 1$ và $r < d$ nên r không thể dương; vậy $r = 0$, tức $d \mid k$.

Since d is the least positive integer with $a^d \equiv 1$ and $r < d$, r cannot be positive; so $r = 0$, i.e. $d \mid k$.

■

HỆ QUẢ 7.18 (Cấp chia φ) / COROLLARY 7.18 (the order divides φ) — $\text{ord}_n(a)$ là ước của $\varphi(n)$. Với p nguyên tố và $p \nmid a$, $\text{ord}_p(a)$ là ước của $p-1$. Nếu $a^k \equiv 1 \pmod{n}$ và $a^l \equiv 1 \pmod{n}$ thì $a^{\gcd(k, l)} \equiv 1 \pmod{n}$.

$\text{ord}_n(a)$ divides $\varphi(n)$. For a prime p with $p \nmid a$, $\text{ord}_p(a)$ divides $p-1$. If $a^k \equiv 1$ and $a^l \equiv 1 \pmod{n}$ then $a^{\gcd(k, l)} \equiv 1 \pmod{n}$.

Chứng minh. / Proof.

Hai ý đầu là Định lý 7.17 với $k = \varphi(n)$ (Định lý Euler) và $k = p-1$ (Fermat). Ý thứ ba: $\text{ord}_n(a)$ chia cả k và l nên chia $\gcd(k, l)$; lại theo Định lý 7.17, $a^{\gcd(k, l)} \equiv 1$.

The first two statements are Theorem 7.17 with $k = \varphi(n)$ (Euler) and $k = p-1$ (Fermat). For the third, $\text{ord}_n(a)$ divides both k and l , hence divides $\gcd(k, l)$; by Theorem 7.17 again $a^{\gcd(k, l)} \equiv 1$.

■

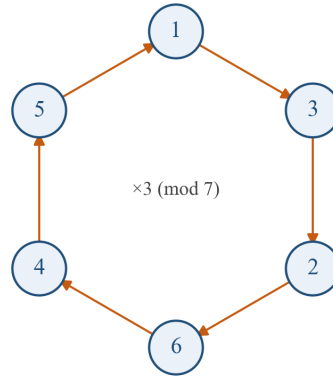
TÍNH CHẤT 7.19 (Cấp của lũy thừa) / PROPERTY 7.19 (order of a power) — Cho $\gcd(a, n) = 1$, $d = \text{ord}_n(a)$ và $k \in \mathbb{Z}^+$. Khi đó $\text{ord}_n(a^k) = d/\gcd(d, k)$.

Let $\gcd(a, n) = 1$, $d = \text{ord}_n(a)$ and $k \in \mathbb{Z}^+$. Then $\text{ord}_n(a^k) = d/\gcd(d, k)$.

Chứng minh. / Proof.

Đặt $g = \gcd(d, k)$. Theo Định lý 7.17, $(a^k)^t \equiv 1$ khi và chỉ khi $d \mid kt$, tức $(d/g) \mid (k/g)t$. Vì $\gcd(d/g, k/g) = 1$ nên điều kiện này tương đương $(d/g) \mid t$. Số t dương nhỏ nhất là d/g .

Put $g = \gcd(d, k)$. By Theorem 7.17, $(a^k)^t \equiv 1$ iff $d \mid kt$, i.e. $(d/g) \mid (k/g)t$. Since $\gcd(d/g, k/g) = 1$, this is equivalent to $(d/g) \mid t$. The least positive t is d/g . ■



Hình 7.4. Phép nhân với 3 modulo 7 đi vòng qua cả sáu lớp dư khác 0: 1, 3, 2, 6, 4, 5, rồi về 1. Vậy $\text{ord}_7(3) = 6$.

Figure 7.4. Multiplication by 3 modulo 7 runs round all six non-zero residues: 1, 3, 2, 6, 4, 5, then back to 1. Hence $\text{ord}_7(3) = 6$.

PHÂN TÍCH / ANALYSIS — Đặt $g = \gcd(2^a - 1, 2^b - 1)$ và xét số lẻ g . Cả hai điều $2^a \equiv 1$ và $2^b \equiv 1$ xảy ra modulo g , nên cấp của 2 modulo g chia a và b (Định lý 7.17), do đó chia $\gcd(a, b)$. Phép chứng minh đảo chiều bằng chia hết đại số.

Put $g = \gcd(2^a - 1, 2^b - 1)$, an odd number. Both $2^a \equiv 1$ and $2^b \equiv 1$ hold modulo g , so the order of 2 modulo g divides a and b (Theorem 7.17), hence divides $\gcd(a, b)$. The reverse direction is algebraic divisibility.

VÍ DỤ 7.9 (Cấp và gcd) / EXAMPLE 7.9 (Order and gcd) — Chứng minh rằng với mọi $a, b \in \mathbb{Z}^+$: $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a, b)} - 1$.

Prove that for all $a, b \in \mathbb{Z}^+$: $\gcd(2^a - 1, 2^b - 1) = 2^{\gcd(a, b)} - 1$.

Lời giải. / Solution.

- Đặt $e = \gcd(a, b)$ và $g = \gcd(2^a - 1, 2^b - 1)$. Vì $e \mid a$ nên $2^e - 1 \mid (2^e)^{a/e} - 1 = 2^a - 1$; tương tự $2^e - 1 \mid 2^b - 1$. Vậy $2^e - 1 \mid g$.
Put $e = \gcd(a, b)$ and $g = \gcd(2^a - 1, 2^b - 1)$. Since $e \mid a$, we have $2^e - 1 \mid (2^e)^{a/e} - 1 = 2^a - 1$; likewise $2^e - 1 \mid 2^b - 1$. So $2^e - 1 \mid g$.
- Ngược lại g lẻ nên $\gcd(2, g) = 1$ và $\text{ord}_g(2)$ tồn tại. Từ $2^a \equiv 1$ và $2^b \equiv 1 \pmod{g}$, Hệ quả 7.18 cho $2^{\gcd(a, b)} \equiv 2^e \equiv 1 \pmod{g}$, tức $g \mid 2^e - 1$.
Conversely g is odd, so $\gcd(2, g) = 1$ and $\text{ord}_g(2)$ exists. From $2^a \equiv 1$ and $2^b \equiv 1 \pmod{g}$, Corollary 7.18 gives $2^{\gcd(a, b)} \equiv 2^e \equiv 1 \pmod{g}$, i.e. $g \mid 2^e - 1$.

Hai số nguyên dương chia hết lẫn nhau nên bằng nhau: $g = 2^e - 1$.

Two positive integers dividing each other are equal: $g = 2^e - 1$. ■

PHÂN TÍCH / ANALYSIS — Gọi p là ước nguyên tố nhỏ nhất của $n > 1$. Từ $n \mid 2^n - 1$ có $2^n \equiv 1 \pmod{p}$, nên $\text{ord}_p(2)$ chia n . Mặt khác $\text{ord}_p(2)$ chia $p - 1$. Mọi ước nguyên tố của $p - 1$ đều nhỏ hơn p , mà n không có ước nguyên tố nào nhỏ hơn p ; điều đó dẫn tới mâu thuẫn.

Let p be the smallest prime divisor of $n > 1$. From $n \mid 2^n - 1$ we get $2^n \equiv 1 \pmod{p}$, so $\text{ord}_p(2)$ divides n . Also $\text{ord}_p(2)$ divides $p - 1$. Every prime divisor of $p - 1$ is smaller than p , yet n has no prime divisor smaller than p ; this leads to a contradiction.

VÍ DỤ 7.10 (Ước nguyên tố nhỏ nhất và cấp) / EXAMPLE 7.10 (Smallest prime factor and order) — Tìm mọi số nguyên dương n sao cho $n \mid 2^n - 1$.

Find all positive integers n with $n \mid 2^n - 1$.

Lời giải. / Solution.

1. $n = 1$ thỏa mãn. Giả sử $n > 1$ thỏa mãn và gọi p là ước nguyên tố nhỏ nhất của n . Vì $2^n - 1$ lẻ nên n lẻ, p lẻ, và $\text{gcd}(2, p) = 1$.

$n = 1$ works. Suppose $n > 1$ works and let p be its smallest prime divisor. Since $2^n - 1$ is odd, n is odd, p is odd and $\text{gcd}(2, p) = 1$.

2. Đặt $d = \text{ord}_p(2)$. Từ $p \mid n \mid 2^n - 1$ có $2^n \equiv 1 \pmod{p}$, nên $d \mid n$ theo Định lý 7.17. Theo Fermat $2^{p-1} \equiv 1 \pmod{p}$, nên $d \mid p - 1$.

Put $d = \text{ord}_p(2)$. From $p \mid n \mid 2^n - 1$ we have $2^n \equiv 1 \pmod{p}$, so $d \mid n$ by Theorem 7.17. By Fermat $2^{p-1} \equiv 1 \pmod{p}$, so $d \mid p - 1$.

3. Vậy $d \mid \text{gcd}(n, p - 1)$. Mọi ước nguyên tố của $p - 1$ nhỏ hơn p , trong khi mọi ước nguyên tố của n đều $\geq p$. Do đó $\text{gcd}(n, p - 1) = 1$, suy ra $d = 1$.

So $d \mid \text{gcd}(n, p - 1)$. Every prime divisor of $p - 1$ is less than p , while every prime divisor of n is at least p . Hence $\text{gcd}(n, p - 1) = 1$ and $d = 1$.

4. $d = 1$ nghĩa là $2^1 \equiv 1 \pmod{p}$, tức $p \mid 1$, vô lý. Vậy không có $n > 1$ thỏa mãn.

$d = 1$ means $2 \equiv 1 \pmod{p}$, i.e. $p \mid 1$, absurd. Hence no $n > 1$ works.

Vậy $n = 1$ là số duy nhất.

Hence $n = 1$ is the only solution. ■

NHẬN XÉT / REMARK — Cùng lập luận cho kết quả tổng quát: nếu p là ước nguyên tố nhỏ nhất của n , $\text{gcd}(a, p) = 1$ và $n \mid a^n - 1$ thì $p \mid a - 1$. Cần chọn ước nguyên tố nhỏ nhất để có $\text{gcd}(n, p - 1) = 1$.

The same argument gives the general statement: if p is the smallest prime divisor of n , $\text{gcd}(a, p) = 1$ and $n \mid a^n - 1$, then $p \mid a - 1$. Take the smallest prime divisor so that $\text{gcd}(n, p - 1) = 1$.

LỖI HAY GẶP / COMMON MISTAKE — Nhầm $\text{ord}_p(a)$ với $p - 1$: cấp của a chỉ là ước của $p - 1$. Ví dụ $\text{ord}_7(2) = 3$ vì $2^3 = 8 \equiv 1 \pmod{7}$, trong khi $p - 1 = 6$.

Confusing $\text{ord}_p(a)$ with $p - 1$: the order of a only divides $p - 1$. For example $\text{ord}_7(2) = 3$ since $2^3 = 8 \equiv 1 \pmod{7}$, while $p - 1 = 6$.

NHẬN XÉT / REMARK — Chu kỳ thập phân. Nếu $\text{gcd}(n, 10) = 1$ thì độ dài chu kỳ của $1/n$ bằng $\text{ord}_n(10)$, vì $10^d \equiv 1 \pmod{n}$ khi và chỉ khi $1/n = t/(10^d - 1)$ với t nguyên, tức $1/n$ lặp sau d chữ số. Ví dụ $1/7 = 0,(142857)$ có chu kỳ $6 = \text{ord}_7(10)$, còn $1/41 = 0,(02439)$ có chu kỳ $5 = \text{ord}_{41}(10)$.

Decimal period. If $\gcd(n, 10) = 1$ then the period length of $1/n$ equals $\text{ord}_n(10)$, because $10^d \equiv 1 \pmod{n}$ exactly when $1/n = t/(10^d - 1)$ for an integer t , i.e. $1/n$ repeats after d digits. For example $1/7 = 0.(142857)$ has period $6 = \text{ord}_7(10)$, while $1/41 = 0.(02439)$ has period $5 = \text{ord}_{41}(10)$.

7.6. Thặng dư bình phương sơ cấp và số nguyên tố dạng $4k + 1$ — Elementary quadratic residues and primes of the form $4k + 1$

ĐỊNH NGHĨA 7.20 (Thặng dư bình phương) / DEFINITION 7.20 (quadratic residue) —

Cho p nguyên tố lẻ và $p \nmid a$. Số a gọi là thặng dư bình phương modulo p nếu phương trình $x^2 \equiv a \pmod{p}$ có nghiệm; ngược lại gọi là không thặng dư bình phương.

Let p be an odd prime and $p \nmid a$. The number a is a quadratic residue modulo p if $x^2 \equiv a \pmod{p}$ is solvable; otherwise it is a non-residue.

ĐỊNH LÝ 7.21 (-1 là thặng dư bình phương) / THEOREM 7.21 (-1 as a quadratic residue) —

Cho p nguyên tố lẻ. Số -1 là thặng dư bình phương modulo p khi và chỉ khi $p \equiv 1 \pmod{4}$.

Let p be an odd prime. The number -1 is a quadratic residue modulo p if and only if $p \equiv 1 \pmod{4}$.

Chứng minh. / Proof.

Giả sử $x^2 \equiv -1 \pmod{p}$. Khi đó $p \nmid x$, và theo Fermat $x^{p-1} \equiv 1$. Mặt khác $x^{p-1} = (x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2}$. Vậy $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$; vì $p > 2$ nên $-1 \not\equiv 1$, buộc $(p-1)/2$ chẵn, tức $p \equiv 1 \pmod{4}$.

Suppose $x^2 \equiv -1 \pmod{p}$. Then $p \nmid x$ and by Fermat $x^{p-1} \equiv 1$. On the other hand $x^{p-1} = (x^2)^{(p-1)/2} \equiv (-1)^{(p-1)/2}$. So $(-1)^{(p-1)/2} \equiv 1 \pmod{p}$; since $p > 2$ we have $-1 \not\equiv 1$, which forces $(p-1)/2$ to be even, i.e. $p \equiv 1 \pmod{4}$.

Ngược lại, nếu $p \equiv 1 \pmod{4}$ thì $p = 4k + 1$ và $(p+1)/2 = 2k + 1$ lẻ. Hệ quả 7.15 cho $((p-1)/2)!^2 \equiv -1 \pmod{p}$, nên $x = ((p-1)/2)!$ là nghiệm của $x^2 \equiv -1$.

Conversely, if $p \equiv 1 \pmod{4}$ then $p = 4k + 1$ and $(p+1)/2 = 2k + 1$ is odd. Corollary 7.15 gives $((p-1)/2)!^2 \equiv -1 \pmod{p}$, so $x = ((p-1)/2)!$ solves $x^2 \equiv -1$. ■

HỆ QUẢ 7.22 (Ước nguyên tố của tổng hai bình phương) / COROLLARY 7.22 (prime divisors of a sum of two squares) —

Cho a, b nguyên tố cùng nhau và p là ước nguyên tố lẻ của $a^2 + b^2$. Khi đó $p \equiv 1 \pmod{4}$. Nếu $p \equiv 3 \pmod{4}$ và $p \mid x^2 + y^2$ thì $p \mid x$ và $p \mid y$.

Let a, b be coprime and p an odd prime divisor of $a^2 + b^2$. Then $p \equiv 1 \pmod{4}$. If $p \equiv 3 \pmod{4}$ and $p \mid x^2 + y^2$ then $p \mid x$ and $p \mid y$.

Chứng minh. / Proof.

Nếu $p \mid b$ thì từ $p \mid a^2 + b^2$ suy ra $p \mid a$, trái với $\gcd(a, b) = 1$. Vậy $p \nmid b$, tồn tại nghịch đảo b' của b modulo p và $(ab')^2 \equiv a^2b'^2 \equiv -b^2b'^2 \equiv -1 \pmod{p}$. Theo Định lý 7.21, $p \equiv 1 \pmod{4}$.

If $p \mid b$ then $p \mid a^2 + b^2$ gives $p \mid a$, contradicting $\gcd(a, b) = 1$. So $p \nmid b$, b has an inverse b' modulo p , and $(ab')^2 \equiv a^2b'^2 \equiv -b^2b'^2 \equiv -1 \pmod{p}$. By Theorem 7.21, $p \equiv 1 \pmod{4}$.

Phần hai: nếu $p \nmid y$ thì cùng lập luận cho -1 là thặng dư bình phương, mâu thuẫn với $p \equiv 3 \pmod{4}$. Vậy $p \mid y$, rồi $p \mid x^2$, nên $p \mid x$.

For the second part: if $p \nmid y$ the same argument makes -1 a quadratic residue, contradicting $p \equiv 3 \pmod{4}$. Hence $p \mid y$, and then $p \mid x^2$, so $p \mid x$. ■

PHÂN TÍCH / ANALYSIS — Muốn chứng minh vô hạn số nguyên tố dạng $4k + 1$ theo kiểu Euclid cho số nguyên tố: giả sử chỉ có hữu hạn $p_1, \dots, p_r$, rồi dựng số N mà mọi ước nguyên tố của nó phải $\equiv 1 \pmod{4}$ nhưng khác các p_i . Hệ quả 7.22 cho tổng hai bình phương nguyên tố cùng nhau, nên chọn $N = (2p_1 \dots p_r)^2 + 1$.

To prove there are infinitely many primes $4k + 1$, argue as Euclid did for primes: assume only $p_1, \dots, p_r$ exist, then build N whose prime divisors must be $\equiv 1 \pmod{4}$ yet differ from every p_i . Corollary 7.22 handles coprime sums of two squares, so take $N = (2p_1 \dots p_r)^2 + 1$.

VÍ DỤ 7.11 (Euclid cho $4k + 1$) / EXAMPLE 7.11 (Euclid's argument for $4k + 1$) —

Chứng minh có vô hạn số nguyên tố dạng $4k + 1$.

Prove that there are infinitely many primes of the form $4k + 1$.

Lời giải. / Solution.

- Giả sử chỉ có hữu hạn số nguyên tố dạng $4k + 1$, là $p_1, \dots, p_r$ ($r \geq 1$ vì 5 là một số như vậy). Đặt $P = 2p_1 \dots p_r$ và $N = P^2 + 1$. N lẻ và $N > 1$.

Suppose there are only finitely many primes $4k + 1$, namely $p_1, \dots, p_r$ ($r \geq 1$ since 5 is one).

Put $P = 2p_1 \dots p_r$ and $N = P^2 + 1$. N is odd and $N > 1$.

- Gọi q là ước nguyên tố của N . Vì $q \mid P^2 + 1^2$ và $\gcd(P, 1) = 1$ nên $q \equiv 1 \pmod{4}$ theo Hệ quả 7.22. Do đó q là một trong các p_i .

Let q be a prime divisor of N . Since $q \mid P^2 + 1^2$ and $\gcd(P, 1) = 1$, Corollary 7.22 gives $q \equiv 1 \pmod{4}$. So q is one of the p_i .

- Nhưng $p_i \mid P$ nên $p_i \mid P^2$, suy ra $p_i \nmid P^2 + 1 = N$. Mâu thuẫn. Vậy có vô hạn số nguyên tố dạng $4k + 1$.

But $p_i \mid P$ gives $p_i \mid P^2$, so $p_i \nmid P^2 + 1 = N$. Contradiction. Hence there are infinitely many primes $4k + 1$. ■

NHẬN XÉT / REMARK — Cùng phương pháp cho nhiều dạng khác: nếu $q \mid P^4 + 1$ thì $\text{ord}_q(P) = 8$ nên $q \equiv 1 \pmod{8}$, dẫn tới vô hạn số nguyên tố dạng $8k + 1$ (Bài tự luyện). Với dạng $4k + 3$ không dùng được tổng hai bình phương, nhưng $4(p_1 \dots p_r) - 1$ có một ước nguyên tố dạng $4k + 3$ (Chương 6).

The same method works for other forms: if $q \mid P^4 + 1$ then $\text{ord}_q(P) = 8$, so $q \equiv 1 \pmod{8}$, which leads to infinitely many primes $8k + 1$ (practice problem). For the form $4k + 3$ sums of two squares are no help, but $4(p_1 \dots p_r) - 1$ has a prime divisor of the form $4k + 3$ (Chapter 6).

PHÂN TÍCH / ANALYSIS — Phương trình $x^2 + y^2 = 7z^2$ có vế phải chia hết cho $7 \equiv 3 \pmod{4}$. Theo Hệ quả 7.22, $7 \mid x$ và $7 \mid y$. Thế vào thì z cũng chia hết cho 7, và mọi bộ nghiệm đều chia được cho 7 mãi: dấu hiệu của lùi vô hạn.

The equation $x^2 + y^2 = 7z^2$ has right side divisible by $7 \equiv 3 \pmod{4}$. By Corollary 7.22, $7 \mid x$ and $7 \mid y$. Substituting shows $7 \mid z$ as well, so every solution can be divided by 7 forever: the signature of infinite descent.