Introduction to elementary number theory
Karel Lepka

Author's preface

The famous German mathematician Karl Friedrich Gauss said that mathematics is the queen of the sciences and that number theory is the queen of mathematics. His no less famous colleague Kronecker claimed that natural numbers are from God and everything else is human creation. It remains a fact that without number theory, mathematics would not be mathematics. Of course we do not take it to be the foundation of the world as Pythagoras and his school held, but it is true that numbers in mathematics have a much deeper role than only counting. In this text, we will first look at the sets of natural and integer numbers, while to begin with, we will not introduce complicated theories for defining these sets of numbers. The set of natural numbers, which will be denoted by $\mathbb{N}$ will intuitively be defined as the numbers of elements of finite sets. The set of integers will in the text be denoted by the symbol $\mathbb{Z}$ and we will agree that it contains the original set $\mathbb{N}$, complemented with negative numbers and the zero. Negative numbers will be introduced intuitively, as debt or temperatures in which water normally changes into ice. The real mathematical theory ofnumber sets will only be shown at the end of this text.

In the following chapters, we will show some properties of the sets of natural numbers and integers. We will make an effort to make the text enjoyable to read, although we will not deviate much from the old habits according to which such texts are written, i.e. that Euclidean style of definition, theorem, proof. We will also try to include in the text illustrative and motivation examples and also with practical applications. The readers may be surprised how close this theory is to everyday life. The reader will of course find solved examples and a number of tasks for practising the theory. We will not forget historical notes, since those who do not know the history of a certain field cannot understand it properly. Let us thus dive into the magical world of numbers and look for interesting properties and surprising connections.

Chapter 1

Theory of divisibility

Let us start this chapter with an old jest. A grandmother has five grandchildren and twelve apples. How can she divide them among the children in a just way? The correct answer is that she makes an apple pie. In the above example, the grandmother has no other choice, but if she would buy three more apples, she would give three apples to each grandchild and could save the work with the apple pie. The grandmother can also not tell the grandchildren about the existence of two apples, these will remain and she can again give out the apples evenly, this time two apples to each child. As follows from the example given, sometimes we succeed in dividing a set of elements into several not intersecting subsets, each of which contains the same, in advance given, number of elements, and sometimes it is not possible.

As the title of this chapter shows, we will deal in it with notions like divisibility of numbers, the least common multiple, and the greatest common divisor. We will also learn some criteria of divisibility.

1.1 Basic notions and theorems

As was already said in the preface, we will understand natural number to be the number of elements of a given finite set. The notion of divisibility can be extended also to negative numbers, because even a large debt can be divided into several smaller debts. Let us now stop giving examples and get on with the theory itself. However, we will start from a non-traditional manner: not with an axiom or a definition, but with a theorem.

Theorem 1.1 *Let $a, b \in \mathbb{Z}$, while $b > 0$. Then the whole numbers q, r with the property*

$$a = bq + r, \qquad 0 \leq r < 0 \tag{1.1}$$

exist. Numbers q, r with the given conditions are uniquely determined.

Proof: We will perform the proof in two steps. We will first prove the existence of the numbers q r for which (1. 1) holds. Let us denote by the symbol M the set of all integers m of the form

$$m = a - bt,$$

where t is an integer with the property $a - bt \geq 0$. Apparently, the set M is a subset of the set of non-negative integers. We will easily see that the set is not empty. If $a \geq 0$, then we assume $t = 0$ and obtain $m = a - b.0 = a \geq 0$. For $a < 0$, it suffices to assume that $t = a$. Then $m = a - b.a = a(1 - b) \geq 0$. The set of non-negative integers is a well-ordered set, and therefore the set M contains the least element; let us denote it r. It holds that $r \geq 0$ and the integer $q = t$ exists such that the following holds

$$0 \leq r = a - b \cdot q \Longrightarrow a = b \cdot q + r.$$

If we take $r \geq b$, then we obtain

$$0 \leq r - b = a - b \cdot (q - 1) \in M.$$

However, then $r - b < r$, which is in contradiction with the assumption that r is the least element (number) of the set M.

To prove the uniqueness of this element, we will again proceed by contradiction. Let us assume that $a = bq_1 + r_1$ holds and at the same time $a = bq_2 + r_2$. When we subtract the first equation from the second, we obtain $0 = b(q_2 - q_1) + r_2 - r_1$, i.e. $r_2 - r_1$ is a multiple of b. However, as $|r_2 - r_1| < b$, then it must hold that $r_1 = r_2$, and thus also $q_1 = q_2$.

The task in which we are to find the pair of numbers q, r to the given pair of integers a, b such that the equality (1. 1) holds is called *division*; number a is called *dividend*, number b *divisor*. Let us now concentrate on the number r. For $r > 0$ we speak of *division with remainder*. In this case q is called the *partial quotient* and r the *remainder*. If $r = 0$, we speak of *division without remainder*; number q is called the *quotient*. We also say that number a is divisible by number b, which we will denote by $b|a$. We say that a is a *multiple* of b.

NB! The remainder is always non-negative, and thus $-41 = 11.(-4) + 3$, and never $-41 = (-3).11 - 8$.

Remark: The condition $b > 0$ is not necessary for the divsion of integers. If we only assumed $b \neq 0$, then we need to demand that the inequality $0 \leq r < |b|$ holds.

The following theorems hold:

Theorem 1.2 *If a is a multiple of m and if at the same time m is a multiple of b, then a is a multiple of b.*

Theorem 1.3 *If in the equality of the type $a_1 + a_2 + \ldots + a_n = b_1 + b_2 + \ldots + b_s$ all members except for one are multiples of the number k, then also this member is a multiple of k.*

Theorem 1.4 *Let $a|b$ and $a|c$. Then $a|(bx + cy)$ for any integers x and y.*

The fact that if number a divides b and c, then it also divides their sum and difference is a consequence of this theorem.

Theorem 1.5 *Let $a|b$. Then $a|bc$, where c is an arbitrary integer.*

Theorem 1.6 *Let $a|b$ and at the same time $b|c$. Then $a|c$.*

This property is called *transitivity.* The proofs of these theorems are easy and we recommend the reader to perform them as an exercise.

A question arises how to find out whether number a is divisible by number b. In the age of computers and calculators, it might appear easiest to simply divide these numbers. The author respects modern computing technology, but this technology cannot deal with some questions connected with number theory, In some cases, employing this technology would be useless, like trying shoot sparrow with a cannon, because we can see whether one number is divisible by another much more easily. Let us state some criteria for divisibility, especially for the cases when the divisor is a small number.

Theorem 1.7 *Natural number n is divisible by:*
a) two, if its last digit is even,
b) three, if the sum of its digits is divisible by three,
c) four, if its last two digits are divisible by four,
d) five, if its last digit is 0 or 5,
e) six, if it is even and divisible by three,
f) seven, if the double of the number of hundreds plus the last two digits is divisible by 7,
g) eight, if the last three digits are divisible by 8,
h) nine, if the sum of its digits is dividsible by 9,
i) ten, if its last digit is 0.

Proof: Every natural number n in the decimal system can be expressed in the following way:

$$n = c_k 10^k + \cdots + c_2 10^2 + c_1 10 + c_0,$$

where $c_i \in \{0, 1, 2, \ldots, 9\}$ and $c_k \neq 0$. From this expression, the rules a), c), d), g) and i) follow immediately.

Let

$$s = c_k + \cdots + c_2 + c_1 + c_0$$

be the sum of the digits of n. Then

$$n - s = (10^k - 1)c_k + \cdots + 99c_2 + 9c_1.$$

As each addend on the right-hand side is divisible by nine and also the number s is divisible by nine, also the number n must be divisible by nine. This proves simultaneously h) and b).

The rule for divisibility by seven remains to be proved. The double of the number of the hundreds of number n augmented by the last two digits is equal to

$$m = 2c_k 10^{k-2} + \cdots + 2c_2 + 1010c_1 + c_0.$$

The difference

$$n - m = 98c_k 10^{k-2} + \cdots + 98c_2$$

is divisible by seven, because $7|98$. Since $7|m$, then n must be divisible by seven.

The rule for divisibility by seven is, compared to the other ones, rather complex and not very useful for practice. Let us give an example. When we want to show whether 7056 is divisible by seven, we must proceed as follows: 70.7+56=546. 546:7=48. Number m is divisible by seven, and thus also 7056 is divisible by seven. The rules for divisibility by two-digit integers smaller than 20 can be found e.g. in [2], pp. 31 and 164.

Let us now present a few tasks connected with divisibility of integers.

Example 1: Determine what day it will be in 39 days, when it is Wednesday today.

Solution: 39=7.5+4. Therefore it will be Sunday in 39 days.

Example 2: Prove that the expression $a(a+1)(2a+1)$ is divisible by 6 for any integer a.

Solution: $a(a+1)(2a+1) = a(a+1)(a+2) + a(a+1)(a-1)$. Both addends are a product of three numbers immediately following each other, one of them must be divisible by 3 and at least one has to be divisible by 2.

Example 3: Prove that for each $\in N$, it holds that $169|3^{3n+3} - 26n - 27$.

Solution: Let us first expand the first term of the given expression: $3^{3n+3} = 27^{n+1} = (26+1)^{n+1}$. Using binomial theorem, we obtain

$$(26+1)^{n+1} = \binom{n+1}{0}26^{n+1} + \binom{n+1}{1}26^{n} + \ldots + \binom{n+1}{n-1}26^{2} + 26(n+1) + 1$$

It is obvious that all terms of this expansion with the exception of the last two are divisible by 169, because they contain at least the square of $26 = 2.13$. The last two terms then give the result $26n + 27$, and when added to the last two terms of the expression, we obtain zero.

1.2 The greatest common divisor and the least common multiple

In this section, we will be dealing with two problems. We will seek the greatest number that divides several different numbers and then the least number that is on the other hand the smallest one that is at the same time divisible by several different numbers.

Definition 1.1 *Each integer that divides at the same time the numbers $a, b, \ldots, l$ is called their common divisor. If at least one of those numbers is lower than zero, then the number of their divisors is finite, and therefore one of them will be the greatest. This number is called the greatest common divisor of the numbers $a, b, \ldots, l$ and we will denote it by $(a, b, \ldots, l)$. If $(a, b, \ldots, l) = 1$, then numbers $a, b, \ldots, l$ are called coprime integers. If each of the numbers $a, b, \ldots, l$ is coprime with any other, then numbers $a, b, \ldots, l$ are called pairwise coprime. Apparently, pairwise coprime integers are always coprime; in the case of two numbers, the notions of coprime and pairwise coprime are identical.*

Examples: a) $(15, 18, 63) = 3$ b) $(15, 21, 28) = 1$ c)$(11, 18, 25) = 1$

In case b) the numbers given are coprime, but not pairwise coprime, because

$(15,21) = 3$, $(21,35) = 7$ and $(15,35) = 5$. On the other hand, in case c) the numbers are also pairwise coprime, because $(11,18) = (11,25) = (18,25) = 1$.

Next, we will consider only the greatest common divisor of two numbers, and for the sake of simplicity and saving space, we will use the abbreviation GCD. If these numbers are not too large, then finding GCD is not very difficult, because we can succeed in factorization of the number (expressing both numbers as products of primes) and from those, we then choose the ones that are common to both numbers. GCD is then their product.

Example: Determine GCD of the numbers 153 and 258. It holds that $153 = 3^2.17$ and $258 = 2.3.43$. Therefore $(153,258) = 3$.

Finding GCD is not always so easy, and especially for large numbers, it is problematic to find even one divisor, let alone expand it into a product of primes, and we can take Fermat numbers as an example. Let us therefore ask whether there exists another way of finding the GCD. It would be ideal if it was an algorithm. The answer is that such an algorithm exists and it is named after the Greek mathematician Euclid.

Let us have natural numbers a and b, and without loss of generality, we can assume that $a > b$. According to the theorem (1. 1) it holds that $a = bq + r$. The common divisor of numbers a and b must also divide the remainder $r = a - qb$, and thus also each common divisor of numbers b and r is also a divisor of number a. It holds that

$$(a,b) = (b,q).$$

If we introduce the notation $a = n_0$, $b = n_1$, and $r = n_2$, this equality has the form

$$(n_0,n_1) = (n_1,n_2).$$

Two cases can occur now: If $n_2 = 0$, then n_1 is the sought greatest common divisor of numbers $n_0 = a$ and $n_1 = b$. If $n_2 \neq 0$, then we must divide n_1 by n_2 and repeat the whole procedure. We obtain the following system of equalities:

$$\begin{array}{rcl}(n_0,n_1) & = & (n_1,n_2)\\ (n_1,n_2) & = & (n_2,n_3)\\ (n_2,n_3) & = & (n_3,n_4)\\ \dots & .. & \dots\\ (n_{k-1},n_k) & = & (n_k,n_{k+1})\end{array}$$

As n_{i+1} is the remainder after dividing n_{i-1} by n_i for $(i = 1,2,\dots,k)$ and the set $\mathbb{N}$ is well-ordered, then

$$n_1 > n_2 \dots \geq 0.$$

It must also hold that $n_{k+1} = 0$ a $(n_{k-1},n_k) = n_k)$. According to the previous considerations, we obtain

$$(n_0,n_1) = (n_1,n_2) = \ldots = (n_{k-1},n_k = n_k),$$

and from there

$$(n_0,n_1) = (a,b) = n_k.$$

GCD is therefore the largest non-zero remainder in Euclid's algorithm.

Example 1: Find the greatest common divisor of numbers 1512 and 110.
Solution: We will use Euclid's algorithm of gradual division, through which we obtain $1512 = 13 \times 110 + 82$; 110=1x82+28; 82=2x28+26; 28=1x26+2; 23=2x13. $(1512, 110) = 2$.
Exammple 2: Determine the greatest common divisor of numbers 988 and 35.
Solution: Just like in the case before, we will use Euclid's algorithms. 988=28x35+8; 35=4x8+3; 8=2x3+2; 3=1x2+1; 2=1x1+1; 1=1x1+0. $(988, 35) = 1$, these numbers are coprime.
Example 3: Prove that two numbers immediately following each other are coprime.
Solution: $(a, a+1)$=$(a, a+1-a)$=$(a, 1)$=1.

1.3 Prime numbers and composite numbers

In this part, we will learn about the notion of prime and composite numbers. We will also introduce the fundamental theorem of arithmetic and some applications.

Definition 1.2 *Let us consider natural numbers greater than one. Each of them has at least two divisors, namely number one and itself. If we cannot find another divisor, then this number is called a* prime (number)*. In the opposite case, we speak of* composite numbers*.*

Number one belongs to neither of those two groups, exactly in compliance with Pythagorean school. Although it may seem that this is a mathematical whim, and a very beautiful one, it is not so. The art of telling a prime from a composite number is very important in practice, as we will show in the text that follows. The word art is very appropriate, especially if the number has many digits and its factorisation is difficult.

For small numbers, we may use the *sieve of Eratosthenes.* Suppose we should find all primes smaller than 100. We order all the numbers in increasing order and we first leave number 2 untouched and cross out all its multiples. After this operation, the lowest uncrossed number is number 3, so we cross out all its multiples. We proceed this way until we reach number 10, and then the crossing out is over and all the numbers that have not been crossed out are primes.

Theorem 1.8 *(The first theorem of Euclid). Let $a, b \in N$, p is a prime and $p|ab$. Then $p|a$ or $p|b$.*

Proof: If $p|a$, the theorem holds. If p is not a divisor of a, then $(a, p) = 1$. Then integers x and y exist such that $ax + py = 1$. If we multiply both sides of the equation by b, we obtain $abx + pby = b$. As both addends on the left-hand side are divisible by p, b must be divisible by p.

The consequence of this is that each natural number $n > 1$ can be uniquely decomposed into the product of natural powers of primes $p_1 < p_2 < \ldots < p_r$. It thus holds that

$$n = P_1^{k_1} P_2^{k_2} \cdots P_r^{k_r} = \prod_{i=1}^{r} p_i^{\alpha_i}$$

The prime p_i is called *prime element.*

Theorem 1.9 *If*

$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s},$$

where $p_1 < p_2 < \cdots < p_r, q_1 < q_2 < \cdots < q_s$ *are primes and* $r, s, \alpha_i, \beta_i \in N$*, then* $r = s$*,* $p_i = q_i$*,* $\alpha_i = \beta_i$ *for each* $i = 1, \ldots, r$*.*

Proof: Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, $n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$ and let $m = n$. If some prime p is a divisor of m, then according to the First Theorem of Euclid, the prime p must be a divisor of p_k for some $k \in \{1, \ldots, r\}$. From the definition of the prime, it follows that $p = p_k$. As $m = n$, then p must also be a divisor of some q_l for $l \in \{1, \ldots, s\}$ and in the same way, we obtain $p = q_l$. From this it follows that $p_k = q_l$. Since the primes p_i a q_j are in increasing order, it must hold that $p_1 = q_1, \ldots, p_r = q_r$ and $r = s$.

Let us further assume that $\alpha_1 > \beta_1$ for some $i \in \{1, \ldots, r\}$. If we divide the inequality $m = n$ by p^{β_i}, we obtain

$$p_1^{\alpha_1} \cdots p_i^{\alpha_i - \beta_i} \cdots p_r^{\alpha_r} = p_1^{\beta_1} \cdots p_i^{0} \cdots p_r^{\beta_r},$$

which is a contradiction, because the left-hand side of the equality is divisible by p_i, while the right-hand side is not divisible by this number. We proceed similarly in the cases when $\alpha_i < \beta_i$. It is thus $\alpha_i = \beta_i$ for all $i \in \{1, \ldots, r\}$.

The theorem about the uniqueness of the factorization in primes seems obvious to us, but there are also algebraic structures in which it does not hold. For example, in the field $Q(\mathrm{i}\sqrt{5})$, this theorem does not hold, because $21 = 3 \cdot 7$ and $(1 + 2\mathrm{i}\sqrt{5})(1 - 2\mathrm{i}\sqrt{5})$. The Fundamental Theorem of Arithmetic is also one of the reasons why we do not call number one a prime. If it was so, the uniqueness of the exponents in the factorization would not be guaranteed.

If we ask a question how many primes there are, we will find the answer in Euclid's elements, book 9, theorem 20. We will first state this theorem in its modern form.

Theorem 1.10 *(Second theorem of Euclid.) There are infinitely many primes.*

Proof: We will prove this theorem by contradiction. We will assume that there are finitely many primes. In that case, we can name them all: they will be numbers $p_1, p_2, \ldots, p_n$. We multiply them all and add one to that product. Such a number $m = p_1 p_2 \cdots p_n + 1$ is neither any of those primes, nor is it divisible by any of those primes. That is a contradiction and therefore there are infinitely many primes.

Let us remark that the number m thus constructed is sometimes a prime (2.3.5.7+1=211), and sometimes a composite number (2.3.5.7.11.13+1 = 30 031 = 59 509). When we look into Elements, we will see that Euclid states this theorem in a slightly different form. As Greek mathematicians did not use the notion of infinity in the same way as we do today, they had to formulate the theorems in a different way. The theorem as formulated by Euclid thus is: there are more primes than any given number of primes. The proof is then the same as above, only the number of known integers is much lower, Euclid was satisfied with three.

1.3.1 Pythagorean triples

Everybody who knows a little bit of geometry knows the theorem of Pythagoras. Every bricklayer can construct a right angle in such a way that he connects three sticks of lengths in the proportion 3:4:5 into a triangle and knows that the sought right angle is facing the longest side of the triangle. Pythagoras theorem is usually stated in words, we say that the area of the square of the hypotenuse is equal to the sum of squares of the two other sides. The proposition formulated in this way, however, is in the form of an implication and Pythagoras theorem does not entitle us to constructing the right angle in the way stated above. It can, however, be proved that also the other implication is correct, and that the following theorem holds:

Theorem 1.11 *A triangle with sides a, b, c is a right-angle triangle with the hypotenuse c if and only if $c^2 = a^2 + b^2$.*

Definition 1.3 *Let for the ordered triple $[a, b, c]$ hold $a^2 + b^2 = c^2$. This triple is called* Pythagorean triple *and the triangle with these lengths of sides is called* Pythagorean triangle*. If, moreover, these numbers do not have a common divisor $d > 1$, we speak of a* primitive Pythagorean triple*.*

Already Diophantus answered the question of constructing a Pythagorean triple.

Theorem 1.12 *An ordered triple of natural numbers $[a, b, c]$ is a primitive Pythagorean triple if and only if there exist natural numbers $m > n$ that are not coprime of different parity such that either*

$$a = m^2 - n^2, \qquad b = 2mn, \qquad c = m^2 + n^2$$

or

$$a = 2mn, \qquad b = m^2 - n^2, \qquad c = m^2 + n^2.$$

Numbers m and n are uniquely determined.

The proof is not difficult, but as it is rather long, we direct the reader e.g. to the book [2]. Not even Diophantus was the first one to devote attention to these triples, their tables were used already in Ancient Babylonia. We encounter Pythagorean triples in number theory quite often. To close this section, we will introduce their application that was for the first time mentioned (and probably also proved) by P. Fermat.

Theorem 1.13 *No number of the form $4k - 1$ for $k \in N$ is not a sum of the squares of two integers.*

The proof is easy when we realise that an even number is of the form $2l$ and odd number of the form $2m + 1$. Their squares are then $4l^2$ and $4m^2 + 4m + 1 = 4n + 1$. The sum of two squares may thus be $4k$, $4k + 1$ or $4k + 2$, it can never be of the form $4k + 3 = 4(k + 1) - 1$. From the above it follows that no number of the form $4k - 1$ can be a square of an integer.

1.4 Properties of primes

First, we will extend the definition of divisibility.

Definition 1.4 *For natural numbers j, m and n we say that m^j* exactly divides n, *and we will write $m^j \| n$, if $m^j | n$, but $m^{j+1} \not| n$. For $j = 0$, the symbol $m^0 \| n$ will mean that $m \not| n$.*

We will prove a theorem that introduces the relation between primes and binomial coefficients.

Theorem 1.14 *A natural number n is a prime if and only if $n \not| \binom{n}{k}$ for each $k \in \{1, \ldots, n-1\}$.*

Proof: Let n be a prime. For $k \in \{1, \ldots, n-1\}$, $n-k$ is between the numbers 1 and $n-1$. Number n divides neither $k!$, nor $(n-k)!$, but divides $n!$. As $\binom{n}{k} = \frac{n!}{k!(n-k)!}$, then this number is divisible by n. Let us, on the contrary, suppose that n is a composite number and that p is the least prime that divides n. Thus $1 < p < n$ and

$$\binom{n}{p} = \frac{n(n-1)\cdots(n-p+1)}{p(p-1)\cdots 2 \cdot 1}. \tag{1.2}$$

Let us further assume that $p^j \| n$ for some natural number j. Among p numbers immediately following each other $n, n-1, \ldots n-p+1$, there is exactly one divisible by p. As $p \mid n$, then $p \not| (n-1)(n-2)\cdots(n-p+1)$. It thus holds that $p^j \| n(n-1)\cdots(n-p+1)$ and apparently also $p \| p(p-1)\cdots 2 \cdot 1$. According to (1.2) we obtain that $p^{j-1} \| \binom{n}{p}$. But $n \not| \binom{n}{p}$ because $p^j \|$.

1.5 Exercises

1.1. The square of any natural number can be written down either as $4k$ or as $4k+1$. Prove.

1.2. If it simultaneously holds that $a|b$ and $b|a$, then $|a| = |b|$. Prove.

1.3. Father with his son drove for holidays from Brno to Croatia. As the journey was long, they decided to swap driving every 80 kilometers. Who was driving the car when they arrived to Split, if the distance between Brno and Split is 888 km?

1.4. Let $a - b$ be a multiple of number c. Then also $a^n - b^n$ is a multiple of c.

1.5. Prove that for any natural number n holds $9 | 4^n + 15n - 1$.

1.6. Prove that the difference of the squares of two odd natural numbers immediately following each other is divisible by eight.

1.7. The sum of three cubes of three natural numbers immediately following natural numbers is a multiple of 9. Prove.

1.8. The sum of two squares of natural numbers immediately following each other is divisible by four. Prove.

1.9. The difference of squares of two odd numbers is a multiple of 8. Prove.

1.10. Number $n^3 + 11n$ is divisible by six for any n. Prove.

1.11. Number $2^{2n+1} + 1$ is divisible by three. Prove.

Solution: $2^{2n+1} + 1 = 2(2^n - 1)(2^n + 1) + 3$.

1.12. Expression $n(n^4 + 35n^2 + 24)$ is divisible by 60 for each integer n. Prove.

Solution: The expressions $A = n(n + 1)(n + 2)(n + 3)(n + 4)$ and $B = n(n-1)(n-2)(n-3)(n-4)$ are divisible by 120, because they represent the product of five integers immediately following each other. Their arithmetic mean is equal to the given expression and that is then divisible by 60.

1.13. Prove that the expression $2^{2n+3}.7^n + 3^n.5^{n+1}$ is divisible by 13.

Solution: We expand the expression as $8.4^n.7^n + 5.3^n.5^n$=$13.28^n - 5.28^n + 5.13^n$=$13.28^n - 5(28^n - 15^n)$. Both addends are divisible by 13.

1.14. Prove that the expression $V = n^2(n^2 - 4)(n^2 - 16)$ is divisible by 11520 for every even n. Solution: $n = 2k$. $V = 64k^2(k^2 - 1)(k^2 - 4) = 64k^2(k - 1)(k - 2)(k+1)(k+2)$.The product of five numbers immediately following each other is divisible by 3, 4, 5. In addition, number three is contained twice in this number. Either $k = 3l$ or three divides simultaneously $k - 2$ and $k + 1$ or $k-2$ and $k+1$. The expression V is thus divisible by $64 \times 9 \times 4 \times 5 = 11520$.

1.15. Prove that no prime grater than 5 can be adapted to the form $N = m^4 + 4n^4$.

Solution: Number $N = (m^2 + 2n^2)^2 - 4m^2n^2$ can be written as $N = [(m + n)^2 + n^2][(m - n)^2 + n^2]$. Since N is a prime, then the contents of the first or the second brackets must be 1. That is possible only for $n = 0$ and $m = 1$ or $m = n = 1$. The first possibility results in $N = 1$, the second one in $N = 5$.

1.16. Prove that numbers of the form $3^{4n+4} - 4^{3n+3}$ are divisible by 17.

Solution: $3^{4n+4} - 4^{3n+3}$= $81^{n+1} - 64^{n+1}$=$(81 - 64)(81^n + 81^{n-1} \times 64 + \ldots)$.

1.17. Prove that number $\frac{n^3+(n+2)^3}{2}$ is for every integer n always an integer and a composite number.

Solution: If we use the known formula for the partition of the sum of the cubic powers, we obtain $(n + 1)(n^2 + 2n + 4)$.

1.18. Prove that the expression $V = 2^{4n+1} - 2^n - 1$ is divisible by nine.

Solution: $V = 2.2^{4n} - 2.2^{2n} + 2^{2n} - 1$=$(2^{2n} - 1)(2^{2n+1} + 1)$. The difference or sum of the cubic powers is divisible by three. Further, for $n = 3k$ and $n = 3k + 1$ is divisible by 27.

1.19. Prove that no number $A_n = 4^n + 5$ is simultaneously divisible by 7 and 9.

Solution: If a number is divisible by 7 and 9 at the same time, it is divisible by $63 = 4^3 - 1$. It holds that $4^n + 5 = 4^3(4^{n-3} + 5) - 5(4^3 - 1)$, i.e. $A_n = 64A_{n-3} - 5.63$. A_n will thus be divisible by 63 if also A_{n-3} is divisible by 63. However, none of the numbers $A_0 = 6$, $A_1 = 9$ and $A_2 = 21$ is divisible by 63.

Chapter 2

Some functions used in number theory

In this chapter, we will mention some functions that are frequently used in number theory. We will also work with these functions further in this text, and therefore it is necessary that we learn their definition and basic properties.

2.1 Function $[x]$, $\{x\}$

The first function that we will introduce is the *floor function*, denoted by $[x]$ and defined for all real numbers x as the largest integer that is not greater than x. So for example, [10]=10, [16,12]=16, and $[\pi]$=3. We will introduce also some examples of the values of this function for negative numbers: [-4]=-4, [-5,2]=-6. Let us notice that for positive numbers, the floor function part is always in absolute number less than the absolute value of the number, while with negative numbers, it is the other way round. It is similar as in the case of divisibility of numbers. If we divide two positive numbers, the product of the divisor and the (incomplete) quotient is always less or equal to the dividend. If we, on the other hand, divide a negative number by a positive one, the absolute value of the product of the divisor and the (incomplete) quotient is always greater or equal to the absolute value of the dividend.

In order not to let the fractional part of the real number feel left behind, we will also define a *fractional part of number x* as the difference $x - [x]$ and we will denote it by $\{x\}$. We now introduce some examples: $\{4\} = 0$, $\{1,6\} = 0,6$ a $\{-6,26\} = 0,74$.

We will introduce the following theorem to demonstrate the usefulness of this function:

Theorem 2.1 *The exponent*[1] *with which a given prime p is contained in the product $n!$ is equal to*

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

[1] In the publication [8], the exponents are mistakenly introduced as coefficients.

Proof: The number of factors of the product $n!$ is $\left[\frac{n}{p}\right]$, among them, there are $\left[\frac{n}{p^2}\right]$ multiples of p^2, among them then again $\left[\frac{n}{p^3}\right]$ multiples of number p^3 etc. By adding up the given numbers, we obtain the given exponent, because every factor of the product $n!$ that is a multiple of number p^m, but not of number p^{m+1}, is calculated the way that has been stated, $m-$times as a multiple of numbers $p, p^2, \ldots, p^m$.

Examples: In number 5!, there is the prime 2 with the exponent 3, as $\left[\frac{5}{2}\right]+\left[\frac{5}{4}\right] = 2+1 = 3$. It can be seen easily that $5! = 600 = 2^3.3.5^2$. In number 57!, number five is contained $\left[\frac{57}{5}\right] + \left[\frac{57}{25}\right] = 11+2 = 13$. Since number 13 is regarded as the unlucky one, we will not check this with the canonical factorization, but we invite the readers to do that themselves.

2.2 Sums related to the divisors of a number

Multiplicative functions play an important role in number theory. These functions can be defined in the following way:

Definition 2.1 *Function $\vartheta(a)$ is called multiplicative, if it si defined for all natural numbers and when it is non-zero for at least one value of a. At the same time, $\vartheta(a_1a_2) = \vartheta(a_1)\vartheta(a_2)$ must hold for $(a_1, a_2) = 1$.*

An example of a multiplicative function is the power of a natural number, because it holds that $a_1^s a_2^s = (a_1a_2)^s$. The reader will get acquainted with more multiplicative functions in the next part of the chapter, but before that, let us introduce further properties of multiplicative functions.

Theorem 2.2 *Let $\vartheta(a)$ be a multiplicative function. Then $\vartheta(1) = 1$.*

Proof: According to the definition, there is at least one natural number for which the function is not equal to zero; let us denote that number by a_0. We then obtain $\vartheta(a_0) = \vartheta(1.a_0) = \vartheta(1)\vartheta(a_0)$.

Theorem 2.3 *Let $\vartheta_1(a)$ and $\vartheta(a_2)$ be multiplicative functions. Then also the function $\vartheta_0(a) = \vartheta_1(a)\vartheta_2(a)$ is a multiplicative function.*

Proof: 1) $\vartheta_0(1) = \vartheta_1(1)\vartheta_2(1) = 1$
2) Let us assume that $(a_1, a_2) = 1$. Then it is

$$\vartheta_0(a_1a_2) = \vartheta_1(a_1a_2)\vartheta_2(a_1a_2) = \vartheta_1(a_1)\vartheta_1(a_2)\vartheta_2(a_1)\vartheta_2(a_2) = \vartheta_1(a_1)\vartheta_2(a_1)\vartheta_2(a_1)\vartheta_2(a_2) = \vartheta_0($$

Theorem 2.4 *Let $\vartheta(a)$ be multiplicative function and $a = p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_k^{\alpha_k}$ is the canonical factorization of a. Then*

$$\sum_{d|a} \vartheta(d) = (1 + \vartheta(p_1) + \vartheta(p_1^2) + \ldots + \vartheta(p_1^{\alpha_k}) \ldots$$

$$\ldots (1 + \vartheta(p_k) + \vartheta(p_k^2) + \ldots + \vartheta(p_k^{\alpha_k})).$$

If $a = 1$, then also the right-hand side is equal to one.

Proof: Let us multiply the expressions on the right-hand side and we obtain the sum of addends in the form

$$\vartheta(p_1^{\beta_1}(p_2^{\beta_2}\dots(p_k^{\beta_k} = \vartheta((p_1^{\beta_1}(p_2^{\beta_2}\dots(p_k^{\beta_k});$$

$$0 \le \beta_1 \le \alpha_1, \qquad 0 \le \beta_2 \le \alpha_2, \dots, \qquad 0 \le \beta_k \le \alpha_k,$$

while none of these addends will be left out and will not be repeated, and thus the sums on the right-hand side and on the left-hand side will be the same.

If $\vartheta(a) = a^s$, then the previous equality has the following form

$$\sum_{d|a} d^s = (1 + p_1^s + p_1^{2s} + \ldots + p_1^{\alpha_1 s}) \ldots (1 + p_k^s + p_k^{2s} + \ldots + p_k^{\alpha_k s}) \tag{2.1}$$

If we put $s = 1$, then the left-hand side of the equation (2.1) is equal to the sum of all divisors of number a, which we will denote by $S(a)$. The right-hand side may be simplified, and thus we obtain the formula for the sum of all the divisors of number a:

$$\sigma(a) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}. \tag{2.2}$$

If we put $s = 0$, then the left-hand side of the equation (2.1) is equal to the number of divisors of number a, where we denote it by $\tau(a)$. The number of all the divisors can then be determined by the formula

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_k + 1) \tag{2.3}$$

Example: Let $a = 36$. Then its canonical factorization is $36 = 2^2 3^2$ and its divisors are numbers $1, 2, 3, 4, 6, 9, 12, 18, 36$. If we add these numbers, we will obtain 91. We will also obtain this number by using the right-hand side of the previous formula —$\frac{2^3-1}{2-1}\frac{3^3-1}{3-1}$. If we add all the divisors as pieces, we end up with number 9. But it is also $(2 + 1)(2 + 1) = 9$.

We will meet functions $S(a)$ and $\tau(a)$ further in this text.

2.2.1 Euler function

This function will be used very often in this text, so it is high time that we define it and state some of its properties.

Definition 2.2 *Euler function $\varphi(a)$ is defined for all natural numbers a as the number of those numbers in sequence $0, 1, \ldots, a - 1$ that are coprime with a.*

Examples: $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(6) = 2$, $\varphi(7) = 6$, $\varphi(9) = 7$, $\varphi(13) = 12$.

Theorem 2.5 *Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ be canonical factorization of the number a. Then*

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right). \tag{2.4}$$

Corollary 1: If p is a prime, then $\varphi(p) = p - 1$ and $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Examples: $\varphi(14) = 14(1 - \frac{1}{2})(1 - \frac{1}{7}) = 6$
$\varphi(512) = 8^3 - 8^2 = 448$
$\varphi(11) = 11 - 1 = 10$

Corollary 2: Euler function is multiplicative.

2.3 Exercises

2.1. Calculate the exponent with which number 3 is contained in the canonical factorization of 1024!

2.2. Find the canonical factorization of the number 18!

2.3. Calculate $\sigma(51450)$ and $\tau(51450)$

2.4. Calculate $\varphi(41)$ and $\varphi(1786050)$

2.5. The canonical factorization of a number is of the form $2^a.7^b$ and the sum of its divisors is 6000. Determine the number.

2.6. Determine the smallest positive number $n = 2^{\varrho}.p_1.p_2\ldots$ such that the sum of its divisors was $2n$, $3n$, $5n$. p_i are odd primes.

Hint for the solution: For the sum of the divisors it hold that $S(n) = \frac{2^{\varrho+1}-1}{2-1}.\frac{p_1^2-1}{p_1-1}.\frac{p_2^2-1}{p_2-1}\ldots$, after simplification $(2^{\varrho+1}-1)(p_1+1).(p_2+1)\ldots$. As number n is divisible by 2^{ϱ}, then it is obvious that there must be exactly ϱ primes p_i. Let us examine the different possibilities.

Results:

508 $2^{16}.3^8.5.7.11.13.17$ 48, 148800 40, 408240 $6000 = (\frac{}{2}{}^{a+1}2-1)(\frac{7^{b+1}}{7-1})$. After simplification, we have $2^5.3^2.5^2 = (2^{a+1})(7^{b+1})$. The first bracket must be an odd number and also a unit greater than any power of 2. Number 15 and $a = 4$ fulfil these conditions. What is left is 4000, which is a number a unit less than the fourth power of seven, i.e. $b = 3$.

Chapter 3

Diophantine equations

In the oldest mathematical textbook written in Czech by Ondřej Klatovský and published in 1530, we find the following task: *Twenty-six people on one party drank beverages for 88 white coins. During this party, there were men, women, and virgins. A man was to give six coins, a woman four coins, and a virgin two coins. How many men, women, and virgins were at that party or gathering?* Let us suppress our anger at seeing also innocent virgins taking part at the party and let us look for the solution. let us denote, as is the habit today, the number of men by x, the number of women y and finally the number of virgins z. This way, we obtain the first equation $x + y + z = 26$. If we calculate the spending of this strange society, we obtain the second equation $6x + 4y + 2z = 88$. If we eliminate y from the first equation and substitute it into the second equation, we receive, after adaptation, the equation $2x + y = 18$. We can see that although there is only one equation, there are two unknowns. We will call such equations in which there are more unknowns than equations *uncertain equations*. However, the term *Diophantine equations* is used much more frequently, derived from the name of the Greek mathematician Diophantus of Alexandria.

3.1 Linear Diophantine equations

In order to come to a satisfactory end with the story of the old Bohemian party, we will now be dealing with equations of the following form:

$$ax + by = c, \tag{3.1}$$

where a, b, c are integers, $a, b \neq 0$. Let us further denote $(a, b) = d$ the greatest common divisor of numbers a and b.

We will first deal with the easiest case when $c = 0$. Let us put $A = \frac{a}{d}$, $B = \frac{b}{d}$. We can transform the equation (3.1) into the form

$$\frac{x}{y} = -\frac{b}{a} = -\frac{B}{A},$$

while the last fraction is in the elementary form.

Theorem 3.1 *All integer solutions of the equation $ax + by = 0$ are the pairs of numbers of the form $x = Bt$, $y = -At$, where t is any integer.*

We leave the proof as an exercise for the students.

Example: Solve the equation $10x - 6y = 0$.
Since $(10, 6) = 2$, all pairs of numbers $x = -\frac{6}{2}t = -3t$, $y = -\frac{10}{2}t = -5t$ for an arbitrary t are solutions.

Let us now turn our attention to the case when $c \neq 0$. We will first determine when the equation has a solution.

Theorem 3.2 *The equation $ax + by = c$ has a solution if and only if $(a, b)|c$.*

Proof: Let us first assume that the given equation has a solution which we will denote by x_0 and y_0, and it therefore holds that $ax_0 + by_0 = c$. It follows from the properties of number d that it divides the left-hand side, and it thus must also divide the right-hand side.

Let us now assume that $d|c$. In that case, the integers x_0 and y_0 for which it holds that $ax_0 + by_0 = d$ must exist. Further, $c = de$, where e is any number. Let us put $x_1 = ex_0$ and $y_1 = ey_0$. Clearly,

$$ax_1 + by_1 = e(ax_0 + by_0) = ed = c.$$

The numbers x_1 and y_1 are a solution of the equation (3.1), by which the proof is complete.

Let us now look for a way of solving equation (3.1). One of the possibilities is the use of Euclidean algorithm and we will show the procedure on a concrete example. We will first show what the solution looks like if $c = (a, b)$.
Example: Solve the equation $21x + 15y = 3$.
Since $(21, 15) = 3$, this equation has a solution. We will find the greatest common divisor of numbers 21 and 15 through using the Euclidean algorithm.

$$21 = 15.1 + 6$$

$$15 = 6.2 + 3$$

$$6 = 3.2 + 0$$

We will extract 3, i.e. the greatest common divisor, from the last equation. We thus obtain

$$3 = 15.1 + 6.(-2) \tag{3.2}$$

Now we will eliminate 6 from the first equation and substitute it into (3.2), and we obtain

$$3 = 15.1 + [21.1 + 15(-1)].(-2) = 21.(-2) + 15.3.$$

One of the solutions of the given equation is thus $x = -2$ and $y = 3$.

The set of solutions of the Diophantine equations will not change if we divide all their coefficients by their common divisor. If there is a number different from d on the right-hand side and if there exists a solution to the equation, then necessarily $c = ed$. We thus first find the solution of the equation for the cases when the right-hand side is d and we then multiply the solution we have found by e.

Example: Solve the equation $21x + 15y = -6$.
In the previous example, we found a solution to the equation in which the right-hand side is equal to 3. We have $-6 = 3(-2)$, $e = -2$ and the solution our equation is $x = (-2)(-2) = 4$ a $y = 3(-2) = 6$.

Example: State at least one way of paying the sum of 37 crowns only with two-crown and five-crown coins.
We are to solve the Diophantine equation $2x + 5y = 37$. As numbers a and b are coprime, then the equation always has a solution. If we put one on the right-hand side, we obtain $5 = 2.2 + 1$, i.e. $1 = 5.1 + 2(-2)$ and $x = -2$, $y = 1$. If we multiply this solution by 37, we obtain $x = -74$ and $y = 37$. We have found a solution, but it does not solve the problem. It is clear that we cannot be content with the fact that we can find one solution of the Diophantine equation and we must find the way of finding all its solutions.

We can find one solution of equation (3.1), let us say that it is the ordered pair $(x_0; y_0)$. Let also the ordered pair $(r; s)$ be a solution of equation (3.1). Then it holds that

$$ar + bs = c = ax_0 + by_0,$$

which we can transform into the form

$$a(r - x_0) = -b(s - y_0)$$

and after dividing this by number $d = (a, b)$ we obtain

$$\frac{a}{d}(r - x_0) = -\frac{b}{d}(s - y_0). \tag{3.3}$$

As $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, the fraction $\frac{a}{d}$ is a divisor of number $s - y_0$, and so $s - y_0 = u\frac{a}{d}$. In a similar way, we find out that $r - x_0 = t\frac{b}{d}$, while u a t are integers. After substituting into (3.3) we obtain

$$\frac{a}{d}\left(\frac{b}{d}t\right) = -\frac{b}{d}\left(\frac{a}{d}u\right),$$

thus $t = -u$. The following numbers are thus the solution to equation (3.1)

$$r = x_0 + \frac{b}{d}t, \qquad s = y_0 - \frac{a}{d}t, \qquad t \in \mathbb{Z}. \tag{3.4}$$

Let on the contrary r and s be two arbitrary numbers in the form (3.4). If we substitute them into the equation (3.1), we have

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = (ax_0 + by_0) + \frac{ab}{d}t - \frac{ab}{d}t = ax_0 + by_0 = c.$$

We have somehow reversed the usual mathematical process, because the ideas stated above are a proof of the following theorem:

Theorem 3.3 *Let $x_0; y_0$ be a solution of the equation (3.1). Then the pair of numbers (r, s) is its solution if and only if it is of the form (3.4).*

Remark: If both coefficients of (3.1) are negative, it is necessary to multiply it by (-1). If only one is negative, let us suppose it is a, then we will introduce the substitution $x = -z$, by which we receive an equation with positive coefficients After solving it, we return to the original unknown.

Equipped with this theory, we can now start solving both previous problems. Let us start with the problem about money. According to theorem (3.3), all the solutions will be of the form

$$x = -74 + 5t, \qquad y = 37 - 2t,$$

where t is an arbitrary integer. As only natural numbers can be the solutions of the problem, we can easily find out that we will only obtain such solutions for $t = 15, 16, 17, 18$. It was our task to find any solution, and we as proper number theorists will choose the only prime offered. Then we can pay 37 crowns with eleven two-crown coins and three five-crown coins.

Now we have some money so we can go to the party. Also in this problem, only integer solutions are allowed. We will easily find out that one of the solutions of the equation is $x = 0$, $y = 18$, and so we may write the general solution in the form $x = t$, $y = 18 - 2t$. We will easily find out that only numbers $t = 1, \ldots, 8$ solve the problem. The solutions ae given in the table below.

x	1	2	3	4	5	6	7	8
y	16	14	12	10	8	6	4	2
z	9	10	11	12	13	14	15	16

It is interesting that Klatovský only gives two solutions, namely the cases with six and eight men. It is, however, surprising how many virgins took part in the party, as in more than a half or the cases, they dominated the party, and besides, in our opinion, it would be much more accurate to call it a ladies' night.

3.2 Diophantine equations of a higher degree

In the previous part, we learnt to solve linear Diophantine equations. We can now claim that we can solve any linear Diophantine equation with two unknowns, if, of course, it has one. However, we can also decide about the solvability of these equations. Solving equations of higher degree, however, is much more difficult and we are often happy with simply finding out whether the equation has any solution at all. For this reason, we will only introduce two types of equations, but we will substitute quality for quantity and will give full solutions of these two types.

Some equations can be transformed into the form

$$(ax + by)(cx + dy) = k \tag{3.5}$$

Before we show the way of solving this equation, we will introduce the following notion:

Definition 3.1 *Integers u and v are called matching divisors of number w if $u.v = w$.*

Let numbers 2 and 5 serve as examples, since they are matching divisors of number 10, since 10=5.2, or numbers -7 and 4 that are matching divisors of -28, since -28=(-7).4.

If numbers x and y are integer solutions of equation (3.5), then numbers $ax+by$ and $cx+dy$ are integers and they are also matching divisors of number k. Therefore we will find the solutions of equation (3.5) in the following way. We will determine a divisor of number k, let it be k_1. We will find the matching divisor k_2 and put

$$ax + by = k_1 \qquad cx + dy = k_2$$

This is, of course, a system of two linear equations with two unknowns. If this system is solvable, then numbers x and y are uniquely determined and so is the solution of equation (3.5).

From the method stated, it follows that the equations of the type (3.5) can only have a finite number of solutions. The number of matching divisors of any number k is finite and there is one or none solution associated with each pair of matching divisors.

Let us have a look at the equation

$$x^2 - y^2 = k \tag{3.6}$$

We will easily see that this equation is not solvable in the case $k = 4t + 2$. Each power of an integer is namely either of the form $4s$ or $4s + 1$. If both powers are of the same form, their difference is of the form $4t$. If $x^2 = 4s + 1$ and $y = 4v$, then their difference is $4t + 1$. If, on the contrary, $x^2 = 4s$ and $y = 4v + 1$, their difference is $4t - 1 = 4w + 3$. On the other hand, if it does not hold that $k = 4t + 2$, the equation is always solvable. For an even number $k = 4t$, we have $x = \frac{k}{4} + 1$ and $y = \frac{k}{4} - 1$. For an odd number $k = 2s + 1$, the solutions are $x = s + 1$ and $y = s$.

Let us look at yet another equation

$$a_n x^n + \ldots + a_1 x + a_0 = ky, \tag{3.7}$$

where a_i and k are integers. The fact that one unknown only appears in a linear term will be important for further considerations.

Not every such equation has a solution, as we will show in the following example. We will try to solve the equation

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

As was already mentioned, the square of an integer is either of the form $4t$ or $4t+1$. If we add two to both expressions, we will never get a number divisible by four.

Let us now prove a theorem which we will need to solve the equation (3.7).

Theorem 3.4 *Let $x = a + kt$, where a,k, t are integers. If $m \in N$, then x^m of the form $kT + a^m$, where T is an integer.*

We will prove the theorem by mathematical induction. If $m = 1$, then the theorem evidently holds. We will thus assume that the theorem holds for $m = n$ and we will prove that it then holds also for $m = n + 1$.

$$x^{n+1} = (a + kt)^{n+1} = (a + kt)^n (a + kt).$$

According to the induction assumption, $(a+kt)^n$ is equal to $kL+a^n$, and thus we can continue expansion and simplification:

$$(kL+a^n)(a+kt) = kLa + k^2Lt + kta^n + a^{n+1}.$$

If we extract k from the first three terms and denote it by $T = La + kLt + ta^n$, the proof is finished.

Theorem 3.5 *Let (x_0, y_0) be the solution of the equation (3.7) and let t be an integer. Then for every number of the form $x = x_0 + kt$, there exists y such that (x, y) is the solution of the equation (3.7).*

We will use the previous theorem for the proof. If (x_0, y_0) is a solution of the equation (3.7), then exponent of the power of the form $x^j = (x_0+kt)^j$ has the form $kT_j + x_0^j$. We thus have

$$a_n(x_0+kt)^n + \ldots + a_1(x_0+kt) + a_0 = a_n(kT_n + x_0^n) + \ldots + a_1(x_0+kt) + a_0 =$$

$$k(a_nT_n + \ldots + a_1t) + (a_nx_0^n + \ldots + a_1x_0 + a_0) = kT + ky_0 = k(T + y_0).$$

The pair $x_0 + kt$, $T + y_0$ is a solution of equation (3.7), by which the proof is finished.

This theorem tells us that if we know one solution, we can find infinitely many solutions, forming a class. That is nice, but can we somehow find at least one solution of the equation (3.7)? Theorem (3.5) has one important consequence for us. If the equation (3.7) has a solution, then there exists such a solution that $\mid X \mid<\mid k \mid$. Really, for given non-negative integers x_0 and k, there exist non-negative numbers s and r such that

$$x_0 = |k|s + r, \qquad 0 \le r < |k|,$$

and thus

$$0 \le x_0 - |k|s = r < |k|.$$

If $k > 0$, we put $t = -s$, for $k < 0$ we put $t = s$ and obtain number $X = x_0 + kt < |k|$. And according to theorem (3.5), there exists also a Y for this number such that the pair (X, Y) is a solution of equation (3.7).

Thanks to this corollary, we can forget our worries. It will suffice to find out whether one of the numbers $0, 1, \ldots, |k|-1$ fulfil the equation (3.7). If we succeed, the equation (3.7) has infinitely many solutions, if not, this equation does not have a solution.

Example: Solve the equation $x^2 + 3x + 1 = 4y$.

We will substitute, one by one, numbers $0, 1, 2, 3$ in the left-hand side of the equation. Numbers $1, 5, 11, 19$ are the results, but none of them is divisible by four, and therefore this equation does not have a solution.

Example: Solve the equation $x^2 + 2x + 4 = 4y$.

Here, we will have more good luck. If we substitute, one by one, numbers $0, 1, 2, 3$ in the left-hand side of the equation, we will obtain $4, 7, 12, 19$; the first and the third number in this sequence is divisible by four, and thus we have two classes of solutions, namely $4t$, $4t + 2$.

3.3 Exercises

3.1. From the given equations, choose those that are solvable:
a) $7x + 3y = 2$ b)$18x + 40y = 3$ c) $64x - 72y = 44$ d) $15x + 35y = 100$

3.2. Solve the equation $15x - 20y = 100$

3.3. For which x is the expression $\frac{17x-2}{15}$ an integer?

3.4. A certain chief led a people of 100 persons. After the harvest, he decided to give away 100 Metze (old hollow measure unit) of grain, while men were supposed to get 3 Metze, women 2 Metze and each child half a Metze. Let he who thinks he knows says how many men, how many women, and how many children [there are].

3.5. A man wanted to buy 100 animals for 100 gold coins. He ordered his servant to buy a camel for 4 gold coins, a donkey for one gold coin, and twenty sheep for one gold coin. Say if you want to how many camels, donkeys and sheep were bought for 100 gold coins.

3.6. Not even among clergy was there equality, as we can see in the following problem: a bishop ordered 12 loaves of bread to be divided among clergy. He ordered that each priest gets two loaves, each deacon half a loaf, and each lector a quarter of a loaf, while there were as many clergymen as loaves of bread. Say, if you can, how many priests, deacons, and lectors there could be.

3.7. Find all triples of mutually different matching divisors of number 36.

3.8. Solve the equation $6x^2 - 5xy + y^2 = 21$

3.9. Solve the equation $2x^2 + 3xy + y^2 = 35$

3.10. Find all integer solutions of the equation $x^2 - 4 = 11y$.

3.11. For which x is the expression $x^3 + 2x + 2$ a multiple of number 125?

3.12. For which n is $6n + 2$ a cubic power of a prime?

3.13. A group of gymnasts started their routine in a rectangle, while on one side of the rectangle, there were two more than on the other. After finishing their routines, whey walked away from the floor in quadruples. In the last row, however, one gymnast was missing. How many gymnasts were performing the routine?

Chapter 4

Congruences

In this chapter, we will deal with congruneces. This notion was introduced into number theory by Gauss and it enables us to write down the relations between numbers in a shortened form.

Let $a, b, m \in Z$, while $m > 1$. We say that number a is congruent with number b modulo m if $m|(a-b)$, or, in other words, numbers a and b give the same remainder after being divided by m. We write $a \equiv b$.

It thus holds that $14 \equiv 39 \mod 5$, because $5|(39-14)$. On the other hand, $5 \not| (27-14)$, therefore we write $27 \not\equiv 14 \mod 5$.

4.1 Properties of congruences similar to properties of equations

From the definition, it follows that congruences are transitive, i.e. the following theorem holds:

Theorem 4.1 *Let $a \equiv b \mod m$ and $b \equiv c \mod m$. Then also $a \equiv c \mod m$.*

Theorem 4.2 *Congruences with the same modulus can be added, term by term.*

Proof: Let $a_1 \equiv b_1 \mod m$ and $a_2 \equiv b_2 \mod m$. In this case, $a_1 = b_1 + mt_1$ and $a_2 = b_2 + mt_2$ and $a_1 + a_2 = b_1 + b_2 + m(t_1 + t_2)$, i.e. $a_1 + a_2 \equiv b_1 + b_2$. As a consequence, it is possible to transfer numbers from one side of the congruence to the other. In other words, we may add the same number to both sides of the congruence.

Theorem 4.3 *Congruences with the same modulus can be multiplied by each other.*

Proof: Let us express a_1 and a_2 in the same way as in the previous example. It then holds that $a_1a_2 = b_1b_2 + mN$, where N is an integer. It is thus $a_1a_2 \equiv b_1b_2$ mod m. As a corollary of this, it holds that we can raise both sides of the congruence to the same power, as we evidently multiply by the correct congruence $k \equiv k$ mod m. Contrary to equations, we can have $k = 0$, although the meaningfulness of this operation can be successfully doubted.

Both sides of congruence can be divided by their common divisor, if it is coprime with the modulus.

Proof: From the conditions $a \equiv b \pmod{m}$, $a = a_1 d$,$b = b_1 d$, $(d, m) = 1$ it follows that the difference $a = b$, equal to $(a_1 - b_1)d$, is divisible by m. Therefore $a_1 - b_1$ is divisible by m, i.e. $a_1 \equiv b_1 \pmod{p}$.

4.2 More properties of congruences

Theorem 4.4 *Both sides of the congruence as well as the modulus can be multiplied by the same integer.*

Proof: From $a \equiv b \pmod{p}$ it follows that $a = b + mt$, $ak = bk + mkt$, and thus $ak \equiv bk \pmod{bk}$

Theorem 4.5 *Both sides of the congruence as well as the modulus can be divided by any of their common divisor.*

Proof: Let $a \equiv b \pmod{p}$, $a = a_1 d$, $b = b_1 d$, $m = m_1 d$. Then we have $a = b + mt$, $a_1 d = b_1 d + m_1 dt$, $a_1 = b_1 + m_1 t$, and it follows that $a_1 \equiv b_1 \pmod{m}_1$.

Theorem 4.6 *If congruence $a \equiv b$ holds for several moduli, then it holds also for the modulus which is equal to the least common multiple of these moduli.*

Proof is obvious, the difference $a - b$ is divisible by all the moduli, and it is therefore divisible by their least common multiple.

Theorem 4.7 *If the congruence holds modulo m, then it holds also modulo d, where d is any divisor of number d.*

Proof is obvious, because if the difference $a - b$ is divisible by number m, then it is divisible by any of its divisors.

Theorem 4.8 *If one side of the congruence and the modulus are divisible by any number, then also the other side of the congruence is divisible by this number.*

Proof: It holds that $a = b + mt$. If m and a are divisible by d, then b must be divisible by this number as well.

Theorem 4.9 *If $a \equiv b \pmod{m}$, then $(a, m) = (b, m)$.*

Proof. The proof follows from the fact that if $a \equiv b \pmod{m}$, then $a = b + mt$. Every number that divides a and m simultaneously must also divide b. On the contrary, every number that divides b and m, must also divide a. Since this holds for any number, it also holds for the greatest common divisor.

4.3 Complete residue system

Numbers congruent modulo m create a *class of numbers modulo m.* From this definition, it follows that there is one and the same remainder r corresponding to all the numbers in the class and that we will obtain all the numbers in the class when we substitute all integers for q in the expression. In compliance with the fact that r can have m different values, there are m classes modulo m.

Any number in this class is called a *residue modulo m.* The residue obtained for $q = 0$, which is equal to the remainder r itself, is called the *least non-negative residue.* The residue ϱ with the least absolute value is called the *least residue in absolute value.* For $r < \frac{m}{2}$ it is obviously $\varrho = r$; for $r > \frac{m}{2}$, it is $\varrho = r - m$; finally, if m is even and $r = \frac{m}{2}$, it is possible to put ϱ equal to any of the two numbers $\frac{m}{2}$ and $-\frac{m}{2}$.

If we take one residue from each class, we obtain the *complete residue system modulo m.* Most often, the least non-negative residues are used, sometimes also the least residues in absolute value are used. Example: The complete residue system modulo 5 can be expressed as $0, 1, 2, 3, 4$ or $-2, -1, 0, 1, 2$.

Theorem 4.10 *Any m numbers, pairwise incongruent modulo m, form a complete residue system m.*

Theorem 4.11 *Let $(a, m) = 1$ and let us substitute each of the numbers in the complete residue system modulo m for x, then for $ax + b$, where b is any integer, we also obtain values of the complete residue system modulo m.*

Proofs of both statements are easy and we leave them to the reader as an exercise.

4.4 Reduced residue system

Numbers of the same residue class modulo m have one and the same greatest common divisor with the modulo. The classes containing residues coprime with the modulo form the *reduced residue system.* Reduced residue system can thus be formed from the numbers in the complete system, choosing the ones that are coprime with the modulo. We usually create the reduced system from the system of the least non-negative residues. As there are exactly $\varphi(m)$ numbers coprime with modulo m in the complete residue system, the quantity of the numbers in the reduced system as well as the quantity of classes containing numbers coprime with module is $\varphi(m)$.

Example: Reduced residue system modulo 16 is 1, 3, 5, 7, 9, 11, 13, 15. If the modulo is a prime, then the reduced residue system is the same as the complete residue system.

Theorem 4.12 *Any $\varphi(m)$ numbers, pairwise incongruent modulo m and coprime with modulo, form a reduced residue system modulo m.*

Theorem 4.13 *If $(a, m) = 1$ and x attains the values of the reduced residue system modulo m, then ax also attains the values of the reduced residue system modulo m.*

Proofs of both theorem are analogous to the proofs of theorems 4.11 and 4.12 and we again leave them to the reader as an exercise.

4.5 Congruences with one unknown

In this chapter, we will study congruences of the following general form:

$$f(x) \equiv 0 \pmod{m}; \quad f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0.(?) \tag{4.1}$$

If a_n is not divisible by m, then n is called the *degree of the congruence.* To solve the congruence means to find all the values x that fulfil it. Two congruences that are fulfilled by the same values of x are called *equivalent.*

If congruence (4.1) is fulfilled by a certain value of x_0, then it is fulfilled also by all the numbers x that fulfil the congruence $x \equiv x_0 \pmod{m}$. This whole class of numbers is considered as one solution. With this agreement, the congruence (4.1) will have as many solutions as there are the residues of the complete residue system fulfilling it.

Example: Congruence $x^3 + 3x^2 + 3 \equiv 0 \pmod{5}$ is fulfilled for $x = 4$. The congruence has only one solution $x \equiv 4 \pmod{5}$.

4.5.1 Linear congruence

We will now study linear congruence, i.e. the congruence of the form

$$ax \equiv b \mod m. \tag{4.2}$$

Let us assume that $(a, m) = 1$. This congruence has exactly as many solutions as there are the remainders of the complete system that fulfil it. If we substitute the complete residue system modulo m for x, then also ax will result in the complete residue system modulo m. Therefore ax will be congruent with b for only one value of x from the complete residue system, in other words, congruence (4.2) has only one solution.

Let now $(a, m) = d > 1$. In order for congruence (4.2) to have a solution, it is necessary that b is divisible by d, otherwise congruence (4.2) does not have a solution for any integer x. We will thus assume that b is a multiple of d and we put $a = a_1 d$, $m = m_1 d$ and $b = b_1 d$. In this case, we can divide both sides of the congruence by d and the newly emerging congruence $a_1 x \equiv b_1 \pmod{m_1}$ will have one solution modulo m_1, because $(a_1, m_1) = 1$. Let x_1 be the least non-negative residue of this solution modulo m_1, then all numbers x of this solution are of the form

$$x \equiv x_1 \pmod{m_1}. \tag{4.3}$$

With modulo m, however, the numbers (4.3) do not form one, but as many solutions as there are least non-negative residues modulo m in the sequence $0, 1, 2, \ldots, m-1$. All these numbers belong here (4.3):

$$x_1,\, x_1 + m\, x_1 + 2m\, \ldots, x_1 + (d-1)m, \tag{4.4}$$

i.e. altogether d numbers (4.3) and thus congruence (4.2) has d solutions.

The considerations above prove the theorem below:

Theorem 4.14 *Let $(a, m) = d$. Congruence $ax \equiv b \pmod{m}$ does not have a solution, if the right-hand side is not divisible by d. If b is a multiple of d, congruence d has a solution.*

We will now show some methods of solving congruences.

Example 1: Solve the congruence $4x \equiv 1 \pmod{6}$.
This congruence does not have a solution, since $(4, 6) = 2$ and $2 \nmid 1$.

If the modulo is not too large, we can solve the congruence by substituting numbers into it and seeing which of them fulfil the congruence, usually from the set of least non-negative residues.
Example 2: Solve congruence $3x \equiv 2 \pmod{5}$.
Since $(3, 5) = 1$, the congruence has exactly one solution. The system of least non-negative residues is of the form 0, 1, $2, 3, 4$. We will easily see that number 4 fulfils this congruence. All numbers $x \equiv 4 \pmod{5}$ therefore fulfil the congruence.

Example 3: Solve the congruence $6x \equiv 9 \pmod{15}$.
Since $(6, 15) = 3$ and $3 \mid 9$, the congruence will have 3 as a solution. If we divide both sides of the congruence by 3, we obtain new congruences $2x \equiv 3 \pmod{5}$. Since the modulo is a relatively small number, we can determine the solution by substituting numbers from the system of least non-negative residues. We will easily see that number $x_1 = 4$ fulfils the congruence. Other solutions are numbers $x_2 = x_1 + 5$ and $x_3 = x_1 + 2.5$. The solution of the original congruence can be given in the following form: $x \equiv 4; 9; 14 \pmod{20}$.

When solving congruences where $(a, m) = 1$, we can use Euler's theorem. Really, if $a^{\varphi(m)} \equiv 1 \pmod{m}$, then also $a^{\varphi(m)}b \equiv b \pmod{m}$. It then follows that $ax \equiv a^{\varphi(m)}b$, and therefore $x \equiv a^{\varphi(m)-1}b$. It thus suffices to calculate the number $a^{\varphi(m)-1}b$. Albeit this number will not be one of the least non-negative residues, finding the least non-negative residue is not a problem.
Example 4: Solve the congruence $6x \equiv 2 \pmod{7}$.
Since $\varphi(7) = 6$, it is $x = 6^5 \cdot 2$ and for the sake of elegance and simplicity, we will write it in the form $x \equiv 5 \pmod{7}$.

4.5.2 System of linear congruences

Since some properties of congruences are the same as or similar to the properties of equations, it is pertinent to pose a question whether we could also solve a system of linear congruences. We will limit ourselves to congruences with one unknown with different, pairwise coprime moduli, i.e. to the system of the form

$$a \equiv b_1 \pmod{m_1}, \quad x \equiv b_2 \pmod{m_2}, \ldots, x \equiv b_k \pmod{m_k}. \tag{4.5}$$

We can solve the system (4.5) according to the following theorem.

Theorem 4.15 *Let numbers M_s and $M_s^{'}$ are defined through conditions*

$$m_1 m_2 \ldots m_k = M_s m_s, \qquad M_s m_s^{'} \equiv 1 \pmod{m_s}$$

and let

$$x_0 = M_1 M_1^{'} b_1 + M_2 M_2^{'} + \ldots + M_k M_k^{'} b_k.$$

Then the set of values x fulfilling the system (4.4) is given by the congruence

$$x \equiv x_0 \pmod{m_1 m_2 \ldots m_k}. \tag{4.6}$$

Indeed, with regard to the divisibility of all numbers M_j different from M_s by number m_s for any $s = 1, 2, \ldots, k$ we have

$$x_0 \equiv M_s\acute{M}_s b_s \equiv b_s \pmod{m_s},$$

and thus the system (4.5) is fulfilled for $x = x_0$. From here, it directly follows that the system (4.5) is equivalent with the system

$$x \equiv x_0 \pmod{m_1}, \qquad x \equiv x_0 \pmod{m_2}, \ldots, x \equiv x_0 \pmod{m_k}, \tag{4.7}$$

i.e. the systems (4.5) and (4.7) are fulfilled for the same values of x. System (4.7) is then fulfilled only by those values x which fulfil the congruence (4.6).

Theorem 4.16 *Let $b_1, b_2, \ldots,$ independently of each other attain the values of the complete residue system moduli $m_1, m_2, \ldots, m_k$, then x_0 attain the values of the complete residue system moduli $m_1, m_2, \ldots, m_k$.*

Proof: Indeed, x_0 attains the values of $m_1, m_2, \ldots, m_k$, with regard to (4.6), noncongruent modulo $m_1, m_2, \ldots, m_k$.

Example: Solve the system of congruences

$$x \equiv b_1 \pmod 4, \qquad x \equiv b_2 \pmod 5, \qquad x \equiv b_3$$

It holds that 4.5.7=4.35=5.28=7.20, while

$$35.3 \equiv 1 \pmod 4, \qquad 28.2 \equiv 1 \pmod 5, \qquad 20.6 \equiv 1 \pmod 7.$$

Therefore it is

$$x_0 = 35.3b_1 + 28.2b_2 + 20.6b_3 = 105b_1 + 56b_2 + 120b_3,$$

and thus the set of all values x fulfilling the system can be expressed in the following form:

$$x \equiv 105b_1 + 56b_2 + 120b_3 \pmod{140}.$$

for example, the set of values x, fulfilling the system

$$x \equiv 1 \pmod 4, \qquad x \equiv 3 \pmod 5, \qquad x \equiv 2 \pmod 7,$$

is

$$x \equiv 105.1 + 56.3 + 120.2 \equiv 93 \pmod{140}.$$

and the set of values x, fulfilling the system

$$x \equiv 3 \pmod 4, \qquad x \equiv 2 \pmod 5, \qquad x \equiv 6 \pmod 7,$$

is

$$x = 105.3 + 56.2 + 120.6 \equiv 27 \pmod{140}.$$

4.6 Congruences of any degree with prime modulo

We will now deal with the congruences of the form

$$a_n x^n + a_1 x^{n-1} + \ldots + a_0 \equiv \pmod{p} \tag{4.8}$$

where p is a prime.

Theorem 4.17 *Congruence ot the form (4.8) is equivalent with congruence of degree at most $p-1$.*

This theorem follows from the fact that $f(x)$ can be written as

$$f(x) = (x^p - x)Q(x) + R(x),$$

where $R(x)$ is the remainder after dividing $f(x)$ by the polynomial $x^p - x$, because its degree cannot be higher than $p-1$. According to Fermat's little theorem, we have $x^p - x \equiv 0 \pmod{p}$, and therefore $f(x) \equiv R(x) \pmod{p}$.

Theorem 4.18 *Let congruence (4.8) have more than n solutions. Then it holds that all coefficients a_i are multiples of p.*

Let us denote remainders of all the solutions of congruence (4.8) by letters $x_1, x_2, \ldots x_n, x_{n+1}$. Polynomial $f(x)$ can be expressed as

$$\begin{aligned} f(x) \quad =& a(x-x_1)(x-x_2)\ldots(x-x_{n-1}(x-x_n)+ \\ & b(x-x_1)(x-x_2)\ldots(x-x_{n-1}+ \\ & +\ldots+ \\ & +l(x-x_1) \\ & +m. \end{aligned}$$

We will transform the addends on the right-hand side into polynomials and we choose b such that the sum of coefficients of the first two polynomials at x^{n-1} be a_1; if we know b, we choose c such that the sum of the coefficients of the first three polynomials at x^{x-2} be a_2 etc. If we gradually put $x = x_1, x_2, \ldots, x_n, x_{n+1}$, we will realize that all the numbers $m, l, k, \ldots, c, b, a$ are multiples of p. As a_i are sums of numbers divisible by p, they are also divisible by p.

4.7 Congruences of second degree

In this section, we will deal with congruences of the form

$$x^2 \equiv a \pmod{p}; \qquad (a,p) = 1, \tag{4.9}$$

where p is an odd prime. If this congruence has a solution, we call number o *a quadratic residue* and in the opposite case, *quadratic nonresidue* modulo p.

Theorem 4.19 *Let a be a quadratic residue modulo p. Then congruence (4.9) has exactly two solutions.*

Proof: Since a is a quadratic residue, the congruence (4.9) must have at least one solution; let us say it is x_1. Since $(-x_1)^2 = x_1^2$, the congruence has also a second solution $x \equiv -x_1 \pmod p$. Further, $x_1 \equiv -x_1 \pmod p$ cannot hold, since then it would be $2x_1 \equiv 0 \pmod p$. That, however, is not possible, since $(2, p) = (x_1, p) = 1$. The congruence cannot have another solution, as was proved in Theorem 4.19

Theorem 4.20 *Reduced residue system modulo p consists of* $\frac{p-1}{2}$ *quadratic residues which are congruent with numbers* $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$ *and* $\frac{p-1}{2}$ *quadratic nonresidues.*

Proof: Among the residues of the reduced system modulo p, quadratic residues are only those that are congruent with squares of numbers

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2} \tag{4.10}$$

modulo p. At the same time, the squares of numbers (4.10) are not congruent modulo p, since from the conditions $k^2 \equiv l^2 \pmod p$, $0 < k < l \leq \frac{p-1}{2}$, it would follow that there are four numbers out of the numbers (4.10) that fulfil congruence $x^2 \equiv l^2 \pmod p$, namely: $x \equiv -l, -k, l, k$, which is a contradiction.

Theorem 4.21 *Let a be a quadratic residue modulo p. Then the following holds:*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p; \tag{4.11}$$

If a is a quadratic nonresidue modulo p, it holds that

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p. \tag{4.12}$$

Proof: Fermat's little theorem says that $a^{p-1} \equiv 1 \pmod p$. This congruence can also be written in this form:

$$\left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \pmod p.$$

Since the difference of both brackets is equal to two, then only one of the congruences (4.11), (4.12) holds. Every quadratic residue a fulfils the congruence

$$a \equiv x^2 \pmod p, \tag{4.13}$$

for some x, and therefore it fulfils the congruence (4.11), which we obtain by taking both sides of the congruence to $\frac{p-1}{2}$. By quadratic residues, all the solutions of congruence (4.11) are exhausted. Quadratic nonresidues must therefore fulfil congruence (4.12).

4.8 Legendre symbol

Legendre symbol $\left(\frac{a}{p}\right)$ is equal to 1 if a is a quadratic residue and is equal to -1, if a is the quadratic nonresidue modulo p, while $(a, p) = 1$. Number a is called the numerator and number p the denominator of Legendre symbol. We read: a with respect to p. It obviously holds that

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Since the numbers of one and the same class are at the same time also quadratic residues or nonresidues, the following theorem also holds:

Theorem 4.22 *Let $a \equiv a_1 \pmod{p}$. Then $\left(\frac{a}{p}\right) = \left(\frac{a_1}{p}\right)$.*

Since $1 = 1^2$, number 1 is a quadratic residue for each modulo and

$$\left(\frac{a}{p}\right) = 1.$$

Odd prime can be expressed either in the form $4k + 1$ or $4k + 3$. In the first case, however, the expression $\frac{p-1}{2}$ is always even, and in the second, it is odd. Number -1 is therefore a quadratic residue of the primes of the form $4k + 1$ and quadratic nonresidue of primes of the form $4k + 3$. It thus holds that

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

For Legendre symbol, it also holds that:

$$\left(\frac{ab \dots l}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{l}{p}\right).$$

Indeed, we have

$$\left(\frac{ab \dots l}{p}\right) \equiv (ab \dots l)^{\frac{p-1}{2}} \equiv (a)^{\frac{p-1}{2}}(b^{\frac{p-1}{2}} \dots (l)^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\cdots\left(\frac{l}{p}\right) \pmod{p}.$$

As a consequence, we can leave out all quadratic terms in the numerator, i.e. it holds that

$$\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right).$$

Theorem 4.23 *Let p and q be odd primes. It then holds that*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

This theorem is known in number theory as *Gauss law of quadratic reciprocity.* Gauss was the first one to prove it and he called it *theorema aurea* (golden theorem). In connection with the properties stated above, this law allows for significant simplification of the computation of the Legendre symbol, as we will show below. Because of its length, we do not include the proof of the quadratic reciprocity law here, but the reader can find it e.g. in XX

Example: Compute Legendre symbol $L = \left(\frac{111}{1999}\right)$.
First we will notice that 111 is a composite number and that it holds that 111 = 3.37. It therefore holds that

$$\left(\frac{111}{1999}\right) = \left(\frac{3}{1999}\right)\left(\frac{37}{1999}\right).$$

We will now use the quadratic reciprocity law, through which we in the "numerator" of Legendre symbol obtain a number larger than in the "denominator". We thus have

$$L = (-1)^{999}\left(\frac{1999}{3}\right) \times (-1)^{999\cdot 18}\left(\frac{1999}{37}\right)$$

If we divide number 1999 by 3 or 37, we obtain 1 as a result in both cases. In other words, 1999 is congruent to 1 modulo 37 as well as modulo 3. We can thus finish the computation:

$$L = (-1)\left(\frac{1}{3}\right)\left(\frac{1}{37}\right) = -1.$$

We now have the opportunity to ask whether a similar symbol could not be introduced also in the case when the "numerator" is not a prime. This problem was tackled by the German mathematician C. G. Jacobi, who extended Legendre symbol in the following way:

Definition 4.1 *Let a be an integer and let $n \geq 3$ be odd. Let further $n = p_1 p_2 \dots p_r$, where p_i are odd primes, not necessarily different. Jacobi symbol is defined by the relation*

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r}\left(\frac{a}{p_i}\right), \tag{4.14}$$

where $\left(\frac{a}{p_i}\right)$ is Legendre symbol.

The properties of Jacobi symbol are analogous to the properties of Legendre symbol, including the law of quadratic reciprocity, but there is one significant difference. If Legendre symbol is equal to one, a is always the quadratic residue modulo p, which follows from the definition. This does not have to hold for Jacobi symbol, as can be seen from the example below:

$$\left(\frac{1}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1,$$

but 2 is not a quadratic residue modulo 15.

4.9 Some important theorems in number theory

To end this chapter, let us introduce a few theorems in number theory.

Theorem 4.24 *Fermat's little theorem. Let p be prime and $(a, p) = 1$. Then*

$$a^{p-1} \equiv 1 \pmod{p}. \tag{4.15}$$

Today, we know several proofs of this theorem, but let the author have his axe to grind and direct the readers to his book [3]. In order not to deprive the readers of everything, let us introduce an elegant proof for the special case of $a = 2$. One of the most important theorems of turbodidactics, the theorem of *Tesák* is most important; it says that $1 + 1 = 2$. Using this theorem, we have

$$2^p = (1+1)^p = \binom{p}{0} + \binom{p}{1} + \cdots + \binom{p}{p-1} + \binom{p}{p}.$$

Since p is a prime, all the binomial coefficients $\binom{p}{k}$ are divisible by p with the exception of $k = 0$ and $k = p$. We may thus proceed directly to the congruence and we obtain

$$2^p \equiv 2 \pmod{p} \Rightarrow 2^{p-1} \equiv 1 \pmod{p}.$$

The last simplification follows from the fact that according to the assumption of Fermat's little theorem, $(2, p) = 1$.

The fact that

$$q(a) = \frac{a^{p-1} - 1}{p}$$

is an integer is a consequence of Fermat's little theorem. The quotient $q(a)$ is called *Fermat quotient*.

Fermat's little theorem was later generalized by Euler.

Theorem 4.25 *(Euler). Let a and n be natural numbers and $(a, n) = 1$. Then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}, \tag{4.16}$$

where $\varphi(n)$ is Euler function, which we defined in Chapter 2.

Let us recall that the expression $n! = n.(n-1)\dots 2.1$ is called n-factorial. The following theorem can be proved:

Theorem 4.26 *(Wilson) Let p is a prime. Then*

$$(p-1)! \equiv -1 \pmod{p}. \tag{4.17}$$

As we have introduced Fermat's little theorem, we should also introduce Last theorem of Fermat, although it does not directly correspond with the theme of this text.

Theorem 4.27 *Diophantine equation*

$$x^n + y^n = z^n \tag{4.18}$$

does not have an integer solution for $n > 2$.

As has already been said, this theorem does not really touch the theme of this textbook, but it is a very well known problem, so when somebody wants to learn more about it, we recommend book [6].

4.10 Exercises

4.1. Determine which of the following congruences are solvable
a) $6x \equiv 1 \pmod{9}$ b) $9x \equiv 3 \pmod{6}$ c) $14x \equiv 21 \pmod{70}$

4.2. Solve the congruence
a) $20x \equiv 4 \pmod{30}$ b) $20x \equiv 30 \pmod{4}$ c) $353x \equiv 254 \pmod{400}$

4.3. Find the smallest natural number bigger than 1 fulfilling the congruence $x \equiv 1 \pmod{3}$, $x \equiv 1 \pmod{5}$, $x \equiv 1 \pmod{7}$.

4.4. Solve the system of congruences $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 5 \pmod{2}$.

4.5. Solve the system of congruences $x \equiv 1 \pmod{4}$, $x \equiv 0 \pmod{3}$, $x \equiv 5 \pmod{7}$.

4.6. Find all the integers that give remainders 1, 2, and 3 when divided by 3, 4, and 5.

Chapter 5

Special types of natural numbers

In this chapter, we will introduce some special kinds of numbers, both primes and composite numbers. This chapter will not be so textbook-like as the previous chapters, but the readers will learn about some special types of numbers and will learn about curiosities connected with number theory which they will be able to use in their teaching. Numbers are namely very interesting and we could also say they are magical. The individual chapters in the text will be ordered alphabetically.[1]

5.1 Perfect numbers

As has already been said, any natural number $n > 1$ has at least two divisors, namely 1 and n. Let us denote by $\sigma(n)$ the sum of all the divisors of number n. It is obvious that $\sigma(n) \geq 1$, but let us also compare the sum of divisors with the double of n. If we choose this limit, the set of natural numbers $n > 1$ will decompose into three non-intersecting subsets. In the first one, there are those numbers for which $\sigma(n) < 2n$ and we will call them *deficient* (numeri deficientes). This set is infinite, because e.g. all primes belong here. The numbers for which $\sigma(n) > 2n$ will be called *abundant* (numeri abundantes). This set is also infinite, we can include numbers of the form $n = 2^k \cdot 3, \qquad k > 1$ here. The proof is easy for anyone who has mastered the formula for the sum of the fist n members of a geometric sequence. It holds that

$$\sigma(n) = \frac{2^{k+1} - 1}{2 - 1} \frac{3^2 - 1}{3 - 1} = (2^{k+1} - 1) \cdot 4 > 2 \cdot (2^k \cdot 3) = 2n.$$

The third set is then formed by those numbers $n > 1$ for which $\sigma(n) = 2n$. These numbers are called *perfect numbers* (numeri perfecti), sometimes we call them perfect numbers of the first kind. Sometimes the perfect number (of the first kind) is also defined as the sum of all its non-trivial divisors, i.e. the divisors smaller than the number itself. The smallest perfect number is 6=1+2+3. In the antiquitiy, three more perfect numbers were known, namely 28, 496, and 8128. It is interesting that already in Euclid's Elements, we can find the sufficient condition for an even number to be perfect, but verifying it was probably beyond the capabilities of

[1] This holds for the order in Czech language.

the computers. As the readers have certainly noticed, the perfect numbers introduced are even. We will therefore introduce the necessary and sufficient condition for a number to be perfect.

Theorem 5.1 *An even number $n > 1$ is perfect if and only if it is of the form*

$$n = 2^{s-1}(2^s - 1), \tag{5.1}$$

where $s > 1$ is a natural number and $M_s = 2^s - 1$ is a prime.

Numbers M_s are called *Mersenne numbers.* In the following proof, we will denote them by p in order to facilitate the notation.

Proof: The proof of the sufficient condition is easier, therefore we will start with that. Let a number be of the form (); this form also presents its canonical factorization. Therefore it is

$$\sigma(n) = \frac{2^s - 1}{2 - 1} \frac{p^2 - 1}{p - 1}.$$

Through an elementary simplification of this expression, we conclude that $\sigma(n) = 2^s p = 2(2^{s-1}p)$, i.e. n is perfect.

Let us prove also the necessary condition. Let n be an even perfect number. We will easily see that its factorization must contain at least one odd prime, because if the factorization were of the form $2^k, k \geq 1$ and $\sigma(n) = 2^{k+1} - 1$ and the number n would thus not be perfect. Let the canonical factorization of n be $n = 2^\alpha p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Let us put $l = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ a $\alpha = s - 1$. Since n is perfect, it must be

$$\sigma(n) = \frac{2^s - 1}{2 - 1} \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_1^{\alpha_k+1} - 1}{p_1 - 1} = (2^s - 1)\sigma(l) = 2^s l,$$

because

$$\sigma(l) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_1^{\alpha_k+1} - 1}{p_k - 1}.$$

The equality

$$(2^s - 1).\sigma(l) = 2^s.l \tag{5.2}$$

shows that 2^s divides the product $(2^s - 1).\sigma(l)$. Number 2^s is, however, only divisible by numbers $\pm 1, \pm 2^r$, kde $1 \leq r \leq s$. Since $2^s - 1$ is odd, it is obvious that numbers 2^s and $2^s - 1$ are coprime, i.e. $2^s \mid \sigma(l)$. A number $q \geq 1$ must exist such that $\sigma(l) = 2^s.q$. If we substitute into the previous equality (), after simplification, we obtain 2^s

$$(2^s - 1).q = l \tag{5.3}$$

or

$$2^s.q = \sigma(l) = l + q. \tag{5.4}$$

Number $l > 1$ is divisible by l and according to () also by q. From equality () it follows that $l \neq q$, the equality () then says that number l cannot have other divisors than l and q. Namely, if a number $d \geq 1$ existed and at the same time d was different from the numbers l and q, the sum of the divisors of number l would be equal to at least $l + q + d$, which is in contradiction with (). Therefore l only has two divisors, namely itself and $q = 1$, it is thus a prime. According to () it holds that $l = 2^s - 1$, the perfect number n is then of the form $2^{s-1}.(2^s - 1)$, $s > 1$ and $2^s - 1$ is a prime.

A perfect number of the second type is a number that is equal to the product of all its proper divisors. An example of this is number 6 (6=1.2.3), which is also a perfect number of the first kind. There is a simple formula for perfect numbers of the second kind as well and it follows from it that there are infinitely many of them.

Theorem 5.2 *Number $n > 1$ is a perfect number of the second kind if and only if it is the third power of a prime or a product of a prime.*

If $n = p^3$, then its divisors are 1, p and p^2 and their product is equal to n. If $n = p_1.p_2$, then these primes are together with number one the only divisors and their product is equal to number n.

Let on the contrary $n > 1$ be a perfect number of the second kind. Let us suppose that its canonical factorization is $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$. We will order all the divisors of number n by size, and it is thus $1 = d_1 < d_2 \dots < d_s = n$. We put $\tau(n) = s$. Then $n = d_1.d_2 \dots d_{s=1}$. If we multiply this equality by number $n = d_s$, we obtain

$$n^2 = d_1.d_2 \dots d_s. \tag{5.5}$$

If d is a divisor of number n, then $\frac{n}{d}$ is also its divisor. We can therefore write

$$n^2 = \frac{n}{d_1} \cdot \frac{n}{n_2} \cdots \frac{n}{d_s}. \tag{5.6}$$

If we multiply the previous two equalities, we have $n^4 = n^s$, from which it follows that $s = 4$. Since $\tau(n) = (\alpha_1 + 1) \dots (\alpha_k + 1)$, all the brackets are greater or equal to two, and therefore $k \leq 2$. Only two canonical factorizations of n are thus possible. Either $n = p_1^{\alpha 1}$, or $n = p_1^{\alpha_1}.p_2^{\alpha_2}$. In the first case, $\alpha_1 = 3$, in the second $\alpha_1 = \alpha_2 = 1$.

5.2 Fermat numbers

In this part, we again meet with the name of Fermat. This man studied the numbers of the form

$$F_m = 2^{2^m} + 1, \qquad m = 0, 1, 2, \dots.$$

Fermat was convinced that these are primes, but did not succeed in proving, nor disproving this, although he had tools for this. The first five of these numbers are indeed primes, and if we hear the name Fermat prime, it will concern precisely these primes.

It might seem that the written form of these numbers is too complicated, but the following theorem will show that Fermat knew very well why he chose this form.

Theorem 5.3 *Let n be a natural number. If $n = 2^n + 1$ is a prime, then $m = 2^m$ for some $m \in \{0, 1, 2, \dots\}$.*

Let k and l be natural numbers, while l is odd and at the same time $l \geq 3$. The following formula then holds

$$2^{kl} + 1 = (2^k + 1)(2^{k(l-1)} - 2^{k(l-2) + \cdots - 2^k + 1)}.$$

The number of the form $2^n + 1$ is always composite when the exponent is divisible by an odd natural number greater than one. The form for Fermat numbers thus secures the fulfilment of the necessary condition for these numbers to be primes.

We will now take a break from numbers and will have a look into geometry, or into planimetrics, if you like. Euclidean constructions with ruler and compass belong to the beautiful parts of mathematics. On one hand, we have absolutely accurate ideas, but these can never be performed in practice. It is thus a nice example of platonic philosophy, when we put on paper only the shadows or mirror images of ideal geometry. Such pencil sharpener that would allow us to have a pencil so sharp that we could construct a perfect line or other ideal geometrical shapes, i.e. length without a width, has not been and will never be invented. Let us choose the construction of an n-gon from the vast number of various constructions. It is a walkaway to draw an isosceles triangle, square, or a regular hexagon and with a little bit of trying, we also can draw a regular pentagon. Although seven is considered a lucky number, it does not hold for a regular heptagon. Generations of geometers tried to crack this nut, but in vain. Only Gauss succeeded in cracking it when he proved the following theorem:

Theorem 5.4 *A regular n-gon can be constructed by a ruler and a compass if and only if $n = 2^i F_{m_1} F_{m_2} \cdots F_{m_j}$, kde $n \geq 3$, $i \geq 0$, $j \geq 0$ a $F_{m_1}, \ldots F_{m_j}$ are mutually different Fermat primes.*

The proof of this theorem is beyond this text, so let us say only that the geometrical problem is transfered into an algebraic one. For example, for the central angle of a regular pentagon, $\cos \frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}$. The cosine is equal to the length of the adjacent side of a right-angle triangle with hypotenuse of the length one and we can construct the line segment with a ruler and a compass. As the only Fermat primes known now are 3, 5, 17, 257 and 65537, it is obvious that Euclidean construction of a regular heptagon (and also many others with odd numbers of sides) are principally impossible. There are also other connections between Fermat primes and geometry, but since they exceed the extent of what is generally taught at elementary and high schools, we do not state them and direct those interested to another publication, e.g. [2].

After returning from the trip to geometry, we will close the part devoted to Fermat numbers. It is a sort of a mystery that Fermat did not find $F_5 = 641.6700417$, which was only found by Euler. On the other hand we nowadays understand why the French genius did mot find any proof of this. The proof has namely not been found until today, although these numbers are given a lot of attention by contemporary mathematicians. These numbers are namely big, or, rather, their decimal expression contains many digits (e.g. F_{18} has almost 80 000 digits). Computers were also employed in the factorization of large numbers, and we have only one certainty now, namely that for $5 \geq m \geq 32$, these numbers are composite, although we know no non-trivial divisor for numbers F_{20} and F_{24}. Mathematicians have so far not succeeded in finding some dependency that would suggest something in this direction. Number theory thus presents another challenge to us.

5.3 Friendly numbers

Definition 5.1 *Two natural numbers a and b are called friendly numbers, if the sum of the proper divisors of number a is equal to number b and at the same time the sum of the proper divisors of number b is equal to a.*

An example of friendly numbers can be the pair 220 and 284, which was known already to the Pythagoreans. Indeed, proper divisors of the first one are 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, and 110; the sum of these numbers is 284. Number 284 does not have as many proper divisors, they are only 1, 2, 4, 71, and 142 and their sum is 220. In publication [7], written primarily for Mathematical Olympiad participants, a small mistake found a way and instead of 71, it says 7.

Theorem 5.5 *Numbers a and b are friendly if and only if $\sigma(a) = \sigma(b) = a + b$.*

Proof: It is obvious that the number of proper divisors of number m is $\sigma(m) - m$. If a and b are friendly numbers, it is also $\sigma(a) - a = b$ and $\sigma(b) - b = a$. If we calculate b from the second equation and substitute it into the first, we have$\sigma(a) = \sigma(b)$. If, on the other hand, $\sigma(a) = \sigma(b) = a + b$, we can easily see that $\sigma(a) - a = b$ and at the same time $\sigma(b) - b = a$ and that the numbers a and b are friendly numbers.

Also in the case of friendly numbers, not everything has been clarified so far. We e.g. do not know whether there are infinitely many of them. All the friendly pairs known until today have a greatest common divisor greater than one. We, however, know a pair of odd friendly numbers $a = 3^3.5.7.11$ and $b = 3.5.7.139$.

We may look for friendly numbers according to the instructions given by the mathematician Ben Korrah in the 9th century. .

Theorem 5.6 *Let for $n > 1$ there exist primes of the form $p = 3.2^{n-1} - 1$, $q = 3.2^n - 1$ and $r = 9.2^{2n-1} - 1$. Then numbers $k = 2^n pq$ a $l = 2^n.r$ are friendly.*

Proof: We will first prove that the sum of all the divisors of number k is equal to the sum of the divisors of number l. For the sum of divisors $\sigma(k)$, it holds that

$$\sigma(2^n.p.q) = (2^{n+1} - 1).(p + 1).(q + 1) = (2^{n+1} - 1).9.2^{2n-1}.$$

For the sum of divisors $\sigma(l)$ it then holds

$$\sigma(2^n.r) = (2^{n+1} - 1)(r + 1) = (2^{n+1} - 1)9.2^{2n-1}.$$

As a second step, we must prove that this sum is equal to $k + l$.

$$k + l = 2^n pq + 2^n r = 2^n(pq + r) = 9.2^{2n-1}(2^{n+1} - 1) = \sigma(k) = \sigma)l).$$

5.4 Conclusion

At the end of this chapter, we will introduce some further special primes. Let us first recall Euclid's proof of the infinite number of primes, in which the expression $n = p_1 p_2 \ldots p_k + 1$ played a major role. Number n may, but does not have to, be a prime. If it is a prime, we will call it *Euclid's prime.* Euclid‘s proof can be easily modified in such a way that instead of number n, we construct the number $m = p! + 1$, where p is the largest prime, of which we assume there is a finite number. Not even in this case is the number m divisible by any prime, since for every $q \leq p$, the remainder after dividing number m by number q is always equal to one. This way, we have constructed a prime greater than p, since m is divisible by a prime greater than p, and in any case we have arrived at a contradiction with the assumption. The primes of the form $k! + 1$ area called *factorial* primes. This name denotes also the primes of the form $k! - 1$. In both cases, we do not require k to be a prime.

Chapter 6

Applications of number theory

If the readers have come this far in this text, they might think the following. Number theory is a very beautiful part of mathematics, it contains a number of interesting theorems, some of the proofs are very elegant, many findings can be used to make teaching more interesting, some not proved and not disproved statements are also interesting, but what is the importance of this for practical life? Is this not just a beautiful, but otherwise useless theory? In this chapter, we will try to prove that it is not so, that number theory is very important for practical life and that its importance has recently been rising. And we will start with the thing with which any citizen of this country is connected from the cradle to the grave. Yes, we will start with the national identification number.

6.1 National identification numbers

Each citizen of the Czech Republic has been given a national identification number, which is constructed in such a way that the first six numbers are determined by the date of birth. The first pair of digits denotes the year, the second month, and the third the day of birth. In order to make it possible to distinguish the sex, the second pair of digits is increased by fifty for girls. The national identification number for boys who were born on December 10, 1996 begins with the six digits 961210, for girls it is 966210. Because more children are born in a single day, more digits are added to these six. Since 1986, four more digit are added, and thus the national identification numbers have ten digits. The last four digits, however, are not chosen at random, but so that the whole national identification number be divisible by 11. What is the motivation for this, would it not be enough to for example order all the children born in one day for example according to the time when they were born and then give them numbers corresponding with that?

In order to answer this question, we will first prove the criteriun for divisibility of numbers by eleven. Let k$\in \{0,1,2,\ldots\}$ and $m=\sum_{n=0}^{k} c_n 10^n$ for $c_n \in \{0,1,2,\ldots,9\}$, $c_k \neq 0$, thus $c_k,\ldots,c_0$ are the digits of the natural number m in the decimal system. Then

$$11 \mid m \Leftrightarrow 11 \mid \left(\sum_{n=0}^{k}(-1)^n c_n\right). \tag{6.1}$$

Proof. According to the formula for the difference of two n-th powers, it holds that

$$10^n - (-1)^n = (10+1)[10^{n-1} + 10^{n-2}(-1) + \cdots + 10(-1)^{n-2} + (-1)^{n-1}], \quad (6.2)$$

where the square brackets contain exactly n addends. The difference $10^n - (-1)^n$ is thus divisible by 11. If we now use the formula () for each addend in () except for the last one, we obtain

$$11 \mid ((-1)^k c_k + (-1)^{k-1} c_{k-1} + \cdots + c_1 + c_0). \quad (6.3)$$

Similarly, we will see that if () holds, then also () holds.

Let us now return to our boy, whose national identification number could be 9612107032. Let us assume that we will make a mistake and enter one digit wrongly. Then the difference between the correctly and incorrectly entered number will be $\pm c \cdot 10^n$, where $c \in \{1, 2, \ldots, 9\}$. This difference will never be divisible by 11, but can be divisible by composite numbers 12, 14, 15 and so on. If we write a one instead of a seven, the difference between the correct and incorrect national identification number is 6 000. Finding all its two-digit divisors is left to the reader. As number 11 allows us to find the mistake, we speak of *error detecting code modulo 11.*

When using single-digit primes, we cannot in general detect a mistake when entering a single wrong digit. The use of larger two-digit primes would then on the other hand diminish the number of national identification numbers which could be used. Number 11 is thus optimal for the needs of the national identification number. To end this section, we will add one curiosity. Czech two-crown coin is a regular 11-gon.

If we put the coin into the basic position and then we turn it alternately clockwise and anti-clockwise as many vertices as the respective number is. After the last turn, the coin must return to its original position.

A similar principle is employed also for the ISBN and ISSN codes for books and journals, identification numbers of organizations, bank account numbers etc. The reader may learn more e.g. at [10]. Self-detecting codes can find the mistake, they cannot correct it. For this reason, *self-correcting codes* were developed. These allow us to find out, with the help of redundant (superfluous) information contained in the coded words, which sign is incorrect and to correct it. The so-called two-dimensional codes with high information capacity and ability to detect and correct errors enjoy great expectations. These codes are used a.o. in American driver's licences or various identification cards. Their advantage is their transfer via printing on paper and the fact that there is no necessity to input the data through a keyboard.

6.2 Encrypting messages with the help of large primes

The need to keep written messages secret is probably as old as the script itself. Over the centuries, people invented many ways of preventing an unauthorized person coming across a secret message from reading it. As an example, the encryption grille Mathias Sandor and his friends were using may serve. It was, however, enough that the bad guy Sarkany got hold of the grille and reading the messages was no longer a problem for him. Sometimes, pure logical thinking was enough to solve the cipher. The genius detective Sherlock Holmes solved such ciphers on a daily basis. He solved the cipher consisting in substituting every letter by a dancing figure by using the frequency of occurrences of the individual letters. While in Czech alphabet, it is the letter a, in English, it is the letter e. The same method is employed by the solvers of the so-called number crossword puzzles. Another method consists in substituting a word with a number determining the order of a word on a certain page in a certain book available to both parties involved. In that case, it is not recommended that the book has more volumes. Good soldier Švejk logically got the first volume of the *Sins of the Fathers,* for the officers, but the second volume was the key and the eleventh march battalion could not use this cipher.

The above-stated examples are older, from the times when the readers of encrypted messages had to rely only on their intelect. In the time of the computer, it seems that it is impossible to come up with encryption that would be safe against potential unintended readers, because what one person invents, another one solves, as Sherlock Holmes said. However, mathematics is not thought to be the queen of the sciences in vain. In 1978, gentlemen Rivest, Shamir and Adelman came up with a method that is nowadays known as RSA, for their initials. The easier the method, the more effective it is, it is not even necessary to keep the encryption key secret, and anybody can use the cipher. Without knowing the decryption key, however, it is now impossible to solve the cipher and it seems that this will be the case in the future as well. The core of the method is that it is no problem to multiply two large numbers. However, the inverse process, finding the factorization of a composite number, is much more difficult.

We will now describe the procedure for encrypting and decrypting the messages. We will first transform the message that we want to encrypt into a natural number x. To do this, we could employ e.g. the ASCII codes, but using them is not necessary, there are also other and perhaps even more effective ways. Further, we will assume that $x < n$, where n is the product of two different primes that are not publicly known and have more than 100 digits. Those who want to encrypt longer messages must of course first cut the message into several shorter ones so that the previous inequality is fulfilled for each of them. We will denote the encrypted message with the symbol $x*$. This natural number is uniquely given by the inequality $x* < n$ and the congruence

$$x* \equiv x^e \pmod{n}, \tag{6.4}$$

where e is called the *encryption exponent.* Numbers e and n are known publicly and are sufficient to perform the encryption.

Decryption is performed analogically. We again define the number $(x*)^0 \in N$ fulfilling the inequality $(x*)^0 < n$ so that $(x*)^0 \equiv (x*)^d \pmod{n}$. *Decryption exponent d*, however, is not publicly known. It is necessary to first solve the question of how to choose the exponents e and d so that $(x*)^0 = x$, i.e. so that after the decryption, the encrypted message was the same as the original message x.

We will first prove the following theorem: Let a natural number n fulfil

$$(e, \varphi(n)) = 1. \tag{6.5}$$

Then there exists exactly one natural number $d < \varphi(n)$ such that

$$ed \equiv 1 \pmod{\varphi(n)}. \tag{6.6}$$

Proof: For natural numbers $k = 1, \ldots, \varphi(n) - 1$, we define remainders $z_k \in \{1, \ldots, \varphi(n)1\}$ with the help of congruence

$$ek \equiv z_k \pmod{\varphi(n)}.$$

If two remainders are equal, for example $z_{k_1} = z_{k_2}$, then the correct congruence is

$$e(k_1 - k_2) \equiv 0 \pmod{\varphi(n)}.$$

Then according to the assumption and Theorem 1. 3. (Křížek) there exist integers v and y such that $ev + \varphi(n)y = 1$, therefore it is $e(k_1 - k_2)v + \varphi(n)(k_1 - k_2)y = k_1 - k_2$. From there, it follows that $k_1 - k_2 \equiv 0 \pmod{\varphi(n)}$, and thus $k_1 = k_2$. All the remainders z_k are mutually different integers, and therefore there exists exactly one d corresponding to the remainder 1 and fulfilling ().

We will further prove that the encrypted message $x*$ is, after the decryption, the same as the original message x.

Theorem 6.1 *Let* $(e, \varphi(n)) = 1$. *Then*

$$(x*)^0 = x. \tag{6.7}$$

Proof: From congruence (), the existence of such number r that

$$ed = 1 + r\varphi(n) \tag{6.8}$$

follows. We distinguish two cases:

1. Let $(x, n) = 1$. Then Euler's relation can be exponentiated to r-th and then multiplied by x, through which we obtain

$$x^{1+r\varphi(n)} \equiv x \pmod{n} \tag{6.9}$$

Now subsequently from (), (), (), and (), it follows that

$$(x*)^0 \equiv (x*)^d \equiv x^{ed} \equiv x^{1+r\varphi(n)} \equiv x \pmod{n}. \tag{6.10}$$

The relation () thus holds, because both natural numbers x and $(x*)^0$ are smaller than n.

2. Let $(x, n) \neq 1$. Then either $x = p$, or $x = q$. Without the loss of generality, we can assume that the second possibility holds. Since $(p, q) = 1$, we can exponentiate Fermat's relation to $r(q-1)$, through which we obtain

$$x^{(p-1)(q-1)} \equiv 1 \pmod{p}.$$

Since $\varphi(n) = (p-1)(q-1)$, the following holds:

$$x^{1+r\varphi(n)} \equiv x \pmod{px}$$

This is again the relation (), since $px = pq = n$. We proceed further as in the case 1.

The encryption exponent e is chosen in such a way that $3 \leq e < \varphi(n)$ and so that $(e, \varphi)n)) = 1$. In addition, it is necessary to choose e such that $e^m \not\equiv 1 \pmod{\varphi(n)}$ for small m, so that it is not possible to decrypt the message for $d = e - 1$, if we do not know the values p and q, and if we do not know them, it is almost impossible to state the value of the decryption exponent d. However, we know from Theorem x. x. that there exists exactly one natural number $d < \varphi(n)$ fulfilling the congruence (). A question arises how to set its value if we know p and q.

If we can factorize $\varphi(n)$, then we can easily calculate the value $\varphi(\varphi(n))$. From Euler's theorem, the implication below follows:

$$(e, \varphi(n)) = 1 \Rightarrow e^{\varphi(\varphi(n))} \equiv 1 \pmod{\varphi(n)}.$$

If we multiply the previous congruence d and if we use (), then we obtain an explicit expression for decryption exponent $d < \varphi(n)$,

$$d \equiv de^{\varphi(\varphi(n))} \equiv ede^{\varphi(\varphi(n))-1} \equiv e^{\phi(\varphi(n))-1} \pmod{\varphi(n)}. \qquad (6.11)$$

If we cannot factorize $\varphi(n)$, we can calculate d directly from congruence (), e.g. with the use of Euclid's algorithm or we simply choose a different p or q.

6.3 Magic with numbers

When I was still a small boy, it was always a great event when a magician came to the village. We were all enchanted by his tricks, whether they be tricks with cards, disappearing or unexpected appearing of things and more and more miracles that fascinated us. The magician usually disclosed one trick during the performance and then everybody was surprised that the tricks are in fact so easy. Anyone, however, can be such an illusionist and will not even need nimble fingers, it will suffice to use some interesting properties of numbers. We could, after all, have been convinced by the text above that numbers hide a lot of magic before us and that it is a question whether we will be able to solve them at all. To conclude this text, let us therefore introduce some magic with numbers. The readers may find more of them in publications on recreational mathematics and if they have enough time for going through old newspapers, then also in the entertainment corners of Sunday or later Saturday newspaper supplements.

Magic number one: Choose any three-digit number so that there was a difference of at least two between the first and the last digit. Form a number whose digits are in reverse order and subtract the smaller number from the greater one. In the result, change the order of digits again and add the two numbers. Let us assume that we chose number 115. Then we need to calculate 511-115=396. Further, we must add 396 and 693. In our example, we obtain 1089. We, in contrast to the magicians, will explain every trick, and thus we will assume that we choose number $100a + 10b + c$, while $a \geq c + 2$. Then $100a + 10b + c - 100c - 10b - a = 100(a - c) - a + c = 100(a - c - 1) + 90 + (10 - a + c)$. If we add $100(10 - a + c) + 90 + (a - c - 1)$ to this result, we obtain 900+180+9=1089. This result is not dependent on the choice of the digits and any number will give the same result.

Magic number two: Let us choose two arbitrary numbers. Let us form a sequence in a similar way as Fibonacci did, i.e. every next term is the sum of two previous ones. Let us add the first ten terms of this sequence and divide it by the seventh term. Let us choose for example 3 and 7. The first ten terms of the sequence will be 3, 7, 10, 17, 27, 44, 71, 115, 186, 301 and their sum 781. If we divide this number by 71, we obtain 11. This number will always be the result. It is namely $f_1 = m$ a $f_2 = n$, je $f_7 = 5m + 8n$ and $\sum_{i=1}^{10} f_i = 55m + 88n = 11f_7$. We can also use complex numbers for this magic, but we have to remember that $f_7 \neq 0$.

Magic number three: Let us choose any natural number divisible by three. We will cube the digits and add them, by which we obtain another natural number. We repeat the procedure, but we will find out that when we reach the number 153, the process will continue in a cycle. Explained in a scientific language, if we repeatedly add the cubes of the digits of a natural number, we will always end up with 153. Let us think number 1422. Then $1^3 + 4^3 + 2^3 + 2^3 = 81 \mapsto 8^3 + 1^3 = 513 \mapsto 5^3 + 1^3 + 3^3 = 153$. If we denote $n = c_k 10^k + \cdots + c_1 10 + c_0$ and $m = c_k^3 + \cdots + c_1^3 + c_0^3$, then it follows from the assumption $3|n$ that $3|m$. From the criterion for divisibility by three, it follows that $n \equiv \sum_{i=0}^{k} c_i^3 \pmod 3$. According to Fermat's little theorem, we have $c_i^3 \equiv c_i \pmod 3$. It is thus

$$m = \sum_{i=0}^{k} c_i^3 \equiv \sum_{i=0}^{k} c_i \equiv n \pmod 3.$$

Further, it is

$$n = \sum_{i=0}^{k} c_i 10^i \geq c_k 10^k \geq 10^k > (k+1)9^3 \geq \sum_{i=0}^{k} c_i^3 = m.$$

If thus $n \geq 10^4$, the sum of the cubes of the digits is always less than the original number. It thus suffices to explore how the string continues after we cross this boundary. With the help of computers, we can verify that there is a finite number of possibilities and that they all lead to number 153. To conclude, let us add that there exist also other numbers that are equal to the sum of cubes of natural numbers. Apart from the singular case of number one, these include also 370, 371 and 407, none of them is, however, divisible by three.

Magic number four: Let us choose a three-digit number whose digits are not all the same. Let us order the digits from the least to the greatest and the other way round and subtract the two numbers. After a finite number of steps, we will reach number 495. If we choose 169, we have 961-169=792; 972-279=693; 963-369=594; 954-459=495. If the difference only has two digits, we have to fill a zero in the front. The same property holds also for four-digit numbers, where we reach number 6174. To commemorate the man who discovered it, the number is called *Kaprekar constant.* As there are finitely many numbers, this curiosity can be verified on a computer.

To conclude this chapter, we will make a short excursion into turbo-didactics. Euler derived the formula $e^{i\pi}+1 = 0$. In this formula, we can find all the arithmetic operations (addition, multiplication, exponentiation) and also the most important mathematical constants (0, 1, i, e, π), exactly once and it is therefore considered the most beautiful one. (We could say it is Miss formula.) Let us perform a turbodidactic magic and expand this form:

$$e^{i\pi} = -1 = (-1)^3 = (e^{i\pi})^3 = e^{3i\pi}.$$

Since the left-hand side is equal to the right-hand one, we can de-logarithmize and we obtain $i\pi$=$3i\pi$ či 1=3. Person to whom complex variable is a known topic will immediately discover the difference between mathematics and turbodidactis; let us, however, add that for a complex variable, logarithmization was not a correct operation.

6.4 Exercises

In order to satisfy the requirements, let us still present a few tasks in which the readers can test their knowledge of the textbook.

6.1. Think any number between six and sixty. Divide this number subsequently by three, four, and five and announce the remainders. A person knowledgeable about remainders will tell you what the original number was. How is this possible?

6.2. Multiply your age by ten and subtract a multiple of nine of any single-digit number. Tell me the result and I will tell you how old you are. How is this possible?

6.3. And once more about age. Multiply your youth (your age) by two, add five, multiply the sum again by five and tell me the result. I will be able to tell you how old you are even from this number. How is this possible?

6.4. It is, however, not enough; we can also guess the exact date of birth, namely through the following procedure. We multiply the number of the month by one hundred. To this, we add the number determining the day and we multiply the result by two. We add eight to the result. Further, we multiply by five and add four. We multiply this result by ten and add four. The last operation is the addition of the age in years. We subtract 444 and divide the result into block of two digits from the right-hand side. In order to balance things, we take this from the left: the first two digits determine the month, the second two the day and the third one the age of the person.

6.5. We can also guess a given number. We subtract one from the number we think, we multiply the rest by two and add the number we think. We find the number thought from the result by adding two and dividing by three.

6.6. Think any number. If the number has an odd number of digits, put a zero in front of the number. Move the digits on odd positions to the even positions in any way and also the other way round. Add the number that has thus originated to the original one. Write down the sum in the reverse order and subtract it from the original sum. Divide the result into two-digit groups and tell me what they are, except for one. I will then tell you what the last group is.

Results of the applications of number theory. If the number we think is x, then we have $x = 3a+r_1$, $x = 4b+r_2$, $x = 5c+r_3$. We express the individual remainders and calculate the expression $S = 40r_1 + 45r_2 + 36r_3 = 121x - 120a - 180b - 180c$. It thus suffices to divide the expression $S = 120k + x$ by $120S$ and the remainder is equal to the number thought.

Let us denote the age by x and the number thought by k. During the procedure, we obtain $10x - 9k = 10(x - k) + k$. Number k is on the position of the units, the remainder is the difference $x - k$. From the above stated, it is clear that your rival must be more than 9 years old.

Let us denote the unknown age again by x. The simplifications are then the following: $(2x + 5).5 = 10x + 25 = 10(x + 2) + 5$. We proceed further as in the previous case, except that in contrast with the previous case, this works also for minima.

We actually calculate $\{[(100m+d).2+8].5+4\}.10+4+r-444=10000m+100d+r$.

We calculate like this: $x = 1$; $2(x - 1)$; $2(x - 1) + x = 3x - 2$; $3x - 2 + 2$.

If we express a number in decimal positional system, we will easily see that the number is divisible by 11. The sum written in the reversed order is also divisible by this number. The difference is thus also divisible by eleven, and it is further divisible by nine. The difference is thus divisible by 99. A number is divisible by 99 if the sum of the two-digit groups is divisible by 99. If we add all the two-digit groups that we are told and complement the sum to the multiple of 99, we obtain the remaining group. The problem has more than one solution if the the sum of the groups is already divisible by 99. Then the unknown two-digit group may be 00 or 99.

Bibliography

[1] Dobrovolný B.: Nové matematické rekreace. SNTL Praha 1967

[2] Křížek M., Somer L., Šolcová A.: Kouzlo čísel (Od velkých objevů k aplikacím. Academia Praha 2011

[3] Lepka K.: Historie Fermatových kvocientů (Fermat-Lerch). Dějiny matematiky sv. 14, Prometheus Praha 2000

[4] Novoveský Š., Križalkovič K., Lečko I.: Zábavná matematika. Státní pedagogické nakladatelství Praha 1974

[5] Sierpiński W.: Co víme a nevíme o prvočíslech. Státní pedagogické nakladatelství Praha 1966

[6] Singh S.: Velká Fermatova věta. Academia Praha 2000

[7] Šalát T.: Dokonalé a spriatelené čísla. Škola mladých matematiků. Mladá fronta Praha 1969

[8] Vinogradov, I. M.: Základy theorie čísel. Nakladatelství Československé akademie věd. Praha 1953

[9] Znám, Š.: Teória čísel. Vydavatelstvo technickej a ekonomickej literatúry Alfa Bratislava 1977.

[10] `http://www.kodys.cz`