

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	4
3	Størmer's method	8
4	Equations in factorial domains	9
5	On the equations of Lebesgue–Nagell type	12
6	Back to the proof of FTA	13

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

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.

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

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.

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

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 $y > 1$.

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.

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

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 $10^x - 7^y = 3$.

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

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

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 .

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.

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 .

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 .

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 .

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.

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

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 .

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 $w(p) = p$.

(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 $p \nmid D y_1$, 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 $w(p) \mid (p - \varepsilon)$.

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 $x_{p-\varepsilon} = x_p x_1 - \varepsilon D y_p y_1 \equiv x_1^2 - D y_1^2 = 1 \pmod{p}$, 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 $U_p \equiv p \pmod{p^2}$.

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

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

For brevity, we write

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

We now introduce

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

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 .

Problem 2.11. Prove that

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

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 $n > 3$.

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

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

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

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

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.

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 $(\frac{x+3}{2})^2$ or $(\frac{x-3}{2})^2$ 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 $q \geq 5$.

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 .

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 .

Problem 3.4. Prove that the equation

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

has no positive integer solutions.

Problem 3.5. Prove that the equation

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

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

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

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

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

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.

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) $1 + 3i$, $3 + 4i$, $5 + 7i$.

Problem 4.4. Find all irreducible Gaussian numbers.

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.

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?

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 $x = u_1 v_1^n$ and $y = u_2 v_2^n$ for some $v_1, v_2 \in R$ and some invertible numbers $u_1, u_2 \in R$.

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.

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

Problem 4.10. Describe all solutions to the equation

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

in integers.

Problem 4.11. Prove that all solutions of the equation

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

in integers are described by

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

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

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 $n \geq 2$.

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 $q \equiv 1 \pmod{4}$.

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 $n \geq 2$.

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 $q \equiv 1 \pmod{4}$.

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.

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.

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 .

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.

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 .

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 .

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.

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

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>