Number theoretical barbecue

Antoine Chambert-Loir

Université de Paris
E-mail: *antoine.chambert-loir@u-paris.fr*

1. Congruences, prime numbers

Exercise **(1.1)**. — *a*) Let n be an integer such that $n \equiv -1 \pmod 4$. Prove that n has some prime factor p such that $p \equiv -1 \pmod 4$.

b) Prove that there are infinitely many primes p such that $p \equiv -1 \pmod 4$.

c) Prove that there are infinitely many prime numbers p such that $p \equiv -1 \pmod 3$.

d) Let n be an integer and let p be a prime factor of n^2+1. Using question *e*) of exercise 1.3, prove that $p = 2$ or $p \equiv 1 \pmod 4$.

e) Prove that there are infinitely many prime numbers p such that $p \equiv 1 \pmod 4$.

f) Let n be an integer and let p be a prime factor of n^2+3 such that $p > 3$. Using that $p \equiv 1 \pmod 3$ (question *a*) of exercise 1.4), prove that there are infinitely many prime numbers p such that $p \equiv 1 \pmod 3$.

Remark: A theorem of Dirichlet (1837) asserts that if a, n are coprime integers, there are infinitely many prime numbers p such that $p \equiv a \pmod n$. The case $a = 1$ admits an elementary proof in the spirit of this exercise, but Dirichlet's proof requires complex analysis.

Exercise **(1.2)**. — *a*) Let $x \geqslant$ be an integer. Let m, n, q, r be positive integers such that $n = mq + r$, with $n, m \geqslant 1$. Prove that $x^r - 1$ is the remainder of the euclidean division of $x^n - 1$ by $x^m - 1$.

b) Let m, n be strictly positive integers and let $d = \gcd(m, n)$. Prove that the greatest common divisor of $x^m - 1$ and $x^n - 1$ is equal to $x^d - 1$.

Let (F_n) be the Fibonacci sequence, defined by $\mathrm{F}_0 = 0$, $\mathrm{F}_1 = 1$ and $\mathrm{F}_{n+1} = \mathrm{F}_n + \mathrm{F}_{n-1}$ for $n \geqslant 1$.

c) Let m, n be integers such that $m, n \geqslant 1$. Prove the identities

$$\mathrm{F}_{m+n} = \mathrm{F}_{m-1}\mathrm{F}_n + \mathrm{F}_m\mathrm{F}_{n+1} \quad \text{and} \quad \mathrm{F}_{n-1}\mathrm{F}_{n+1} - \mathrm{F}_n^2 = (-1)^n.$$

d) Let m, n be strictly positive integers. Prove that $\gcd(\mathrm{F}_m, \mathrm{F}_n) = \gcd(\mathrm{F}_n, \mathrm{F}_{m+n})$.

e) Let $d = \gcd(m, n)$. Prove that $\gcd(\mathrm{F}_m, \mathrm{F}_n) = \mathrm{F}_d$.

Exercise **(1.3)** (Fermat, Wilson, Euler…) — Let p be a prime number.

a) Let a, b be integers and assume that p does not divide a. Prove that there exists a unique integer x such that $0 \leqslant x \leqslant p-1$ and p divides $ax+b$. In particular, there is a unique integer x (the "inverse" of a modulo p) such that $ax \equiv 1 \pmod{p}$ and $1 \leqslant x \leqslant p-1$.

b) Prove *Fermat's little theorem:* for every integer a such that p does not divide a, one has $a^{p-1} \equiv 1 \pmod{p}$. (*One possibility is to show that the products* $1 \cdot 2 \dots (p-1)$ *and* $a \cdot 2a \cdot\cdot (p-1)a$ *are equal modulo* p.)

c) Prove *Wilson's congruence:* the product $1 \cdot 2 \dots (p-1)$ is congruent to -1 modulo p. (*In the product, match each integer* m *with its inverse modulo* p*, unless they coincide.*)

d) Assume that $p \equiv 3 \pmod{4}$. Prove that there does not exist an integer a such that a^2+1 is divisible by p.

e) Assume that $p \equiv 1 \pmod{4}$, prove that there exists an integer a such that a^2+1 is divisible by p. Can you turn your proof into a feasible method? (*In Wilson's congruence, match* m *with* $p-m$.)

f) Still assume that $p \equiv 1 \pmod{4}$. For $x \in \{1, \dots, p-1\}$, what can be the values of $x^{(p-1)/4}$ modulo p? With what frequencies are they obtained. Deduce from this a practical way to solve the question of the preceding question. (*You may assume that the random generator of your computer is not flawed, or that you have a fair dice at your disposal.*)

g) Assume that p is odd and let $a \in \{1, \dots, p-1\}$. Prove *Euler's criterion:* there exists $x \in \{1, \dots, p-1\}$ such that $x^2 - a$ is divisible by p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

Exercise **(1.4)**. — Let p be a prime number such that $p \geqslant 3$.

a) Prove the equivalence between the three properties:

(1) There exists an integer u such that p divides u^2+u+1;
(2) There exists an integer a such that p divides a^2+3;
(3) One has $p \equiv 1 \pmod{3}$.

b) Let m be an integer such that $p = 2^m + 1$ is a prime number. Prove that m is a power of 2: there exists an integer n such that $p = 2^{2^n} + 1$.

c) Writing $F_n = 2^{2^n} + 1$, prove that F_1, F_2, F_3, F_4 are indeed prime numbers. Prime numbers of this form are called *Fermat primes.*

d) Prove that F_5 is divisible by 641 (hence is not a prime number). (*You can compute* F_5 *and check it by hand, but there is a lighter argument using congruences.*)

e) Let n be an integer. Prove that F_n is a prime number if and only if $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ (*Pépin's test*). (*If* F_n *is prime, use question* a*) and Euler's criterion from exercise 1.3 to prove the relation. In the other direction, prove that* $3^a \equiv 1 \pmod{F_n}$ *if and only if* a *is a multiple of* $F_n - 1$ *and conclude that* F_n *is a prime number.*)

Remark : F_1, F_2, F_3, F_4 *are the only known Fermat primes, and it is believed that there are no other. According to Wikipedia (2021), it is known that* F_n *is not prime if* $5 \leqslant n \leqslant 32$*, the*

primality of F_{33} *is unknown, and* $F_{18\,233\,954}$ *is the largest number of this kind which is known to be composite.*

f) From the relation $F_0 \dots F_n = F_{n+1} - 2$, prove that Fermat numbers are pairwise coprime. In particular, the set of prime factors of Fermat numbers F_n is infinite.

Exercise **(1.5)** (Sophie Germain's theorem). — Let p be an odd prime number and assume that $q = 2p + 1$ is again a prime number. *The goal of the exercise is to prove the "first case of Fermat's last theorem for p", namely that if* x, y, z *are integers such that* $x^p + y^p + z^p = 0$*, then* p *divides at least one of* x, y, z.

The proof runs by contradiction, considering such a triple where $p \nmid xyz$.

a) Reduce to the case where x, y, z are pairwise coprime.

b) In the expression

$$-x^p = y^p + y^p = (y + z)(y^{p-1} - y^{p-2}z + \cdots + z^{p-1}),$$

prove that both factors of the right hand side are coprime.

c) Prove that there exist coprime integers a, u such that $y + z = a^p$ and $x = au$.

d) By symmetry, there exist coprime integers b, v, such that $x + z = b^p$ and $y = bv$, and coprime integers c, w such that $x + y = c^p$ and $z = cw$.

e) Considering that $x^p + y^p + z^p = 0 \pmod q$, prove that q divides xyz.
By symmetry, you may assume that q divides x.

f) Prove that q does not divide b nor c. Then prove that q divides a.

g) Prove that $p \equiv \pm 1 \pmod q$, and observe that this is impossible.

2. Diophantine equations and infinite descent

Exercise **(2.1)** (Pythagorean triples). — *In this problem, you will determine all "pythagorean triples", that is all triples* (a, b, c) *of integers which satisfy* $a^2 + b^2 = c^2$*, hence are the sizes of a rectangle triangle.*

First assume that a, b, c *are mutually coprime (in which say we say that the triple* (a, b, c) *is primitive.*

a) Prove that a, b are coprime, as well as a, c and b, c.

b) Prove that c is odd, and that exactly one of a, b is even.
Assume also that b is even (so that a is odd and c is odd).

c) Prove that the gcd of $c - a, c + a$ is equal to 2.

d) Writing $b^2 = (c - a)(c + a)$, prove that there exists integers u, v such that $c + a = 2u^2$ and $c - a = 2v^2$. Conclude that $a = u^2 - v^2$, $b = 2uv$ and $c = u^2 + v^2$.

e) Describe all pythagorean triples (without assuming that a, b, c are coprime, nor than b is even).

f) Compare the obtained formulas with the parameterization of a circle given in the lectures.

Exercise **(2.2)**. — Fermat for $n = 4$ *In this exercise, you will prove that the equation* $a^4+b^4 = c^2$ *has no solutions in strictly positive integers. In particular, the Fermat equation for* $n = 4$ *has no nontrivial solutions.*

The proof runs by contradiction, and considers a putative triple (a, b, c) *such that* c *is minimal.*

a) Let d be the gcd of a, b. Prove that d^2 divides c. Using the minimality assumption, conclude that $d = 1$, hence that a, b are coprime.

b) Using the solution of pythagorean triples, reduce to the case where there are coprime integers u, v such that $a^2 = u^2 - v^2$, $b^2 = 2uv$ and $c^2 = u^2 + v^2$.

c) Prove that u is odd and v is even.

d) Observe that (v, a, u) is a primitive pythagorean triple and find coprime strictly positive integers x, y such that $b^2 = 4xy(x^2 + y^2)$.

e) Prove that there exists integers m, n, p such that $x = m^2$, $y = n^2$ and $x^2 + y^2 = p^2$, and observe that this contradicts the minimality assumption made at the beginning of the proof.

f) In an analogous manner, prove that the diophantine equation $x^4 - y^4 = z^2$ has no solutions in strictly positive integers.

Exercise **(2.3)**. — In this exercise, you will show that the diophantine equation $y^2 = x^3 - x$ (which represents an "elliptic curve") has no other solutions in rational number than $(0, 0)$ and $(0, \pm 1)$.

We consider such a solution (x, y) and let $c \geqslant 1$ be a minimal common denominator to x and y, let $a = cx$ and $b = cy$, so that (a, b, c) are coprime integers satisfying $a^3 = ac^2 + b^2c$.

a) Prove that b, c are coprime.

b) Let d be the gcd of a, c. Prove that $c = d^3$ and that a/d is $\pm$ a perfect square. (*For every prime number* p*, analyse the multiplicity of* p *in the decomposition of* c *and* a *into prime factors.*)

c) Prove that there exists an integer v such that $b = uv$ and that $u^4 - d^4 = \pm v^2$. Using exercise 2.2, conclude.

Exercise **(2.4)**. — Let a, b be coprime integers. The goal of the exercise is to prove that every odd factor of $a^2 + 3b^2$ can be written in the form $x^2 + 3y^2$.

a) Expanding $(x + y\sqrt{-3})(a + b\sqrt{-3})$, explain and prove the identity

$$(x^2 + 3y^2)(a^2 + 3b^2) = (ax + 3by)^2 + 3(xb + ay)^2.$$

Argue by contradiction and consider the smallest odd factor m *of an integer of the form* $a^2 + 3b^2$*, where* a, b *are coprime integers, which cannot be written as* $x^2 + 3y^2$*. One has* $m \geqslant 3$.

Prove that there are integers d, u, v, x, y such that $1 \leqslant |u|, |v| < m/2$, u, v are coprime and $a = mx + du$, $b = my + dv$.

b) Prove that there exists an odd integer n such that $u^2 + 3v^2 = 4mn$ and $1 \leqslant n < m$.

c) By the minimality assumption on m, there are integers x, y such that $n = x^2 + 3y^2$. Considering $(a+b\sqrt{-3})/(x+y\sqrt{-3})$, prove that there are integers u, v such that $m = u^2+3v^2$.

Remark: This is a proof by infinite descent, and it was written as a reductio at absurdum. *However, contrary to the impossibility proofs of this problem list, the argument can be rewritten as a proof by induction.*

Exercise **(2.5)**. — In this exercise, you will solve Fermat's last theorem for $n = 3$, presumably following Euler's lost proof. Consider a triple (x, y, z) of nonzero integers such that $x^3 + y^3 = z^3$. The goal is to prove that one of x, y, z vanishes.

Arguing by contradiction, consider one such triple where $\inf(|x|, |y|, |z|$ *is minimal.*

a) Prove that x, y, z are coprime, and then that x, y are coprime, as well as x, z and y, z.

b) Explain how can assume that z is even. In this case, prove that one can write $x = u + v$ and $y = u - v$, where u, v are coprime integers, and that $2u(u^2 + 3v^2)$ is a cube.

c) Prove that $\gcd(2u, u^2 + 3v^2)$ is 1 or 3.

d) If $\gcd(2u, u^2 + 3v^2) = 1$, then $2u$ and $u^2 + 3v^2$ are cubes. Using exercise 2.4, prove that there are integers a, b such that $u^2 + 3v^2 = (a^2 + 3b^2)^3$. Using algebra, obtain a smaller solution.

e) If $\gcd(2u, u^2 + 3v^2) = 3$, prove that 12 divides u, but neither 3 nor 4 divides v. Writing $u = 3w$, prove that $2w$ and $v^2 + 3w^2$ are cubes. As in the previous question, prove that there are integers a, b such that $v^2 + 3w^2 = (a^2 + 3b^2)^3$, and obtain a contradiction.

3. Diophantine approximation

Exercise **(3.1)** (Dirichlet's theorem). — Let α be a real number and let Q be an integer such that $Q \geqslant 1$.

a) For $n \in \{0, 1, \dots, Q\}$, let $x_n = n\alpha - \lfloor n\alpha \rfloor$. Prove that there exists two indices m, n such that $0 \leqslant m < n \leqslant Q$ and an integer $k \in \{1, \dots, Q\}$ such that x_m, x_n both belong to the interval $[(k-1)/Q, k/Q[$. (*Use Dirichlet's Schubfachprinzip!*)

b) Conclude that there exist integers p, q such that $1 \leqslant q \leqslant Q$ and $|q\alpha - p| < 1/Q$.

Exercise **(3.2)**. — Let α be an irrational real number. One sets $c(\alpha)$ to be the inferior limit $|(q\alpha - p)q|$, where p, q are integers and $q \to +\infty$.

a) Using Dirichlet's theorem (exercise 3.1), prove that $c(\alpha) \leqslant 1$.

b) Assume that α is the golden ratio, the positive root of the equation $f(T) = T^2 - T - 1 = 0$; denote with β the other root. Prove that $c(\alpha) \geqslant 1/\sqrt{5}$. (*Consider p_n, q_n are integers such that $q_n \to +\infty$ and $|(q_n\alpha - p_n)q_n| \to c(\alpha)$, observe that $q_n^2|f(p_n/q_n)| \geqslant 1$.*)

c) Assume that α is the solution of an irreducible quadratic equation $f(T) = aT^2+bT+c = 0$, where a, b, c are integers, so that $b^2 - 4ac \neq 0$. Prove that $c(\alpha) \geqslant 1/\sqrt{|b^2 - 4ac|}$.

It is a theorem of Klaus Roth (1955) that if α is the solution of any irreducible polynomial equation of degree $\geqslant 2$, then $c(\alpha)$ is strictly positive.

d) Let (F_n) be the Fibonacci sequence, defined by $F_0 = 0$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for $n \geqslant 1$. Prove that $F_n = (\alpha^n - \beta^n)/(\alpha - \beta)$, where α is the golden ratio and $\beta = -1/\alpha$. Considering the pairs (F_{n+1}, F_n), deduce that $c(\alpha) = 1/\sqrt{5}$.

4. Quadratic forms and the Pell equation

Exercise **(4.1)**. — Let a, b, c be real numbers such that $a, c > 0$ and discriminant $\Delta = b^2 - 4ac < 0$. and let $f(x, y) = ax^2 + bxy + cy^2$ be the associated "quadratic form".

a) Prove that $f(x, y) > 0$ for all non-zero $(x, y) \in \mathbf{R}^2$. ("q is positive definite.")

b) Prove that there exists a pair $(u, v) \in \mathbf{Z}^2$, distinct from $(0, 0)$, such that $m = f(u, v)$ is minimal.

The goal is to prove that $m \leqslant \sqrt{-\Delta/3}$.

c) Prove that u, v are coprime.

d) Explain how to perform a unimodular change of variables so that $m = a$. (Check that such a change of variables does not change the discriminant.)

e) Making the change of variable $X = x + py$, $Y = y$, for some well chosen integer p, explain how you can also assume that $|b| \leqslant a \leqslant c$.

f) Prove the desired inequality.

Exercise **(4.2)** (Primes which are sums of two squares). — *a*) Let x, y be integers such that $x^2 + y^2$ is a prime number p. Prove that $p = 2$ or that $p \equiv 1 \pmod 4$. (*Use exercise 1.3.*)

b) Let p be a prime number such that $p \equiv 1 \pmod 4$. Let $u \in \mathbf{Z}$ be such that p divides $u^2 + 1$ (exercise 1.3). Consider the quadratic form given by $f(x, y) = (px + uy)^2 + y^2$ Choose a nonzero pair (x, y) of integers such that $m = f(x, y)$ is minimal. Prove that p divides m.

c) Using the result of exercise 4.1, prove that $m = p$. Conclude that p is a sum of two squares.

Exercise **(4.3)** (Bhramagupta-Pell-Fermat equation). — Let $d \geqslant 1$ be any integer which is not a square.

a) Applying Dirichlet's theorem (exercise 3.1) to $\sqrt{2}$, prove that there exist an integer $N \neq 0$ and increasing sequences (p_n), (q_n), with limit $+\infty$, such that $p_n^2 - dq_n^2 = N$.

b) Consider two pairs (p, q) and (u, v) such that $p^2 - dq^2 = u^2 - dv^2 = \mathrm{N}$, $p \equiv u \pmod{\mathrm{N}}$ and $q \equiv v \pmod{\mathrm{N}}$. Show that there are nonzero integers x, y such that

$$\frac{p + q\sqrt{d}}{u + v\sqrt{d}} = x + y\sqrt{d}.$$

Prove that $x^2 - dy^2 = 1$.

Among all pairs (u, v) such that $u^2 - dv^2 = 1$ and $u, v \geqslant 1$, consider the one such that u is minimal.

c) Let (x, y) be a pair of integers such that $x, y \geqslant 0$ and $x^2 - dy^2 = 1$. Prove that there exists a unique integer $n \geqslant 0$ such that $x + y\sqrt{d} = (u + v\sqrt{d})^n$.

d) Treat explicitly the cases $d = 2, 3, 5$.

e) Imagine a triangular flock of geese, one goose on the first row, two geese on the second, etc., up to n geese on the last row. After a hunter shot at them (without killing any of them), the flock splits into two similar triangular flocks, now with m rows. How many birds were there?

Exercise **(4.4)** (Markov triples). — Markov triples are triples (x, y, z) of strictly positive integers such that $x^2 + y^2 + z^2 = 3xyz$. Two Markov triples are identified if the differ by the order of its elements only.

a) Let (x, y, z) be a Markov triple. Prove that x, y, z are pairwise distinct, unless $(x, y, z) = (1, 1, 1)$ or $(x, y, z) = (1, 1, 2)$.

b) Let (x, y, z) be a Markov triple. Find another Markov triple of the form (x, y, z').

c) Assuming that x, y, z are pairwise distinct, prove that $\sup(x, y)$ lies strictly between z and z'.

Two Markov triples are called neighbours if (up to reordering) they differ by exactly one element.

d) Conclude that Markov triples consisting of pairwise distinct integers have exactly three neighbours. What happens in the remaining cases.

e) Prove that all Markov triples can be obtained from $(1, 1, 1)$ using such modifications and its two variants.

f) Draw the graph whose vertices are Markov triples (x, y, z) with $x, y, z \leqslant 500$ and in which neighbours are linked by an edge.

g) Let (x, y, z) be a Markov triple. Prove that x, y, z are coprime.

h) Let $k \geqslant 1$ be an integer. If $k \neq 1$ and $k \neq 3$, prove that the diophantine equations $x^2 + y^2 + z^2 = kxyz$ has no solution in integers besides $(0, 0, 0)$. The case $k = 3$ corresponds to Markov triples; what happens for $k = 1$?

Remark: Markov numbers are integers which appear in some Markov triple; they are the object of many unproven conjectures. For example, it is expected that Markov numbers appear as the greatest element of a exactly one Markov triple; there is also a conjecture about the

asymptotic growth of the number of Markov numbers below a bound, when this bound grows to infinity.

Some books for further reading

M. Aigner (2013), *Markov's Theorem and 100 Years of the Uniqueness Conjecture*, Springer International Publishing, Heidelberg.

M. Aigner & G. M. Ziegler (2018), *Proofs from THE BOOK*, Springer Berlin Heidelberg, Berlin, Heidelberg, sixth edition.

J. W. S. Cassels (1957), *An Introduction to Diophantine Approximation*, Cambridge Tracts in Mathematics and Mathematical Physics, No. 45, Cambridge University Press, New York.

J. W. S. Cassels (1959), *An Introduction to the Geometry of Numbers*, Springer Berlin Heidelberg, Berlin, Heidelberg.

G. H. Hardy & E. M. Wright (2008), *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford, sixth edition.

L. J. Mordell (1969), *Diophantine Equations*, Academic Press, London; New York.