

Exponential Diophantine equations

The project is prepared and presented by:
I. Klimanova, P. Kozlov, A. Miroshnikov.

Abstract

In this project we will introduce you to some exponential Diophantine equations and methods for solving them. It consists of several sections, and we recommend solving the problems in the order in which they are presented.

In Section 1 we investigate exponential Diophantine equations of the form $a^x - b^y = c$.

Section 2 is devoted to finding pairs of consecutive numbers all of whose prime divisors lie in a given set. We will show that there are finitely many such pairs, and all of them can be obtained from solutions of finitely many Pell's equations.

In Section 3 several classical and olympiad problems are presented that reduce to the generalized Pell's equation and are solved by studying prime divisors of one of the components of its solutions.

With the help of Section 4 you will learn how to solve some equations in factorial rings, and the problems of Section 6 will help you prove factoriality of rings of a certain type.

Finally, Section 5 contains several classical Lebesgue–Nagell equations, which you can solve by applying the methods described in the project.

Contents

1	On the equation $a^x - b^y = c$	2
2	On a Størmer problem	8
3	Størmer's method	22
4	Equations in factorial domains	27
5	On the equations of Lebesgue–Nagell type	34
6	Back to the proof of FTA	41

Acknowledgements.

The authors of the project would like to thank O. Nikitenko, M. Surkov, and Y. Khromin for their invaluable assistance in verifying the solutions of conference participants.

1 On the equation $a^x - b^y = c$

This section is devoted to the:

Theorem. For any positive integers $a, b \geq 2$ and c the next equation

$$a^x - b^y = c \quad (*)$$

has no more than two solutions in positive integers.

The proof of this difficult theorem is beyond the scope of this project. Instead, we will *search* and *count* all solutions to the equation (*) for specific values of positive integers a, b, c with $a, b \geq 2$.

Further, we assume that all equations below are solved in positive integers x, y .

Problem 1.1. Solve the equations (a) $2^x - 3^y = 1$; (b) $3^x - 2^y = 1$.

Solution. (a) From $3^y \not\equiv -1 \pmod{8}$ it follows that $x \leq 2$. It is left to check $x = 1, 2$.

Answer: $(2, 1)$.

(b) If $y \geq 3$ then $3^y \equiv 1 \pmod{8}$. This congruence is true iff y is divisible by 2. Let $y = 2t$ then $(3^t - 1)(3^t + 1) = 2^y$ and $3^t - 1, 3^t + 1$ are both powers of 2. It is possible iff $t = 1, y = 3$.

Answer: $(1, 1), (2, 3)$. ■

Sometimes, modular arithmetic gives us a lot of information about the structure of the solutions to the equation (*). An example of how it helps is given below:

Problem 1.2. Suppose $2^x - 3^y = c$ with positive integers c, x, y . Prove that

(a) if $x \geq 3$, then $c \equiv 5, 7 \pmod{8}$;

(b) if $c = 2^k + 3^l$ for some $k \geq 3, l \geq 1$ then there are no solutions.

Solution. Consider modulo 8. ■

Problem 1.3. Find all positive integers $c \leq 100$ such that the equation $2^x - 3^y = c$ has two solutions.

Solution. *Step 1: narrowing down c .* If $2 \mid c$ or $3 \mid c$, then $2^x - 3^y = c$ is impossible. For $x = 1$ the equation gives $3^y < 0$, while for $x = 2$ we obtain only $c \in \{1\}$ (when $y = 1$). Hence, for two solutions it is necessary that $x \geq 3$, whence by Problem 1.2a

$$c \equiv 5 \text{ or } 7 \pmod{8}.$$

Step 2: small x . A direct check for $3 \leq x \leq 9$ (that is, $2^x \leq 512$) among numbers $c \leq 100$ satisfying the conditions of Step 1 shows that only $c = 5$ and $c = 13$ have two solutions.

Step 3: excluding large x . We show that for $x \geq 10$ there are no new solutions for any of the remaining c . We work modulo $2^{10} = 1024$ and 257 (a prime; the order of 2 modulo 257 is 16, and the order of 3 is 256).

For each c we solve the congruence $3^y \equiv -c \pmod{1024}$: since the order of 3 modulo 1024 is 256, we obtain a finite set of admissible residues $y \pmod{256}$. For each such y the value $3^y + c \pmod{257}$ is fixed (the order of 3 mod 257 is also 256).

It remains to check that none of the obtained values $3^y + c \pmod{257}$ coincides with any of the 16 residues $\{2^x \pmod{257}\}$. This is a finite check, which for all admissible $c \leq 100$ gives a negative answer.

Therefore, for $x \geq 10$ the equation $2^x - 3^y = c$ has no solutions, and the answer is exhausted by $c \in \{5, 13\}$.

Answer: $c = 5, 13$. ■

Consider some particular cases of the equation (*).

Problem 1.4. Suppose that positive integers a, b, c are not pairwise coprime. Prove that the equation (*) has a finite number of solutions.

Solution. If any two numbers share a common prime divisor p , it follows from the equation that all three numbers are divisible by p . If $x, y > m = v_p(c)$ then the left side of the equation is divisible by p^{m+1} , while the right side is not. Hence one of the variables x, y is bounded from above which implies that the second variable is bounded as well. ■

Problem 1.5. Suppose every prime dividing a also divides b . Prove that the equation (*) has at most one solution.

Solution. Suppose there exist two solutions (x_1, y_1) and (x_2, y_2) such that $x_1 < x_2$, which consequently implies $y_1 < y_2$. Then

$$a^{x_1}(a^{x_2-x_1} - 1) = b^{y_1}(b^{y_2-y_1} - 1).$$

Since any prime divisor p of a also divides b , we have $v_p(a^{x_1}) = v_p(b^{y_1})$. Thus, a^{x_1} divides b^{y_1} and so $c = a^{x_1} - b^{y_1} < 0$, but $c > 0$. Contradiction. ■

Further, we assume that a, b, c are pairwise coprime. First, we pay more attention to the equation (*) with $c = 1$.

Problem 1.6. Prove that for any integer $b > 1$ the equation $2^x - b^y = 1$ has no solutions with $y > 1$.

Solution. Suppose y is even. Since b is odd, we have $b^y + 1 \equiv 2 \pmod{4}$. This implies $2^x \equiv 2 \pmod{4}$, from which it follows that $x = 1$, yielding no solutions.

Suppose y is odd. Then

$$2^x = b^y + 1 = (b + 1)(b^{y-1} - b^{y-2} + \dots - b + 1),$$

which implies that $b^{y-1} - b^{y-2} + \dots - b + 1 = 2^k$ for some integer k . However, the number $b^{y-1} - b^{y-2} + \dots - b + 1$ is odd, being a sum of an odd number of odd terms. Therefore, $b + 1 = 2^x$ and $y = 1$. ■

Definition. The *order* of z modulo M , denoted by $\text{ord}_z(M)$, is the smallest positive integer h such that $z^h \equiv 1 \pmod{M}$, provided that z and M are coprime.

Thanks to Euler's theorem, the number $\text{ord}_z(M)$ is well-defined for coprime z, M and divides $\varphi(M)$. Also, it is easy to see that if (x, y) is a solution to the equation $(*)$ with $c = 1$, then $x = \text{ord}_a(b^y)$.

Problem 1.7. Let $b = p$ be an odd prime.

(a) Prove that there is an integer v such that

$$\text{ord}_a(p^{n+1}) = \begin{cases} \text{ord}_a(p^n), & \text{if } n < v \\ p \cdot \text{ord}_a(p^n), & \text{if } n \geq v. \end{cases}$$

(b) Prove that the equation $a^x - p^y = 1$ has no more than one solution.

Solution. (a) Let $v > 0$ be the maximal power of the prime p that divides the number $a^{\text{ord}_a(p)} - 1$. Then $\text{ord}_a(p) = \dots = \text{ord}_a(p^v)$ by definition. It remains to prove the equality $\text{ord}_a(p^{n+1}) = p \cdot \text{ord}_a(p^n)$ for all $n > v$. Let us fix an arbitrary n . We shall show that the number $a^{p \cdot \text{ord}_a(p^n)} - 1$ is divisible by p^{n+1} , but is not divisible by p^{n+2} . Indeed,

$$a^{p \cdot \text{ord}_a(p^n)} - 1 = \left(a^{\text{ord}_a(p^n)}\right)^p - 1 = (1 + p^n q)^p - 1 \stackrel{(1)}{=} \sum_{i=1}^p \binom{p}{i} p^{in} q^n = p^{n+1} Q.$$

Equality (1) holds by the Binomial Theorem. Since all terms of the form $\binom{p}{k} p^{kn} q^n$ are divisible by p^{n+2} for $k > 1$, we have $Q \equiv q \not\equiv 0 \pmod{p}$ by the definition of $\text{ord}_a(p^n)$ and since all terms of the form $\binom{p}{k} p^{kn} q^n$ are divisible by p^{n+2} for $k > 1$. It remains to prove that for no m in the range $\text{ord}_a(p^n) < m < p \cdot \text{ord}_a(p^n)$ is the number $a^m - 1$ divisible by p^{n+1} . Suppose such an m exists. Then $p \cdot \text{ord}_a(p^n)$ is divisible by m , and m is divisible by $\text{ord}_a(p^n)$. However, since p is prime, this is impossible.

(b) Suppose there exist two solutions $(\text{ord}_a(p^n), n)$ and $(\text{ord}_a(p^{n+m}), n+m)$, where $m > 0$. Then by part a), we have $\text{ord}_a(p^{n+m}) = p^m \text{ord}_a(p^n)$. Thus,

$$a^{\text{ord}_a(p^{n+m})} - 1 = \left(a^{\text{ord}_a(p^n)}\right)^{p^m} - 1 = (1 + p^n)^{p^m} - 1 = p^{n+m} + Q > p^{n+m},$$

where Q represents the remaining non-zero terms from the expansion of the Binomial Theorem. ■

Problem 1.8. Prove that the equation $a^x - b^y = 1$ has no more than one solution except the case $a = 3, b = 2$.

Solution. Suppose that there are two distinct solutions. Write them so that $x < s$:

$$a^x - 1 = b^y, \quad a^s - 1 = b^{y+n}$$

for some $n > 0$. Then

$$a^s - 1 = (a^x - 1) b^n,$$

that is, $a^x - 1 \mid a^s - 1$. Let us show that this implies $x \mid s$. Let $s = qx + r$, where $0 \leq r < x$. Then

$$a^s - 1 = (a^x)^q a^r - 1 = (a^x - 1)((a^x)^{q-1} + (a^x)^{q-2} + \cdots + 1) + (a^r - 1).$$

Since $a^x - 1$ divides the left-hand side and the first summand, it also divides $a^r - 1$. But $0 \leq a^r - 1 < a^x - 1$, hence $a^r - 1 = 0$, that is, $r = 0$. Therefore, $s = kx$ for some integer $k > 1$.

Let p be an odd prime divisor of b . Since $a^x - 1 = b^y$, we have $p \mid a^x - 1$. By LTE,

$$v_p(a^{kx} - 1) = v_p(a^x - 1) + v_p(k) = v_p(b^y) + v_p(k).$$

On the other hand, $a^{kx} - 1 = a^s - 1 = b^{y+n}$, so

$$v_p(a^{kx} - 1) = v_p(b^{y+n}) = v_p(b^y) + v_p(b^n).$$

Hence, $v_p(k) = v_p(b^n)$ for every odd $p \mid b$. Denote by b_0 the odd part of b . Then

$$b_0^n \mid k.$$

Case 1: b has an odd prime divisor. Then $b_0 \geq 3$. From $a^x = 1 + b^y$ we obtain

$$b^{y+n} = a^{kx} - 1 = (1 + b^y)^k - 1 \geq b^{yk} \geq b^{yb_0^n}.$$

For $b_0 \geq 3$ and $n \geq 1$, we have $b_0^n > n + 1$. Therefore,

$$b^{y+n} \geq b^{yb_0^n} > b^{y(n+1)}.$$

Comparing exponents, we get $y + n > y(n + 1)$, that is, $n(y - 1) < 0$. Contradiction. Consequently, if $b_0 > 1$, there cannot be two solutions.

Case 2: $b = 2^e$, where $e \geq 1$. Then a is odd and

$$a^x - 1 = 2^{ey}. \tag{1}$$

If $x = 1$, then $a = 2^{ey} + 1$; for fixed a and $b = 2^e$ this gives at most one solution.

Now let $x > 1$. We factor

$$a^x - 1 = (a - 1)(a^{x-1} + a^{x-2} + \cdots + 1) = 2^{ey}.$$

Both factors are positive and their product is a power of two, so each of them is a power of two. The sum $S = a^{x-1} + \cdots + 1$ has the same parity as x , since a is odd. Since $S > 1$ and S is a power of two, S is even, and hence x is even.

Let $x = 2t$. Then

$$a^{2t} - 1 = (a^t - 1)(a^t + 1) = 2^{ey}.$$

The numbers $a^t - 1$ and $a^t + 1$ are two consecutive even powers of two. The only such pair is 2 and 4: if 2^r and 2^s ($s > r$) differ by 2, then $2^r(2^{s-r} - 1) = 2$, so $r = 1$ and $s - r = 1$. Therefore,

$$a^t - 1 = 2, \quad a^t + 1 = 4,$$

that is, $a^t = 3$. Hence $t = 1$, $a = 3$, $x = 2$, and from (1) we obtain

$$3^2 - 1 = 8 = 2^{ey},$$

so $ey = 3$.

Thus the only possible solution with $x > 1$ has the form $a = 3$, $x = 2$, $ey = 3$. For $b = 2^e$ this gives $e = 1$ or $e = 3$. For $e = 3$ there is only this solution ($y = 1$). For $e = 1$ we obtain $b = 2$, $a = 3$, and besides the solution $x = 2$, $y = 3$, there is also the solution $x = 1$, $y = 1$, since $3^1 - 2^1 = 1$. This is the exceptional case.

Thus, for all a, b the equation $a^x - b^y = 1$ has at most one solution, except for the pair $a = 3$, $b = 2$, for which there are two solutions:

$$3^1 - 2^1 = 1, \quad 3^2 - 2^3 = 1.$$

■

For arbitrary $a, b, c > 1$, we do not know if there exists an elementary algorithm that finds all the solutions of the corresponding equation (*). Nevertheless, the following two ideas can help you prove that this equation has no solutions for sufficiently large x and y :

- (1) For any x_0, y_0 and any solution (x, y) of (*) with $x \geq x_0$ and $y \geq y_0$, the remainders of numbers x and y modulo $\text{ord}_a(b^{y_0})$ and $\text{ord}_b(a^{x_0})$ are respectively fixed.
- (2) If there exists a *magic prime* P such that the sets of residues modulo P of the sequences $\{a_n\}$ and $\{b_m\}$ are disjoint, then $a_n \neq b_m$ for all n and m .

It may be hard to find such a magic prime even if it exists. We suggest searching for it among primes of the form $dn + 1$, where d equals $\text{ord}_a(b^{y_0})$ or $\text{ord}_b(a^{x_0})$.

To give an example of how these ideas work we find all solutions to the equation

$$2^x - 11^y = 5.$$

1. It's easy to find a solution $(x, y) = (4, 1)$. Next, we prove there is no solution with $x \geq 5$.
2. We calculate $\text{ord}_{11}(2^5) = 8$. Solving a congruence $11^y \equiv -5 \pmod{2^5}$, we get another one $y \equiv 5 \pmod{8}$.
3. Then we test magic primes of the form $8n+1$. We start with $P = 17$. Let $a_k = 11^{5+8k} + 5$ and $b_m = 2^m$. After calculations, we get that numbers a_k give residues $-2, -5$ while numbers b_m give residues $\pm 1, \pm 2, \pm 4, \pm 8$ modulo 17. That means $a_k \equiv b_m \equiv -2 \pmod{17}$ — no contradiction in this case.
4. Next, we may test either another degree of 2 or 11, or we may choose another magic prime. We check that there is no solution with $x = 5$ and continue with 2^6 , the next degree of 2, as we take the same steps as before.

5. Solving a congruence $11^y \equiv -5 \pmod{2^6}$, we get another one $y \equiv 13 \pmod{16}$. We test primes of the form $16n + 1$ and we choose $P = 17$ again. Let $a_k = 11^{13+16k} + 5$ and $b_m = 2^m$. We see that

$$a_k \equiv -5 \pmod{17}$$

but

$$b_m \equiv \pm 1, \pm 2, \pm 4, \pm 8 \pmod{17},$$

so $a_k \neq b_m$. It follows that $P = 17$ — is a magic prime, and the equation $2^x - 11^y = 5$ has no solutions with the restriction $x \geq 6$.

Below, we suggest solving the equations for which the ideas provided above do work.

Problem 1.9. Solve the equation $10^x - 7^y = 3$.

Solution. Considering the equation modulo $2^3 = 8$, we get $x < 3$. **Answer:** $(1, 1)$. ■

Problem 1.10. Solve the equation $2^x - 5^y = 3$.

Solution. By checking small solutions in natural numbers, we find that $(3, 1)$ and $(7, 3)$ are solutions to this equation. To prove that no other solutions exist, we assume that there exists a solution (x, y) satisfying the condition $x \geq 8$. Consider the equation modulo $2^8 = 256$. For $x \geq 8$, the congruence $2^x \equiv 0 \pmod{256}$ holds. The original equation becomes $5^y + 3 \equiv 0 \pmod{256} \implies 5^y \equiv 253 \pmod{256}$. Solving this congruence, we obtain $y \equiv 35 \pmod{64}$. Let us check the remainders of the number $5^y + 3$ upon division by the magic prime $257 = 4 \cdot 64 + 1$. We find that

$$5^y + 3 \equiv 17, 36, 227, \text{ or } 246 \pmod{257},$$

but none of these remainders lie in the set $\{2^k \pmod{257} \mid k \in \mathbb{N}^*\}$, a contradiction. Therefore, the assumption $x \geq 8$ is false. By enumerating the values $x \in \{1, 2, \dots, 7\}$, we can verify the absence of other solutions.

Answer: $(3, 1), (7, 3)$. ■

Problem 1.11. Solve the equation $3^x - 7^y = 2$.

Solution. If $y = 1$ then $x = 2$. Suppose there is a solution with $y \geq 2$, then $x \geq 4$, and $3^x - 9 = 7^y - 7$. Let $a = x - 2 \geq 2$, $b = y - 1 \geq 1$, then rewrite equation as

$$9(3^a - 1) = 7(7^b - 1).$$

Since $7|3^a - 1$, we have $\text{ord}_3(7) = 6|a$, so $3^a - 1$ is divisible by $3^6 - 1$ which is divisible by 13. Hence $13|7^b - 1$, so $\text{ord}_7(13) = 12|b$.

It follows that $7^b - 1$ is divisible by $7^{12} - 1$ which is divisible by 43. It means that $43|3^a - 1$, therefore $\text{ord}_3(43) = 42|a$ and $3^a - 1$ is divisible by $3^{42} - 1$ which is divisible by 49. It is impossible because $7(7^b - 1)$ is not divisible by 49.

Answer: $(2, 1)$. ■

Problem 1.12. (a) Find at least one integer $c > 4$ such that equation

$$(c + 2)^x - 2^y = c$$

has more than one solution.

(b) Solve this equation with the found c .

Solution. We prove that the equation

$$91^x - 2^y = 89$$

has two solutions. By checking small values of x , we find that $(1, 1)$ and $(2, 13)$ are solutions to this equation. Suppose there exists a solution with $x \geq 3$. Considering the equation modulo $7^3 = 343$, we obtain $2^y \equiv 254 \pmod{343}$. It follows that $y \equiv 76 \pmod{147}$. Let us check the remainders of the number $2^y + 89$ upon division by the magic prime $2647 = 18 \cdot 147 + 1$. We find that

$$2^y + 89 \equiv 2083, 941, 1900, 1046, 1536, 1602, 2432, 437, 2059 \pmod{2647}.$$

However, this set of remainders does not intersect with the set of remainders of the powers of 91 upon division by 2647, a contradiction.

Answer: $(1, 1), (2, 13)$. ■

In addition to the theorem mentioned at the beginning of this section, we believe that the following conjecture is true:

Conjecture. The number of positive integer triples a, b, c such that equation $(*)$ has exactly two solutions is finite.

The jury knows 15 such triples. How many triples can you find?

Problem 1.13. Find at least 8 positive integer triples a, b, c such that equation $(*)$ has exactly 2 solutions.

Solution. The complete list of triples currently known to the jury is as follows:

$$(2, 3, 5), (2, 3, 13), (4, 3, 13), (16, 3, 13), (2, 5, 3), (3, 2, 1), (13, 3, 10), (91, 2, 89),$$

$$(6, 2, 4), (6, 3, 1215), (6, 9, 1215), (6, 81, 1215), (15, 6, 9), (280, 5, 275), (4930, 30, 4900).$$
■

2 On a Størmer problem

The finiteness of solutions of the Diophantine equation $(*)$ can be reformulated as follows: take all powers of a and all powers of b , and arrange them in increasing order. Here is an example for $a = 2, b = 3$:

$$2^1, 3^1, 2^2, 2^3, 3^2, 2^4, 3^3, 2^5, 2^6, 3^4, 2^7, \dots$$

Then the distance between consecutive terms in the sequence approaches infinity. In other words, for any given integer, there is a point in the sequence after which all subsequent gaps are larger than that integer.

The following statement generalises the previous one. Fix some finite set Q of prime numbers. Take those numbers whose prime factors belong to the set Q and arrange them in increasing order. An example for the set $Q = \{2, 3, 5\}$ is given below:

$$2^1, 3^1, 2^2, 5^1, 2^1 \cdot 3^1, 2^3, 3^2, 2^1 \cdot 5^1, 2^2 \cdot 3^1, 3 \cdot 5, \dots$$

Then the distance between consecutive terms in the sequence approaches infinity.

The proof of this difficult statement is not part of our project. Instead, we will prove an upper bound on the number of pairs of consecutive numbers in the given sequence. This bound depends only on the cardinality of Q .

Further, throughout the project, we suppose that Q consists of t prime numbers

$$q_1 < q_2 < \dots < q_t.$$

Definition. Q -smooth numbers are defined as the set of integers

$$\{q_1^{e_1} q_2^{e_2} \cdots q_t^{e_t} \mid e_i \geq 0\}.$$

Problem 2.1. Find all consecutive pairs of $\{2, 3\}$ -smooth numbers. That is, solve the equation $2^x 3^y - 2^z 3^t = 1$ in nonnegative x, y, z, t .

Solution. Since $\gcd(2^x 3^y, 2^z 3^t) = 1$, only the following 4 cases are possible:

- 1) $x = 0, y = 0$. Then $1 - 2^z 3^t = 1$, and there are no solutions;
- 2) $z = 0, t = 0$. Then we immediately find the pair $(1, 2)$;
- 3) $y = 0, z = 0$. Then $2^x - 3^t = 1$. By Problem 1.1.a we find the pair $(3, 4)$;
- 4) $x = 0, t = 0$. Then $3^y - 2^z = 1$. By Problem 1.1.b we find the pairs $(2, 3)$ and $(8, 9)$.

Answer: There are exactly 4 pairs of consecutive $\{2, 3\}$ -smooth numbers:

$$(1, 2), (2, 3), (3, 4), (8, 9).$$

■

Further, throughout the project, D is a positive integer that is not a perfect square. Denote by (x_1, y_1) the *fundamental* (minimal positive) solution of Pell's equation

$$x^2 - Dy^2 = 1.$$

All the positive solutions (x_n, y_n) to this equation are given by

$$x_n + y_n \sqrt{D} = (x_1 + y_1 \sqrt{D})^n.$$

Problem 2.2. (a) Prove that y_1 divides y_n for every integer n .
 (b) Prove that if k divides n then y_k divides y_n .

Solution. (a) Follows from part (b) with $k = 1$.

(b) Since n is divisible by k , we have $n = km$ for some m . Then the assertion follows from Problem 2.5.g after substituting $y_i = y_1 U_i$ for $i = k, n$:

$$y_n = y_{km} = y_k \sum_{i \geq 0} \binom{m}{2i+1} D^i x_k^{m-1-2i}.$$

■

Sometimes it is useful to know the structure of prime divisors of y_n . For example, solving the equation $a^{2k} - b^{2m+1} = 1$, a partial case of (*), can be reduced to solving the Pell's equation with $x = a^k$, $D = b$ and $y = b^m$. It turns out that, under the conditions of this example, verifying the existence of a solution is straightforward using the following problem.

Problem 2.3. Prove that Pell's equation has at most one positive integer solution (x, y) for which every prime divisor of y divides D .

Solution. Notice immediately that if (x, y) is a solution to Pell's equation, then $(x, D) = 1$ and $(x, y) = 1$. Otherwise, the left-hand side of the equation $x^2 - Dy^2 = 1$ is divisible by their greatest common divisor, while the right-hand side is not, which is impossible.

Now assume that the statement of the problem is false, meaning that two such solutions exist. At least one of them is different from the fundamental solution (x_1, y_1) . Let such a solution be denoted by (x_n, y_n) . Notice that since $y_1 \mid y_n$ (by Problem 2.2.a), every prime divisor of y_1 also divides D .

Therefore, we will now actually prove that there exists no solution (x, y) , other than the fundamental one, such that every prime divisor of y divides D . Furthermore, for any prime $p \mid n$, we have $y_p \mid y_n$ (by Problem 2.2.b), which means that for the solution (x_p, y_p) , it is also true that every prime divisor of y_p divides D .

Consider U_p and its prime divisor q . By definition $y_p = U_p y_1$, therefore $U_p \mid y_p$, whence $q \mid y_p \Rightarrow q \mid D$.

According to Problem 2.5.e:

$$U_n = \sum_{i \geq 0} \binom{n}{2i+1} D^i y_1^{2i} x_1^{n-1-2i}$$

Consider this expression modulo q . In the right-hand side, all terms starting from the second one are divisible by D , meaning they are congruent to zero modulo q , and we are left only with the first term:

$$0 \equiv p x_1^{p-1}$$

Now notice that if $p \neq q$, then $q \mid x_1^{p-1} \Rightarrow q \mid x_1 \Rightarrow q \mid (x_1, D)$, a contradiction. Thus, $p = q$, and $U_p = p^k$ for some natural number k . Also notice that $x_1 > 1$, since $D y_1^2 \neq 0$. Therefore $U_p \geq p x_1^{p-1} > p$. This means $k \geq 2$, and $p^2 \mid U_p$.

- Consider the case $p > 3$. Notice that all terms

$$\binom{p}{2i+1} D^i y_1^{2i} x_1^{p-1-2i}$$

for $i \geq 2$ are divisible by D^2 , which means they are divisible by p^2 . Thus,

$$px_1^{p-1} + \binom{p}{3} Dy_1^2 x_1^{p-3} \equiv 0 \pmod{p^2}.$$

We have $\binom{p}{3} = \frac{p(p-1)(p-2)}{6}$. If $p > 3$, then $p \mid \binom{p}{3}$. Since $p \mid D$, it follows that $p^2 \mid \binom{p}{3} Dy_1^2 x_1^{p-3}$, and then $p^2 \mid px_1^{p-1}$. Whence $p \mid x_1^{p-1}$, which cannot be the case, as we proved earlier. Contradiction. Thus, our assumption turned out to be false, and the problem is proven.

- Now consider the case $p = 3$. Then $U_3 = 3x_1^2 + Dy_1^2 = 3^k$.

Let $D = 3d$, then $x_1^2 + dy_1^2 = 3^{k-1}$.

It is also known that $x_1^2 - Dy_1^2 = 1$, which is $x_1^2 - 3(3^{k-1} - x_1^2) = 1$, whence $(2x_1 - 1)(2x_1 + 1) = 3^k$.

This means each of the brackets is some power of three. Notice that the difference between the brackets is 2, so they cannot be divisible by 3 simultaneously. Therefore we get $2x_1 - 1 = 1, 2x_1 + 1 = 3^k$. But then $x_1 = 1$, a contradiction.

- It remains to analyze the case $p = 2$.

By Problem 2.5 b: $U_2 = 2x_1 U_1 = 2x_1$. Thus, $x_1 = 2^{k-1}$, where $k \geq 2$, so $2 \mid x_1$. And since $2 \mid U_p$, then $2 \mid D$, and we get a contradiction with the fact that $(x_1, D) = 1$.

■

In 1897, this idea enabled Størmer to prove the upper bound we promised.

Problem 2.4. (a) Prove that number of consecutive pairs of Q -smooth numbers does not exceed number of Q -smooth numbers of the form $n^2 - 1$.

(b) Prove that there are no more than 3^t consecutive pairs of Q -smooth numbers.

Solution. (a) Let two consecutive Q -smooth numbers be denoted by S and $S + 1$. Note that since one of them is necessarily even, 2 belongs to the set Q as a divisor of a Q -smooth number.

We then prove that the number $4S(S + 1)$ is also Q -smooth. Indeed, any of its prime divisors p divides one of the numbers 4, S , $(S + 1)$. Since all three numbers are Q -smooth, their prime divisors belong to Q .

Notice that $4S(S + 1) = (2S + 1)^2 - 1$. Let $n = 2S + 1$. Then the expression takes the form $n^2 - 1$. The number n is uniquely determined by S ; therefore, different pairs of consecutive Q -smooth numbers correspond to different Q -smooth numbers of the form $n^2 - 1$. Thus, the number of such pairs does not exceed the number of Q -smooth numbers of the form $n^2 - 1$.

(b) According to part (a), it is sufficient to estimate the number of Q -smooth numbers of the form $n^2 - 1$. We will prove that there are at most 3^t of them, where $t = |Q|$.

Consider a Q -smooth number of the form $n^2 - 1$. We will construct a Pell's equation from it. Let $n^2 - 1 = p_1^{a_1} \dots p_k^{a_k}$, where all $p_i \in Q$ and all $a_i > 0$. Then set $D = p_1^{b_1} \dots p_k^{b_k}$, where $b_i = 1$ if a_i is odd, and $b_i = 2$ if it is even. Such a D is Q -smooth by construction.

At the same time, the ratio $\frac{n^2-1}{D} = p_1^{a_1-b_1} \dots p_k^{a_k-b_k}$ is a perfect square, since the exponents of all primes in the factorization are even and non-negative.

Let $y_n = \sqrt{\frac{n^2-1}{D}}$. Then the pair (n, y_n) is a solution to the equation $x^2 - Dy^2 = 1$. Moreover, this solution possesses the following property: every prime divisor of y_n divides D . Indeed, if $p \mid y_n$, then p is present in the factorization of $n^2 - 1$, and therefore, by definition, $p \mid D$.

Now we prove that different numbers $n^2 - 1$ correspond to different values of D . Suppose not, and for some $n^2 - 1$ and $m^2 - 1$ ($n^2 - 1 \neq m^2 - 1$, i.e., $n \neq m$), the same value of D was obtained. Then the equation $x^2 - Dy^2 = 1$ would have two distinct solutions (n, y_n) and (m, y_m) (since $n \neq m$) in which all prime divisors of the y -component divide D . By Problem 2.3, we reach a contradiction.

We have shown that different Q -smooth numbers of the form $n^2 - 1$ yield different values of D . Now let us estimate the number of such D . These are Q -smooth numbers in which the exponents of all prime factors do not exceed 2. This means that for each prime p_i in Q , there are three possible exponents: 0, 1, 2. All other primes are not included in the factorization. Therefore, there are at most 3^t possible values for D . ■

The resulting upper bound is determined by the number of Pell's equations that must be checked for the existence of a special solution. Further, we present an alternate approach that requires solving only $2^t - 1$ Pell's equations. This requires some additional technical aspects, but it gives a better estimate of the number of consecutive pairs of Q -smooth numbers.

By Problem 2.2a numbers $U_n := y_n/y_1$ are integers. We take a closer look at «non-trivial» divisors of y_n and study the properties of the sequence $\{U_n\}$.

Problem 2.5. Prove that

- (a) $x_{2n} = 2x_n^2 - 1$, (b) $U_{2n} = 2x_n U_n$,
- (c) $x_{m \pm n} = x_m x_n \pm D y_m y_n$, (d) $U_{m \pm n} = x_n U_m \pm x_m U_n$,
- (e) $x_n = \sum_{i \geq 0} \binom{n}{2i} D^i y_1^{2i} x_1^{n-2i}$, f) $U_n = \sum_{i \geq 0} \binom{n}{2i+1} D^i y_1^{2i} x_1^{n-1-2i}$,
- (g) $U_{mn} = \sum_{i \geq 0} \binom{n}{2i+1} D^i U_m^{2i+1} y_1^{2i} x_m^{n-1-2i}$.

Solution. (a) $x_{2n} = 2x_n^2 - 1$

Consider the expansion for $x_{2n} + y_{2n} \sqrt{D}$:

$$x_{2n} + y_{2n} \sqrt{D} = (x_1 + y_1 \sqrt{D})^{2n} = ((x_1 + y_1 \sqrt{D})^n)^2 = (x_n + y_n \sqrt{D})^2 = x_n^2 + D y_n^2 + 2x_n y_n \sqrt{D}$$

From here, $x_{2n} = x_n^2 + D y_n^2$. Given that (x_n, y_n) is a solution to Pell's equation ($x_n^2 - D y_n^2 = 1$), we have $D y_n^2 = x_n^2 - 1$. Substituting this, we get:

$$x_{2n} = x_n^2 + (x_n^2 - 1) = 2x_n^2 - 1.$$

(b) $U_{2n} = 2x_n U_n$

From the same expansion in part (a), it follows that $y_{2n} = 2x_n y_n$. Dividing both sides by y_1 , we obtain:

$$\frac{y_{2n}}{y_1} = 2x_n \frac{y_n}{y_1} \implies U_{2n} = 2x_n U_n.$$

(c) $x_{m\pm n} = x_m x_n \pm D y_m y_n$

We use the representation in terms of the fundamental solution:

$$x_{m\pm n} + y_{m\pm n} \sqrt{D} = (x_1 + y_1 \sqrt{D})^m \cdot (x_1 + y_1 \sqrt{D})^{\pm n} = (x_m + y_m \sqrt{D}) \cdot (x_n + y_n \sqrt{D})^{\pm 1}$$

Moreover, since $(x_n + y_n \sqrt{D}) \cdot (x_n - y_n \sqrt{D}) = x_n^2 - D y_n^2 = 1$, then

$$(x_n + y_n \sqrt{D})^{-1} = (x_n - y_n \sqrt{D}).$$

Therefore,

$$x_{m\pm n} + y_{m\pm n} \sqrt{D} = (x_m + y_m \sqrt{D})(x_n \pm y_n \sqrt{D}) = (x_m x_n \pm D y_m y_n) + (x_m y_n \pm x_n y_m) \sqrt{D}.$$

Comparing the rational parts: $x_{m\pm n} = x_m x_n \pm D y_m y_n$.

(d) $U_{m\pm n} = x_n U_m \pm x_m U_n$

Comparing the irrational parts from the expansion in part (c):

$$y_{m\pm n} = x_m y_n \pm x_n y_m.$$

Divide by y_1 :

$$\frac{y_{m\pm n}}{y_1} = x_m \frac{y_n}{y_1} \pm x_n \frac{y_m}{y_1} \implies U_{m\pm n} = x_m U_n \pm x_n U_m.$$

(e) $x_n = \sum_{i \geq 0} \binom{n}{2i} D^i y_1^{2i} x_1^{n-2i}$

Expand the expression $x_n + y_n \sqrt{D} = (x_1 + y_1 \sqrt{D})^n$ using the Binomial Theorem:

$$x_n + y_n \sqrt{D} = \sum_{k=0}^n \binom{n}{k} x_1^{n-k} (y_1 \sqrt{D})^k.$$

The rational part x_n corresponds to even indices $k = 2i$:

$$x_n = \sum_{2i \leq n} \binom{n}{2i} x_1^{n-2i} (y_1 \sqrt{D})^{2i} = \sum_{i \geq 0} \binom{n}{2i} D^i y_1^{2i} x_1^{n-2i}.$$

f) $U_n = \sum_{i \geq 0} \binom{n}{2i+1} D^i y_1^{2i} x_1^{n-1-2i}$

The irrational part from the expansion above corresponds to odd indices $k = 2i + 1$:

$$y_n \sqrt{D} = \sum_{2i+1 \leq n} \binom{n}{2i+1} x_1^{n-(2i+1)} (y_1 \sqrt{D})^{2i+1} = \sum_{i \geq 0} \binom{n}{2i+1} x_1^{n-2i-1} y_1^{2i+1} D^i \sqrt{D}.$$

Divide by $y_1 \sqrt{D}$:

$$U_n = \frac{y_n}{y_1} = \sum_{i \geq 0} \binom{n}{2i+1} D^i y_1^{2i} x_1^{n-1-2i}.$$

$$(g) \quad U_{mn} = \sum_{i \geq 0} \binom{n}{2i+1} D^i U_m^{2i+1} y_1^{2i} x_m^{n-1-2i}$$

Note that $x_{mn} + y_{mn}\sqrt{D} = (x_m + y_m\sqrt{D})^n$. Applying the formula from part (f) to the pair (x_m, y_m) , we obtain:

$$y_{mn} = \sum_{i \geq 0} \binom{n}{2i+1} y_m^{2i+1} D^i x_m^{n-2i-1}.$$

Divide by y_1 :

$$U_{mn} = \frac{y_{mn}}{y_1} = \sum_{i \geq 0} \binom{n}{2i+1} \frac{y_m^{2i+1}}{y_1} D^i x_m^{n-1-2i}.$$

Since $y_m = U_m y_1$, then $\frac{y_m^{2i+1}}{y_1} = \frac{(U_m y_1)^{2i+1}}{y_1} = U_m^{2i+1} y_1^{2i}$. Substituting this, we obtain the required identity. ■

Definition. Let p be a prime, and let $w(p)$ be the rank of apparition of p in the sequence $\{U_n\}$, that is, the least positive j for which U_j is divisible by p .

Problem 2.6. Prove that a prime p divides U_n iff $w(p)$ divides n .

Solution. ($\Leftarrow$): Let n be divisible by $\omega(p)$, that is, $n = k\omega(p)$ for some natural number k . According to the formula for U_{mn} (Problem 2.5.g), the number $U_{k\omega(p)}$ is divisible by $U_{\omega(p)}$. Since, by the definition of $\omega(p)$, $U_{\omega(p)}$ is divisible by p , then U_n is also divisible by p .

($\Rightarrow$): Let U_n be divisible by p . Suppose the contrary, i.e., n is not divisible by $\omega(p)$. Then consider: $n = t\omega(p) + r$, where $1 \leq r < \omega(p)$. By Problem 2.5.d:

$$U_n = U_{t\omega(p)+r} = x_r U_{t\omega(p)} + x_{t\omega(p)} U_r$$

Since $p \mid U_n$ and $p \mid U_{t\omega(p)}$, p must divide the remaining term: $p \mid x_{t\omega(p)} U_r$. Notice that $(x_k, U_k) = 1$, since $x_k^2 - D y_1^2 U_k^2 = 1$. Since $p \mid U_{t\omega(p)}$, p cannot divide $x_{t\omega(p)}$. Thus, from $p \mid x_{t\omega(p)} U_r$, it follows that $p \mid U_r$. However, since $\omega(p)$ is the smallest positive index for which U is divisible by p , we arrive at a contradiction. ■

It is easy to see that $w(2) = 2$. The next problem shows that $w(p)$ exists for any prime p .

Problem 2.7. (Law of Apparition). Let p be an odd prime. Prove that

(a) $w(p) = p$ if p divides $D y_1$,

(b) $w(p)$ divides $(p - \varepsilon)/2$ if p does not divide $D y_1$, where

$$\varepsilon := \left(\frac{D}{p} \right) \equiv D^{(p-1)/2} \pmod{p}.$$

Proof. (a) If $p \mid D y_1$, by part 2.5.e we have: $U_n = \sum_{i \geq 0} \binom{n}{2i+1} D^i y_1^{2i} x_1^{n-1-2i}$. Consider this expression modulo p . All terms for $i \geq 1$ are divisible by $D y_1$, and therefore are divisible by p . Thus:

$$U_n \equiv n x_1^{n-1} \pmod{p}.$$

Since $(x_1, p) = 1$, then $U_n \equiv 0 \pmod{p} \iff n \equiv 0 \pmod{p}$. The minimal such n is p , hence $\omega(p) = p$.

(b) Using the expansions from problems 2.5.de and noting that $\binom{p}{k} \equiv 0 \pmod{p}$ for $0 < k < p$, we obtain:

$$x_p \equiv x_1^p \pmod{p}, \quad U_p \equiv D^{\frac{p-1}{2}} y_1^{p-1} \pmod{p}.$$

Note that $x_1^p \equiv x_1 \pmod{p}$, because either $p \mid x_1$, in which case both sides are $\equiv 0 \pmod{p}$, or $p \nmid x_1$, and by Fermat's Little Theorem $x_1^{p-1} \equiv 1 \pmod{p}$. Also, since $p \nmid Dy_1$, it follows that $y_1^{p-1} \equiv 1 \pmod{p}$. Then $x_p \equiv x_1 \pmod{p}$ and $U_p \equiv \varepsilon \pmod{p}$.

Now we apply the formula from Problem 2.5.g for $y_{p-\varepsilon}$:

$$y_{p-\varepsilon} = y_p x_1 - \varepsilon x_p y_1 \equiv (\varepsilon y_1) x_1 - \varepsilon x_1 y_1 = 0 \pmod{p}.$$

In writing this formula, we used the fact that $\varepsilon = \pm 1$. Now we have $U_{p-\varepsilon} = y_{p-\varepsilon}/y_1 \equiv 0 \pmod{p}$. By problem 2.6, this implies $\omega(p) \mid (p - \varepsilon)$.

Using formulas 2.5.ab:

$$U_{p-\varepsilon} = 2x_{\frac{p-\varepsilon}{2}} U_{\frac{p-\varepsilon}{2}} \equiv 0 \pmod{p}, \quad x_{p-\varepsilon} = 2x_{\frac{p-\varepsilon}{2}}^2 - 1.$$

Since $x_{p-\varepsilon} = x_p x_1 - \varepsilon Dy_p y_1 \equiv x_1^2 - Dy_1^2 = 1 \pmod{p}$, we have:

$$2x_{\frac{p-\varepsilon}{2}}^2 - 1 \equiv 1 \pmod{p} \implies x_{\frac{p-\varepsilon}{2}}^2 \equiv 1 \pmod{p}.$$

Thus, $x_{\frac{p-\varepsilon}{2}} \not\equiv 0 \pmod{p}$. From the equality $2x_{\frac{p-\varepsilon}{2}} U_{\frac{p-\varepsilon}{2}} \equiv 0$ it follows that $U_{\frac{p-\varepsilon}{2}} \equiv 0 \pmod{p}$. And by problem 2.6, the condition $p \mid U_{\frac{p-\varepsilon}{2}}$ is equivalent to the fact that $\omega(p) \mid \frac{p-\varepsilon}{2}$. ■

Problem 2.8. Let $p > 3$ be a prime dividing Dy_1 . Prove that $U_p \equiv p \pmod{p^2}$.

Solution. By Problem 2.5.e:

$$U_p = \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{2i+1} D^i y_1^{2i} x_1^{p-1-2i}.$$

Expanding the first two terms of this sum, we have:

$$U_p = \binom{p}{1} x_1^{p-1} + \binom{p}{3} Dy_1^2 x_1^{p-3} + \sum_{i=2}^{\frac{p-1}{2}} \binom{p}{2i+1} D^i y_1^{2i} x_1^{p-1-2i}.$$

Consider this expression modulo p^2 .

All terms for $i \geq 2$ are divisible by $(Dy_1)^2$, and since $p \mid Dy_1$, they are also divisible by p^2 . For $i = 1$, the term is also divisible by p^2 because Dy_1 is divisible by p , and $\binom{p}{3} = \frac{p(p-1)(p-2)}{6}$ is divisible by p (for $p > 3$).

Therefore, $U_p \equiv px_1^{p-1} \pmod{p^2}$. Since $(x_1, D) = 1$, $(x_1, y_1) = 1$, and $p \mid Dy_1$, it follows that $p \nmid x_1$, and thus $x_1^{p-1} \equiv 1 \pmod{p}$. Then $px_1^{p-1} \equiv p \pmod{p^2}$. ■

Problem 2.9. (Law of Repetition). Prove that for every prime divisor p of U_n , positive integer k coprime with p and $\lambda \geq 0$ the next equality holds

$$\nu_p(U_{knp^\lambda}) = \nu_p(U_n) + \lambda.$$

Solution. Notice that since $\nu_p(U_n) = v \geq 1$, it follows from $x_n^2 - Dy_1^2 U_n^2 = 1$ that $p \nmid x_n$.

- Let us prove that $\nu_p(U_{kn}) = \nu_p(U_n)$ if $(k, p) = 1$.

By Problem 2.5.g:

$$U_{nk} = \sum_{i \geq 0} \binom{k}{2i+1} D^i U_n^{2i+1} y_1^{2i} x_n^{k-1-2i}.$$

For $i \geq 1$, all terms are divisible by U_n^3 , which means they are divisible by p^{3v} . Since $v \geq 1$, we obtain that modulo p^{v+1} :

$$U_{nk} \equiv k U_n x_n^{k-1} \equiv k U_n \pmod{p^{v+1}}$$

Then, since $(k, p) = 1$, we have $\nu_p(k U_n) = v$. Thus, $\nu_p(U_{nk}) = v$.

- Now let us prove that $\nu_p(U_{pn}) = \nu_p(U_n) + 1$.

Again, we expand using Problem 2.5.g:

$$U_{np} = \sum_{i \geq 0} \binom{p}{2i+1} D^i U_n^{2i+1} y_1^{2i} x_n^{p-1-2i}.$$

For $i \geq 1$, all terms are divisible by U_n^3 , meaning they are divisible by p^{3v} . Since $v \geq 1$, we obtain that modulo p^{v+2} :

$$U_{np} \equiv p U_n x_n^{p-1} \equiv p U_n \pmod{p^{v+2}}$$

We have $\nu_p(p U_n) = v + 1$. Thus, $\nu_p(U_{np}) = v + 1$.

Applying the reasoning of the second case λ times, we obtain $\nu_p(U_{np^\lambda}) = \nu_p(U_n) + \lambda$. Combining this with Step 1, we get $\nu_p(U_{knp^\lambda}) = \nu_p(U_n) + \lambda$. ■

For brevity, we write

$$\alpha = x_1 + y_1 \sqrt{D}, \quad \beta = x_1 - y_1 \sqrt{D}.$$

We now introduce

$$G_n := \prod_{\substack{h < n \\ (h, n) = 1}} \left(\alpha - \beta e^{2\pi i h/n} \right).$$

For example,

$$G_1 = 1, \quad G_2 = \alpha + \beta = 2x_1 = U_2, \quad G_3 = \alpha^2 + \alpha\beta + \beta^2 = U_3.$$

Problem 2.10. Prove that G_n is an integer, being a symmetric polynomial of α and β .

Solution. Note that if $(h, n) = 1$, then $(n - h, n) = 1$. Introduce the notation $e_h = e^{2\pi i h/n}$. Then note that $e_h \cdot e_{n-h} = 1$.

We first prove that $G_n(\alpha, \beta) = G_n(\beta, \alpha)$. To this end, consider the product:

$$\prod_{\substack{h < n \\ (h, n) = 1}} e^{2\pi i h/n}.$$

Note that it equals $(-1)^{\varphi(n)}$. Indeed, all e_h split into pairs (e_h, e_{n-h}) , and in each pair the product is 1. Only $e_{n/2}$ could remain unpaired. However, for $n > 2$ we do not have $(n/2, n) = 1$, so it does not appear in the product. For $n = 2$ we have $\varphi(n) = 1$, and the product contains only $e_1 = -1$.

Now multiply $G_n(\alpha, \beta)$ by this product. We obtain:

$$G_n(\alpha, \beta) \cdot \prod_{\substack{h < n \\ (h, n) = 1}} e^{2\pi i h/n} = \prod_{\substack{h < n \\ (h, n) = 1}} \left(\alpha - \beta e^{2\pi i h/n} \right) e^{2\pi i (n-h)/n},$$

$$G_n(\alpha, \beta) \cdot (-1)^{\varphi(n)} = \prod_{\substack{h < n \\ (h, n) = 1}} \left(\alpha e^{2\pi i (n-h)/n} - \beta \right),$$

$$G_n(\alpha, \beta) \cdot (-1)^{\varphi(n)} = \prod_{\substack{h < n \\ (h, n) = 1}} \left(\alpha e^{2\pi i h/n} - \beta \right).$$

The last transition is valid because in the product, whenever there is a factor with e_h , there is also the same factor with e_{n-h} , and conversely.

It remains to multiply both sides by $(-1)^{\varphi(n)}$:

$$G_n(\alpha, \beta) = \prod_{\substack{h < n \\ (h, n) = 1}} \left(\beta - \alpha e^{2\pi i h/n} \right).$$

Note that the right-hand side is exactly $G_n(\beta, \alpha)$.

Now we prove that $G_n(\alpha, \beta)$ is a polynomial with integer coefficients. To do this, consider the polynomial $P_n(x) = \prod_{(h, n) = 1} (x - e^{2\pi i h/n})$. We prove that this polynomial has integer coefficients.

Note that its leading coefficient is equal to one. Also note that

$$x^n - 1 = \prod_{d|n} P_d(x).$$

Indeed, the left-hand side factors as

$$x^n - 1 = \prod_{1 \leq k \leq n} \left(x - e^{2\pi i k/n} \right).$$

Here, if we set $d = (n, k)$ and $h = \frac{k}{d}$, then $(h, d) = 1$. This decomposition is unique, so to the factor $(x - e^{2\pi i k/n})$ there corresponds exactly one factor $(x - e^{2\pi i h/d})$ in the product $\prod_{d|n} P_d(x)$. Conversely, from any factor of the product $\prod_{d|n} P_d(x)$ the corresponding factor on the left-hand side is uniquely determined.

We prove by induction that the coefficients of $P_n(x)$ are integers.

Base: $P_1(x) = 1$.

Inductive step: denote $Q_n(x) = \prod_{\substack{d|n \\ d < n}} P_d(x)$; then $x^n - 1 = P_n(x)Q_n(x)$.

Note that the polynomial $Q_n(x)$ has integer coefficients, since it is a product of polynomials with integer coefficients. If we divide the polynomial $x^n - 1$ by $Q_n(x)$, the coefficients of the resulting polynomial will be rational. Since the leading coefficient of $Q_n(x)$ is one (as the product of the unit leading coefficients of the $P_d(x)$), the coefficients will in fact be integers.

For $n > 1$ we have $G_n(\alpha, \beta) = P_n(\frac{\alpha}{\beta}) \cdot \beta^{\varphi(n)}$, so its coefficients are also integers. Note also that $\alpha\beta = x_1^2 - Dy_1^2 = 1$.

Since G_n is symmetric, the coefficients of $\alpha^m \beta^{\varphi(n)-m}$ and $\beta^m \alpha^{\varphi(n)-m}$ are equal.

For $n = 2$ the statement of the problem is obvious from the explicit form of G_n , so consider $n > 2$. Then $\varphi(n)$ is even, and after expanding the brackets in G_n all terms split into pairs: $c \cdot \alpha^m \beta^{\varphi(n)-m} + c \cdot \beta^m \alpha^{\varphi(n)-m} = c(\alpha^m \beta^{\varphi(n)-m} + \beta^m \alpha^{\varphi(n)-m})$. Without loss of generality, assume $\varphi(n) - m = m + t$, $t \geq 0$. Then the sum takes the form $c \cdot \alpha^m \beta^m (\alpha^t + \beta^t) = c(x_t + y_t \sqrt{D} + x_t - y_t \sqrt{D}) = 2cx_t$. We obtain an integer. Therefore G_n is an integer as a sum of several integers. $\blacksquare$

Problem 2.11. Prove that

$$U_n = \prod_{\delta|n} G_\delta.$$

Solution. Note that the terms of the sequence U_n are expressed by the formula:

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}.$$

We use the factorization obtained in the previous problem, first multiplying it by $\beta^{\varphi(n)}$:

$$\alpha^n - \beta^n = \beta^{\varphi(n)} \prod_{\delta|n} P_\delta \left(\frac{\alpha}{\beta} \right).$$

Since $P_1 \left(\frac{\alpha}{\beta} \right) \beta = \alpha - \beta$, we have:

$$U_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} = \prod_{\delta|n, \delta > 1} P_\delta \left(\frac{\alpha}{\beta} \right) \beta^{\varphi(\delta)}.$$

Defining $G_1 = 1$ and $G_\delta = P_\delta \left(\frac{\alpha}{\beta} \right) \beta^{\varphi(\delta)}$ for $\delta > 1$, we obtain the desired representation:

$$U_n = \prod_{\delta|n} G_\delta.$$

It follows from the previous problem that G_n is a factor of U_n .

We distinguish two kinds of prime factors of G_n . A prime factor of G_n that divides n is called *intrinsic*. The other prime factors of G_n are called *extrinsic*.

Problem 2.12. Let p be an intrinsic prime factor of G_n .

- (a) Prove that p is the largest prime factor of n .
- (b) Prove that G_n is not divisible by p^2 if $n > 3$.

Solution. (by M. Akimova) Let p be the largest prime divisor of n and let $v = v_p(n)$. Set $m = n/p^v$.

- (a) Take an arbitrary prime divisor q of m . By Problem 2.11 we have

$$U_n = U_m \cdot \prod_{p|d|n} G_d, \quad \text{hence} \quad v_q(U_n) = v_q(U_m) + \sum_{p|d|n} v_q(G_d).$$

But since $q \neq p$, by Problem 2.9 we have $v_q(U_n) = v_q(U_m)$. Hence, for any d dividing n and divisible by p , we have $v_q(G_d) = 0$. In particular, $v_q(G_n) = 0$.

- (b) By Problem 2.11 write

$$U_n = U_{mp^v} = U_{mp^{v-1}} \cdot \prod_{p^v|d|n} G_d, \quad \text{hence} \quad v_p(U_{mp^v}) = v_p(U_{mp^{v-1}}) + \sum_{p^v|d|n} v_p(G_d).$$

By Problem 2.9 we have $v_p(U_{mp^v}) = v_p(U_{mp^{v-1}}) + 1$, whence $\sum_{p^v|d|n} v_p(G_d) = 1$. In particular, $v_p(G_n) \leq 1$. ■

Problem 2.13. Let $n > 3$ be an integer.

- (a) Prove that G_n has extrinsic prime factor q .
- (b) Prove that $q \geq 2n - 1$.

Solution. Let

$$n = \prod_{i=1}^t p_i^{\alpha_i}$$

be the prime factorization of n , among whose primes p_t is the largest. Then

$$\varphi(n) = \prod_{i=1}^t p_i^{\alpha_i-1} (p_i - 1) \geq p_t - 1.$$

Hence

$$\begin{aligned} |G_n| &= \prod_h |\alpha - \beta \exp(2\pi i h/n)| > (\alpha - \beta)^{\varphi(n)} \\ &= (2y_1 \sqrt{D})^{\varphi(n)} > 2^{p_t-1} \geq p_t. \end{aligned}$$

Here the estimate for the modulus of the product could be made by splitting the factors into pairs and estimating each pair by $(\alpha - \beta)^2$.

Thus we have obtained $G_n > p_t$. Suppose that G_n has no external prime divisor. Then by Problem 2.12a every prime divisor of it is the largest prime divisor of n (as an internal one). That is, $G_n = p_t^k$. Since $n > 3$, by Problem 2.12b we have $p_t^2 \nmid G_n$, so $k \leq 1$, and $G_n \leq p_t$. This contradicts the relation just obtained.

Therefore, G_n has an external prime divisor p^* . Let $w = w(p^*)$ be the rank of apparition of p^* . Since p^* divides G_n and consequently U_n , we have $w \mid n$. Suppose that $w < n$, so that G_n divides the integer

$$U_n/U_w = \prod_{\delta \mid n, \delta \nmid w} G_\delta.$$

Then p^* divides this quotient. But p^* , being external, divides neither n nor w , and therefore, by Problem 2.9, U_n/U_w is not divisible by p^* . This contradiction proves that $w = n$. But then $p^* \neq w$, since p^* does not divide n . Consequently, by Problem 2.7b, w , and hence n , divides $\frac{1}{2}(p^* \pm 1)$. Thus, $p^* \geq 2n - 1$. ■

It is convenient to introduce the number $M(Q)$ defined by

$$M(Q) = \max(3, (q_t + 1)/2).$$

Problem 2.14. Let Q' be the subset of all $2^t - 1$ square-free Q -smooth numbers with the exception of 2. Let S be an integer such that both S and $S + 1$ are Q -smooth. Prove that $S = (x_n - 1)/2$ where (x_n, y_n) is a solution to the Pell's equation

$$x^2 - 2dy^2 = 1$$

in which

$$d \in Q', \quad 1 \leq n \leq M(Q).$$

Solution. Suppose first that (x_n, y_n) is a solution of the Pell's equation

$$x^2 - 2dy^2 = 1, \quad d \in Q', \quad 1 \leq n \leq M(Q).$$

Then, since x_n is odd and y_n is even, we have

$$S(S + 1) = \frac{x_n^2 - 1}{4} = 2d \left(\frac{y_n}{2} \right)^2 \in Q.$$

Now suppose that $S(S + 1) \in Q$, that is,

$$S(S + 1) = 2q_1^{\alpha_1} q_2^{\alpha_2} \dots q_t^{\alpha_t},$$

where

$$\alpha_i = \varepsilon_i + 2\beta_i, \quad \varepsilon_i \in \{0, 1\}.$$

Moreover,

$$x = 2S + 1, \quad y = 2q_1^{\beta_1} q_2^{\beta_2} \dots q_t^{\beta_t} \in Q, \quad d = q_1^{\varepsilon_1} q_2^{\varepsilon_2} \dots q_t^{\varepsilon_t} \in Q'.$$

Multiplying the expression $S(S+1)$ by 4, we see that

$$4S^2 + 4S = x^2 - 1 = 2dy^2.$$

Consequently, every such S leads to some solution (x, y) of the equation $x^2 - 2dy^2 = 1$, in which y and d belong to Q and Q' , respectively. As is well known, (x, y) must be (x_n, y_n) for some $n \geq 1$. It remains to show that $n \leq M$.

Suppose instead that $n > M$. Applying Problem 2.13 and using the fact that $G_n \mid U_n \mid y_n$, we conclude that y_n is divisible by a prime p such that

$$p \geq 2n - 1 > 2M - 1 \geq q_t.$$

Therefore, y_n does not belong to Q , a contradiction. Thus, $n \leq M$. ■

The next theorem is a direct consequence of the previous problem:

Theorem. There exist no more than $(2^t - 1) \cdot M(Q)$ consecutive pairs of Q -smooth numbers.

Problem 2.15. Find all consecutive pairs of $\{2, 3, 5\}$ -smooth numbers.

Solution. We use the previous problem. $Q' = \{1, 3, 5, 6, 10, 15, 30\}$, $M(Q) = 3$.

Then it suffices to consider 7 choices of the parameter d for the Pell's equation, and for each such equation to consider the solutions with $n \leq 3$.

- $x^2 - 2y^2 = 1$

In this case $(x_1, y_1) = (3, 2)$, $(x_2, y_2) = (17, 12)$, $(x_3, y_3) = (99, 70)$.

From them we obtain the following pairs: $(1, 2)$, $(8, 9)$.

- $x^2 - 6y^2 = 1$

In this case $(x_1, y_1) = (5, 2)$, $(x_2, y_2) = (49, 20)$, $(x_3, y_3) = (485, 198)$.

From them we obtain the following pairs: $(2, 3)$, $(24, 25)$.

- $x^2 - 10y^2 = 1$

In this case we similarly obtain the pair $(9, 10)$.

- $x^2 - 12y^2 = 1$

In this case we obtain the pair $(3, 4)$.

- $x^2 - 20y^2 = 1$

We obtain the pairs $(4, 5)$, $(80, 81)$.

- $x^2 - 30y^2 = 1$

We obtain the pair $(5, 6)$.

- $x^2 - 60y^2 = 1$

We obtain the pair $(15, 16)$. ■

3 Størmer's method

In Section 2 we mentioned how the fact stated in Problem 2.3 helped Størmer prove an upper bound on the number of pairs of consecutive Q -smooth numbers. A similar study of the structure of prime divisors of solutions to the generalized Pell's equation can be useful for solving many number-theoretic problems. We suggest you to solve some of them.

Problem 3.1. Let (x, y) be a solution of the equation $x^2 - 1 = y^q$ for prime $q \geq 5$.

- (a) Prove that x can not be even.
- (b) Prove that either $\left(\frac{x+3}{2}\right)^2$ or $\left(\frac{x-3}{2}\right)^2$ is represented by a difference of two perfect q -powers.
- (c) Prove that x is not divisible by q .
- (d) Prove that $y + 1$ is a perfect square.
- (e) Prove that equation

$$x^2 - 1 = y^q$$

has no solutions for prime $q \geq 5$.

Solution. (a) Suppose that x is even, then y is odd and $x - 1$ and $x + 1$ are coprime. It follows that that $x - 1$ and $x + 1$ are both q -th powers. Let $x - 1 = s^q$ and $x + 1 = t^q$. We have $t^q - s^q = 2$ for some $s, t \in \mathbb{Z}$. It is possible only if $t = 1, s = -1$. But this implies $x = 0$, which leads to a contradiction.

(b) By (a) x is odd and $(x + 1, x - 1) = 2$. Let $\varepsilon = \pm 1$ be such that $x \equiv \varepsilon \pmod{4}$. Then

$$x + \varepsilon = 2w^q, \quad x - \varepsilon = 2^{q-1}z^q, \quad y = 2wz$$

for $w, z \in \mathbb{Z}$ such that $\gcd(w, 2z) = 1$. Hence

$$\left(\frac{x - 3\varepsilon}{2}\right)^2 = \left(\frac{x - \varepsilon}{2} - \varepsilon\right)^2 = \left(\frac{x - \varepsilon}{2} + \varepsilon\right)^2 - 4\varepsilon\frac{x - \varepsilon}{2} = (w^2)^q - (2\varepsilon z)^q.$$

(c) **Lemma.** If $a, b \in \mathbb{Z}$, $(a, b) = 1$ and p is a prime number, then

$$\left(\frac{a^p - b^p}{a - b}, a - b\right) = 1 \text{ or } p.$$

Proof: Note that

$$\frac{a^p - b^p}{a - b} = \sum_{i=0}^{p-1} a^i b^{p-1-i} \equiv pb^{p-1} \equiv pa^{p-1} \pmod{a - b}.$$

It follows that $\left(\frac{a^p - b^p}{a - b}, a - b\right)$ divides both pb^{p-1} and pa^{p-1} . Since a and b are coprime, we find that $\left(\frac{a^p - b^p}{a - b}, a - b\right) \mid p$, $\left(\frac{a^p - b^p}{a - b}, a - b\right) = 1$, or p . $\square$

By lemma we have

$$\left(\frac{(w^2)^q - (2\varepsilon z)^q}{w^2 - 2\varepsilon z}, w^2 - 2\varepsilon z\right) = 1 \text{ or } q.$$

If $\frac{(w^2)^q - (2\varepsilon z)^q}{w^2 - 2\varepsilon z}$ and $w^2 - 2\varepsilon z$ are coprime then it follows from (b) that $w^2 - 2\varepsilon z$ is a perfect square, so $w \leq z$. But it is impossible for $x > 1$ since

$$\left(\frac{w}{z}\right)^q = 2^{q-2} \frac{x + \varepsilon}{x - \varepsilon} > 1.$$

Hence $x = 1$ and $y = 0$, which is a contradiction.

Otherwise, both numbers $\frac{(w^2)^q - (2\varepsilon z)^q}{w^2 - 2\varepsilon z}$ and $w^2 - 2\varepsilon z$ are divisible by q , so $\left(\frac{x-3\varepsilon}{2}\right)^2 = (w^2)^q - (2\varepsilon z)^q$ is divisible by q too. Hence x is not divisible by q as $q \geq 5$.

(d) By lemma we have

$$\left(\frac{y^q + 1}{y + 1}, y + 1\right) = 1 \text{ or } q.$$

If $\frac{y^q + 1}{y + 1}$ and $y + 1$ are both divisible by q then $x^2 = y^q + 1$ is divisible by q too, which contradicts (c). If $\frac{y^q + 1}{y + 1}$ and $y + 1$ are coprime then $y + 1$ is a perfect square.

(e) If (x, y) is a positive solution of the equation $x^2 - 1 = y^q$ then $y + 1 = s^2$ by (d). It follows that Pell's equation

$$z^2 - y \cdot t^2 = 1$$

has at least two solutions $(z, t) = (s, 1)$ and $(z, t) = (x, y^{\frac{q-1}{2}})$ for which all prime divisors of t divides y . This contradicts to the result of the Problem 2.3. ■

Problem 3.2. (a) Prove that all solutions of the equation

$$ax^2 - (a - 1)y^2 = 1$$

for integer $a > 1$ are given by

$$x_t \sqrt{a} + y_t \sqrt{a - 1} = (\sqrt{a} + \sqrt{a - 1})^{2t+1}$$

with nonnegative integer t .

(b) Solve the equation

$$\frac{x^{2k+1} - 1}{x - 1} = y^2$$

for positive integer k .

Solution. (a) Note that the number $\sqrt{\frac{a-1}{a}}$ is irrational, so the representation of a number in the form $x\sqrt{a} + y\sqrt{a-1}$ is unique.

Consider the numbers $z = x\sqrt{a} + y\sqrt{a-1}$ and $\tilde{z} = x\sqrt{a} - y\sqrt{a-1}$; then $z\tilde{z} = 1$. Choose t such that

$$(\sqrt{a} + \sqrt{a-1})^{2t-1} < x\sqrt{a} + y\sqrt{a-1} \leq (\sqrt{a} + \sqrt{a-1})^{2t+1}.$$

Set

$$w = k\sqrt{a} + \ell\sqrt{a-1} = (x\sqrt{a} + y\sqrt{a-1})(\sqrt{a} - \sqrt{a-1})^{2t}.$$

Then $w\tilde{w} = 1$ (in particular, $k\ell \neq 0$) and

$$\sqrt{a} - \sqrt{a-1} < w \leq \sqrt{a} + \sqrt{a-1}.$$

One of the numbers w and $\tilde{w}$ (the one whose coefficients have the same sign) is at least $\sqrt{a} + \sqrt{a-1}$, while the other (from the equality $w\tilde{w} = 1$) is at most $\sqrt{a} - \sqrt{a-1}$. Taking into account the inequalities for w , we obtain $w = \sqrt{a} + \sqrt{a-1}$, from which the required formula follows.

(b) Let (a, s) be a positive integer solution of the equation

$$\frac{x^{2k+1} - 1}{x - 1} = y^2.$$

Note that $a > 1$ by definition.

Then

$$a \cdot b^2 - (a-1) \cdot s^2 = 1$$

with $b = a^k$.

From (a) we obtain

$$b = a^k = a^t + \binom{2t+1}{2} a^{t-1}(a-1) + \binom{2t+1}{4} a^{t-2}(a-1)^2 + \dots + \binom{2t+1}{2t} (a-1)^t. \quad (*)$$

Since $a > 1$ and from (*) we get $k > t$. Next, denote by L and R the left-hand and right-hand sides of (*) and consider several cases.

Case 1. Let $2 \mid a$. Then L is even, while in R all summands except the last one are even. This is impossible.

Case 2. Suppose that the prime factorization of a contains $p^\alpha > 3$ for an odd prime p . Then L is divisible by $p^{k\alpha}$. We will show that R is divisible by a smaller power of p , obtaining a contradiction.

Set $\beta = v_p(2t+1) \leq t < k$. We will show that all summands in R , except the last one, are divisible by $p^{\beta+1}$, from which it will follow that $v_p(R) = \beta < k \leq k\alpha$.

For this it suffices to show that

$$v_p \left(\binom{2t+1}{2(t-i)} \right) > \beta - i\alpha$$

for all $1 \leq i \leq \beta/\alpha$. Recall that either $p > 3$, or $p = 3$ and $\alpha > 1$; then under our restrictions on i we have $2i+1 < p^\beta$, and then the left-hand side equals $v_p(2t+1) - v_p(2i+1) = \beta - v_p(2i+1)$. It remains to note that for $p^\alpha > 3$ the inequality $v_p(2i+1) < i\alpha$ holds, since

$$2i+1 < (p^\alpha)^i.$$

Case 3. Only the case $a = 3$ remains. Again set $\beta = v_3(2t+1)$. If $\beta = 0$, then in the sum R only the last summand is not divisible by 3, that is, R is not divisible by a , which is impossible. Hence $\beta > 0$, and then $t = 3l+1$. For $l = 0$ we obtain $k = 2$, and the pair $(3, 11)$ is a solution. Let $l \geq 1$. Then the sum of the last two summands in R equals

$$R' = 2^t(2t+1) + 2^{t-2}(2t+1)2t(2t-1) = 2^{t-1}(2t+1)(18l^2 + 9l + 3),$$

and $v_3(R') = \beta + 1$. But in each of the remaining terms 3 enters to a higher power (this is proved in the same way as above, using the inequality $v_3(2i + 1) < i - 1$ for $i > 1$). Therefore, R cannot be a power of three, and hence there are no other solutions. ■

Problem 3.3. (a) Solve the equation

$$\frac{x^{4k+2} - 1}{x - 1} = 2y^2$$

for positive integer k .

(b) Solve the equation

$$\frac{x^{4k} - 1}{x - 1} = 2y^2$$

for positive integer k .

Solution. (a) Suppose there is a positive integer k such that given equation has positive integer solution. Notice that x is odd. Rewrite the equation as

$$\frac{x^{2k+1} - 1}{x - 1} \cdot \frac{x^{2k+1} + 1}{2} = y^2.$$

It is easy to see that numbers $\frac{x^{2k+1}-1}{x-1}$ and $\frac{x^{2k+1}+1}{2}$ are coprime, therefore they are both perfect squares. It follows from Problem 3.2b that $x = 3$ and $k = 2$. But then $\frac{x^{2k+1}+1}{2} = \frac{3^5+1}{2} = 122$, which is not perfect square, contradiction.

(b) (**by A. Shturman**) Assume there is a positive integer $n > 1$ such that the equation

$$\frac{x^{2n} - 1}{x - 1} = 2y^2$$

has a positive integer solution. Choose the minimal $n = n_0$ with this property. Again notice that x is odd. By (a) n_0 is even, so $n_0 = 2l$. Rewrite the equation as

$$\frac{x^{2l} - 1}{x - 1} \cdot \frac{x^{2l} + 1}{2} = y^2.$$

It is easy to see that numbers $\frac{x^{2l}-1}{x-1}$ and $\frac{x^{2l}+1}{2}$ are coprime, therefore they are both perfect squares, respectively z^2 and t^2 . Notice that

$$z^2 = \frac{x^{2l} - 1}{x - 1} = \frac{x^l - 1}{x - 1}(x^l + 1). \quad (*)$$

If l is odd then $\frac{x^l-1}{x-1}$ is odd too, and it is coprime with $x^l + 1$. Hence $\frac{x^l-1}{x-1}$ and $x^l + 1$ are perfect squares. It follows from Problem 3.2b that either $l = 1$ or $x = 3, l = 5$. The second case is impossible because $3^5 + 1 = 244$ is not a perfect square. Hence $l = 1$, and numbers $x + 1, \frac{x^2+1}{2}$ are both perfect squares.

Number $x + 1$ is even, so there are positive integer a, b such that $x + 1 = 4a^2, x^2 + 1 = 2b^2$. It follows that

$$8a^4 - 4a^2 + 1 = b^2.$$

This equation in a, b has no positive integer solutions but the jury are unaware of elementary proofs. We accepted solution modulo of proof of this fact.

If l is even then

$$\left(\frac{x^l - 1}{x - 1}, x^l + 1\right) = 2,$$

and $\frac{x^l - 1}{x - 1}$ is a twice a square by (*). It follows that $l = 2$, otherwise we have contradiction with choice of n_0 as $l < 2n_0 = 4l$. Hence $\frac{x^2 + 1}{2}$ and $\frac{x^4 + 1}{2}$ are perfect squares. It is impossible because

$$\frac{x^4 + 1}{2} < \frac{x^2(x^2 + 1)}{2} < \left(\sqrt{\frac{x^4 + 1}{2}} + 1\right)^2.$$

■

Problem 3.4. Prove that the equation

$$(2^x - 1)(3^x - 1) = y^2$$

has no positive integer solutions.

Solution. Assume the opposite, let (n, m) be a positive integer solution. If n is odd, then $v_2((2^n - 1)(3^n - 1)) = 1$, a contradiction. So n is even. Since $(2^n - 1)(3^n - 1) = m^2$, we can assume that $2^n - 1 = da^2$ and $3^n - 1 = db^2$ with positive integers a, b and squarefree d .

It is easy to see that $d > 1$. Then $(2^{\frac{n}{2}}, a)$ and $(3^{\frac{n}{2}}, b)$ are solutions to Pell's Equation

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

The first components of solutions to this Pell's equation are described by the recurrence relation

$$x_0 = 1, x_1 = t, x_{k+2} = 2tx_{k+1} - x_k$$

for some integer t . It follows that $2^{\frac{n}{2}}$ and $3^{\frac{n}{2}}$ are both terms of the sequence x_k .

If t is odd then every term of $\{x_k\}$ is odd while $2^{\frac{n}{2}}$ is even, a contradiction. So t is even. It follows from the recurrence relation that x_k is even iff k is odd.

If $t \equiv 1 \pmod{3}$ then $x_k \equiv 1 \pmod{3}$ for any k , while $3^{\frac{n}{2}}$ is a multiple of 3, a contradiction. If $t \equiv 2 \pmod{3}$, then $x_k \equiv 1 \pmod{3}$ when k is even and $x_k \equiv 2 \pmod{3}$ when k is odd. But $3^{\frac{n}{2}}$ is a multiple of 3, a contradiction.

Hence t is a multiple of 3. It follows from the recurrence relation that x_k is a multiple of 3 iff k is odd. But we already know that k is odd iff x_k is even, so x_k can not be a power of 3, a contradiction. ■

Problem 3.5. Prove that the equation

$$(2^x - 1)(5^x - 1) = y^n$$

has no positive integer solutions for $n > 3$.

Solution.

If $n \mid x$, then the left side is bounded between $(10^{\frac{x}{n}} - 1)^n$ and $(10^{\frac{x}{n}})^n$, a contradiction.

Assume without loss of generality n is a prime or 4, 6, 9. We deal with the second case first. As $4 \mid 5^x - 1$, we get that $\nu_2(5^x - 1) \geq 4$, so $4 \mid x$. Therefore, $3 \mid 2^x - 1$, so $\nu_3((2^x - 1)(5^x - 1)) \geq 4$, implying $9 \mid x$. So $36 \mid x$, it is impossible when $n = 4, 6, 9$.

Now, let p be prime. We show by induction on p that if $n \geq \max(p, 4)$ then every prime $q \leq p$ must divide y and $p \mid x$. The cases $p = 2, 3$ have already been shown. For the inductive step, we already know that every prime $q < p$ must divide y . Then, as $\nu_q((2^x - 1)(5^x - 1)) \geq n \geq p$ and $\nu_q((2^{q-1} - 1)(5^{q-1} - 1)) \leq \max(2, q-1) \leq q$ (it is easy to show for $q = 2, 3, 5, 7$, then bound for $q \geq 11$), this implies by LTE that $q^{\lceil \frac{n-q}{2} \rceil} \mid x$. Since $q^{\frac{n-q}{2}} > n - 2$, this means the largest power of q dividing x is at least $n - 1 \geq p - 1$, so $p - 1 \mid x$. This implies $p \mid y$. Furthermore, the exponent of p in $(2^x - 1)(5^x - 1)$ is at most $p - 1 < n$ as $p \geq 5$, so $p \mid x$.

Therefore, there are no positive integer solutions when $n \geq 4$. ■

4 Equations in factorial domains

A subset R of the set of real numbers or of the set of complex numbers is called a **ring** if $1 \in R$ and if R is closed under addition, subtraction, and multiplication, i.e., for any $x, y \in R$ we have $x + y, x - y, x \cdot y \in R$. Trivial examples of rings: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. For a complex number α , denote by $\mathbb{Z}[\alpha]$ the minimal ring containing α . The ring $\mathbb{Z}[i]$ is called the *Gaussian ring* and has a short description:

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}.$$

Problem 4.1. Prove this and similarly describe the rings

$\mathbb{Z}[\sqrt{2}], \mathbb{Z}[\sqrt{2}, \sqrt{3}], \mathbb{Z}[\sqrt[3]{2}], \mathbb{Z}[\omega], \mathbb{Z}[\pi]$, where $\omega := e^{2\pi i/3} = (-1 + i\sqrt{3})/2$.

(You may use without proof the transcendence of π .)

Solution. Answers:

$$\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}, \quad \mathbb{Z}[\sqrt{2}, \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Z}\},$$

$$\mathbb{Z}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Z}\}, \quad \mathbb{Z}[\omega] = \{a + b\omega \mid a, b \in \mathbb{Z}\},$$

$$\mathbb{Z}[\pi] = \{P(\pi) \mid P \in \mathbb{Z}[x]\}.$$

Proof sketch: In each equality, the set on the right-hand side is contained in the left-hand side by the closure property of a ring. At the same time, in each equality the left-hand set is contained in the right-hand one, since the right-hand set is a ring. ■

Definition. We say that a number $a \in R$ is *divisible* by a nonzero number $b \in R$ in the ring R if there exists a number $q \in R$ such that $a = bq$.

For example, the real number $1 + \sqrt{2}$ is divisible by the real number $3 + 2\sqrt{2}$ in the ring $\mathbb{Z}[\sqrt{2}]$, since $1 + \sqrt{2} = (3 + 2\sqrt{2})(\sqrt{2} - 1)$.

It turns out that for some rings an **analogue of the Fundamental Theorem of Arithmetic (FTA)** holds. In order to state this assertion, we need to define analogues of “units” and “prime” numbers in an arbitrary ring.

Definition. A *unit* or *invertible number* in a ring R is a number that divides in R every number of the ring R .

In the ring $\mathbb{Z}$ the units are the numbers ± 1 . However, in other rings the list of units can be larger. For example, the number $3 + 2\sqrt{2}$ is a unit in $\mathbb{Z}[\sqrt{2}]$.

Problem 4.2. Describe all units in the rings $\mathbb{Z}[i]$ and $\mathbb{Z}[\sqrt{D}]$, where D is a positive integer and is not a perfect square.

Solution. Answer: for $\mathbb{Z}[i] - \pm 1, \pm i$, for $\mathbb{Z}[\sqrt{D}]$ — the solutions of the equation $a^2 - Db^2 = \pm 1$.

Proof sketch for $\mathbb{Z}[i]$: A number $z = a + bi$ is a unit of the ring $\mathbb{Z}[i]$ if and only if $1/z \in \mathbb{Z}[i]$.

By the equality

$$\frac{1}{z} = \frac{1}{a + bi} = \frac{a - bi}{(a + bi)(a - bi)} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i$$

this is equivalent to a and b being divisible by $a^2 + b^2$. This is equivalent to $a^2 + b^2 = 1$, whence $z = \pm 1, \pm i$.

Proof sketch for $\mathbb{Z}[\sqrt{D}]$: A number $z = a + b\sqrt{D}$ is a unit of the ring $\mathbb{Z}[\sqrt{D}]$ if and only if $1/z \in \mathbb{Z}[\sqrt{D}]$. By the equality

$$\frac{1}{z} = \frac{1}{a + b\sqrt{D}} = \frac{a - b\sqrt{D}}{(a + b\sqrt{D})(a - b\sqrt{D})} = \frac{a}{a^2 - Db^2} - \frac{b}{a^2 - Db^2}\sqrt{D}$$

this is equivalent to a and b being divisible by $a^2 - Db^2$. In the next paragraph we prove that this is equivalent to $a^2 - Db^2 = \pm 1$.

Since a and b are divisible by $n = a^2 - Db^2$, it follows that a^2 and b^2 are divisible by n^2 , whence n is divisible by n^2 , which is possible only when $n = \pm 1$. ■

Definition. A non-invertible number is called *irreducible* in the ring R if in every representation of this number as a product of two numbers from R , one of the factors is a unit of this ring.

Problem 4.3. Determine whether the following Gaussian numbers are irreducible. If not, decompose them into a product of irreducible numbers:

(a) 2, 3, 5, 7, 11, 13; (b) $1 + i$, $3 + 2i$, $2 + 3i$; (c) $1 + 3i$, $3 + 4i$, $5 + 7i$.

Solution. Answer: $2 = (1 + i)(1 - i)$, $5 = (2 + i)(2 - i)$, $13 = (2 + 3i)(2 - 3i)$, $1 + 3i = (1 + i)(2 + i)$, $3 + 4i = (2 + i)^2$, $5 + 7i = (1 + i)(6 + i)$; the rest numbers are irreducible.

Lemma 1. If the norm $N(a + bi) = a^2 + b^2$ of a Gaussian number $z = a + bi$ equals a prime number p then z is irreducible.

Proof: take an arbitrary factorization $z = xy$. By multiplicativity of the norm, $p = N(z) = N(xy) = N(x)N(y)$. Since p is prime, without loss of generality $N(x) = 1$. Hence x is a unit. $\square$

Lemma 2. Let p be a prime of the form $4k + 3$; then it is irreducible in $\mathbb{Z}[i]$.

Proof sketch: take an arbitrary factorization $p = xy$. By multiplicativity of the norm, $p^2 = N(p) = N(xy) = N(x)N(y)$. Suppose that neither x nor y is a unit. Then $N(x) = N(y) = p$. Then p is representable as a sum of two squares. But every square gives remainder 0 or 1 upon division by 4, so the sum of two squares cannot be congruent to 3 modulo 4. Contradiction. $\square$

Proof of irreducibility: By Lemma 1 the numbers from item b, as well as the numbers $1 - i$, $2 + i$, $2 - i$, $2 - 3i$, $6 + i$, are irreducible. By Lemma 2 the numbers 3, 7, 11 are irreducible. $\blacksquare$

Problem 4.4. Find all irreducible Gaussian numbers.

Solution. We prove that a Gaussian number z is irreducible if and only if its norm is a prime number, or it is itself a prime of the form $4k + 3$.

From right to left this assertion is proved in the solution of Problem 4.3. We prove it from left to right.

Let the norm $a^2 + b^2$ of an irreducible number $z = a + bi$ be divisible by a prime p of the form $4k + 3$. Then $a^2 + b^2 \equiv 0 \pmod{p}$. If $b = 0$, then a is divisible by p and z is itself a prime. Otherwise $b \neq 0$, so b is invertible modulo p and $(ab^{-1})^2 \equiv -1 \pmod{p}$. Hence -1 is a quadratic residue modulo p , which does not happen for primes of this form.

Let the norm of z be composite and divisible by a prime p representable as a sum of two squares: $p = x^2 + y^2$. By Fermat's theorem on sums of two squares, such a representation exists for 2 and for any prime of the form $4k + 1$. We have $a^2 \equiv -b^2 \pmod{p}$ and $x^2 \equiv -y^2 \pmod{p}$, whence $a^2x^2 \equiv b^2y^2 \pmod{p}$ and $(ax + by)(ax - by) \equiv 0 \pmod{p}$. Consider cases.

First: if $ax + by$ is divisible by p , then

$$0 \equiv ax + by \equiv ax^2 + byx \equiv a(-y^2) + byx \equiv bx - ay \pmod{p}$$

and

$$a + bi = (x + yi) \left(\frac{ax + by}{p} + \frac{bx - ay}{p}i \right),$$

where both factors are non-units. Contradiction.

Second: if $ax - by$ is divisible by p , then

$$0 \equiv ax - by \equiv axy + b(-y^2) \equiv axy + bx^2 \equiv ay + bx \pmod{p}$$

and

$$a + bi = (x - yi) \left(\frac{ax - by}{p} + \frac{bx + ay}{p}i \right),$$

where both factors are non-units. Contradiction. ■

Definition. We call two nonzero numbers in a ring **associated** if their ratio is a unit of this ring. A *complete factorization* of a nonzero non-invertible number $x \in R$ is a representation of the form

$$x = p_1 \cdot \dots \cdot p_m,$$

where $p_1, \dots, p_m$ are irreducible numbers in R . Two complete factorizations

$$x = p_1 \cdot \dots \cdot p_m = q_1 \cdot \dots \cdot q_k$$

are called *equivalent* if $m = k$ and there exists a bijection

$$\pi : \{1, \dots, m\} \rightarrow \{1, \dots, k\}$$

such that p_i and $q_{\pi(i)}$ are associated for each $i = 1, \dots, m$.

Finally, a ring is called **factorial** if every nonzero non-invertible number in this ring has a complete factorization, and any two of its complete factorizations are equivalent. For example, the ring $\mathbb{Z}$ is factorial — this is precisely the fundamental theorem of arithmetic.

Theorem. The Gaussian ring $\mathbb{Z}[i]$, as well as the rings $\mathbb{Z}[i\sqrt{2}]$ and $\mathbb{Z}[\omega]$, are factorial.

Section 6 is devoted to the proof of this theorem. In the following problems of this section, as well as in the problems of Section 5, you may use this theorem without proof.

Problem 4.5. Find a ring in which for some number

- (a) there is no complete factorization;
- (b) there exist two complete non-equivalent factorizations.

Solution. (a) Let $\pi_n = \sqrt[2^n]{\pi}$ and consider

$$R = \mathbb{Z}[\pi, \sqrt{\pi}, \sqrt[4]{\pi}, \sqrt[8]{\pi}, \sqrt[16]{\pi}, \dots] = \bigcup_{n=1}^{\infty} \mathbb{Z}[\pi_n].$$

Lemma 1. If x is transcendental, then $\sqrt{x}$ is also transcendental.

Since π is transcendental, repeated application of Lemma 1 gives the transcendence of the numbers π_n for each n .

Lemma 2. The number π is not invertible in R .

Proof of Lemma 2. Assume the contrary; let $1/\pi \in R$. Then there exists n such that $1/\pi \in \mathbb{Z}[\pi_n]$ and $\pi = \pi_n^{2^n}$. Take $P \in \mathbb{Z}[t]$ such that $1/\pi = P(\pi_n)$. Then $\pi_n^{2^n} P(\pi_n) - 1 = 0$, which contradicts the transcendence of π_n . □

Suppose that the non-invertible π has a complete factorization in R , i.e.,

$$\pi = p_1 \cdot \dots \cdot p_m$$

for some irreducible $p_1, \dots, p_m \in R$. There exists n such that $p_1, \dots, p_m \in \mathbb{Z}[\pi_n]$.

Lemma 3. Let x be transcendental, let $k \geq 0$ be an integer, and suppose that

$$x^k = P(x)Q(x),$$

where $P, Q \in \mathbb{Z}[t]$ are polynomials with integer coefficients. Then there exist $a, b \geq 0$ with $a + b = k$, and $\varepsilon = \pm 1$, such that $P(x) = \varepsilon x^a$ and $Q(x) = \varepsilon x^b$.

Applying Lemma 3 with $x = \pi_n$ and $k = 2^n$, we obtain that $p_i = \varepsilon_i \pi_n^{k_i}$, where $\varepsilon_i = \pm 1$ and $k_i \geq 0$ for each $i = 1, \dots, m$. But for any k , the number π_n^k is not irreducible in R , because $\pi_n = \pi_{n+1}^2$.

Proof of Lemma 1. Assume the contrary; let $\sqrt{x}$ be algebraic. Then there exists $P \in \mathbb{Z}[t]$ such that $P(\sqrt{x}) = 0$. Consider $Q(t) = P(t)P(-t) \in \mathbb{Z}[t]$. The polynomial Q is even, so there exists $R \in \mathbb{Z}[t]$ such that $Q(t) = R(t^2)$. Then $R(x) = Q(\sqrt{x}) = 0$. Contradiction. $\square$

Proof of Lemma 3. Since x is transcendental, for a number of the form $P(x)$, where $P \in \mathbb{Z}[t]$, the maximal and minimal degrees of monomials of the polynomial P are well-defined, denoted by $\deg(P)$ and $\mindeg(P)$, respectively. Apply the trivial inequality $\deg(P) \geq \mindeg(P)$ to the equality from the condition of Lemma 3:

$$k = \deg(PQ) = \deg(P) + \deg(Q) \geq \mindeg(P) + \mindeg(Q) = \mindeg(PQ) = k.$$

Hence $\deg(P) = \mindeg(P)$ and $\deg(Q) = \mindeg(Q)$. Therefore P and Q are monomials. $\square$

(b) In the ring $\mathbb{Z}[i\sqrt{5}]$ we have $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$. We show that these factors are pairwise non-associated and irreducible.

Similarly to the solution of Problem 4.2, the only units of $\mathbb{Z}[i\sqrt{5}]$ are ± 1 . Consequently, the factors are pairwise non-associated.

If these factors had a nontrivial divisor, then the norm of this divisor would be a nontrivial divisor of the norms of these factors. The norms of these factors belong to the set $\{2^2, 2 \cdot 3, 3^2\}$, i.e., the norm of a nontrivial divisor would be either 2 or 3. But the equations $a^2 + 5b^2 = 2$ and $a^2 + 5b^2 = 3$ have no solutions in integers. Therefore these factors are irreducible in $\mathbb{Z}[i\sqrt{5}]$. $\blacksquare$

The greatest common divisor $\gcd(a, b)$ of elements a and b , not both zero, in a ring R is any number $d \in R$ such that:

- (i) d is a common divisor of a and b , and
- (ii) if c is a common divisor of a and b , then c is also a divisor of d .

The existence of $\gcd(a, b)$ in an arbitrary ring is not guaranteed, but it exists for factorial rings (think about why). The numbers a and b are called *coprime* if every $\gcd(a, b)$ is a unit in R .

Problem 4.6. (a) Find a greatest common divisor of the numbers $4 + i$ and $3 + 4i$.

(b) For which integers z, t are the Gaussian numbers 2 and $z + ti$ coprime?

Solution. (a) The numbers $4 + i$ and $3 + 4i$ are coprime, since their norms are coprime.

(b) Let r_z and r_t be the remainders of z and t upon division by 2, respectively. Then $d = (2, z + ti) = (2, r_z + r_t i)$. Since $r_z, r_t \in \{0, 1\}$, by quickly checking cases we obtain that d is a unit only when $r_z \not\equiv r_t \pmod{2}$. $\blacksquare$

Problem 4.7. Let x and y be relatively prime numbers in a factorial ring R , such that $xy = z^n$ for some $z \in R$ and an integer $n \geq 2$. Prove that $x = u_1v_1^n$ and $y = u_2v_2^n$ for some $v_1, v_2 \in R$ and some invertible numbers $u_1, u_2 \in R$.

Solution. For an irreducible $p \in R$, introduce $v_p(r)$ as the largest power of p that divides $r \in R$. This function is well defined since the ring R is factorial. Then, for any irreducible p dividing x , we have

$$v_p(x) \stackrel{(1)}{=} v_p(xy) = v_p(z^n) = nv_p(z),$$

where equality (1) is true since x, y are relatively prime. Therefore, any irreducible number occurs in x to a power that is a multiple of n , that is, $x = u_1v_1^n$. Similarly, $y = u_2v_2^n$. ■

The developed theory allows us to solve equations with variables in an arbitrary factorial ring. In particular, you are now able to solve the following problem.

Problem 4.8. Prove using the Theorem that all integer solutions to the equation $x^2 + y^2 = z^2$ (Pythagorean triples), up to signs and permutation of the variables x and y , are described by the formulas:

$$x = k(m^2 - n^2), \quad y = k(2mn), \quad z = k(m^2 + n^2),$$

where k, m, n are integer.

Solution. Without loss of generality, we may assume that x, y, z are pairwise coprime in $\mathbb{Z}$. Looking at the equation modulo 4, we find that x and y must have opposite parity. It is easy to verify that, in this case, the numbers $x + yi$ and $x - yi$ are coprime in $\mathbb{Z}[i]$. Let us rewrite the equation in the form

$$(x + yi)(x - yi) = z^2.$$

By Problem 4.7, there exist a unit $\varepsilon \in \mathbb{Z}[i]$ and integers m, n such that

$$x + yi = \varepsilon(m + ni)^2$$

from which the parameterization specified in the condition is obtained up to sign and permutation of variables. ■

The problem below is useful for solving equations both in the ring of integers $\mathbb{Z}$ and in an arbitrary factorial ring.

Problem 4.9. Suppose that the ring R is factorial and $x, y, z, t \in R$. Prove that all solutions to the equation $xy = zt$ in R are described

$$x = uv, \quad y = wr, \quad z = uw, \quad t = vr,$$

where $u, v, w, r \in R$.

Solution. If $(x, y, z, t) = (uv, wr, uw, vr)$, then $xy = uvwr = zt$. Conversely, assume that $xy = zt$. If $x = 0$ then $zt = 0$, this implies that either $z = 0$ or $t = 0$. In the first case, take $u = 0, v = t, w = y, r = 1$, while in the second case take $u = z, v = 0, w = 1, r = y$.

Now assume that $x \neq 0$ and let $u = (x, z)$. Then $x = uv$ and $z = uw$ with $v, w \in R$ coprime and $v \neq 0$. Substituting this into the equation $xy = zt$, we obtain $uvy = uwt$, or $vy = wt$. Because v and w are coprime, and v is a divisor of wt , the Theorem implies that v is a divisor of t , so we can write $t = vr$ for some $r \in R$. Then $vy = w(vr)$, hence $y = wr$. ■

Problem 4.10. Describe all solutions to the equation

$$x^2 + y^2 = zt$$

in integers.

Solution. First, we describe solutions for coprime and positive x, y, z, t . Then

$$(x + yi)(x - yi) = zt,$$

and by Problem 4.9

$$x + yi = mn, \quad x - yi = pq, \quad z = np, \quad t = mq. \quad (1)$$

Because np and mq are positive integers, it follows that $n = k\bar{p}$ and $q = l\bar{m}$ for some positive rational numbers k and l . On the other hand, $N(mn) = N(pq)$ implies $N(km\bar{p}) = N(lp\bar{m})$ and $k = l$.

Let u and v be relatively prime positive integers such that $k = \frac{u}{v}$. Then

$$x + yi = \frac{u}{v}m\bar{p}, \quad x - yi = \frac{u}{v}p\bar{m}, \quad z = \frac{u}{v}p\bar{p}, \quad t = \frac{u}{v}m\bar{m}.$$

This means that $u \mid x, y, z, t$ and thus $u = 1$. We also have

$$x + yi = \frac{v}{u}n\bar{q}, \quad x - yi = \frac{v}{u}q\bar{n}, \quad z = \frac{v}{u}n\bar{n}, \quad t = \frac{v}{u}q\bar{q},$$

implying $v \mid x, y, z, t$ and thus $v = 1$. Let $n = u + vi$ and $m = w + ri$, where $u, v, w, r \in \mathbb{Z}$. Then (1) yields

$$x = uw + vr, \quad y = ur - vw, \quad z = u^2 + v^2, \quad t = w^2 + r^2.$$

It is easy to check that for u, v, w, r not necessarily positive and coprime the next parameterization holds

$$x = s(uw + vr), \quad y = s(ur - vw), \quad z = s(u^2 + v^2), \quad t = s(w^2 + r^2).$$

with integers s, u, v, w, r . ■

Problem 4.11. Prove that all solutions of the equation

$$x^2 + x + 1 = yz$$

in integers are described by

$$x = ab + bc + cd, y = \varepsilon(a^2 + ac + c^2), z = \varepsilon(b^2 + bd + d^2),$$

where $\varepsilon = \pm 1$ and a, b, c, d are integers that satisfy $ad - bc = 1$.

Solution. Rewrite the equation as

$$(x - \omega)(x - \omega^2) = yz.$$

By Problem 4.9 it is true that

$$x - \omega = uv, x - \omega^2 = wr, y = uw, z = vr$$

for some $u, v, w, r \in \mathbb{Z}[\omega]$. If $u = a - c\omega^2$, $v = b - d\omega$, then

$$x - \omega = ab + bc + cd - (ad - bc)\omega,$$

so $ad - bc = 1$ and $x = ab + bc + cd$.

Notice that $u/\bar{w} = uw/(w\bar{w}) = y/(w\bar{w}) \in \mathbb{Q}$. Hence $qu = p\bar{w}$ for some coprime p, q in $\mathbb{Z}$. It is easy to see that p, q are also coprime in $\mathbb{Z}[\omega]$. Since qu is divisible by p , we see by the Theorem that $u = pu'$ for some $u' \in \mathbb{Z}[\omega]$. But then $(x - \omega)/p = u'v \in \mathbb{Z}[\omega]$, therefore $|p| = 1$ and $u = \varepsilon_1\bar{w}$, or $w = \varepsilon_1\bar{u}$ with $\varepsilon_1 = \pm 1$. Analogously $r = \varepsilon_2\bar{v}$ with $\varepsilon_2 = \pm 1$.

Further,

$$y = uw = \varepsilon_1 u\bar{u} = \varepsilon_1(a - c\omega^2)(a - c\omega) = \varepsilon_1(a^2 + ac + c^2).$$

Analogously $z = \varepsilon_2(b^2 + bd + d^2)$. It is left to notice that $yz = x^2 + x + 1 > 0$, so $\varepsilon_1\varepsilon_2 = 1$ and $\varepsilon_1 = \varepsilon_2$. ■

5 On the equations of Lebesgue–Nagell type

The history of the Lebesgue–Nagell exponential equations $x^2 + C = Ay^n$ began in 1850 when the French mathematician V. Lebesgue solved the equation with coefficients $A = C = 1$ for an arbitrary integer number n . In the first half of the 20th century, the Norwegian researcher T. Nagell significantly developed solution methods for a number of similar equations, including the famous Ramanujan–Nagell equation $x^2 + 7 = 2^n$. A major theoretical breakthrough occurred in the 1970s and 1980s, when mathematicians T. Schorey and R. Tijdeman proved that, for fixed coefficients, the equation has only a finite number of solutions with integers $n \geq 3$. A significant result was the work of scientists J. Bugeaud, M. Mignotte, and S. Siksek, published in 2006. The authors completely solved the equation $x^2 + C = y^n$ for $1 \leq C \leq 100$.

Currently, the Lebesgue–Nagell equations remain unsolved in their general form. The main difficulty is that different parameters produce structures with dissimilar properties. Nevertheless, all the equations presented below can be solved by elementary means.

Problem 5.1. Solve the equation

$$x^2 + 1 = y^n$$

for integer $n \geq 2$.

Solution. It is easy to see that the case of even n is impossible because two positive perfect squares can not differ by 1. Therefore we may assume that $n = p$ is an odd prime. Suppose there exists a positive integer solution of $x^2 + 1 = y^p$. If y is even then $y^2 \equiv 3 \pmod{4}$, which of course leads to a contradiction. So y is odd and it immediately follows that x has to be even.

In the ring $\mathbb{Z}[i]$ we have $y^p = x^2 + 1 = (x - i)(x + i)$. Now there is no prime $\pi \in \mathbb{Z}[i]$ such that $\pi | x - i$ and $\pi | x + i$. For suppose there is such a prime, then it has to divide $x + i - (x - i) = 2i$, so π divides 2, since i is a unit. It follows that 2 divides y , which we have proven to be impossible. It follows from problem 4.7 that, up to units, $x + i$ and $x - i$ are both p -th powers in $\mathbb{Z}[i]$. Since p is odd, all units in $\mathbb{Z}[i]$ are p -th powers, so there are $a, b \in \mathbb{Z}$ such that $x - i = (a + bi)^p$ and $x + i = \overline{x - i} = (a - bi)^p$.

Using Newton's Binomial Theorem, we can write

$$x - i = (a + bi)^p = \sum_{j=0}^p \binom{p}{j} a^j (bi)^{p-j}.$$

Taking the imaginary part at both sides, we get

$$-1 = \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} a^{2j} b^{p-2j} i^{p-2j-1} = b \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} a^{2j} b^{p-2j-1} i^{p-2j-1}. \quad (1)$$

So b divides -1 , which yields $b = \pm 1$.

Now we know that $y^p = (a + bi)^p (a - bi)^p = (a + i)^p (a - i)^p = (a^2 + 1)^p$, so $y = a^2 + 1$ and a is even. It is obvious that a is a nonzero integer, because otherwise $y = 0$.

Going back to (1), we have

$$-1 = b \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} a^{2j} (-1)^{\frac{p-1}{2}-j} = b(-1)^{\frac{p-1}{2}} \sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} (-a^2)^j.$$

From this we obtain

$$\sum_{j=0}^{\frac{p-1}{2}} \binom{p}{2j} (-a^2)^j = \pm 1.$$

Viewing this equality modulo 4, all terms with $j > 0$ vanish as a is even, so if we take the sum modulo 4 we get 1. It follows that at the right-hand side we also have 1. Therefore $\sum_{j=1}^{\frac{p-1}{2}} \binom{p}{2j} (-a^2)^j = 0$. We find

$$a^2 \binom{p}{2} = \sum_{j=2}^{\frac{p-1}{2}} \binom{p}{2j} (-a^2)^j. \quad (2)$$

Note that this equation also holds if $p = 3$, then it says that $a^2 \binom{p}{2} = 0$, which implies excluded case $a = 0$.

Since

$$\binom{p}{2k} = \frac{p(p-1)}{2k(2k-1)} \binom{p-2}{2k-2},$$

we obtain for $j > 1$

$$v_2 \left(a^{2j} \binom{p}{2j} \right) \geq 2jv_2(a) + v_2 \left(\binom{p}{2} \right) - v_2(j) > 2v_2(a) + v_2 \left(\binom{p}{2} \right) = v_2 \left(a^2 \binom{p}{2} \right).$$

We got the inequality

$$v_2 \left(a^2 \binom{p}{2} \right) < v_2 \left(\sum_{j=2}^{\frac{p-1}{2}} \binom{p}{2j} (-a^2)^j \right),$$

which contradicts to (2). ■

Problem 5.2. (a) Prove that the equation

$$x^2 + 9 = y^q$$

has no solutions for prime $q \equiv 3 \pmod{4}$.

(b) Prove that the equation

$$x^2 + 9 = y^q$$

has no solutions for prime $q \equiv 1 \pmod{4}$.

Solution. Like in the previous problem we get that y is odd, x is even and number $3+ix$ and $3-ix$ are coprime in $\mathbb{Z}[i]$. So there are integer a, b such that $3+ix = (a+bi)^p, y = a^2 + b^2$.

Equating real parts, we have

$$3 = a^q - \binom{q}{2} a^{q-2} b^2 + \dots - \binom{q}{q-1} (-1)^{\frac{q-1}{2}} a b^{q-1}.$$

Therefore, $a|3$ and since $q| \binom{q}{k}$ for $1 \leq k < q$, we get $a^q \equiv a \equiv 3 \pmod{q}$. So, we have either $a = -3, q = 3$ or $a = 3$. In the first case, we get the equality $x^2 + 1 = (y-2)(y^2 + 2y + 4)$. It is impossible because the right side is divisible by some prime $p \equiv 3 \pmod{4}$ while prime divisors of the left side are only of a form $4n + 1$.

So, $a = 3$ and therefore transposing the terms, we get

$$3^{q-1} - 1 = \binom{q}{2} 3^{q-3} b^2 - \dots - \binom{q}{q-1} (-1)^{\frac{q-1}{2}} b^{q-1}.$$

Since $y = 9 + b^2$ is odd, b must be even. Now, we write

$$3^{q-1} - 1 = b^2 \left(\binom{q}{2} 3^{q-3} - \dots - \binom{q}{q-1} (-1)^{\frac{q-1}{2}} b^{q-3} \right).$$

(a) If $q \equiv 3 \pmod{4}$, then $v_2(3^{q-1} - 1) = 3$. But

$$\frac{\text{RHS}}{b^2} \equiv \binom{q}{2} 3^{q-3} \equiv 1 \pmod{2}.$$

Therefore, $v_2(\text{RHS}) = v_2(b^2) = 2v_2(b)$ which is even, contradiction.

(b) If $q \equiv 1 \pmod{4}$, let $c = v_2(q - 1)$, $d = v_2(b)$. Then, $v_2(3^{q-1} - 1) = c + 2$. From the identity

$$\binom{q}{2k} b^{2k-2} = \binom{q}{2} \cdot \binom{q-2}{2k-2} \cdot \frac{2b^{2k-2}}{(2k-1)(2k)}$$

we infer that $v_2\left(\binom{q}{2}\right) < v_2\left(\binom{q}{2k} b^{2k-2}\right)$ for $k > 1$. Therefore

$$v_2(\text{RHS}) = v_2(b^2) + v_2\left(\binom{q}{2}\right) = 2d + c - 1$$

which has parity different from $c + 2$, contradiction. ■

The following problem illustrates the powerful effect of combining Størmer's method with the theory in Section 4.

Problem 5.3. (a) Describe all solutions of Pell-like equation

$$x^2 - (a^2 + 2)y^2 = -2$$

for positive integer a .

(b) Prove that for odd a this equation has at most two positive integer solutions (x, y) for which every prime divisor of y divides $a^2 + 2$.

(c) Solve the equation

$$x^2 + 2 = y^n$$

for integer $n \geq 2$.

Solution. (a) It follows from solution of Problem 1.13 of the project "Diophantine equations" (<https://t-o-t.org/lktg/2025/1/1-1-diophantine-eng.pdf>) that equation $x^2 - (a^2 + 2)y^2 = -2$ has no more than one class of solutions. One can easily find that $(a, 1)$ is a solution. Since $(a^2 + 1, a)$ is the fundamental solution of Pell's equation $x^2 - (a^2 + 2)y^2 = 1$, we obtain that all positive solutions of the equation

$$x^2 - (a^2 + 2)y^2 = -2$$

are described by

$$x_t + y_t \sqrt{a^2 + 2} = \left(a + \sqrt{a^2 + 2}\right) \left(a^2 + 1 + a\sqrt{a^2 + 2}\right)^t = \frac{(a + \sqrt{a^2 + 2})^{2t+1}}{2^t}$$

with nonnegative integer t .

(b) First note that $y_1 = 1$. Suppose that there is $t > 0$ such that all prime divisors of y_t divide $a^2 + 2$. It follows from the equality

$$2^t \left(x_t + y_t \sqrt{a^2 + 2}\right) = \left(a + \sqrt{a^2 + 2}\right)^{2t+1}$$

that if prime $p = 2u + 1$ divides $2t + 1$ then y_u divides y_t . Using the equality

$$2^{\frac{p-1}{2}} y_u = (a^2 + 2)^{\frac{p-1}{2}} + \dots + \binom{p}{p-3} (a^2 + 2) a^{p-3} + p a^{p-1},$$

we get that y_u has the only prime factor p . If $p > 3$ then the right side of the last inequality is more than $2^{\frac{p-1}{2}} p$ and it gives remainder p modulo p^2 , so y_t cannot be a power of p .

We now left with the case $p = 3$, so $2t + 1$ and y_t are powers of 3. It follows from the equality

$$y_4 = 16a^8 + 56a^6 + 60a^4 + 20a^2 + 1 = (2a^2 + 1)((8a^6 + 24a^4 + 18a^2 + 1)$$

that the only index $t > 0$ that meets the conditions described above is $t = 1$.

(c) It is easy to see that the case of even n is impossible because two positive perfect squares can not differ by 2. Rewrite the equation for odd n

$$x^2 - (a^2 + 2) \left((a^2 + 2)^{\frac{n-1}{2}} \right) = -2.$$

It follows from (b) that $n = 3$ and $\left((a^2 + 2)^{\frac{n-1}{2}} \right) = 2a^2 + 1$. Hence $a = 1$ and $(5, 2)$ is the only solution. ■

Problem 5.4. (a) Solve the equation

$$x^2 + 4 = y^3.$$

(b) Prove that the equation

$$x^2 + 4 = y^q$$

has no solutions for prime $q \equiv 1 \pmod{4}$.

Solution. (a) Let x be odd. The equation can be written as $(2 + ix)(2 - ix) = y^3$. We will show that $2 + ix$ and $2 - ix$ are relatively prime in the ring $\mathbb{Z}[i]$. Indeed, let $z = (2 + ix, 2 - ix)$, $z = c + di$. Then z divides $(2 + ix) + (2 - ix) = 4$ hence; $\bar{z} \mid 4$. It follows that $z \cdot \bar{z} = c^2 + d^2$ divides 16. On the other hand, $z \mid 2 + ix$ implies $\bar{z} \mid 2 - ix$; hence $c^2 + d^2 \mid 4 + x^2$. But x is odd, so $c^2 + d^2 = 1$, implying that z is a unit in $\mathbb{Z}[i]$.

Because $2 + ix$ and $2 - ix$ are relatively prime, from $(2 + ix)(2 - ix) = y^3$ it follows that $2 + ix = (a + bi)^3$ for some integers a and b . Identifying the real and imaginary parts, we get $a(a^2 - 3b^2) = 2$ and $3a^2b - b^3 = x$. The first equation gives $a = \pm 1$ or $a = \pm 2$, yielding a positive solution $(11, 5)$.

If x is even, then y is even. Let $x = 2u$ and $y = 2v$. The equation becomes $u^2 + 1 = 2v^3$, i.e., $(u + i)(u - i) = 2v^3$. Since u is odd, we have $i \pm 1 \mid u \pm 1$. Because $(u + i, u - i) = 1$ and $2 = (1 + i)(1 - i)$, we obtain

$$\frac{u + i}{i + 1} \cdot \frac{u - i}{i - 1} = v^3$$

Since $\frac{u+i}{i+1}$ and $\frac{u-i}{i-1}$ are coprime, it follows from Problem 4.7 that

$$u + i = (1 + i)(a + bi)^3$$

for some integers a and b .

Identifying the real and imaginary parts, we get

$$a^3 - 3a^2b - 3ab^2 + b^3 = u \quad \text{and} \quad a^3 + 3a^2b - 3ab^2 - b^3 = 1.$$

The last relation can be written as

$$(a - b)(a^2 + 4ab + b^2) = 1,$$

yielding the systems

$$\begin{cases} a - b = 1, \\ a^2 + 4ab + b^2 = 1, \end{cases} \quad \text{and} \quad \begin{cases} a - b = -1, \\ a^2 + 4ab + b^2 = -1. \end{cases}$$

The second system has no solutions. Indeed, one can observe that

$$a^2 + 4ab + b^2 = (a + 2b)^2 - 3b^2 \equiv 0, 1 \pmod{3}.$$

The first system has integer solutions $(a, b) = (1, 0)$ and $(a, b) = (0, -1)$, yielding a positive solution $(2, 2)$ to the original equation.

Answer: $(2, 2)$, $(11, 5)$.

(b) If x is even, say $x = 2u$, then y is even, $y = 2v$. The equation becomes $u^2 + 1 = 2^{q-2}v^2$. It has no solutions as $q - 2 > 2$ and 4 does not divide $u^2 + 1$.

If x is odd then numbers $x + 2i$ and $x - 2i$ are coprime in $\mathbb{Z}[i]$. By Problem 4.7 $x + 2i = (a + bi)^q$, for some integers a and b having different parities. Identifying the real and imaginary parts, we obtain

$$2 = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} (a^2)^{(q-1)/2-r} b^{2r+1} (-1)^r. \quad (1)$$

Considering it modulo q , we get

$$2 \equiv b^q (-1)^{(q-1)/2} \equiv b (-1)^{(q-1)/2} \pmod{q},$$

so

$$b = 2(-1)^{(q-1)/2},$$

as $b|2$. Inserting this expression for b in (1), we obtain

$$(-1)^{(q-1)/2} = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} (a^2)^{(q-1)/2-r} (-4)^r. \quad (2)$$

It is given that $q \equiv 1 \pmod{4}$, suppose $\nu_2(q - 1) = s \geq 2$. Now, equation (2) may be written

$$1 - q + q(1 - (a^2)^{(q-1)/2}) = \sum_{r=1}^{(q-1)/2} \binom{q}{2r+1} (a^2)^{(q-1)/2-r} (-4)^r. \quad (3)$$

Every general term in the right-hand side of this equation has the following shape

$$\frac{q(q-1)}{2r(2r+1)} \binom{q-2}{2r-1} (a^2)^{(q-1)/2-r} (-4)^r.$$

Since $2^{2r} > 2r$ for any positive integer r , we conclude that every such term is divisible by 2^{s+1} . As $\nu_2((1 - (a^2)^{(q-1)/2}) = \nu_2(1 - a^2) + \nu_2(q-1) - 1 \leq s+1$ by LTE, we have that the left-hand side is divisible by 2^s but not divisible by 2^{s+1} , which is a contradiction. ■

Problem 5.5. Let (x, y) be a solution of the equation $x^2 + 4 = y^q$ for prime $q \equiv 3 \pmod{4}$ and $q > 3$. Prove that (a) $q \equiv 3 \pmod{8}$; (b) $y - 8$ divides $y^{\frac{q-1}{2}} + 1$; (c) the equation $x^2 + 4 = 5^q$ has no solutions; (d) the equation $x^2 + 4 = y^q$ has no solutions.

Solution. (a) As in solution of Problem 5.4b we get

$$(-1)^{(q-1)/2} = \sum_{r=0}^{(q-1)/2} \binom{q}{2r+1} (a^2)^{(q-1)/2-r} (-4)^r. \quad (1)$$

Treating (1) as a congruence modulo 8, we get

$$-1 \equiv q + 4 \pmod{8},$$

so $q \equiv 3 \pmod{8}$.

(b) Putting $u = a + 2i, v = a - 2i$ it follows from $x + 2i = (a + bi)^q$ with

$$b = 2(-1)^{(q-1)/2} = -2$$

that

$$\frac{u^q - v^q}{u - v} = -1.$$

The following identity is easily verified

$$\frac{u^{(q-1)/2} - v^{(q-1)/2}}{u - v} \cdot (u^{(q+1)/2} + v^{(q+1)/2}) = -(uv)^{(q-1)/2} + \frac{u^q - v^q}{u - v}.$$

Since $q = 8t + 3$ it may be written

$$\frac{u^{4t+1} - v^{4t+1}}{u - v} \cdot (u^{4t+2} + v^{4t+2}) = -y^{4t+1} - 1. \quad (2)$$

The second factor on the left-hand side of (2) is divisible by $(u^2 + v^2)/2 = y - 8$, q.e.d

(c) We have $a = 1$. Suppose $\nu_2(q - 3) = t \geq 3$. Then it follows from (1) that

$$-1 \equiv q - 4 \binom{q}{q-3} \pmod{2^{t+2}},$$

hence $q \equiv 3 \pmod{2^{t+1}}$, a contradiction.

(d) Suppose now $a > 1$, then $a^2 - 4 > 0$. Since $y - 8 = a^2 - 4 \equiv 5 \pmod{8}$, this number contains at least one prime factor $p \equiv 7 \pmod{8}$ or $p \equiv 5 \pmod{8}$.

It follows from (b) that $(-y)^{4t+1} \equiv 1 \pmod{p}$, so

$$1 = \left(\frac{-y}{p} \right) = \left(\frac{-8 - (y-8)}{p} \right) = \left(\frac{-8}{p} \right) = \left(\frac{-2}{p} \right),$$

i.e. $p \equiv 1 \pmod{8}$ or $p \equiv 3 \pmod{8}$ that contradicts to the choice of p . ■

6 Back to the proof of FTA

A ring R is called **Euclidean** if there exists a function $f : R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ such that

- (i) $f(a) \leq f(ab)$ for all nonzero $a, b \in R$, and
- (ii) if $a, b \in R$ and $b \neq 0$, then there exist q and r in R such that $a = bq + r$ and either $r = 0$ or $f(r) < f(b)$.

The function f in this case is called a *Euclidean norm*.

For example, the set of integers is a Euclidean ring with Euclidean norm $f(a) = |a|$, where r is the remainder of the division of a by b . Intuitively, a Euclidean ring is a ring in which one can perform “division with remainder”.

Problem 6.1. Consider the mapping $N(a + bi) = a^2 + b^2$. Prove that it is
 (a) multiplicative, that is, $N(zw) = N(z)N(w)$ for any complex numbers z, w ;
 (b) a Euclidean norm in the Gaussian ring, that is, the ring $\mathbb{Z}[i]$ is Euclidean.

Solution. (a) Let $z = a + bi$ and $w = c + di$. The multiplicativity of the norm is proved by direct verification:

$$(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + cb)^2.$$

(b) Take nonzero Gaussian numbers a, b . We prove property (i): since $b \neq 0$, we have $N(b) \geq 1$, and hence $N(ab) = N(a)N(b) \geq N(a)$, where the equality holds by part (a).

For the proof of (ii), write the complex number a/b in the form $u + iv$ for some rational numbers u, v . Choose integers x and y closest to u and v , respectively, that is, $|u - x| \leq 1/2$ and $|v - y| \leq 1/2$. Then $q = x + iy$ and $r = a - bq$ are Gaussian. Moreover,

$$\begin{aligned} N(r) &= N(a - bq) = N(b)N(a/b - q) = N(b)N((u - x) + (v - y)i) \\ &= N(b)((u - x)^2 + (v - y)^2) \leq N(b)((1/2)^2 + (1/2)^2) \\ &= N(b)/2 < N(b). \end{aligned}$$

■

Next, we will show that many properties of integers that we used for solving equations carry over naturally to Euclidean rings with essentially the same proof.

Problem 6.2. Let R be a Euclidean ring, and let $a, b \in R$ not both be zero. Prove that there exist $x, y \in R$ such that $ax + by$ is a greatest common divisor of a and b .

Solution. Denote

$$S = \{ax + by \mid x, y \in R\}.$$

Choose an arbitrary Euclidean norm f and a nonzero $d \in S$ with the smallest value of $f(d)$. Then $d = ax_0 + by_0$. Divide a by d with remainder: take $q, r \in R$ such that $a = qd + r$ and either $r = 0$ or $f(r) < f(d)$. However,

$$r = a - qd = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0) \in S.$$

If $r \neq 0$, then $f(r) < f(d)$, which contradicts the choice of d . Hence, $r = 0$, and d divides a . Similarly, d divides b . Therefore, d is a common divisor of a and b . Now, if c is any other common divisor of a and b , then c divides $ax_0 + by_0 = d$. Thus, d is a greatest common divisor of a and b . ■

As a consequence of the previous problem, a and b are coprime if and only if there exist $x, y \in R$ such that

$$ax + by = 1.$$

Problem 6.3. Let R be a Euclidean ring, and let $a, b, c \in R$. Prove that:

- (a) if $a \neq 0$, a and b are coprime, and bc is divisible by a , then c is divisible by a ;
- (b) if a and c are coprime, and also b and c are coprime, then ab and c are coprime.

Solution. (a) By Problem 6.2 there exist $x_0, y_0 \in R$ such that $ax_0 + by_0 = 1$. Then

$$c = c(ax_0 + by_0) = (a)cx_0 + (bc)y_0 \equiv 0 + 0 = 0 \pmod{a}.$$

(b) By Problem 6.2 there exist $x_1, y_1, x_2, y_2 \in R$ such that $ax_1 + cy_1 = 1$ and $bx_2 + cy_2 = 1$. Then

$$1 = (ax_1 + cy_1)(bx_2 + cy_2) = ab(x_1x_2) + c(ax_1y_2 + by_1x_2 + cy_1y_2).$$

Consequently, ab and c are coprime by Problem 6.2. ■

Problem 6.4. Let R be a Euclidean ring, $a_1, \dots, a_n \in R$, and let an irreducible $p \in R$ divide the product $\prod_{i=1}^n a_i$. Prove that p divides a_i for some i .

Solution. We prove the assertion by induction on n . The base case $n = 1$ is trivial. Let $n > 1$ and $b = \prod_{i=2}^n a_i$. If a_1 and p are coprime, then by Problem 6.3(a), p divides b . Then by the induction hypothesis, p divides a_i for some $2 \leq i \leq n$. If a_1 and p are not coprime, then $d = \gcd(a_1, p)$ for some non-invertible $d \in R$. Then $p = du$ and $a_1 = dv$ for some $u, v \in R$. Since p is irreducible and d is non-invertible, u is invertible, and p divides a_1 . ■

Next we establish some useful properties of Euclidean norms.

Problem 6.5. Let R be a Euclidean ring, and let f be any Euclidean norm. Prove that:

- (a) $f(ab) = f(a)$ for any nonzero $a \in R$ and any unit $b \in R$;
- (b) $f(ab) > f(a)$ for any nonzero $a \in R$ and any nonzero non-invertible $b \in R$;
- (c) $f(a) \geq f(1)$ for any nonzero $a \in R$, and equality holds if and only if a is a unit in R .

Solution. (a) Let c be the inverse of b . Then by property (i) of a Euclidean norm we have

$$f(a) \leq f(ab) \leq f((ab)c) = f(a(bc)) = f(a).$$

(b) Suppose the contrary, that $f(ab) = f(a)$ for some $a \neq 0$ and non-invertible b . Divide a by ab with remainder: take $q, r \in R$ such that $a = (ab)q + r$. Then $r = a(1 - bq)$. Since

b is non-invertible, $1 - bq \neq 0$. Hence $r \neq 0$. From the following inequality we arrive at a contradiction:

$$f(a) = f(ab) > f(r) = f(a(1 - bq)) \geq f(a).$$

(c) If a is invertible, then by part (a) we have $f(a) = f(a \cdot 1) = f(1)$. Otherwise, by part (b) we have $f(a) = f(a \cdot 1) > f(1)$. ■

Now we are ready to prove the Fundamental Theorem of Arithmetic for Euclidean rings.

Problem 6.6. Prove that every Euclidean ring R is factorial, i.e.

- (a) every nonzero non-invertible number in R has a complete factorization in R ;
- (b) any two complete factorizations of a number in R are equivalent.

Solution. Take a Euclidean norm f in R .

(a) Suppose the contrary; take a nonzero non-invertible number $x \in R$ of minimal norm that does not have a complete factorization. If x is irreducible, then x itself is its own complete factorization. Contradiction. Otherwise there are non-invertible y and z such that $x = yz$. By Problem 6.5(b) we have $f(x) > f(y)$ and $f(x) > f(z)$. Then y and z have complete factorizations by the minimality of the choice, and the product of their complete factorizations will be a complete factorization of x . Contradiction.

(b) We prove the equivalence of any two complete factorizations by induction on the number m of factors in the first factorization.

Base of induction: $m = 1$. Let $x = p_1 = q_1 \cdot \dots \cdot q_k$. Since p_1 is irreducible, k must equal 1 (otherwise p_1 decomposes into a product of non-invertible elements). Hence $x = p_1 = q_1$, and the factorizations are trivially equivalent.

Inductive step: assume that the statement is true for all factorizations whose first factorization has length less than m . Let two complete factorizations be given:

$$x = p_1 \cdot \dots \cdot p_m = q_1 \cdot \dots \cdot q_k.$$

By Problem 6.4 with $p = p_1$, $n = k$ and $a_i = q_i$, we have that for some i the number p_1 divides q_i . Since both p_1 and q_i are irreducible, they are associated: $q_i = up_1$ for some unit u of the ring R . Without loss of generality, we may assume that $i = 1$ (otherwise we need to take the composition of the transposition $(1i)$ with the bijection π constructed below).

Substitute this into the original equality and cancel p_1 :

$$x/p_1 = p_2 \cdot \dots \cdot p_m = (uq_2) \cdot q_3 \cdot \dots \cdot q_k.$$

Thus we have obtained two complete factorizations of x/p_1 , and the first factorization consists of $m - 1$ factors.

By the induction hypothesis, these factorizations are equivalent: $m - 1 = k - 1 \implies m = k$, and there exists a bijection $\pi' : \{2, \dots, m\} \rightarrow \{2, \dots, k\}$ such that p_j is associated with the corresponding factor of the second factorization.

Extend the bijection π' to a bijection $\pi : \{1, \dots, m\} \rightarrow \{1, \dots, k\}$ by setting $\pi(1) = 1$ and $\pi(j) = \pi'(j)$ for $j \geq 2$. We obtain the desired equivalence. ■

Problem 6.7. Prove that the following rings are Euclidean: (a) $\mathbb{Z}[i\sqrt{2}]$; (b) $\mathbb{Z}[\omega]$.

Solution. (a) We prove that the function $N(x) = a^2 + 2b^2$ for $x = a + bi\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ is a Euclidean norm of the ring $\mathbb{Z}[i\sqrt{2}]$.

Proof of property (i): for nonzero $x, y \in \mathbb{Z}[i\sqrt{2}]$ we have

$$N(xy) = N(x)N(y) \geq N(x),$$

since N is multiplicative and $N(y) \geq 1$ (because $y \neq 0$).

For the proof of (ii), write the complex number a/b in the form $u + vi\sqrt{2}$ for some rational numbers u, v . Choose integers x and y closest to u and v , respectively, that is, $|u - x| \leq 1/2$ and $|v - y| \leq 1/2$. Then $q = x + yi\sqrt{2}$ and $r = a - bq$ belong to $\mathbb{Z}[i\sqrt{2}]$. Moreover,

$$\begin{aligned} N(r) &= N(a - bq) = N(b)N(a/b - q) = N(b)N\left((u - x) + (v - y)i\sqrt{2}\right) \\ &= N(b)((u - x)^2 + 2(v - y)^2) \leq N(b)((1/2)^2 + 1/2) \\ &= 3N(b)/4 < N(b). \end{aligned}$$

(b) We prove that the function $N(x) = a^2 - ab + b^2$ for $x = a + b\omega \in \mathbb{Z}[\omega]$ is a Euclidean norm of the ring $\mathbb{Z}[\omega]$.

Proof of property (i): for nonzero $x, y \in \mathbb{Z}[\omega]$ we have

$$N(xy) = N(x)N(y) \geq N(x),$$

since N is multiplicative and $N(y) \geq 1$ (because $y \neq 0$).

For the proof of (ii), write the complex number a/b in the form $u + v\omega$ for some rational numbers u, v . Choose integers x and y closest to u and v , respectively, that is, $|u - x| \leq 1/2$ and $|v - y| \leq 1/2$. Then $q = x + y\omega$ and $r = a - bq$ belong to $\mathbb{Z}[\omega]$. Moreover,

$$\begin{aligned} N(r) &= N(a - bq) = N(b)N(a/b - q) = N(b)N((u - x) + (v - y)\omega) \\ &= N(b)((u - x)^2 - (u - x)(v - y) + (v - y)^2) \leq N(b)((1/2)^2 + (1/2)^2 + (1/2)^2) \\ &= 3N(b)/4 < N(b). \end{aligned}$$

■

References.

1. Cai, Z. (2025). An Effective Method for Solving a Class of Transcendental Diophantine Equations. arXiv. <https://arxiv.org/abs/2510.11753>
2. Bennett, M. A. (2001). On some exponential equations of S. S. Pillai. *Canadian Journal of Mathematics*, 53(5), 897–922.
3. Klazar, M. (2010). Størmer's solution of the unit equation $x - y = 1$. Unpublished manuscript, Department of Applied Mathematics, Charles University, Prague. Retrieved from <https://kam.mff.cuni.cz/%7Eklazar/othertexts.html>
4. Lehmer, D. H. (1964). On a Problem of Størmer. *Illinois Journal of Mathematics*, 8(1), 57–79.
5. Daems, J. (2002). A Cyclotomic Proof of Catalan's Conjecture: Master's Thesis. Leiden: Universiteit Leiden, 64 p.
6. Grechuk, B., Wilcox, A. (2024). Polynomial Diophantine Equations: A Systematic Approach. Springer. <https://doi.org/10.1007/978-3-031-62949-5>
7. Andreescu, T., Andrica, D., Cucurezeanu, I. (2010). An introduction to Diophantine equations: A problem-based approach. Birkhäuser.
8. <https://artofproblemsolving.com/community/c6h418604p2361782>
9. <https://mathoverflow.net/questions/206645/on-a-result-attributed-to-w-ljunggren-and-t-nagell>
10. <https://mathoverflow.net/questions/285507/a-modification-of-the-ljunggren-nagell-equation>
11. <https://artofproblemsolving.com/community/c6h254153p1389586>
12. <https://artofproblemsolving.com/community/c6h3524470p34235849>
13. <https://artofproblemsolving.com/community/c6h553400p3215430>
14. <https://mathoverflow.net/questions/490280/on-a-paper-of-wilhelm-ljunggren>
15. <https://artofproblemsolving.com/community/c6h3048886p27466981>