Independent University of Moscow
Translation Series

A. I. Sgibnev

Divisibility of Integers and Prime Numbers

MCCME, IUM
Moscow, 2022

Sgibnev A. I.

Divisibility of Integers and Prime Numbers. — Moscow: MCCME: IUM, 2022. — 128 p.

ISBN 978-5-4439-4632-0

Translated into English on the initiative and with financial support of Alexander Gerko

Translated from the Russian language edition
Сгибнев А. И. Делимость и простые числа. — М.: МЦНМО, 2019.

ISBN 978-5-4439-4632-0 © MCCME, IUM, 2022

Preface

In presenting the course "Divisibility and prime numbers", there are two main approaches. The first approach focuses on the logic of the presentation: all statements are proved, and those that are not proved are not used. See, for example, [1]. The second approach focuses on problems: the fundamental theorem of arithmetic is stated at the beginning and is given without proof, which makes it possible to avoid theoretical subtleties, and immediately proceed to solving meaningful problems. See, for example, [5].

The author tried to use the middle way. It seemed to him fundamentally important in a mathematical course to prove all the statements sooner or later. However, without support by problems, proofs of theorems often turn into formal texts. For example, what is the following statement worth to an unprepared student:

"For any coprime a and b, there exists an x and a y such that $ax + by = 1$"!

Therefore, the different stages of the proofs are spread through several lessons in which the appropriate ideas and constructions are motivated and used in problems. In addition, the author sometimes "borrowed" extra statements, sacrificing the consistency of presentation to make it more lively[1]. As a result (in the author's view), the stages of proofs have become more understandable, and interesting problems are solved along the way. True, the exposition in

[1]For example, in Lesson 2, the coprime divisor theorem is stated and used to solve problems involving divisibility tests; in Lesson 6, the prime factor cancellation theorem, needed to solve inhomogeneous Diophantine equations, is presented.

several stages of the proof of the fundamental theorem of arithmetic obscures its logical structure to some extent.

Here is a brief outline for teachers and trained students[1]:

1. The notion of prime number is introduced, and we prove that any number can be factored into primes; however, the question of uniqueness of this factorization is studied later (Lesson 4).

2. Euclid's algorithm is introduced (Lesson 5).

3. Euclid's algorithm is used to prove the fundamental lemma (Lesson 6).

4. The prime divisor theorem is deduced from the fundamental lemma (Lesson 7).

5. The prime divisor theorem is used to prove the uniqueness of factoring into primes (Lesson 8).

Also, in Lesson 6, the fundamental lemma is used to deduce the theorems on coprime divisors and factor cancellation (but they are optional in a minimal logical scheme).

Divisibility theorems are given names to make them easier for students to "recognize by sight". In order to grasp the underlying ideas, these theorems must be actively used to solve problems; after their solutions, the author tried to give comments, control questions, counterexamples, and additional problems for the same ideas.

When solving problems from the first lessons, students may be tempted to refer to the properties of prime numbers that have not been proved yet, such as the uniqueness of factoring into primes, etc. However, all these problems can be solved on the basis of the material proved within the framework of the lesson in which they are given. It is useful to urge students to do this and teach them to find "rigorous" solutions.

[1]Appendix 3 provides an alternative outline for the course.

The vast majority of problems was not invented by the author, but taken from the literature (often with some changes in the formulation). The book [1] influenced the logical structure of the course (proof of the fundamental theorem of arithmetic). The book [5] gave many ideas for problems and sequences of problems. A lot of striking formulations was taken from the book [4] (especially problems on Diophantine equations). Attention was paid to problems involving geometric interpretations.

The author is grateful to A. D. Blinkov, A. S. Vorontsov, E. A. Ermakova, A. V. Zabelin, I. B. Pisarenko, A. B. Skopenkov, and also to his students. The author expresses special gratitude to A. V. Shapovalov, whose help considerably exceeded the usual amount of an editor's work.

Please send feedback and comments to the e-mail address `sgibnev@mccme.ru`.

Lessons 1–4 are intended for students of intermediate forms, and Lessons 5–8 for students of upper forms.

The most important problems are marked with the "+" sign, and the most difficult problems are marked with the "*" sign. Unless stated otherwise, "numbers" are understood as "integers".

Table of contents

Lesson 1

Divisibility of Numbers

Definition. A number a is called *divisible* by a number b (or a is a *multiple* of b, or b is a *divisor* of a) if there is an integer q such that $a = b \cdot q$. Notation: $a \vdots b$.

Visual interpretation: if a coins can be laid out into b identical stacks, then a is a multiple of b. Another interpretation: if a coins can be laid out into several stacks of b coins each, then a is a multiple of b. It follows that only an even number can be divided into pairs.

Note that if $a \vdots b$, then $a \vdots (-b)$ (prove this!). Therefore, unless stated otherwise, we will only search for *positive divisors* of numbers.

Problem 1.1. Find all the divisors of the number 36.

Solution. We will successively check the numbers 1, 2, 3, 4, and so on: if their product by some number gives 36, we write this out:

$$36 = 1\cdot 36 = 2\cdot 18 = 3\cdot 12 = 4\cdot 9 = 6\cdot 6 = 9\cdot 4 = 12\cdot 3 = 18\cdot 2 = 36\cdot 1.$$

Note that, in the expression $a = bq$, both b and q are divisors of a. Therefore, the search can be stopped at the product of $6 \cdot 6$.

This method is useful when orally finding the integer roots of reduced quadratic equations $x^2 + mx + n = 0$ with integer coefficients m and n by using Vieta's inverse theorem: decompose n into two factors and check whether their sum is equal to $(-m)$.

Problem 1.2^{+}. In the table below, the topmost row indicates what is **given**. The left column, what is **asked**. Fill in the empty cells: if "yes", then write "+", if "no", write "−", and if there is not enough data, write "?". Justify your answers.

	$a \vdots m$ and $b \vdots m$	$a \vdots m$ and $b \not\vdots m$	$a \not\vdots m$ and $b \not\vdots m$
$a+b \vdots m$?			
$a-b \vdots m$?			
$a \cdot b \vdots m$?			

Solution. Consider the first row of the table. Since $a = km$ and $b = lm$, it follows that $a+b = (k+l)m$, that is, $a+b$ is divisible by m. In the cell below (the difference), everything is similar. The following reasoning is also possible: since $b \vdots m$, then $-b \vdots m$, and hence the sum $a + (-b)$ is divisible by m.

Now consider the third cell in the first row. $5 \not\vdots 3$ and $1 \not\vdots 3$, but $5 + 1 \vdots 3$. However, $5 \not\vdots 3$ and $2 \not\vdots 3$ and also $5 + 2 \not\vdots 3$. Therefore, the data is insufficient for an answer. Similar examples can also be given for the difference.

Consider the second cell in the first row. Suppose that $c = a + b \vdots m$. Then $b = c - a$ must also be divisible by m, since it is the difference of two numbers divisible by m. The resulting contradiction shows that $a + b$ is not divisible by m. The same applies to the difference.

Now consider the divisibility of the product (the third line). Since $a = km$, then $ab = (kb)m \vdots m$ regardless of the divisibility of b by m.

In the last cell of the third row, it is possible that ab is not divisible by m (for example, $a = b = 1$, $m = 2$), but it may also be divisible (for example, $a = b = 2$, $m = 4$). This means that there is not enough data.

A visual interpretation of most of the answers can be given: if each one of the two stacks of coins is laid out in stacks of m coins, then the combined stack can also be laid out, and so on.

It is beneficial to remember the results of the above problem:

	$a \vdots m$ and $b \vdots m$	$a \vdots m$ and $b \not\vdots m$	$a \not\vdots m$ and $b \not\vdots m$
$a+b \vdots m$?	$+$	$-$	?
$a-b \vdots m$?	$+$	$-$	?
$a \cdot b \vdots m$?	$+$	$+$	?

Draw the students' attention to the fact that the answers in the first and second rows are the same (in this sense, sum and difference are indistinguishable from the point of view of divisibility). In Lesson 7, we will understand what determines the divisibility of the numbers in the third column.

If, in the filled in table, instead of "a is divisible by m", we write "a is rational", and, instead of "a is not divisible by m", that "a is irrational", and the same with b, then we will get a correct table for the rationality of the sum and difference of numbers. The logic of the proof is the same as for divisibility: for the first column we use definitions, the second is "by contradiction", and the third is where we give two examples with different results.

Problem 1.3. Find out, without performing the divisions, whether a) $18^2 - 7^2$ is divisible by 11; b) $45^3 + 55^3$ by 2500; c) $1^3 + 2^3 + ... + 82^3$ by 83.

Solution. a) Is divisible:

$$18^2 - 7^2 = (18 - 7)(18 + 7) = 11 \cdot 25 \mathrel{\vdots} 11.$$

b) Is divisible:

$$45^3 + 55^3 = (45 + 55)(45^2 - 45 \cdot 55 + 55^2).$$

The first bracket is 100, the second is divisible by $5^2 = 25$.

c) Is divisible: divide the summands into pairs and prove that the sum in each pair is divisible by 83. For example, $1^3 + 82^3 \mathrel{\vdots} 83$, $2^3 + 81^3 \mathrel{\vdots} 83$.

Using the formula for the sum of the cubes of a positive integers, we can prove that this sum is divisible even by 83^2.

Problem 1.4. Peter believes that if a^2 is divisible by $a - b$, then b^2 is divisible by $a - b$. Is he right?

Solution. Consider the difference between Peter's two expressions:

$$a^2 - b^2 = (a - b)(a + b) \mathrel{\vdots} (a - b).$$

Since the minuend and the difference are divisible by $a - b$, then, according to Problem 1.2, the subtrahend must also be divisible by $a - b$. So Peter is right.

The following wording may be useful: if the sum (difference) of two numbers is divisible by m, then either both numbers are divisible by m or both are not divisible.

Problem 1.5. a) Find the number of divisors of the integers 4, 9, 16, 36, 81. Do the results lead you to make a general conjecture? b) Is the statement converse to the conjecture valid?

Solution. a) We will find the divisors in the same way as in Problem 1.1; the results can be presented in the following table:

Number	Divisors	Number of divisors
4	1, 2, 4	3
9	1, 3, 9	3
16	1, 2, 4, 8, 16	5
36	1, 2, 3, 4, 6, 9, 12, 18, 36	9
64	1, 2, 4, 8, 16, 32, 64	7

We put forward the following conjecture: “The square of a positive integer has an odd number of divisors”.

Let us group together the divisors of $n = m^2$: if d is a divisor of the number n, then n/d is also a divisor; let's pair them. Only m will be paired with itself, while all the other divisors of n will form pairs. Therefore, the square of an integer has an odd number of divisors.

b) If the number of divisors is odd, then there is a pair of identical divisors. Therefore, the number is a square, and the converse of our conjecture also holds.

Problem 1.6. Prove that: a) the product of two consecutive numbers is divisible by 2; b) the number $(n^2+n)/2$ is an integer.

Solution. a) Note that, among two consecutive numbers, at least one is divisible by 2. In Problem 1.2, the product is also divisible by 2.

b) Let us factor the numerator: $n^2 + n = n(n + 1)$.

We obtain the product of two consecutive numbers, which is even by item a).

A similar result for three numbers is proved in Problem 2.12.

Problems for individual solution

Problem 1.7. For what numbers a and b is a divisible by b and b is divisible by a? (The numbers can also be negative!)

Problem 1.8[†]**.** a) Is it true that if $a \mathbin{\vdots} m$ and $b \mathbin{\vdots} n$, then $ab \mathbin{\vdots} mn$? b) Is it true that if $a \mathbin{\vdots} b$ and $b \mathbin{\vdots} c$, then $a \mathbin{\vdots} c$?

Problem 1.9. Paul believes that if $ab + cd$ is divisible by $a - c$, then $ad + bc$ is also divisible by $a - c$. Is he right?

Problem 1.10. In the Triple Kingdom, only coins of 9 and 15 ducats are in circulation. Is it possible to assemble such coins to obtain a) 48 ducats, b) 50 ducats?

Problem 1.11. a) Mary demonstartes the following trick: given any three-digit number, she writes the given number twice, obtaining a six-digit number, and then, in a second, mentally divides this six-digit number by 1001. How does she do it?

b) Alex noticed that all of Mary's six-digit numbers are divisible by 7. How? By what other numbers are they divisible?

Problem 1.12. In an ancient kingdom, there was a prison with one inmate in each of its hundred cells. The prison cells are numbered from 1 to 100 and the locks in them were arranged so that the door opens when the key was turned once, but, at the next turn of the key, the door closes, and so on. At that time, the king was at war with the neighboring kinddom and, at some point, it seemed to him that he was winning.

Filled with joy, the king sent a messenger with instructions to unlock all the cell doors, but then the luck turned, and the king sent another messenger after the first, instructing him to turn the key in the lock in every second cell; then the next messenger was sent to turn the key in the lock of every third cell, and so on. In this way, 100 messengers arrived at the prison one after another and turned the locks in the cells in succession. How many prisoners were, as a result, set free and from what cells?

Answers and solutions

Problem 1.7. Since a is divisible by b, we see that $|a| \geqslant |b|$. The fact that b is divisible by a implies that $|b| \geqslant |a|$. The two inequalities together give $|a| = |b|$, that is, the numbers can only differ in sign.

Problem 1.8. a) True: since $a = lm$ and $b = kn$, it follows that $ab = (kl)(mn)$, and hence, by definition, ab is divisible by mn.

b) True: since $a = kb$, $b = lc$, it follows that $a = (kl)c$, and hence, by definition, a is divisible by c.

These exercises are fairly simple, but it is important for the students get used to giving correct proofs by referring to definitions. For example, in the previous exercise, it is more useful to say "the product is a multiple of mn" than "the quotient will be an integer".

Problem 1.9. Arguing just as Problem 1.4, we find the difference between the two expressions:

$$(ab + cd) - (ad + bc) = a(b - d) - c(b - d) = (a - c)(b - d).$$

The first expression is divisible by $a - c$, hence so is the second expression.

Problem 1.10. a) It is possible: $48 = 9+9+15+15$. b) Note that 9 and 15 are divisible by 3, so any sum composed of such coins is also divisible by 3. However, 50 is not divisible by 3.

It will be shown in Lesson 6 that if you and I have an unlimited amount of 9- and 15-unit coins, then I can pay you any sum divisible by 3, provided you are allowed to give me change.

Problem 1.11. a) Note that $\overline{abcabc} = 1001\overline{abc}$. So the quotient is simply equal to the original number.

b) $1001 = 7 \cdot 11 \cdot 13$, so numbers of the form $\overline{abcabc}$ are divisible by 7, by 11, by 13, and by their pairwise products.

Problem 1.12. Note that the prisoners were released from those cells in which the key was turned an odd number of times, that is, from the cells whose numbers have an odd number of divisors. Referring to Problem 1.5, we see that the numbers of such cells are exact squares, i.e., 1, 4, 9, 16, ..., 100. There are ten of them in all.

The topic of this lesson also covers Problems 1–8 from the section "Additional problems".

Lesson 2

Divisibility Tests

Sometimes we need to quickly determine whether one number is divisible by another without performing the division itself. In such cases, it is useful to use divisibility tests.

It is suitable to start the lesson with the following trick. The teacher asks each student to pick a three-digit number, then subtract its first digit from it, then subtract the second and, finally, the third digit. If the student obtains a two-digit number, then he or she must add zero to its beginning. All the students do the calculations at the same time, and then the teacher asks each of the students in turn to name any two of their three digits and guesses the third. The key to the trick will appear during the lesson.

Problem 2.1. a) Prove that a number is divisible by 2 if and only if its last digit is divisible by 2. b) Derive a divisibility test by 4 associated with the last two digits.

Solution. a) Let's imagine that a saleswoman has N eggs, which she puts in boxes of ten, one hundred, one thousand, and so on. The number of eggs equal to the last digit d of N remains outside the boxes. In each box, the number of eggs is divisible by 2, so if d is even, then N is even, and if d is odd, then N is odd. In short, d and N are divisible or not divisible by 2 at the same time.

b) Put N eggs into boxes of one hundred, one thousand, etc. The number t of eggs equal to the two-digit number composed of the last two digits of N remains outside the boxes. In each box, the number of eggs is divisible by 4, so t and N are divisible or not divisible by 4 simultaneously.

Here is an algebraic solution of item b) for students familiar with algebraic techniques. Consider the number $\overline{abcd} = 1000a + 100b + 10c + d$. Note that all the summands, except the last two, are obviously divisible by 4. Therefore, the sum is divisible by 4 if and only if the number $\overline{cd}$ is divisible by 4.

Divisibility tests by 8, 16, and so on, can be derived in a similar way.

Problem 2.2. Peter noticed that if one subtracts the sum of its digits from a number, then one gets a number which is a multiple of 9. a) Prove this fact. b) On its basis, formulate divisibility tests by 9 and by 3.

Solution. a) Let's carry out the proof using a three-digit number N as an example. We will put N eggs in boxes of one hundred, ten, and one. After that, we will take one egg from each box and put them together in a basket: one from each box of one hundred, one from each box of ten, and one from each one-egg box. Note that the number of eggs in the basket is exactly equal to the sum of the digits of the number N. In each of the largest boxes 99 eggs will remain, in the medium boxes, 9 eggs, and, in the smallest boxes, nothing. This means that the total number of eggs in the large and medium cells is a multiple of 9.

b) Thus, *a number N is divisible by 9 if and only if the sum of its digits is divisible by 9.* For divisibility by 3, the test can be stated similarily (since the difference is also a multiple of 3).

For students familiar with algebraic techniques, we can give the following proof. Consider the number $\overline{abc} = 100a + 10b + c$. Subtract the sum of its digits from it: $\overline{abc} - (a + b + c) = 99a + 9b$. The difference is a multiple of 9, so the minuend is a multiple of 9 if and only if the subtrahend is a multiple of 9.

The logic of divisibility by n tests is seen from the examples given above: we replace the given number N by a"part" of it (for example, by the number d composed of the last digits or the sum of the digits), and the part d will be divisible (or not divisible) by n simultaneously with the original number N.

Now we can explain our trick: the students subtracted the sum of its digits from the given number and hence the result was a multiple of 9. From any two digits of the result, the teacher chose a third one so that the sum is divisible by 9. This can be done in a unique way, except in the case where the sum of the two reported digits is itself a multiple of 9. In this case, the teacher says: "0 or 9".

Problem 2.3. Johnny found the number

$$100! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 99 \cdot 100.$$

He added all its digits, obtaining a new number, in which he again added all the digits, and so on until he got a one-digit number. What was it?

Solution. Note that $100! \vdots 9$, so the sum of the digits of this number is also divisible by 9. Since the new number is divisible by 9, then its sum of digits is divisible by 9, and so on. Therefore, the desired single digit number must also be divisible by 9, that is, it is equal to 9 (it cannot be 0, because the sum of the digits must be positive).

Note the fact that the statement of this problem does not indicate that it can be solved by a divisibility test; hence the students themselves must figure out that a divisibility test should be applied here.

Problem 2.4. a) The digits of a positive integer are numbered from right to left (the first being the 1's digit, the second the 10's digit, and so on). After that, the sum of digits located at even places is added to the given number and, after that, the sum of the digits at the odd places is subtracted. Prove that the resulting number is divisible by 11.

b) State a divisibility by 11 test.

Solution. a) Let's prove it using a four-digit number N as an example. Let the saleswoman put N eggs in boxes of one thousand, one hundred, ten, and one. After that, she takes out one egg from each one-egg box and from each 100-egg box and puts in one egg into each 10-egg box and into each 1000-egg box. (Note that this is equivalent to adding the sum of the digits at the even places to N and subtracting the sum of the digits at the odd places.) Now there are 1001, 99, and 11 eggs in the boxes. All these numbers are divisible by 11. So, the resulting number is divisible by 11.

b) Let us assign to the given number the alternating sum of its digits: we put a plus or a minus in front of the digits so that they alternate and there is a plus in front of the rightmost digit. For example, the alternating sum of the digits of the number 2011 is $-2+0-1+1=-2$. Then it turns out that, in item a), we actually subtracted the alternating sum of its digits from the number. Since the difference found in this case is always a multiple of 11, we obtain

Divisibility by 11 test.
A number is a multiple of 11 *if and only if its alternating sum of digits is a multiple of* 11.

Let's prove that this test also applies to numbers of arbitrary length. To do this, note that $10^{2n}-1$ for any n is divisible by 11 as a positive integer made up of an even number of identical digits. Now let us prove that $10^{2n+1}+1$ for any n is divisible by 11. Add these two numbers:

$$(10^{2n}-1)+(10^{2n+1}+1)=11\cdot 10^{2n}.$$

Since the sum and one of its summands are divisible by 11, then the other summand is also divisible by 11.

Problem 2.5. Is it true that if a number n is divisible by two other numbers, then it is also divisible by their product? Check this by dividing the number n by the following numbers: a) 6 and 4, b) 3 and 2, c) 9 and 4.

Solution. a) Incorrect: $12 \vdots 6$, $12 \vdots 4$, but $12 \not\vdots\ (6\cdot 4)$.

b) True. By assumption $n=2k=3l$. Note that we have $3n=3\cdot 2k=6k \vdots 6$, $2n=2\cdot 3l=6l \vdots 6 \Rightarrow n=3n-2n \vdots 6$.

c) True. By assumption, $n=4k=9l$. Note that we have $9n=9\cdot 4k \vdots 36$, $4n=4\cdot 9l \vdots 36 \Rightarrow n=9n-2\cdot 4n \vdots 36$.

It is useful to give students time to try to prove assertion b) on their own. Then analyze the errors in their proofs (as a rule, this will be the use of statements that have not yet been proved) and show the proof given above. Then ask to independently prove assertion c) by analogy.

The following theorem shows when the assertion of 2.5 is valid.

Definition. Two numbers are said to be *relatively prime*, or *coprime*, if their only common divisor is 1.

Theorem on coprime divisors. *If the number n is divisible by each of two coprime numbers a and b, then it is divisible by their product ab.*

We will give the proof in Lesson 6. On the basis of this theorem, it is possible to state new divisibility tests by combining the already familiar ones. For example, $18=9\cdot 2$, 9 and 2 are coprime numbers, so a number is divisible by 18 if it is divisible by 9 and by 2.

Problem 2.6. In the number 65432789, cross out the least number of digits so that the remaining number is divisible by 36.

Answer: 5328, four crossed-out digits.

Solution. We must obtain a number which is a multiple of 4 and 9. We must cross out the digit 9; otherwise, the result will be an odd number and, therefore, not a multiple of 4. We must also cross out 7; otherwise, the result will end in 7 or 78 and hence is not a multiple of 4. Thus, we obtain the number 654328. The sum of its digits is 28, which is not a multiple of 9, and this means that the obtained number (654328) is not a multiple of 9, and at least one more digit must be crossed out. After any crossing out, the sum of the digits will be less than 27, but it must be a multiple of 9, that is, it must be equal to 18 or 9.

In all cases, we must reduce the sum 28 by at least 10, that is, delete at least two digits in 654328. So, it is impossible to cross out less than 4 digits. And exactly 4 is possible: consider the number 5328. It is a multiple of 4 and 9, and since 4 and 9 are coprime, this number is a multiple of 36, and so 5328 is the answer to our problem.

Problems for individual solution

Problem 2.7. a) Prove the divisibility by 5 test.

b) Derive a divisibility by 25 test.

Problem 2.8. A machine prints the digit “4” one by one on a strip of paper. Is it be possible to stop it so that a multiple of 8 is printed?

Problem 2.9. Several digits in a number were interchanged, which resulted a number three times greater than the original one. Prove that the resulting number is divisible by 27.

Problem 2.10. Find the smallest natural number that contains only the digits 1 and 0 and is divisible by 225.

Problem 2.11. Professor Snape wrote a prescription containing the numbers

EVILLIVE and LEVICORPUS

(the same letters are replaced by the same digits and different letters by different digits). Professor McGonagall claims that both of these numbers are composite. Is the professor right?

Problem 2.12. a) Prove that the product of three consecutive numbers is divisible by 6. b) Prove that the number $(n^3 - n)/6$ is an integer.

Answers and solutions

Problem 2.7. a) Let's put N eggs into boxes of 10, 100, 1000, and so on. There will remain d eggs, d being equal to the last digit of the number N. Since the number of eggs in all boxes is divisible by 5, the number d is divisible or not divisible by 5 at the same time as N.

b) Let's put N eggs into boxes of 100, 1000 and so on. Arguing in the same way as in item a), we see that the number N is divisible or not divisible by 25 simultaneously with the number composed of its last two digits.

Problem 2.8. Answer: It's impossible.

The number 4 will be printed first, then 44, then 444. These numbers are not divisible by 8. The further addition of digits can be represented as adding a multiple of 1000 to 444. Thus, we keep obtaining a number which is the sum of a number which is a multiple of 8 and a number which is not a multiple of eight (444). Such a sum cannot be a multiple of 8.

Problem 2.9. Let $3A$ be obtained by interchanging digits in the number A. But the sum of the digits of $3A$ is a multiple of 3, which applies to A as well, because the sums of the digits of these two numbers are the same. Hence A is a multiple of 3. Therefore, $3A$ is a multiple of 9. Thus, the sum of the digits of both A and $3A$ is a multiple of 9. It follows that A is a multiple of 9, and hence $3A$ is a multiple of 27.

Here it is useful to ask the students why is it impossible to prove divisibility by 81 and so on in the same way?

Numbers specified in the condition exist, for example, $A = 1035$; $3A = 3105$.

Problem 2.10. Let us decompose 225 into coprime factors: $225 = 25 \cdot 9$. Therefore, the required number must be divisible by 25 and by 9. In order for a number to be divisible by 25, the last two digits must be 00, 25, 50, or 75. In our case, only 00 is possible.

Further, for a number to be divisible by 9, it is necessary that the sum of its digits be divisible by 9. This means that the sum of the digits is at least 9, and there are at least nine 1's in the number.

The smallest number with nine 1's and 00 at the end, is 11111111100. This suits us.

Problem 2.11. Answer: The professor is right.

The first number is divisible by 11, since the alternating sum of its digits is zero because of the symmetry.

The second number contains 10 different digits, each of them appearing once, so its sum of digits is

$$0 + 1 + 2 + 3 + 4 + 5 + 6 + 7 + 8 + 9 = 45.$$

But this sum is divisible by 3, hence the number itself is divisible by 3.

Problem 2.12. a) Among any three consecutive numbers, at least one is divisible by 2 and one by 3. Hence the product of these three numbers is divisible by 2 and by 3. But 2 and 3 are coprime, so, by the coprime divisor theorem, this product is divisible by $2 \cdot 3 = 6$.

b) Note that $n^3 - n = (n - 1)n(n + 1)$ is the product of three consecutive numbers, that is, it is a multiple of 6.

The subject of this lesson also includes problems 9–23 from the section “Additional problems”.

Lesson 3

Division with Remainder

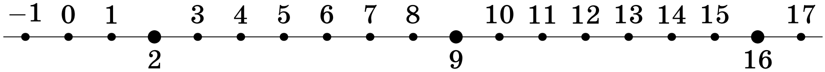
Imagine an automatic machine that changes the given sum of money into 5-ruble coins and gives the remainder of less than 5 rubles in one-ruble coins. For example, $33 = 5 \cdot 6 + 3$; the machine gives six 5-ruble coins and the remainder in three 1-ruble coins. From the mathematical point of view, the machine performs a division by 5 with a remainder.

Let's recall the definition of division of positive integers with remainder.

> **Definition.** If a number a can be written as $a = b \cdot q + r$, where $0 \leqslant r < b$, then it is said that a gives, when divided by b, the (incomplete) *quotient* q and the *remainder* r.

It is useful to discuss with students that, according to this definition, it is impossible to divide the number $b = 0$ with remainder. In addition, it is important to understand that a division producing a whole number as a quotient is a special case of division with remainder (the remainder is 0).

Let's extend this definition by allowing the dividend to be negative. Note that numbers with the same remainder are located on the numerical line at equal intervals. For example, on a straight line, let us mark off natural numbers that, when divided by 7, give the remainder 2.



The adjacent marked numbers are at a distance of 7 from each other: 2, 9, 16, and so on. Let's extend this picture to the left without breaking the pattern: mark -5, -12, -19, and so on. It will be convenient to define division with remainders of negative numbers in such a way that -5, -12, -19, and so on, also have a remainder of 2 when divided by 7, that is, so that the expressions $-5 = 7 \cdot (-1) + 2$, $-12 = 7 \cdot (-2) + 2$, $-19 = 7 \cdot (-3) + 2$, and so on, can be regarded as division with remainder. To this end, it suffices to take the same definition for any integer a, allowing the incomplete quotient q to be negative! But the remainder r must still be non-negative.

It is important to emphasize that the definitions in the case of positive integers and in the case of arbitrary integers are the same. It follows from our picture that the difference of two numbers with equal remainders when divided by b is a multiple of b.

Problem 3.1$^+$. Mary was absent from the lesson due to illness and worked out examples of division with remainder as follows: a) $20 = 3\cdot4+8$; b) $19 = 3\cdot5+4$; c) $-11 = 2\cdot(-5)-1$. Explain her mistakes.

Solution. a) This is incorrect, because $4 < 8$, that is, the divisor is less than the remainder.

b) In this form, this is incorrect, because $3 < 4$. But if we interchange the factors: $19 = 5 \cdot 3 + 4$, then the assertion is correct.

c) This is incorrect, because the remainder cannot be negative.

We can divide with remainder in different ways. The first way is to use ordinary long division (with a corner). Positive numbers are divided directly. Instead of negative numbers, we can divide the corresponding positive numbers and then perform the operation described in the solution of Problem 3.12.

Another way is the graphic one. On the coordinate axis, let's mark off the numbers 0, $\pm b$, $\pm 2b$, and so on. Now let's put the number a on this marked axis. It will fall either on one of the marked numbers (and then it is divisible by b) or inside the segment between two adjacent marked numbers. Then the multiplier of b in the left number is the quotient and the distance from the left number to a is the remainder (why will it be less than b?).

But how do we know whether different division methods always give the same result? The answer is given by the following theorem.

> **Uniqueness theorem for division with remainder.** *Division with remainder is carried out in a unique way. In other words, if a number a is written in two ways in the required form*:
>
> $$a = bq_1 + r_1, \quad 0 \leqslant r_1 < b,$$
> $$a = bq_2 + r_2, \quad 0 \leqslant r_2 < b,$$
>
> *then both expressions must coincide* (*that is* $q_1 = q_2$ and $r_1 = r_2$).

Proof. Subtract the second equality from the first, obtaining $b(q_1 - q_2) + r_1 - r_2 = 0$, that is, $b(q_1 - q_2) = r_2 - r_1$. Note that, by the definition of remainder, $-b < r_2 - r_1 < b$, or $-b < b(q_1 - q_2) < b$; hence $-1 < q_1 - q_2 < 1$. But this means that $q_1 = q_2$. Substituting the last relation into the first equality of this paragraph, we see that $r_1 = r_2$ as well.

Problem 3.2. What remainder will the number 123321 give when divided by 999?

Solution.

$$\begin{aligned} 123321 &= 1000 \cdot 123 + 321 = 999 \cdot 123 + (123 + 321) \\ &= 999 \cdot 123 + 444 \end{aligned}$$

The remainder is 444.

Problem 3.3. The divisor and the dividend are increased threefold. How will the quotient and remainder change?

Solution. First, we will give a visual solution, and then a rigorous one, using the definition.

Let's imagine that we put nuts in equal piles and put the remainder in a smaller pile. And now we have three times as many nuts, but we have been ordered to make the piles three times bigger. Obviously, the number of piles will not change, but, in the smaller pile, there will be three times as many nuts.

Let $a = bq + r$, where $r < b$. Multiply both parts of the equality by 3, obtaining $3a = (3b) \cdot q + 3r$, where $3r < 3b$. Consequently, the quotient has not changed, and the remainder has increased threefold.

This problem shows that, in some cases, it is more convenient to write division with remainder as a product (as in the definition) rather than as a quotient.

Problem 3.4. A number a is a multiple of 3. Can the remainder in the division of the number a by 12 be equal to 2?

Solution. Let's assume that it can. Then the number a can be written as $3x$ and as $12y+2$. Equating these quantities and moving the unknowns to the left, we get $3x - 12y = 2$. Note that the left side of the equality is divisible by 3, but the right is not. Thus, equality is impossible. Therefore, the remainder from the division of the number a by 12 is not equal to 2.

The following incorrect solution to this problem is often given: "Suppose it can. Then a is not divisible by 12. So it cannot be divisible by 3. A contradiction." Find the error in this argument.

Problem 3.5. a) Find the least integer (greater than one) that gives the remainder 1 under division by 2, by 3, by 5, and by 7.

b) Find *all* such integers.

Solution. a) Note that if the desired number is reduced by 1, then we get a number that is divisible by 2, 3, 5, and 7. Since 2 and 3 are coprime, such a number is divisible by their product 6, since 6 and 5 are coprime, the desired number is divisible by $6 \cdot 5 = 30$, and since the numbers 30 and 7 are coprime, the desired number is divisible by $30 \cdot 7 = 210$. Therefore, the smallest such number will be 210, and the desired number 211.

b) In view of the above, the answer consists of all the numbers of the form $210k + 1$, where k is an arbitrary integer.

Problem 3.6^{+}. Back to Problem 1.2. Fill in the table using the remainders: “0” if the number is divisible by m without remainder, and “not 0” if it is divisible with remainder.

Solution. The problem reduces to the following equalities: $0+0=0$, $0+$“not 0” $=$ “not 0”, “not 0”$+$“not 0” $=?$, $0\cdot x=0$, “not 0” $\cdot$ “not 0” $=?$.

Almost all the equalities are obvious, which shows the strength of the remainder method. The last equality is unusual for students; it will become more understandable after Lesson 7.

Problem 3.7. Each of the numbers from 1 to 1000000 is replaced by the sum of its digits. Each of the resulting numbers is again replaced by the sum of its digits. We proceed in his way until one million single digits remain. Which numbers prevail: 1’s or 2’s?

Solution. Note that by replacing a number by the sum of its digits, we reduce it by a multiple of nine (see Problem 2.2). This means that under this operation, the remainder does not change! Thus, it suffices to compare the quantity of numbers from 1 to 1000000 that give the remainders 1 and 2 in the division by 9. The remainders 1 and 2 are repeated in pairs, starting from the first number. Since the last number gives the remainder 1, it follows that there are more 1’s.

Thus, in the course of solving the problem, we have generalized the divisibility test: the remainder in the division of a number by 9 is equal to the remainder in the division of the sum of its digits by 9. By analogy with divisibility tests, the last assertion can be called an “equal remainder” test. If the remainder is 0, then we obtain a divisibility test.

Problems for individual solution

Problem 3.8. Divide with remainder

a) 239 by 6;
b) -239 by 6;
c) -99 by 10;
d) -101 by 100.

It is necessary to solve a number of simple examples so that the students can firmly grasp the definition. To make it interesting, the teacher can ask the students to solve the problems orally, competing for the quickest solution.

Problem 3.9. When the Miserly Knight puts his coins in stacks of nine, he has eight coins left. How many coins will there be left when he puts the coins in stacks of 18?

Problem 3.10. The number a gives the remainder 6 when divided by 12. Can it give the remainder 12 when divided by 20?

Problem 3.11. Find the smallest positive integer that gives the remainder 1 when divided by 2, the remainder 2 when divided by 3, the remainder 3 when divided by 4, the remainder 4 when divided by 5, and the remainder 5 when divided by 6.

Problem 3.12. A number a, when divided by b, gives the quotient q and the remainder r. What quotient and remainder will the number $-a$ give when divided by b?

Problem 3.13. The number 2 is written on the blackboard. Every second the sum of its digits is added to the number on the board. Can the number 123456 appear on the board after a while?

Answers and solutions

Problem 3.8. a) $239 = 6 \cdot 39 + 5$;

b) $-239 = 6 \cdot (-40) + 1$;

c) $-99 = 10 \cdot (-10) + 1$;

d) $-101 = 100 \cdot (-2) + 99$.

Problem 3.9. Answer: 8 or 17.

We will combine stacks of 9 coins into pairs. If there were an even number of stacks, then there would be 8 coins left. If the number of stacks were odd, then there would be 8 coins and another stack of 9 coins, making a total of 17 coins.

Problem 3.10. If the second assertion were true, then a would be a multiple of 4. However, it follows from the first assertion that the remainder in the division of a by 4 is 2.

The resulting contradiction shows that a cannot have the remainder 12 when divided by 20.

The same solution can be written in algebraic terms; see the solution of Problem 3.4.

Problem 3.11. Answer: 59.

The statement of the problem is equivalent to the assertion that the number increased by 1 must be divisible by 2, 3, 4, 5, and 6. Since 5 and 6 are coprime, it follows that this number is divisible by 30. But 30 is not suitable, since it is not divisible by 4. However, $2 \cdot 30 = 60$ is already suitable. So the desired number is $60 - 1 = 59$.

Problem 3.12. Answer: if $r = 0$, the quotient is $-q$, and the remainder is 0. Otherwise, the quotient is $(-q - 1)$, and the remainder is $b - r$.

If $r = 0$, then both a and $-a$ are divisible by b, which means that the remainder is 0. If $r \neq 0$, we multiply both sides of the equality $a = bq + r$ by -1, obtaining

$$-a = b(-q) + (-r) = b(-q - 1) + (b - r).$$

Since $0 < r < b$, we have $0 < b - r < b$. In this case, the remainder is $b - r$.

Problem 3.13. Since the number and the sum of its digits differ by a multiple of 9, they yield the same remainders when divided by 3. It is not difficult to check that the sum of a number which is not a multiple of 3 and the sum of its digits cannot be a multiple of 3. Indeed, when adding two numbers with remainder 1, we get a number with remainder 2 and when adding two numbers with remainder 2, we get a number with remainder 1. Since the number 123456 is a multiple of 3, it cannot be obtained.

The subject of this lesson also includes problems 24–39 from the section “Additional problems”.

Lesson 4

Prime Numbers

Problem 4.1. a) A rectangle on square-lined paper consists of 31 squares of side 1. What is its perimeter equal to?

b) A rectangle on square-lined paper consists of n squares of side 1. What property must n have so that the rectangle's perimeter can be uniquely determined?

Solution. a) $31 = 1 \cdot 31$, and there are no other divisors, so the length is 31 and the width is 1. Hence the perimeter is $(31 + 1) \cdot 2 = 64$.

b) If n is decomposable into the product of exactly two factors, then the perimeter is uniquely determined. Since the number n is always divisible by 1 and by n, these factors can only be 1 and n.

Suppose there is another decomposition: $n = km$, where $2 \leqslant k \leqslant m$. Then, in addition to the $1 \times n$ rectangle with perimeter $2(n+1)$, there is also a $k \times m$ rectangle with perimeter $2(k + m)$. However, $k \leqslant m = n/k \leqslant n/2$, that is, the second perimeter does not exceed $2n$ and is not equal to the first.

> **Definition.** A number $p > 1$ is said to be *prime* if it has no other divisors besides 1 and p. A number is called *composite* if it has a divisor greater than 1, but less than the number itself.

It follows from the definition that a prime has exactly two divisors, while a composite number has more than two.

Problem 4.2. Find the largest a) two-digit; b) three-digit prime.

Answer: a) 97; b) 997.

Solution. a) We will argue "from top to bottom". The number 99 is divisible by 3, 98 is divisible by 2. Let's check the number 97. It is not divisible by 2, 3, 4, 5, 6, 7, 8, or 9. This means that if 97 has any divisors (other than 1), then they are all greater than or equal to 10. However, $10 \cdot 10 > 97$. So there is no need to check any further.

b) The nearest candidate is 997. Divisibility must be checked up to 31, since $31^2 < 997$, and $32^2 > 997$. Note that each number $n > 1$ has a prime divisor. Such is, for example, the smallest of the divisors greater than 1. Indeed, if it were not a prime, then any of its divisors would even be smaller and would divide n. Therefore, if the number 997 has a divisor not exceeding 31, then, by taking a prime divisor of that divisor, we will find a prime divisor of 997 not exceeding 31. Thus, we can reduce the amount of search by checking only that 997 is not divisible by primes 2, 3, 5, ..., 29, 31.

Problem 4.3. a) Give an example of three numbers that are not divisible by each other and such that the product of any two of them is divisible by the third.

b) The same question for numbers greater than one hundred.

Solution. a) 6, 10, and 15.

b) Let p, q, r be three distinct primes greater than 10. Consider their pairwise products pq, pr, qr. They are not divisible by each other (if, for example, pq were divisible by pr, then $pq = kpr \Leftrightarrow q = kr$, that is, the prime q would be divisible by another prime, namely r). However, the product of any two of these numbers is divisible by the third, for example $(pr) \cdot (qr)/(pq) = r^2$.

Before the next problem, the teacher can play the following game with the students: each student picks a prime greater than 3. The teacher asks each student to divide this number by 6 and tell him the remainder. As the result, columns of 1's and 5's appear on the blackboard. (If one of the students makes a mistake in calculations, then we can immediately do the calculations on the blackboard over again.)

Problem 4.4†**.** Prove that a prime greater than 3 can be expressed either in the form $6n + 1$ or in the form $6n + 5$, where n is a natural number or 0.

Solution. What remainders can a prime greater than 3 have when divided by 6? There are six possible options, let's consider them.

A remainder of 0 is impossible, since the number will then be divisible by 6.

A remainder of 1 is possible.

A remainder of 2 is impossible, since the number will then be divisible by 2, and there is only one such prime, namely, 2.

A remainder of 3 is impossible, since the number will then be divisible by 3, and there is only one such prime, namely, 3.

A remainder of 4 is impossible, since the number will then be greater than 2 and be divisible by 2.

The remaining number 5 is possible.

Problem 4.5. Can the positive integers $n - 2012$, n, and $n + 2012$ be primes at the same time?

Answer: They cannot.

Solution. Consider the remainder in the division of these three numbers by 3. Since 2012, when divided by 3, gives a remainder of 2, then the numbers $n - 2012$, n, and $n + 2012$ give three different remainders when divided by 3. This means that one of these numbers is obviously divisible by 3. If it is not 3, then it is a composite number and the problem is solved. Let it be 3. Then $n = 2015$ is a composite number.

Problem 4.6†**.** Two boys play the following game: Peter dictates to John a number (this is where his role ends), and John writes that number on the blackboard. Next, John represents the number as the product of two factors other than 1, and replaces it by the product of these two factors. Then John does the same with one of the factors, and so on.

Can Peter choose the original number so that John a) cannot even make the first move; b) John will perform the moves endlessly?

Solution. a) He can, if he chooses a prime.

b) He can't. Note that if, at some point, John writes out a prime, then it remains on the blackboard. If John writes out a composite number, then he will decompose it sooner or later into the product of two factors other than 1 and replace it by that product. Thus, at each step, the new numbers written out decrease. Since the factors cannot become less than 1, the process will eventually stop and, on the blackboard, a product of primes will appear. This product is called the *decomposition of a number into prime factors*.

Thus, it was proved in the previous problem that any number can be decomposed into prime factors in finitely many operations. The question of the uniqueness of such a decomposition (can John obtain two different decompositions of the same number) will be discussed in Lesson 8.

Problem 4.7^{+}. Consider the set of all primes. Denote them by $p_1, p_2, \dots, p_n$. Let's construct the number $p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$. Obviously, this number is not divisible by any prime. So it's also a prime. However, it is not included in our set of all primes, because it is greater than each of them. We arrived at a contradiction. Where is the mistake?

Solution. The whole argument appears flawless, except for one point, namely the assumption that the set of primes is finite. Since we have come to a contradiction, it follows that *there are infinitely many primes* (and our argument is actually a proof of this fact by contradiction).

The statement about the infinity of the set of primes is one of the most ancient theorems of arithmetic. The above proof is the one given by Euclid. Note that, in the proof, we can also take the number $p_1p_2\dots p_n - 1$ or even $p_1p_2\dots p_k \pm p_{k+1}\dots p_n$ (why?). See also the additional problem D47.

Problems for individual solution

Problem 4.8. a) Let m and n be positive integers, and let $m^2 - n^2$ be a prime. Find $m - n$.

b) A smaller square in a large square on square-lined paper was painted green, and 79 unpainted cells remained. Can all the corners of the large square remain unpainted?

Problem 4.9. Is there a hundred consecutive composite numbers?

Problem 4.10. Let us call a number *simplified* if it is the product of exactly two primes (not necessarily different). What is the largest number of consecutive simplified numbers?

Problem 4.11. Can the remainder in the division of a prime by 30 be composite?

Problem 4.12. a) Find five primes such that the distance between any two adjacent primes is 6.

b) Are there six such primes?

Answers and solutions

Problem 4.8. a) $m^2 - n^2 = (m + n)(m - n)$. The prime p can only be expressed as $p \cdot 1$. Since $m - n < m + n$, we have $m - n = 1$.

b) Let the side of the larger square be contained in m cells (i.e., little squares of side 1), and that of the smaller one, in n cells. Then $m^2 - n^2 = 79$ is a prime. Therefore, by item a), $m - n = 1$. This means that the sides of the two squares differ by 1, and so the smaller square necessarily contains one of the corners of the larger one.

Problem 4.9. Let's try to construct a number N such that the numbers $N + 2$, $N + 3$, ..., $N + 101$ are composite (one hundred numbers, in all). The easiest way is to require that $N + 2$ be divisible by 2, $N + 3$ be divisible by 3, and so on, $N + 101$ be divisible by 101. This will happen if N is divisible by $2, 3, \ldots, 101$. And it's easy to construct such a number: simply take $N = 101!$. Thus, the numbers $101! + 2$, $101! + 3$, ..., $101! + 101$ are the required composite numbers.

Note that, in this way, we can obtain an arbitrary amount of consecutive composite numbers!

Problem 4.10. Since there is only one even prime, namely, 2, it follows that simplified numbers cannot be divisible by 4. The exception is the number $4 = 2{\cdot}2$, but the numbers 3 and 5 adjacent to 4 are not simplified. This means that there are no more than three consecutive simplified numbers. Examples of triples of simplified numbers exist:

$$33 = 3 \cdot 11, \quad 34 = 2 \cdot 17, \quad 35 = 5 \cdot 7.$$

Problem 4.11. Experiments yield only prime remainders or 1. Let's try to prove that it will always be so. Let $p = 30k + r$, where p is a prime and $0 \leqslant r < 30$. Assume that r is composite. Then r is divisible by 2, 3, or 5 (why?). Since 30 is divisible by each of these numbers, it follows that p must also be divisible by one of them. However, if $p = 2$, 3, or 5, then r is a prime. While if $p > 5$, then p itself is composite. In both cases, we come to a contradiction.

In this problem, the number 30 can be replaced by any of the numbers 3, 4, 6 (see problem 4.4), 8, 12, 18, 24.

Problem 4.12. a) 5, 11, 17, 23, 29.

b) Note that if the numbers differ by 6, then their remainders from the division by 5 differ by 1. In addition, among all primes, only the number 5 has the remainder 0 in the division by 5. Therefore, the five primes must begin with 5 (that is, the example from item a) is unique), and six consecutive primes do not exist.

The subject of this lesson also includes problems 40–52 from the section "Additional problems".

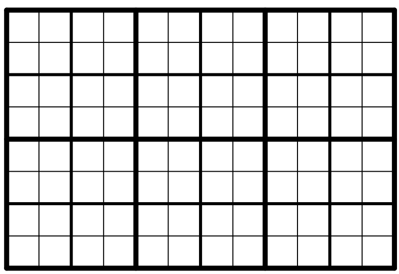
Lesson 5

Common Divisors and Common Multiples. Euclid's Algorithm

The following two problems aim to give a visual representation of common divisors and common multiples.

Problem 5.1. Let's draw a rectangle of 8×12 little 1×1 squares on square-lined paper. What equal squares can the rectangle be partitioned into?

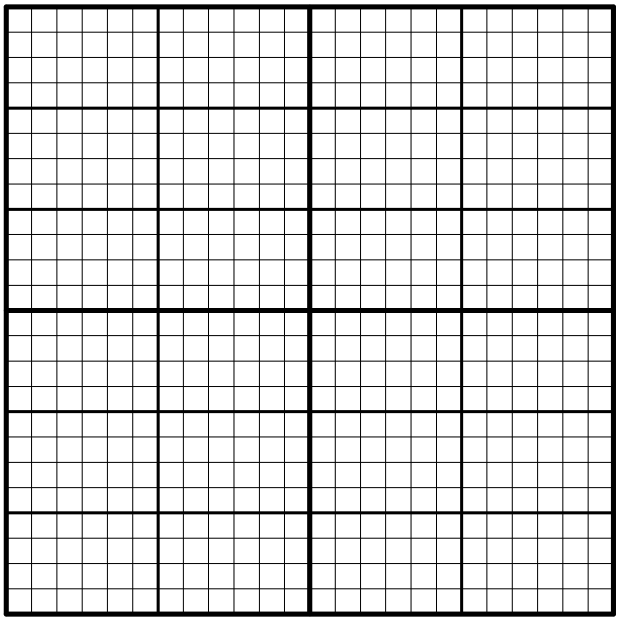
Solution. It is clear that it is possible to divide the rectangle into 1×1 squares. The width of the rectangle can be divided into segments of length 1, 2, 4, or 8, and its length into segments of length 1, 2, 3, 4, 6, or 12. Thus, squares of size 1, 2, and 4 will work.



Mathematically, the problem is reduced to finding the *common divisors* of the numbers 8 and 12. Note that if we are partitioning the rectangle into squares of the largest size, then we should take 4×4 squares, i.e., we would use the *greatest common divisor*.

Problem 5.2. What squares can be constructed by putting together 4×6 rectangles (with the long sides of all rectangles being parallel)?

Solution. We can obtain rectangles of length 6, 12, 18, 24, 30, 36 and, and so on, and of width 4, 8, 12, 16, 20, 24, 28, 32, 36, and so on. Thus, squares of size 12, 24, 36, and so on, can be obtained by the construction indicated.



Mathematically, the problem is reduced to finding *common multiples* of the numbers 4 and 6. The smallest square is of size 12, which is equal to the *least common multiple* of the numbers 4 and 6.

The *greatest common divisor* of two numbers a and b will be denoted by (a, b) and the *least common multiple* by $[a, b]$.

The model proposed in these problems clearly explains the fact that the greatest common divisor of two numbers can be divided by all of their other common divisors, and all common multiples can be divided by the least common multiple. The following formulas are also obvious from this model:

$$(a, a) = [a, a] = a, \qquad (ca, cb) = c(a, b), \qquad [ca, cb] = c[a, b].$$

Problem 5.3[†]. Find the common divisors of the numbers n and $n + 1$.

Solution. Let d be a common divisor of the numbers n and $n+1$. Then their difference $(n+1)-n=1$ must also be divisible by d. Therefore, $d=\pm 1$.

Recall that if $(m,n)=1$, then the numbers m and n are called *coprime* (see Lesson 2). The previous problem shows us that *consecutive numbers n and $n+1$ are always coprime.*

The same problem implies the following statement.

> **Lemma.** *Let $a=bq+r$. Then the greatest common divisor of the numbers a and b is equal to the greatest common divisor of the numbers b and r, that is, $(a,b)=(b,r)$.*

Proof. Let c be a common divisor of the numbers a and b. It follows from the equality $r=a-bq$ that r is also divisible by c, that is, c is a common divisor of the numbers b and r.

Conversely, let c' be a common divisor of the numbers b and r. Then the number $a=bq+r$ is also divisible by c', that is, c' is a common divisor of a and b. Thus, the numbers a and b have the same common divisors as the numbers b and r. Thus, the greatest common divisor of the numbers a and b coincides with the greatest common divisor of the numbers b and r.

> **Corollary.** *Let a and b be positive integers (where $b<a$), and let r be the remainder in the division of a by b. Then $(a,b)=(b,r)$.*

Applying the Corollary several times, we obtain a method for quickly finding the greatest common divisor of two numbers.

> **Euclid's algorithm.** First, divide a by b. If there is no remainder, then $(a,b)=b$. If there is a nonzero remainder r, then we divide b by this remainder, obtaining a new remainder r_1. Next we divide r by r_1. And so we continue and stop when the last remainder divides the previous one with zero remainder (why does this necessarily happen?). This last nonzero remainder will be the greatest divisor of all the numbers appearing in the calculations, including the two original ones.

In our illustrative model, Euclid's algorithm is as follows: from the rectangle of sides a and b (where $b < a$), we cut off several squares of side b until we get a rectangle whose one side is less than b. From the resulting rectangle, as long as it is possible, we cut off squares whose sides are equal to its smaller side, and so on. When the last rectangle is cut entirely into squares, the problem is solved, because the side of these squares is (a, b). See Problem 5.9 and the additional problem D61. An interactive model is available on the website: `http://www.etudes.ru/ru/etudes/nod/`.

Problem 5.4. Find $(846, 246)$.

Answer: 6.

Solution.

$$846 = 246 \cdot 3 + 108, \qquad 246 = 108 \cdot 2 + 30,$$
$$108 = 30 \cdot 3 + 18, \qquad 30 = 18 \cdot 1 + 12,$$
$$18 = 12 \cdot 1 + \boxed{6}, \qquad 12 = \boxed{6} \cdot 2 + 0.$$

Of course, somewhere around the numbers 30 and 18, it is already possible to figure out what the answer will be and not carry out the calculations to their logical end.

If the numbers a and b are coprime (that is, $(a, b) = 1$), then, by the theorem on coprime divisors (Lesson 2), any of their multiples must be divisible by ab, and hence $[a, b] = ab$. That is, in this case, $(a, b) \cdot [a, b] = ab$. It turns out that this is also true in the general case.

Problem 5.5^{+}. Prove that, for any two positive integers a and b, the following equality $(a, b) \cdot [a, b] = ab$ holds.

Proof. Let d be the greatest common divisor of the numbers a and b. Then these numbers must have the form $a = dl$, $b = dm$, where l and m are coprime. Their least common multiple c must be divisible by d. Consider the quotient c/d. It must be divisible by l and m, which are coprime. By the theorem on coprime divisors, $c/d \,\vdots\, lm$, that is, $c = dlm$. Therefore, $d \cdot c = d \cdot (dlm) = dl \cdot dm = ab$, which gives the required equality.

Using this relation, it is not difficult to find $[a, b]$ by calculating ab directly and (a, b) by Euclid's algorithm (see Problem 5.8).

Problem 5.6. Solve each of the following systems:

a) $\begin{cases} (x, y) = 5, \\ [x, y] = 10 \end{cases}$; b) $\begin{cases} (x, y) = 1, \\ [x, y] = 4 \end{cases}$; c) $\begin{cases} (x, y) = 5, \\ [x, y] = 31. \end{cases}$

Solution. a) Note that the numbers x and y are both multiples of 5 and divisors of 10. Also, they are not equal (why?). There are only two such numbers, namely 5 and 10. Hence $x = 5$, $y = 10$, or vice versa, $x = 10$, $y = 5$.

b) Note that the numbers x and y are coprime and both are divisors of 4. Decompose 4 into two factors in all possible ways $4 = 1 \cdot 4 = 2 \cdot 2$ and choose the coprime pairs: the pairs $(1, 4)$ and $(4, 1)$ suit us.

c) A common multiple of two numbers must be divisible by any common divisor of these numbers, but $31 \not\vdots\, 5$. Therefore, the system has no solutions.

Problems for individual solution

Problem 5.7. Is it true that the following numbers are coprime:

a) two adjacent odd numbers;

b) an odd number and half the even number following it?

Problem 5.8. Find: a) $(1960, 588)$; b) $[1960, 588]$ by using Euclid's algorithm.

Problem 5.9. An automaton can cut off from any rectangle a square with a side equal to the smaller side of the rectangle. Find some pair of numbers a and b such that when cutting the $a \times b$ rectangle, the automaton obtains squares of six different sizes.

Problem 5.10. Find all values of m for which the fraction $\dfrac{11m + 3}{13m + 4}$ is cancellable.

Problem 5.11. Solve each of the two following systems:

a) $\begin{cases} (x, y) = 5, \\ [x, y] = 30 \end{cases}$; b) $\begin{cases} (x, y) = 1, \\ [x, y] = 30. \end{cases}$

Problem 5.12. The Fibonacci numbers 1, 1, 2, 3, 5, 8, 13, 21, 34, ... are defined by the equalities $\varphi_{n+2} = \varphi_{n+1} + \varphi_n$ (the next number is equal to the sum of the previous two) and $\varphi_1 = \varphi_2 = 1$. Find $(\varphi_{100}, \varphi_{101})$.

Answers and solutions

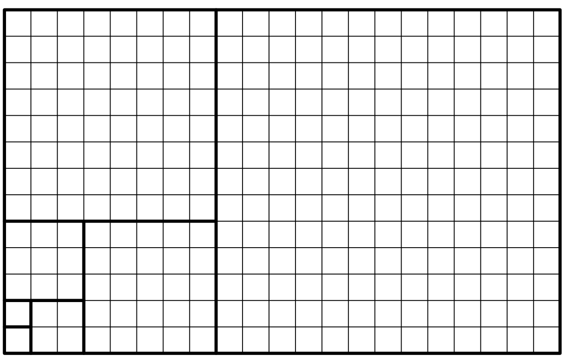
Problem 5.7. By Euclid's algorithm a) $(2n - 1, 2n + 1) = (2, 2n - 1) = 1$ is true; b) $(n, 2n - 1) = (n, n - 1) = 1$ is true.

Note that by using Euclid's algorithm, the problem is solved by considering two simple equalities.

Problem 5.8. a) $1960 = 588 \cdot 3 + \boxed{196}$, $588 = 3 \cdot \boxed{196} + 0$

b) $[1960, 588] = 1960 \cdot 588 : (1960, 588) = 1960 \cdot 588 : 196 = 10 \cdot 588 = 5880$.

Problem 5.9. In other words, we need to find numbers a and b so that Euclid's algorithm stops after 6 steps. It is convenient to start from the end. Suppose, for example, that there were two squares of side 1 at the end (for simplicity, we take figures of the smallest size). Then, before this, there was a square of side 2, in front of it a square of side 3, in front of it a square of side 5, then 8, then 13 (see the figure). Thus, the original rectangle can have the dimensions 21×13.



Problem 5.10. $(13m + 4, 11m + 3) = (11m + 3, 2m + 1) = (2m + 1, m - 2) = (m - 2, 5) \neq 1$ if and only if $(m - 2) \vdots 5$, that is, $m = 5k + 2$, where k is an integer.

Problem 5.11. a) $xy = (x, y) \cdot [x, y] = 150$. We can decompose 150 into two factors that are multiples of 5 as follows: $150 = 5 \cdot 30 = 10 \cdot 15$. Both options are correct answers.

b) $xy = (x, y)[x, y] = 30$, where x and y are coprime. Decompose 30 into two coprime factors as follows:

$$30 = 1 \cdot 30 = 2 \cdot 15 = 3 \cdot 10 = 5 \cdot 6.$$

All four options are correct answers.

Problem 5.12. By Euclid's algorithm,

$$(\varphi_{100}, \varphi_{101}) = (\varphi_{100}, \varphi_{101} - \varphi_{100}).$$

But, by the definition of Fibonacci numbers,we can write $\varphi_{101} - \varphi_{100} = \varphi_{99}$. Therefore, $(\varphi_{100}, \varphi_{101}) = (\varphi_{99}, \varphi_{100})$. Note that both subscripts have decreased by 1. Repeatedly applying Euclid's algorithm, we obtain

$$(\varphi_{100}, \varphi_{101}) = (\varphi_{99}, \varphi_{100}) = (\varphi_{98}, \varphi_{99}) = \ldots = (\varphi_1, \varphi_2) = 1.$$

Thus, we have proved that neighboring Fibonacci numbers are coprime. Note that, in solving Problem 5.9, we actually constructed a Fibonacci sequence!

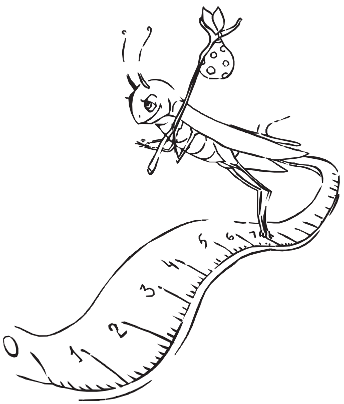
Another solution is based on the fact that the sum of two coprimes is coprime to each summand.

The subject of this lesson also includes problems 53–65 from the section “Additional problems”.

Lesson 6

Diophantine Equations

Problem 6.1. A grasshopper jumps along the number line. First, it takes one or more jumps of length 3 inches in one direction (right or left), and then one or more jumps of length 5 in the other direction. How can he get from point 0 to point 7? Find all the options.



Solution. It is easy to find one of the solutions: one jump of length 3 to the left and two jumps of length 5 to the right. To get the other options, note that, to the solution found, we can "add" additional jumps as a result of which the grasshopper will remain at the same place.

The grasshopper can take 5, 10, 15, ... jumps to the left of length 3, and, after that, 3, 6, 9, ... jumps of length 5 to the right. It may, on the contrary, take 5, 10, 15, ... jumps of length 3 to the right and then 3, 6, 9, ... jumps of length 5 to the left.

In fact, the previous paragraph shows all of the jump options. To explain this in rigorous terms, we will use algebra. Let's denote the number of jumps of length 3 by x and that of jumps of length 5 by y. Let's agree that if $x > 0$, then the jumps were to the right, and if $x < 0$, then they were to the left. Similarly, for y. (Then the equality

$$3 \cdot (-6) + 5 \cdot (+5) = 7$$

can be "read" as follows: the grasshopper takes jumps of length three 6 times to the left and jumps of length five 5 times to the right, arriving at the point located 7 inches away from the origin.) Thus, we obtain the equation

$$3x + 5y = 7.$$

It is easy to guess a *particular* solution (i.e., one of the solutions): $x_0 = -1$, $y_0 = 2$. Let us subtract the equality $3x_0 + 5y_0 = 7$ from the equation displayed above. We obtain the new equation $3(x - x_0) + 5(y - y_0) = 0$. Denote $x - x_0 = s$, $y - y_0 = t$. We have $3s + 5t = 0$. Hence it can be seen that $3s \vdots 5$, $5t \vdots 3$. Since 3 and 5 are coprime, it follows that $s \vdots 5$, $t \vdots 3$ (see the theorem on the cancellation of a factor at the end of this lesson). Let's put $s = 5n$, $t = -3n$, where n may be any integer. Then, $x - x_0 = 5n$, $y - y_0 = -3n$, that is, $x = -1 + 5n$, $y = 2 - 3n$, where n is any integer. There are no other solutions.

Problem 6.2. A seller and a buyer have an unlimited number of coins of two denominations. The seller can give change. The buyer was able to pay 7 doublons. Can the buyer pay

a) 14 doublons;

b) 35 doublons;

c) 36 doublons?

Solution. a), b) He can. The buyer and the seller simply repeat the operations involved in paying 7 doublons twice or five times, respectively.

c) It is not be possible to do this by repeating the operations as explained above, since 36 is not a multiple of 7. If there were coins of one doublon, then it would, of course, be possible to pay both 7 and 36 doublons. And if there were coins of 7 and 14 doublons, then, even if change may be given, only sums that are multiples of 7 doublons can be paid, and hence 36 doublons cannot be paid.

In Problem 6.1, it was easy to guess a particular solution. But what if the numbers are large? Or how can one teach a computer to find particular solutions?

Problem 6.3$^+$. Find an integer solution of the equation a) $15x + 17y = 1$; b) $15x + 17y = 9$.

Solution. a) To find a particular solution, let us find $(15, 17)$ by using Euclid's algorithm:

$$17 = 15 \cdot 1 + 2, \quad 15 = 2 \cdot 7 + \boxed{1}.$$

Now let's express $\boxed{1}$ from the second equality, then 2 from the first: $\boxed{1} = 15 - 2 \cdot 7 = 15 - (17 - 15) \cdot 7 = 8 \cdot 15 - 7 \cdot 17$. We see that the pair of numbers $x_0 = 8$, $y_0 = -7$ is a particular solution of the equation.

b) From item a) we know integer values of x_0 and y_0 such that $15x_0 + 17y_0 = 1$. Multiply both sides of this equality by 9. This gives $15 \cdot (9x_0) + 17 \cdot (9y_0) = 9$. Therefore, the pair $(9x_0; 9y_0) = (72; -63)$ is a solution of equation b).

Problems 6.1 and 6.3 can be reduced to equations of the form

$$ax + by = c, \tag{1}$$

where a, b, c are given integers, and a and b are nonzero (for example, in the last problem, $a = 15$, $b = 17$, $c = 1$, or 9) and x, y are *unknown* integers.

> Such equations in integers are called *Diophantine* in honor of the Ancient Greek mathematician Diophantus. If $c \neq 0$, the equation is called *inhomogeneous* and if $c = 0$, then it referred to as *homogeneous*.

In the previous problems, we obtained the following scheme for solving Diophantine equations.

1. Find a partial solution of the inhomogeneous equation (guessing or using Euclid's algorithm).
2. Find the general solution of the homogeneous equation.
3. Add these solutions.

Note that this is a general idea which is used when solving systems of linear algebraic equations, linear differential equations, and also, in general, in linear problems.

Problem 6.4. Using a blue felt-tip pen, a craftsman puts marks spaced 34 cm apart on a long ribbon starting from its beginning, while another craftsman puts marks on it with a red felt-tip pen every 27 cm. Can any blue mark be at the distance of 2 cm from any red one?

Answer: Yes, it can.

Solution. Let the first craftsman put x marks, and the second y marks. If the equation $34x - 27y = 2$ has positive solutions, then the blue mark with number x is 2 cm away from the red mark with number y. We will look for a particular solution using Euclid's algorithm:

$$34 = 27 \cdot 1 + 7, \quad 27 = 7 \cdot 3 + 6, \quad 7 = 6 \cdot 1 + \boxed{1}.$$

Now "in reverse" we express $\boxed{1}$:

$$1 = 7 - 6 = 7 - (27 - 7 \cdot 3) = 7 \cdot 4 - 27 \\ = (34 - 27) \cdot 4 - 27 = 34 \cdot 4 - 27 \cdot 5.$$

Multiplying the equality by 2, we obtain $34 \cdot 8 - 27 \cdot 10 = 2$, which means, in particular, that the eighth blue mark is 2 cm away from the tenth red one.

In all of the previous equations, a solution existed. The question whether equation (1) is always solvable arises. We will now prove that, *for coprime a and b*, the equation

$ax + by = 1$ is always solvable. Hence the solvability of the equation $ax+by = c$ will follow (simply multiply the solution by c).

> **Fundamental lemma.** *If the numbers a and b are coprime, then there exist two numbers x_0 and y_0 that satisfy the equality $ax_0 + by_0 = 1$.*

Proof. Let us find (a, b) by applying Euclid's algorithm. Since the numbers a and b are coprime, we will finally obtain 1. Finding 1 sequentially by working through a chain of residues from end to beginning (just as in the previous two problems), we will express 1 in terms of a and b with some coefficients, that is, we necessarily obtain the numbers x_0 and y_0.

> **Corollary.** *If the numbers a and b are coprime, then, for any integer c, there exist two numbers x_0 and y_0 such that $ax_0 + by_0 = c$.*

On the basis of these statements, it is possible to prove a number of important theorems on primes and coprime numbers (see Problems 6.6, 6.11 and also the next lesson).

Problem 6.5. Do the following Diophantine equations have a solution:

a) $6x+8y = 9$; b) $5x+10y = 17$; c) $25x+10y = 55$;
d) $12x + 15y = 22$; e) $24x + 18y = 2010$?

Solution. a) No, there is no solution. For integers x and y, the left side is even, while the right side is odd.

b) No, there is no solution. Both terms on the left side are multiples of 5, and hence the right side must be a multiple of 5.

c) Yes, there is a solution. It is possible to guess one: for example, $x = 3$, $y = -2$. One can also divide both sides of the equation by 5, obtaining the equation $5x + 2y = 11$ with coprime coefficients, which is solvable by the corollary of the fundamental lemma.

d) No, there is no solution. The left side is a multiple of 3, while the right side is not.

e) Yes, there is a solution. The left and right sides are multiples of 6. Dividing them by 6 gives us the equation $4x + 3y = 335$ with coprime coefficients. By the corollary of the fundamental lemma, it has solutions.

Problem 6.6. Prove the theorem on coprime divisors (Lesson 2). *If a number n is divisible by each of two coprime numbers a and b, then it is divisible by their product ab.*

Proof. Let's recall the solution of Problem 2.5 b), c) and generalize it. Note that the numbers an and bn are both multiples of ab. Thus, $x \cdot an + y \cdot bn$ is a multiple of ab for any x and y. If there exist numbers x_0 and y_0 such that $x_0 \cdot an + y_0 \cdot bn = n$, then n is a multiple of ab. Cancelling n from both sides of the last equality, we see that such numbers x_0 and y_0 can be found by the fundamental lemma.

Homework problems

Problem 6.7. Use arguments similar to Problem 6.5 in general form and prove the following statement:

> **Theorem** (criterion for the solvability of Diophantine equations). a) *If c is divisible by (a, b), then equation* (1) *has infinitely many solutions.* b) *If c is not divisible by (a, b), then equation* (1) *has no solutions.*

Problem 6.8. n points are marked on the circle at equal distances from one another (as in the dial of a clock). One of these points is the starting point. It is connected by a segment to a point which is d arcs away from it clockwise.

We also connect this new point by a segment to a point which is d arcs away from it. We continue in this way until the last point coincides with the starting point. Thus, we will obtain a closed polygonal line (possibly, a self-intersecting one).

a) For what values of d will all of the n points turn out to be vertices of a polygonal line?

b) How many revolutions will the polygonal line perform before closing?

It is useful to the draw polygonal lines first, for example for: $n=5$, $d=3$; $n=6$, $d=4$.

Problem 6.9. It is required to lay a gas pipeline on a 450 m long plot of land. There are pipes of length 9 and 13 m at the disposal of the builders. How many pipes of these lengths must be taken to lay the route so that the number of welds is minimal? The pipes must not be cut.

Problem 6.10. a) Prove that amounts of 8, 9, and 10 francs can be paid out in three and five-franc bills.

b) What are the largest amounts that can be paid in three- and five-franc bills?

Problem 6.11. Arguing as in Problem 6.6, prove the following statement, which we used when solving homogeneous Diophantine equations.

> **Theorem on the cancellation of a factor.** *If the product of ac is divisible by b and the numbers a and b are coprime, then the number c is divisible by b.*

Problem 6.12.

Forty grey mice ran with forty grains of rice,
Two thinner ones strained, with a load of two grains,
A few ran all smiles, without any rice,
The big ones were serving, carrying seven,
Small mice, through the door, ran carrying four.
How many grey mice ran without any rice?

(A. Akulich. “Quantum”, №4, 1995, transl. by A. Sossinsky)

Problem 6.7. a) Divide both sides of equation (1) by (a, b). We obtain the equation $a_1x + b_1y = c_1$ with coprime coefficients a_1 and b_1. By the fundamental lemma, it has a solution $(x_0; y_0)$. Adding to this particular solution the solution $(b_1n; -a_1n)$ of the homogeneous equation, we obtain an infinite series of solutions (here n is an arbitrary integer).

b) Let x_0 and y_0 be numbers such that $ax_0+by_0 = c$. Then the left side of this equality is divisible by (a, b), while the right side is not. The resulting contradiction shows that the equation is unsolvable.

Problem 6.8. Let us number the points clockwise, starting with 0. Then, after x steps, we will be at the point with number dx. More precisely, if y revolutions around the circle are performed, then we will be at the point with number $dx-ny$.

a) The question can be restated as follows: For what values of d and n can any number be obtained?

The answer is given by the criterion for the solvability of Diophantine equations: for coprime d and n.

b) Since the polygonal line is closed, we have again reached the point with number 0. Therefore, we need to find the first positive solution of the Diophantine equation $dx - ny = 0$. Cancelling (d, n) from both sides of the equation, we obtain the equation $d_1x - n_1y = 0$, where $d_1 = d/(d, n)$ and $n_1 = n/(d, n)$ are coprime. Since the number d_1x must be divisible by n_1, according to the theorem on the cancellation of a factor, it follows that the number x must also be divisible by n_1 . The smallest value is $x = n_1$, $y = d_1 = d/(d, n)$.

Answer: $\dfrac{d}{(d, n)}$.

In Lesson 8 (see Problems 8.6, 8.13), we will be able to answer the following question: How many closed polygonal lines with equal links and vertices at all n points are there?

Problem 6.9. Since we want to use as few pipes as possible, we must use as many pipes of length 13 as possible.

The number of such pipes is divisible by 9 (prove this!). It is impossible to take 36 of them, because $13 \cdot 36 > 450$. Thus, only 27 long pipes can be used and the number of short pipes will then be $(450 - 13 \cdot 27) : 9 = 11$.

Answer: 11 short pipes and 27 long ones.

Problem 6.10. a) $8 = 5 + 3$, $9 = 3 \cdot 3$, $10 = 5 \cdot 2$.

b) One can pay out any amount greater than the given ones: the required number of three franc bills must be added to one of these three amounts.

Thus, it is proved that any amount greater than 7 can be paid out using three and five franc notes.

In other words, the equation $3x + 5y = c$ has solutions in non-negative numbers for all $c \geqslant 8$.

Problem 6.11. Since the numbers a and b are coprime, by the fundamental lemma, there exist integers x_0 and y_0 such that $ax_0 + by_0 = 1$. Multiply this equality by c:

$$c = acx_0 + bcy_0.$$

Both terms on the right side are divisible by b (why?) and, therefore, their sum c is divisible by b.

Problem 6.12. Answer: 32 mice.

Let's denote the number of mice that carried no rice by n, the number of big mice by b, and the number of the other mice by s. We obtain the equation $2 + n + b + s = 40$ for the total number of mice and the equation

$$40 = 2 \cdot 2 + n \cdot 0 + b \cdot 7 + s \cdot 4$$

for the amount of grains of rice. Simplifying this equation gives the Diophantine equation $7b + 4s = 36$. Hence $b = 4k$, $s = 9 - 7k$, where k is an integer. Choosing the positive solutions, we obtain the unique solution $b = 4, s = 2$. Now we can find n from the first equation: $n = 38 - b - s = 32$.

The subject of this lesson also includes problems 66–78 from the section “Additional problems”.

Lesson 7

Prime Divisor Theorem

Now we will prove an important theorem concerning primes.

> **Prime divisor theorem.** *If the product ab is divisible by a prime p, then a or b is divisible by p.*

Proof. If a is divisible by p, then no further proof is needed. Suppose that a is not divisible by p; then a and p are coprime (why?). In this case, by the fundamental lemma, there exist integers x_0, y_0 such that $ax_0 + py_0 = 1$. Multiply this equality by b:

$$b = abx_0 + bpy_0.$$

Both terms on the right side are divisible by p (why?) and, therefore, their sum b, is divisible by p.

Thus, a or b are obviously divisible by p.

Note that this theorem is also easily deduced from the factor cancellation theorem.

It is useful to discuss with the students the fact that in this theorem the condition that the divisor be prime is essential, that is, if it is omitted, then the theorem will be incorrect (for example, $4 \cdot 3$ is divisible by 6, but neither 4 nor 3 is divisible by 6).

> **Corollary.** *If the product of several numbers is divisible by a prime p, then at least one of these numbers is divisible by p.*

Proof. Let $a_1 a_2 \ldots a_n \vdots p$. Let us express this product as $a_1 a_2 \ldots a_n = (a_1 a_2 \ldots a_k) \cdot (a_{k+1} \ldots a_n)$. By the prime divisor theorem, one of the two products is divisible by p. Let's repeat this argument for that product, and keep doing that until there is only one number left, a_i.

Problem 7.1. Does the rebus $\mathrm{AB}\cdot\mathrm{CD}=\mathrm{EEFF}$ have a solution?

Solution. Note that the number on the right is a multiple of 11 by the divisibility criterion. Therefore, by the prime divisor theorem, one of the factors on the left must also be a multiple of 11. But this is not so; hence the rebus has no solutions.

Problem 7.2. Prove that if an exact square is divisible by a prime p, then it is divisible by p^2.

Proof. Let a^2 be a multiple of p, then, by the prime divisor theorem, a is a multiple of p, $a = pb$. But then $a^2 = p^2b^2$, that is, a^2 is divisible by p^2.

Problem 7.3. Nick boasts that he can solve any problem. The teacher gives him one hundred cards with 0 written on it, one hundred cards with 1 on it, and one hundred cards with 2 on it, and asks him to use all these cards to compose a number which is a complete square. Will Nick be able to solve this problem?

Solution. Note that the sum of the digits of this number is 300, that is, it is a multiple of 3, but not a multiple of 9. Therefore, the number is divisible by 3, but not by 9. However, in view of the previous problem, a square divisible by 3 must also be divisible by 9. Therefore, Nick will not be able to cope with this problem.

Problem 7.4. Let p be a prime. Prove that if the product of several numbers is divisible by p^2, then one of the factors is divisible by p^2 or there are at least two factors, each of which is divisible by p.

Solution. Let $ab...h = kp^2$. Then $ab...h$ is also divisible by p. By the prime divisor theorem, one of the factors is divisible by p; let it be $a = pa'$. Cancel p from both sides of the equality, obtaining $a'b...h = kp$. Repeating the argument, we see that either a' is a multiple of p, that is, a is a multiple of p^2, or some other factor is a multiple of p.

Problem 7.5. Three numbers have the same remainder when divided by 3. Prove that their product either is not divisible by 3 or is a multiple of 27.

Proof. Under division by 3, the remainders 0, 1, and 2 can be obtained. If the remainder is 0, then all three numbers are divisible by 3 and the product is divisible by 27. But if the remainders are 1 or 2, then all three numbers are not divisible by 3. Hence their product is not divisible by 3; otherwise, we would obtain a contradiction due to the prime divisor theorem.

In the course of solving the problem, we obtained a useful reformulation of the prime divisor theorem: if some numbers are not multiples of a prime p, then their product is not a multiple of p. See Problem 3.6.

Problem 7.6. For what values of n is the number $(n-1)!$ divisible by n without remainder?

Answer: If n is a composite number greater than 5.

Solution. If n is a prime and divides $(n-1)!$, then, by the prime divisor theorem, n also divides one of the factors. However, this is impossible, since all the factors are less than n. So $(n-1)!$ is not divisible by the prime n.

Now let n be a composite number. Then either n can be expressed as $n = ab$, where $a > 1$, $b > 1$, $a \neq b$, or $n = p^2$, where p is prime.

Consider the first case. Since the numbers a and b are both less than $n-1$ and different, they are both among the factors $1 \cdot 2 \cdot \ldots \cdot (n-1) = (n-1)!$. Therefore, $(n-1)!$ is divisible by ab.

Consider the second case. If $n > 5$, then $(n-1)!$ contains the factors p and $2p$ (since $2p < p^2 = n$), that is, it is divisible by n. It remains to check the number 4, which is the only composite number less than 5. This number is not a solution, since $3! = 6$ is not divisible by 4.

Problems for individual solution

Problem 7.7. Can a number whose digits are one 1, two 2's, three 3's, ..., nine 9's be an exact square?

Problem 7.8. A prime was squared to give a ten-digit number. Can all the digits of the resulting number be different?

Problem 7.9. What is the smallest natural number n for which $n!$ is divisible by 100?

Problem 7.10. Let p_1, p_2, p_3, p_4 be different primes. Find prime common divisors of the numbers: a) p_1p_2 and p_3p_4, b) p_1p_2 and p_2p_4.

Problem 7.11. a) Write positive integers at the vertices of a square so that, at every pair of adjacent vertices, the integers will not be coprime, but, at every pair of non-adjacent vertices, they will be coprime.

b) The same problem for a cube (if the vertices are connected by an edge, then the integers must not be coprime, and if they are not connected by an edge, then they must be coprime).

Problem 7.12. The integers x, y, and z satisfy

$$(x-y)(y-z)(z-x) = x+y+z.$$

Prove that the number $x+y+z$ is divisible by 27.

Answers and solutions

Problem 7.7. The sum of the digits of such a number is $1\cdot1+2\cdot2+\ldots+9\cdot9$; it is a multiple of 3, but not a multiple of 9. According to Problem 7.2, a complete square is either not divisible by 3 or divisible by 9. This means that the number in question cannot be a complete square.

Problem 7.8. Answer: No, they cannot.

If all the digits were different, then their sum would be 45 and the square of the given number would be divisible by 9. Hence, by Problem 7.4, the number itself would be divisible either by 9 or by 3. This is impossible, since the number is prime and, obviously, greater than 3.

Problem 7.9. Answer: 10.

Since the number $n!$ must be divisible by 100, then among its factors there are two 2's and two 5's. Looking at the initial factors of $n!$, let us write out the needed factors 2, 4, 5, 10.

Problem 7.10. a) Let p be a prime common divisor of the numbers p_1p_2 and p_3p_4. Then, by the prime divisor theorem, one of the factors in both products must be divisible by p. Since all of the factors are prime, this factor must be equal to p. But this is impossible, since all the numbers p_1, p_2, p_3, p_4 are different by assumption. Therefore, the products have no common divisors, except 1.

b) Arguing in a similar way, we obtain $p = p_2$.

Problem 7.11. a) Near the sides of a square we write the numbers 2, 3, 5, 7, and, at each vertex, we write the product of the numbers indicated on the sides that are incident to it. Then the numbers at adjacent vertices are divisible by the number indicated on their common side, and they are not coprime. The numbers in non-adjacent vertices are equal to the product of different primes, and hence they cannot simultaneously be divisible by any prime.

If the problem remains unsolved for a long time, then, the teacher can write, for example, the sequence of numbers 6, 14, 35, and 15 at the vertices, and let the students guess how to obtain them.

b) Let us repeat the same construction: we write various primes on the edges and, at each vertex, we write the product of the numbers written on the edges incident to this vertex. The proof is similar to item a).

Problem 7.12. Consider the remainders in dividing x, y, and z by 3. There are three possible cases.

1. All three remainders are the same. Then each of the three brackets on the left side is divisible by 3, which means that their product is also divisible by 27.

2. Two remainders are the same. Then one of the brackets is divisible by 3; therefore, $x + y + z$ is divisible by 3, and

hence the third remainder is equal to the first two, and we return to case 1.

3. All three remainders are different (0, 1, and 2). Then $x + y + z$ is a multiple of 3. However, the left side is not a multiple of 3, since it is the product of three numbers that are not multiples of 3. So this is impossible.

An example of such numbers: 15, 18, 21.

The subject of this lesson also includes problems 79–85 from the section “Additional problems”.

Lesson 8

Factorization into Primes. The Fundamental Theorem of Arithmetic

We know from Lesson 4 that any number can be factored into primes. Is this factorization unique?

The answer is given by the following theorem (for completeness, we will also repeat the proof of item A).

> **The fundamental theorem of arithmetic.**
> A. *Every natural number, greater than 1, can be factored into primes.*
> B. *Any two factorizations of the same number may differ only by the order of the factors.*

Proof. A. If the number itself is prime, then there is nothing left to prove. If the number is composite, then, by definition, it factors into the product of two smaller numbers. If they are both prime, then everything is proved. If either one the products is composite, then it must be factored further. Since we are dealing with positive integers and the products decrease at each step, the process will stop sooner or later, and only prime factors will remain.

B. Suppose we have two different prime number factorizations:

$$p_1p_2 \cdot \ldots \cdot p_n = q_1q_2 \cdot \ldots \cdot q_m.$$

Since the first expression is divisible by p_1, it follows that the second one must also be divisible by p_1. As a consequence of the prime divisor theorem, one of the numbers q_1, q_2, ..., q_m must be divisible by p_1, and since they are all prime, that number must be equal to p_1. Let $q_s = p_1$. Let's cancel $p_1 = q_s$

from both sides and repeat the whole argument with respect to p_2, p_3, and so on. By cancelling all the factors, we will come to the equality $1 = 1$. Therefore, the factorizations must coincide.

Usually the prime factorization of a number is written in the form $p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$, where $p_1 < p_2 < ... < p_n$. Such an expression is called the *canonical factorization into primes* of a number.

Problem 8.1. Four natural numbers are written at the vertices of a square. On each side, the product of the numbers at its ends is written. The sum of these products is 77. Find the sum of the numbers written at the vertices.

Solution. Let the numbers a, b, c, and d be written at the vertices. Then the numbers ab, bc, cd, and da are written at the sides. Their sum is $ab+bc+cd+da = (a+c)(b+d) = 77$. Factor the number 77 as: $77 = 7 \cdot 11 = 1 \cdot 77$. There are no other factorizations, since 7 and 11 are prime. The option $1 \cdot 77$ is not suitable, since the sum of positive integers cannot equal 1. Therefore, $a + c = 7$, $b + d = 11$, or vice versa. In both cases, $a + b + c + d = 7 + 11 = 18$.

Problem 8.2. Prove that, in the factorization into primes of an exact cube, all the exponents are multiples of 3.

Proof. Let's write out the factorization into primes for the base of the cube and raise the resulting equality to the third power. Then, in the factorization, all the exponents will be tripled. By uniqueness, the factorization of the cube is canonical.

Problem 8.3^{+}**.** Find the number of divisors of the following numbers: a) p^k; b) $p^k q^s$, where p and q are primes. c) Generalise the results obtained.

Solution. a) Let us enumerate all the divisors: 1, p, p^2, ..., p^k. They are $k + 1$ in all. There are no other divisors, since p^k is not divisible by greater powers of p nor by any other primes.

b) The easiest way to enumerate divisors is via their factorization into primes: the divisors are all numbers of the form $p^a q^b$, where $0 \leqslant a \leqslant k$, $0 \leqslant b \leqslant s$ (in particular, $1, p, p^2, \ldots, p^k$, $q, q^2, \ldots, q^s$). They are suitable because we have the equality $p^k q^s = p^a q^b \cdot p^{k-a} q^{s-b}$.

Why can't there be divisors of any other kind? Suppose $p^k q^s = m \cdot n$. Replace m and n by their factorizations into primes and multiply by adding the exponents. Due to the uniqueness of factorization into primes, we must obtain the expression $p^k q^s$. This means that there are no other prime divisors in the factorization of m and n, and since all the exponents are non-negative, p appears with an exponent not exceeding k and q appears with an exponent not exceeding s. Thus, the number of divisors is equal to the number of pairs of exponents, that is, it equals $(k+1)(s+1)$.

c) Arguing in a similar way for three or more prime divisors, we see that we must multiply the exponents increased by 1 of each number.

We can say that prime numbers are "bricks" from which a number is built. At the same time, "bricks" of one type cannot be replaced by those of another.

Problem 8.4. Let the factorizations into primes of the numbers a and b contain the prime factor p to the mth and nth power, respectively, and let $m \geqslant n$. Prove that p appears in the factorization into primes of the number $[a, b]$ raised to the mth power, and in the factorization into primes of the number (a, b) raised to the nth power.

Proof. Note that divisibility by a prime p (or its power) does not depend on the divisibility by other primes. Therefore, the smallest common multiple must include the smallest power of the number p divisible by p^m and p^n, that is, by p^m. Similarly, the greatest common divisor must include the greatest power of the number p that divides both p^m and p^n, that is, p to the nth power.

Problem 8.5^{+}. A even positive integer is said to be *evenly-prime* if it cannot be represented as a product of two smaller even numbers. (For example, the numbers 2, 6, 10 are evenly-prime, and $4 = 2 \cdot 2$, $8 = 4 \cdot 2$ are not.) State the analogue of the fundamental theorem of arithmetic for even numbers, replacing the words "natural" by "even", and "prime" by "evenly-prime". Check both parts of the resulting statement.

Solution. A. Every even number can be factored into evenly-prime factors. B. Any two factorizations of the same even number may differ only by the order of their factors.

Part A is correct (you can repeat the proof of the fundamental theorem of arithmetic, appropriately replacing the corresponding words). But part B is wrong! The numbers 2, 6, 10 and 30 are evenly-prime, but $60 = 30 \cdot 2 = 10 \cdot 6$ can be factored in two ways. (The reason is that for evenly-prime numbers the prime divisor theorem does not hold.)

Usually, students take the fundamental theorem of arithmetic for granted. The given example shows that, in some other arithmetics, that theorem can no longer be correct.

In Lesson 6, we dealt with a problem related to counting numbers smaller than a given n and coprime to it (Problem 6.8). This quantity plays an important role in number theory, and it has a special name and notation.

> **Definition.** The quantity of numbers from 1 to n that are coprime to n is called the *Euler function* and is denoted by $\varphi(n)$.

Problem 8.6. Find a) $\varphi(p)$; b) $\varphi(p^2)$; c) $\varphi(p^k)$, where p is prime.

Solution. Any prime p has common divisors different from 1 only with multiples of p. Therefore,

a) $\varphi(p) = p - 1$;

b) $\varphi(p^2) = p^2 - p$ (we throw out the numbers p, $2p$, ..., $(p-1)p$, that is, we throw out $p - 1$ numbers in all);

c) $\varphi(p^k) = p^k - p^{k-1}$ (we throw out the numbers p, $2p$, $3p$, ..., $(p^{k-1} - 1)p$, that is, we throw out $p^{k-1} - 1$ numbers in all).

Problems for individual solution

Problem 8.7. Is there an integer whose product of digits is a) 1990; b) 2000; c) 2010?

Problem 8.8. We are given two rectangular pieces of cardboard of dimensions 49×51 and 99×101. They are cut into identical rectangular, but not square, parts with integer sides. Find the dimensions of these parts.

Problem 8.9. Is there a set of a) two; b) ten natural numbers such that none of them is divisible by any of the others, and the square of each of them is divisible by each of the others?

Problem 8.10. Is there a positive integer whose product by 2 is a square, by 3 is a cube, and by 5 a fifth power?

Problem 8.11. Can a number having exactly 15 divisors be divisible by a) 100; b) 1000?

Problem 8.12. Your friend has chosen several arbitrary positive integers, and you want to guess all of them exactly in the order in which he chose those numbers. You are allowed to ask your friend to make an arbitrary calculation related to his numbers, for example, to find the product or sum of some of them, or a more complex combination and tell you the result. Let's call each such calculation a move. What is the smallest number of moves needed for you to be able to determine those numbers?

Problem 8.13. For coprime numbers a and b, consider the following table:

$$\begin{array}{ccccc}
1, & 2, & 3, & \ldots, & b; \\
b+1, & b+2, & b+3, & \ldots, & 2b; \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
(a-1)b+1, & (a-1)b+2, & (a-1)b+3, & \ldots, & ab.
\end{array}$$

a) Prove that there are exactly $\varphi(b)$ columns in which all numbers are coprime to b.

b) Prove that, in each column, all the remainders in the division by a are different.

c) Prove that, in each column, there are exactly $\varphi(a)$ numbers coprime to a.

d) Find $\varphi(ab)$ from $\varphi(a)$ and $\varphi(b)$.

Answers and Solutions

Problem 8.7. Factor these numbers into primes. If factors greater than 9 appear in the factorization, then numbers with such digits do not exist, and if all the factors are smaller than 9, then we have:

a) $1990 = 2 \cdot 5 \cdot 199$ — no;

b) $2000 = 2^4 \cdot 5^3$ — yes, for example, 2222555;

c) $2010 = 2 \cdot 3 \cdot 5 \cdot 67$ — no.

Problem 8.8. The area of the rectangular parts must divide the area of each of the given cardboard rectangles. Since $49 \cdot 51 = 3 \cdot 7^2 \cdot 17$, while $99 \cdot 101 = 3^2 \cdot 11 \cdot 101$, by Problem 8.4, we obtain $(49 \cdot 51, 99 \cdot 101) = 3$. Therefore, the area of a rectancular part must be is 1 or 3. Since rectangular parts are not squares, only dimensions 1×3 are suitable.

Problem 8.9. a) Yes, there is: 12 and 18.

b) The number a is divisible by b if each prime factor appears in the factorization of a to a power not less than that in the factorization of b. This suggests the following construction. Let's take ten different primes p_1, p_2, ..., p_{10} and construct the numbers

$$a_1 = p_1^2 p_2 ... p_{10}, \quad a_2 = p_1 p_2^2 ... p_{10}, \quad a_{10} = p_1 p_2 ... p_{10}^2.$$

It is easy to verify that they suit us.

Problem 8.10. For a number to be a square, it is necessary and sufficient that the exponents of all of its prime factors be divisible by 2; for a number to be a cube, to be divisible by 3; to be a fifth power, to be divisible by 5. Let the number be of the form $2^a 3^b 5^c$. Then the numbers $a+1$, b, and c must be divisible by 2; the numbers a, $b+1$, and c, by 3; and the numbers a, b, and $c+1$, by 5. For example, $a = 15$, $b = 20$, and $c = 24$ are suitable. Therefore, the number $2^{15}3^{20}5^{24}$ satisfies the condition.

Problem 8.11. a) $15 = 15 \cdot 1 = 3 \cdot 5$. Therefore, just as in Problem 8.3, a number having 15 divisors has the form either p^{14} or p^2q^4, where p and q are primes. In turn, we have $100 = 2^2 \cdot 5^2$. It is clear that, for example, the number $2^4 \cdot 5^2 = 800$ is suitable.

b) The number $1000 = 2^3 \cdot 5^3$ has $(3+1)(3+1) = 16$ divisors. If N is divisible by 1000, then N has at least 16 divisors. Therefore, it is not divisible by 1000.

Problem 8.12. One move is enough! Suppose, for example, the numbers a, b, and c are chosen. Let's ask the friend to calculate $2^a3^b5^c$. By the fundamental theorem of arithmetic, we can uniquely recover the exponents.

This solution can be beautifully demonstrated: the students call the results of their calculations, and the teacher determines the chosen number by using a computer program or an online factorization into primes.

Problem 8.13. a) The differences of numbers in each column are multiples of b. Therefore, all the numbers in the same column are either coprime to b or not, and this is determined by the very first number in the column. Among the first numbers there are $\varphi(b)$ numbers that are coprime to b, and hence there are as many columns.

b) The differences of numbers in a column is a multiple of b. If the remainders are the same, then the difference is also divisible by a and since a and b are coprime, this difference is also divisible by ab. But this is impossible, since the difference is greater than 0, but less than ab.

c) A number is coprime to a if and only if its remainder in the division by a is coprime to a.

d) If a number is coprime to a and b, then it is coprime to ab (why?). We have $\varphi(b)$ columns in which the numbers are coprime to b. In each of them, $\varphi(a)$ numbers are coprime to a. Thus, there is a total of $\varphi(a)\varphi(b)$ numbers that are coprime to ab.

Therefore, if a and b are coprime, then $\varphi(ab) = \varphi(a)\varphi(b)$. This property of the Euler function is called *multiplicativity*. Note that the number of divisors of a given number has the same property (Problem 8.3). It is not difficult to prove this property for the sum of divisors. Therefore, it is possible to simplify problems associated with these functions by solving them separately for each prime factor. Also see Problem 8.4 and the additional problems D90, D96, D97, D98.

The subject of this lesson also includes problems 86–100 from the section "Additional problems".

Additional Problems

D1. Peter divided the numbers a, b, and $a + b$ by some number c. Two of the numbers were divided without remainder, and one number was not. Wasn't Peter mistaken?

D2. a) Nancy noticed that $555 \vdots 37$ and $777 \vdots 37$. State and prove a more general statement. b) Find, without using a calculator, whether the numbers 718718, 539539, 174173 are divisible by 77?

D3. Are there nonzero numbers a and b such that one of them is divisible by their sum and the other by their difference?

D4*. In the Decimal Kingdom, the following coins are in circulation: 1 ducat, 10 ducats, 100 ducats, 1000 ducats. Is it possible to pay off one million ducats using exactly half a million coins?

D5. There are three heaps of stones: 51 stones in the first, 49 stones in the second, and 5 stones in the third. We are allowed to combine heaps into one as well as to divide a heap consisting of an even number of stones into two equal ones. Can we obtain 105 heaps of one stone each?

D6. There are pears, plums, and apples in six baskets. The number of plums in each basket is equal to the total number of apples in all the other baskets, and the number of apples in each basket is equal to the total number of pears in all the other baskets. Prove that the total number of pears, plums, and apples is divisible by 31.

D7. A regular triangle and a regular n-gon are inscribed in equal circles. For what values of n will the triangle be covered by the n-gon?

D8. Each of the numbers a, b, c, d is divisible by $ab - cd$. Prove that either $ab - cd = 1$ or $ab - cd = -1$.

D9. Alex thought up two divisibility tests by 27:

a) if a number is divisible by 3 and 9, then it is also divisible by 27;

b) if the sum of the digits of a number is divisible by 27, then the number itself is divisible by 27.

Verify the validity of Alex's tests.

D10. How many four-digit numbers with the two middle digits 97 are divisible by 45?

D11. Is there a digit (the same one) such that if this digit is written next to the number 97 on the left and on the right, then the resulting four-digit number will be divisible by 27?

D12. The following number was written on the blackboard:

$$35! = 10333147966386144929{*}66651337523200000000.$$

But the digit marked with the asterisk was erased by mistake. Can it be recovered?

D13. To open the safe, a code consisting of seven digits: 2's and 3's is needed. The safe will open if there are more 2's than 3's and the code is divisible by 12. Devise a code that opens the safe.

D14. The last digit of the square of a positive integer is 6. Prove that its last-but-one digit is odd.

D15. Is $7 \cdot 10^{2011} + 8$ a) divisible by 3; b) by 9?

D16. Is the number a) 111...1 (nine 1's) divisible by 9?

b) 111...1 (twenty seven 1's) by 27?

c) Generalise the statements obtained and prove the general statement.

D17. The sum of its digits is subtracted from a positive integer, and then one digit from the resulting difference is crossed out. The sum of the remaining digits of the difference equals 131. What digit was crossed out?

D18. Prove that the number $\overline{abcd}$ is divisible by 99 if and only if the number $\overline{ab} + \overline{cd}$ is divisible by 99.

D19. Prove that if $\overline{abc}$ is divisible by 37, then $\overline{bca} + \overline{cab}$ is also divisible by 37.

D20*. Find, without direct calculations, whether

a) 256905940884 is divisible by 4930496;

b) 140359156002848 is divisible by 4206377084.

D21*. a) Replace the same letters in the word REACHIEVEMENT by the same digits and different letters by different digits. Will the resulting number be a prime?

b) The same problem for the word SUPERREGENERATOR.

D22*. A numerical sequence is constructed: its first term is equal to 3^{2010} and each subsequent term, beginning with the second one, is equal to the sum of the digits of the previous term. Find the tenth term of this sequence.

D23*. Find the largest positive integer from which it is impossible to get a number divisible by 11 by crossing out some digits.

D24. Find all the numbers whose division by 7 yields a quotient equal to the remainder.

D25. Mom sent Alex to the store to buy bottles of yoghurt for 22 rubles each, as many as possible. Using the change, Alex wants to buy lollipops that cost 5 rubles apiece for himself. What is the largest number of lollipops that he can buy?

D26. Alan noticed that when dividing a number a by a number b with remainder: $a = b \cdot q + r$, one can swap b and q. Therefore, he believes that when dividing a by q, the quotient is b, and the remainder is r. When does this method work?

D27. When dividing a number m by 13 and 15, Peter obtained the same quotients, but with different remainders 8 and 0, respectively. Find the number m.

D28. If one subtracts 6 from a certain three-digit number, then the resulting number will be divisible by 7, if one subtracts 7, then it will be divisible by 8, and if one subtracts 8, then it will be divisible by 9. Find this number.

D29. a) Peter claims that when he puts nuts in heaps of 9 there remain 2 nuts and when he puts nuts in heaps of 6, 1 nut is left. Is Peter mistaken?

b) Mary puts nuts first in heaps of 3, then in heaps of 6, and then in heaps of 9. The sum of the leftovers turns out to be 15. Peter claims that he can use these data to find each leftover. Is Peter mistaken?

D30. When laying out books in stacks of 2 books, there remains one book, but when the books are laid out in stacks of 3, two books remain. How many books will be left if we arrange them in stacks of six?

D31*. Find a four-digit number that under division by 131 gives the remainder 112 and when divided by 132 gives the remainder 98.

D32. In a certain year, no month had a certain day as Sunday. What is the number of that day?

D33. Is there a power of 2 from which it is possible to get another power of 2 by interchanging its digits?

D34. Piglet and Pooh were given identical boxes of chocolates and instructed to put them on plates. Piglet spread out his box on 6 plates in equal amounts and took the rest, which was less than 6, for himself. Pooh did the same with 7 plates.

After Pooh persuaded Piglet to give him all the chocolates from one plate, he had 16 chocolates. How many chocolates does Piglet have?

D35. Prove that the rebus

$$\text{POLYGRAM} - \text{ROPMALYG} = 2013 \cdot 2014$$

has no solution.

D36. Find all the values of the digits x and y for which the number $\overline{84x5y}$ is divisible by 198.

D37. Using the uniqueness theorem for division with remainder, prove that any positive integer can be written in any positional number system and, moreover, in a unique way.

D38. Find the smallest natural number that gives the remainder 22 when divided by the sum of its digits.

D39. Is it possible to obtain the square of a positive integer using only the digits 2, 3, 7, 8 (possibly, several times)?

D40. Is each of the following numbers prime or composite:

a) 3999991?

b) 1000027?

c) $9^{10} + 6^{10} + 4^9$?

D41. In the Guinness Book of Records, it is written that the largest known prime is $23021^{377} - 1$. Is this a typo?

D42. Find all primes p for which $p + 10$ and $p + 14$ are primes.

D43. *The Sieve of Eratosthenes.* Eratosthenes begins by writing out the numbers of the natural sequence from 2 to some large N and selects the value of the variable $p = 2$. He then crosses out all the numbers in the list which are multiples of p, but greater than p itself. Next, he selects the first uncrossed number greater than p, puts the variable p equal to this number, and repeats his crossing-out procedure. a) What numbers remain at the end? b) At what number can the crossing-out procedure be stopped? See the presentation in the Wikipedia article "Sieve of Eratosthenes".

D44. For what values of n can the sum of n consecutive natural numbers be a prime?

D45. Let us call a number *primary* if it is a power of a prime (for example, 7^1 or 13^4). Find the longest chain of consecutive primary numbers.

D46. Four odd numbers are such that, in any pair, the larger number is divisible by the smaller one and all quotients are different. Prove that there is at least one number among them greater than 100.

D47. Is it true that all numbers of the form $2 \cdot 3 \pm 1$, $2 \cdot 3 \cdot 5 \pm 1$, $2 \cdot 3 \cdot 5 \cdot 7 \pm 1$, ..., $p_1 \cdot p_2 \cdot \ldots \cdot p_k \pm 1$ are prime? Here $p_1 = 2 < p_2 < p_3 < \ldots < p_k$ are consecutive primes in increasing order.

D48. Are there ten consecutive positive integers, the first of which is a multiple of 3, the second, a multiple of 5, the third, a multiple of 7, the fourth, a multiple of 9, ..., the tenth, a multiple of 21?

D49. Are there 50 natural numbers none of which is divisible by the other, and the product of any two of them is divisible by any one of the remaining numbers?

D50. For what positive integers n is the number a) n^2+n, b) $|n^2-4|$, c) (the Sophie Germain problem) n^4+4, d) $2^{4n+2}+1$ prime, and for what positive integers is it composite?

D51. Can the polynomial $1 + x + x^2 + \ldots + x^{p-1}$, where p is a prime, be decomposed into the product of two polynomials with integer non-negative coefficients?

D52. The roots of the equation $x^2 + ax + 1 = b$ are nonzero integers. Prove that the number $a^2 + b^2$ is composite.

D53. Devise a three-dimensional geometric interpretation for the greatest common divisor and the least common multiple of *three* numbers a, b, c.

D54. What may $(n, n + 12)$ be equal to?

D55. The programmer Alex wrote a program that finds the LCM of all numbers from 1 to 100. But the hacker Peter erased the numbers from 1 to 50, and now the program counts the LCM of all numbers from 51 to 100. How will the answer change?

D56. What may $[n, n + 1, n + 2]$ be equal to?

D57. Find formulas that give all possible pairs of coprime numbers with difference a) 2; b) 3.

D58. Reduce the fraction $377/261$ by first calculating the GCD by means of Euclid's algorithm.

D59. Prove that for any positive n, the fraction $\dfrac{10n+2}{6n+1}$ is irreducible.

D60. Find the obviously equal quantities among (a, b), (a, a), $(a, a+b)$, $(a, a-b)$, (b, b).

D61. An automatic device can cut off a square from any rectangle with a side equal to the smaller side of the rectangle. Peter cut the rectangle into two large squares, three smaller ones, and five smallest ones with a 10 cm side. Find the dimensions of the original rectangle.

D62*. a) Prove that $(a, b) = (13a + 8b, 5a + 3b)$.

b) Continue the above equality into a chain.

D63. Find

a) $(2^{100} - 1, 2^{120} - 1)$;

b*) $(2^a - 1, 2^b - 1)$.

D64. a) Find $(\underbrace{111...11}_{100 \text{ ones}}, \underbrace{111...11}_{90 \text{ ones}})$.

b*) Generalise the result.

D65*. There is a chocolate bar in the shape of a regular triangle of side n; it is divided by grooves into small equal triangles of side 1 (each side is divided into n equal parts, the dividing points on each pair of sides being connected by lines parallel to the third side). There are two players moving in turn. In each move, the player can break off a triangular piece from the chocolate bar (along some groove), eat it, and pass the rest to the opponent. Whoever gets the last piece, a triangle with side 1, is the winner. The one who can't make a move loses ahead of time.

For each n, find out which of the players can always win no matter how the opponent plays?

D66. The bad boy Peter cut out the sheet with the mark "very poor" from his school diary and cut it up into 3 or 5 parts (pieces). He took some of the resulting parts again and cut them up into 3 or 5 parts, and so on until he got bored. Can Peter obtain exactly a) 60 parts, b) 61 parts?

D67. Devise a Diophantine equation in non-negative integers that has exactly

a) one solution;

b) two solutions;

c) n solutions.

D68. Solve the equation $65x - 43y = 2$ in positive integers x and y.

D69. a) Find at least one solution in positive integers of the system

$$\begin{cases} x + y + z = 12, \\ 28x + 30y + 31z = 365. \end{cases}$$

b) Find all the solutions of this system.

D70. Find all positive integers lying between 1 and 100000 that are divisible by 73 and give the remainder 1 when divided by 1000.

D71. A floor of width 3 m must be covered with boards whose width is 11 cm and 13 cm without gaps between them. How many boards of each size are needed?

D72. Solve the equation $2x + 3y + 5z = 11$.

D73. *The Fibonacci problem.* William bought 30 birds for 30 coins. In this purchase, 1 coin was paid for each of three sparrows, also 1 coin for each of two turtledoves and, finally, 2 coins for each pigeon. How many birds of each breed did he buy?

D74. An amount of \$500 is in the bank. Two operations are allowed: take \$300 from the bank or put in \$198. These operations can be performed many times; however, there is no spare money, except the amount initially in the bank. What is the maximal amount that can be taken from the bank and how does one get it?

D75*. Find the smallest natural number that can be represented in exactly two ways as $3x + 4y$, where x and y are positive integers.

D76. It is known that $56a = 65b$. Can the number $a + b$ be prime?

D77. Solve the following equations in integers:

a) $x^2 - y^2 = 17$;

b) $x^2 = y^2 + 2010$.

D78. Three automata print pairs of integers on cards. After reading any card, each automaton issues a new card: after reading a card with the pair $\{m, n\}$, the first machine produces the card with $\{m - n; n\}$, the second one, the card with $\{m + n; n\}$, and the third one, the card with $\{n, m\}$. Suppose the initial card contained the pair of numbers $\{20; 11\}$. Is it possible to get a card with a) $\{12; 21\}$; b) $\{31; 13\}$ by using the automata in any order?

D79. The sum and product of two integers are multiples of p. Is it true that each of these numbers is a multiple of p if a) p is prime? b) p is composite?

D80. We know that a rectangle on square-lined paper consisting of n unit squares must have dimensions $1 \times n$ if n is a prime (see Problem 4.1). Let us generalize this problem. We draw several figures (polyominos, not necessarily congruent) consisting of n unit squares each such that they can be made into a rectangle without spaces and overlaps. Is it true that such a rectangle can be cut into $1 \times n$ rectangles if a) n is prime, b) n is composite?

D81. Find the smallest natural number which is not a divisor of $50!$.

D82. Determine the form of a number n (prime or composite) if it is known that $(n - 1)! + 1$ is divisible by n.

D83*. Find all numbers n such that the number $(n - 1)!$ is not divisible by n^2.

D84. Are there five two-digit composite numbers any two of which are coprime?

D85. a) Tom and Paul found a pack of eleven ruble banknotes each lying on the sidewalk. In a cafe, Thomas drank three glasses of tea, ate four rolls, and five bagels. Paul drank nine glasses of tea, ate one roll and four bagels. A cup of tea, a roll, and a bagel cost an integer number of dollars. It turned out that Paul could pay with eleven dollar banknotes without change. Show that so can Tom.

b) The integers t, c, and b are such that $9t + c + 4b$ is a multiple of 11. Is it true that $3t+4c+5b$ is a multiple of 11?

D86. The sum of the house numbers on one side of the block is 247. (Note that houses on one side of the street have odd numbers, while those on the other side are even-numbered.) What is the number of the seventh house from the corner?

D87. At the end of the spring term, Eddie wrote out his current marks for singing in a row and put the multiplication sign between some of them. The product of the resulting numbers turned out to be equal to 2007. What mark did Eddie get for singing at the end of the term? (The music teacher marks 2 for "very poor", 3 for "poor", 4 for "good", and 5 for "very good".)

D88. Is it possible to delete one of the factorials from the product $1! \cdot 2! \cdot \ldots \cdot 100!$ so that the product of the remaining factorials is the square of an integer?

D89. a) Prove that if a number has exactly 6 divisors, then it has the form p^5 or the form pq^2, where p and q are primes.

b) A number has exactly N divisors. Describe its factorization into primes.

D90. When the number a is multiplied by 2, the number of its divisors increases by 20%. a) Prove that a is divisible by 16, but not divisible by 32. b) How will the number of divisors increase if a is multiplied by 4?

D91. Find a positive integer of the form $n = 2^x \cdot 3^y \cdot 5^z$, if half of it has 30 less divisors, a third of it, 35 less divisors less, and a fifth, 42 less divisors than the number itself.

D92. Find a number which is a multiple of 12 and has fourteen divisors.

D93. Find a number equal to twice the number of its divisors.

D94. a) Prove that, among the numbers from 1 to a (inclusive), there are $[a/b]$ numbers divisible by b. *Here and further, $[x]$ is the integer part of the number x.*

b) Prove that the number 2 occurs in the factorization of $n!$ into primes with power exponent

$$k = \left[\frac{n}{2}\right] + \left[\frac{n}{4}\right] + \left[\frac{n}{8}\right] + \dots .$$

c) For what values of n is $n!$ divisible by 2^n?

d) What is the greatest power of 2 by which the product of all the natural numbers from $n+1$ to $2n$ is divisible?

e) Generalising the formula from item b), prove that the product of n consecutive numbers is divisible by $n!$ (see Problems 1.6 and 2.12).

D95*. Seventeen two-digit numbers were written on the blackboard. A mathematician chose one of them and raised it to the hundredth power. It turned out that the resulting number is divisible by each of the remaining sixteen. Is it true that it is also divisible by their product?

D96. Using the result of Problem 8.4, prove the formula $(a,b)[a,b] = ab$.

D97. a) Does the formula

$$(a,b,c)[a,b,c] = abc$$

hold?

b) What inequality will always hold for the numbers $(a,b,c)[a,b,c]$ and abc?

c) Express (a,b,c) in terms of a, b, c, $[a,b]$, $[b,c]$, $[a,c]$, $[a,b,c]$.

d) Express $[a, b, c]$ in terms of a, b, c, (a, b), (b, c), (a, c), (a, b, c).

D98. a) By what inequality are $\varphi(a)$, $\varphi(b)$, and $\varphi(ab)$ related if a and b are *not* coprime?

b) By what inequality are $\tau(a)$, $\tau(b)$, and $\tau(ab)$ related if $\tau(n)$ is the number of divisors of n.

D99. Let us write out in a row all the proper fractions with denominator n and make all possible cancellations. For example, for $n = 12$, the following sequence of numbers will be obtained:

$$\frac{0}{12}, \frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{11}{12}.$$

How many fractions with denominator d will be obtained if d is a divisor of the number n?

D100. Prove the Gauss identity:

$$\sum_{d|n} \varphi(d) = n,$$

where $\varphi(\cdot)$ is the Euler function and the sum is taken over all the divisors of the number n.


Hints

Answers and Hints

D1. Answer: Peter was mistaken.

If a and b are divisible by c without remainder, then their sum is also divisible. If only one of the numbers a and b is divisible by c, then the sum is not divisible. If none of the numbers is divisible, then nothing can be said about the sum. Thus, here either 0, or 1, or 3 divisions without remainder are possible.

D2. a) Statement: a number of the form $\overline{aaa}$ is divisible by 37. Indeed, $\overline{aaa} = 111a = 37 \cdot (3a)$.

b) Generalization: numbers of the form $\overline{abcabc} = 1001\overline{abc}$ are divisible by 77, because $1001 = 7 \cdot 11 \cdot 13$.

D3. Answer: no.

Show that either the sum or the difference is greater in absolute value than each of the given numbers.

D4. Answer: no.

Assume the converse: let the desired set be obtained. Let us exchange every large coin for ducats. Then, in the end, we will get one million ducats. But the number of coins increases with each step by a multiple of 3 (more precisely, by 9, 99, or 999), but eventually it will have increased by half a million, which is not a multiple of 3. A contradiction.

D5. Answer: no.

Since there is an odd number of stones in each heap at the beginning, then, in the first step, we can only combine some pair of heaps into one. If we combine the first two heaps, then we obtain 100 and 5 stones. If we combine the second and third heaps, then we obtain 51 and 54 stones. If the first and third heaps are combined, then we obtain 56 and 49 stones. Note that, in all three cases, the numbers of stones have the common divisors 5, 3, and 7, respectively. This means that, performing further divisions, we will not be able to divide the groups into heaps smaller than 5, 3 or 7 stones, respectively (This can be proved rigorously by using the fact that 2 is coprime to 3, 5, 7.)

D6. It is convenient to think not of each basket separately, but of all of them. Summing up the first condition over all baskets, we find that there are 5 times more plums than apples. Similarly, summing up the second condition, we find that there are 5 times more apples in total than pears. Therefore, there are in all 31 times more fruits than pears.

D7. Answer: for any n which is multiples of 3.

Note that if n is a multiple of 3, then it is possible to combine the vertices of the triangle with some vertices of the n-gon, and the triangle will be covered. Suppose that the triangle is covered. If the circumscribed circles of the triangle and the polygon do not coincide, then the arc of the circumscribed circle of the triangle greater than a semicircle will be outside the circumscribed circle of the polygon. The vertex of the triangle will then fall on this arc and remain uncovered. If the circles coincide, the vertices of the triangle must fall on the vertices of the polygon, and this is only possible if n is a multiple of 3.

D8. Note that, as in Problem 1.8, ab is divisible by $(ab-cd)^2$. The same can be said about cd. Then $ab - cd$ is divisible by $(ab - cd)^2$. Hence $ab - cd = k(ab - cd)^2$, and thus we have $1=k(ab-cd)$. Therefore, $k=1$, $ab-cd=1$ or $k=-1$, $ab-cd=-1$.

D9. Answer: both tests are false.

a) For example, the number 9 is a multiple of 3 and 9, but not of 27. Alex made a mistake by applying the divisibility test to the product for *non-coprime divisors*. (By the way, it is not difficult to prove that if a and b are not coprime, then there exists a number n which is a multiple of a and b, but not ab.)

b) $9981 \not\vdots\, 27$.

D10. Answer: two numbers.

The last digit must be 0 or 5, and the sum of the digits is a multiple of 9.

D11. Answer: yes.

It is necessary that any such number be divisible by 9. Find all the options and check by longhand whether they are divisible by 27.

D12. Answer: 6.

The given number is divisible by 9.

D13. Answer: 2222232.

In order for the code number to be divisible by 4, it must end in 32.

D14. It is easy to see that n^2 ends in 6 only if n ends in 4 or 6. Therefore, n is divisible by 2. But then n^2 is divisible by 4. By the divisibility test, the last two digits can be 16, 36, 56, 76, and 96.

D15. Answer: a) yes, b) no.

Write out the number in decimal form.

D16. Answer: a) yes, b) yes.

Generalization: a number consisting of 3^n digits 1 (or other identical digits) is divisible by 3^n. In fact, $111 \vdots 3$. Next, $111111111 = 111 \cdot 1001001$, where the second factor is divisible by 3 on the basis of the divisibility test. Similarly, the number 111...1 (27 ones) is decomposed into the factors 111111111, a multiple of 9, and a multiple of 3. And so on.

D17. Answer: 4.

When subtracting the sum of its digits from a number, a multiple of 9 is obtained. The sum of digits of the number 131 is equal to 5, which means that 4 was crossed out.

D18. Note that $\overline{abcd} - \overline{ab} - \overline{cd} = 99 \cdot \overline{ab}$.

D19. Let us add all three numbers:

$$\overline{abc} + \overline{bca} + \overline{cab} = 100a + 10b + c + 100b + 10c + a + 100c + 10a + b = 111a + 111b + 111c.$$

Since 111 is a multiple of 37, it follows that the sum is a multiple of 37. By assumption, the first term is divisible by 37, and hence the sum of the other terms is also divisible by 37.

D20. Answer: a) no, b) no.

a) Note that the divisor is divisible by 8, but the dividend is not.

b) Express the divisor as

$$4206377084 = 42 \cdot 10^8 + 63 \cdot 10^5 + 77 \cdot 10^3 + 84.$$

Each of the terms is divisible by 7, and hence the sum is also divisible by 7. Similarly, the number 140359156002848 can be expressed as the sum of terms all of which, with the exception of the last one (48), is divisible by 7. This means that the number is not divisible by 7.

D21. a) **Answer:** No.

Let us count the letters in the word REACHIEVEMENT. The letter E appears 4 times, each of the other 9 letters appear once. This means that all digits will appear once, but one of the digits (the one corresponding to the letter E) will appear 3 more times. The sum of all digits from 0 to 9 equals 45, and so is divisible by 3. The sum of three identical digits is divisible by 3. Hence, no matter how we replace letters by digits in the word REACHIEVEMENT, the sum of these digits will be divisible by 3. Therefore, by the divisibility by 3 test, the obtained number will be divisible by 3. But the only prime number divisible by 3 is 3 itself, and our number is certainly greater than 3, so the obtained number cannot be prime.

b) **Answer:** No.

There are ten different letters in the word SUPERREGENERATOR, the letter E appears 4 times, the letter R appears 4 times, the other letters appear once each. The rest of the argument is similar to that in item a) and is left to the reader.

D22. Answer: 9.

If a number is divisible by 9, then the sum of its digits is also divisible by 9. Since 3^{2010} is divisible by 9, it follows that all the terms of the given sequence are divisible by 9. Let us estimate their values: $3^{2010} = 9^{1005} < 10^{1005}$, and so there are no more than 1005 digits in the original number. Therefore, the second term of the sequence is not greater than $9 \cdot 1005 < 10^4$, that is, it has 4 digits at most. Then the third term of the sequence is not greater than $9 \cdot 4 = 36$, and the fourth is less than 18. Since the fourth term, like the previous ones, is divisible by 9, it is equal to 9. This means that all the subsequent terms are equal to 9.

D23. The number must not contain the digit 0, because, otherwise, all the other digits can be crossed out, and 0 is divisible by 11. Also, there must not be any identical digits, because, otherwise, we can cross out all the other digits and get a number which is a multiple of 11. The largest number satisfying these requirements contains all 9 digits in decreasing order: 987654321. Let us show that it satisfies the assumptions of the problem. Let us assume that, after crossing out $n \geqslant 0$ digits from 987654321, we obtain the number

$$\overline{a_{2k}a_{2k-1}...a_2a_1},$$

in which $a_{2k} > a_{2k-1} > ... > a_2 > a_1$ (if the number of digits in the resulting number is odd, then we will write 0 at the end, which will not affect the divisibility by 11). Then

$$(a_{2k} - a_{2k-1}) + (a_{2k-2} - a_{2k-3}) + ... + (a_2 - a_1) > 0,$$
$$a_{2k} - (a_{2k-1} - a_{2k-2}) - (a_{2k-3} - a_{2k-4}) - ... - a_1 \leqslant a_{2k} \leqslant 9.$$

Therefore, the number

$$a_{2k} + a_{2k-2} + ... + a_2 - a_{2k-1} - a_{2k-3} - ... - a_1$$

is not divisible by 11, which means that the number

$$\overline{a_{2k}a_{2k-1}...a_2a_1}$$

is also not divisible by 11.

D24. Answer: $N = 0, 8, 16, 24, 32, 40, 48$.

Denote the quotient by c. Then the given number can be written $N = 7c + c = 8c$. At the same time, c runs through all values from 0 to 6.

D25. The largest change was less than 22 rubles. Therefore, the largest number of lollipops will be 4.

D26. Answer: the method works if $r < b$ and $r < q$. Otherwise, some of the entries will not be read as a division with remainder.

D27. Answer: $m = 60$.

Solve the equation $m = 13k + 8 = 15k$.

D28. Answer: 503. Consider the number greater by 1 than the desired number. Use the fact that 7, 8, and 9 are coprime.

D29. a) Assume that Peter is right, and let us put the nuts into heaps of 3. Then, by virtue of the first condition, 2 nuts must remain and, by virtue of the second condition, only 1. Hence Peter is mistaken.

b) Under division by 3, 6, and 9, the greatest remainders will be 2, 5, and 8. Their sum is exactly 15. Therefore, Peter is right.

D30. Answer: 5.

Let N be the number of books. Then $N = 2x + 1 = 3y + 2$. Multiplying the first equality by 3, we obtain $3N = 6x + 3$. Multiplying the second equality by 2, we obtain $2N = 6y + 4$. Let us express N from the last two equalities:

$$N = 3N - 2N = 6(x - y) - 1 = 6(x - y - 1) + 5.$$

Thus, the remainder is 5.

Here is another way to solve the problem. Since 2 books remain after the books have been put in stacks of 3, it follows that either 2 or 5 books remain after the books have been put in stacks of 6 (see the solution of Problem 3.9). It follows from the first condition that the number of books is odd; therefore, 2 cannot be the remainder.

Finally, the shortest solution (although difficult to generalise): let's add another book; then the books are put in stacks of 2 books and of 3 books without remainder. By the coprime divisor theorem, $N + 1$ is divisible by 6 without remainder; then N has the remainder 5 under division by 6.

D31. Answer: 1946.

Let N be the desired number. By assumption, we have $N = 131k + 112 = 132l + 98$, where k and l are positive integers. Besides, $N < 10\,000$, and hence

$$l = \frac{N - 98}{132} < \frac{10\,000 - 98}{132} < 76.$$

Next, $131k + 112 = 132l + 98$, and so $131(k - l) = l - 14$. Therefore, if $k \neq l$, then $|l - 14| \geqslant 131$. But $l < 76$, and hence $k = l$ and $l - 14 = 0$. Thus,

$$N = 131 \cdot 14 + 112 = 132 \cdot 14 + 98 = 1946.$$

D32. Answer: 31.

Prove that during any year each of the numbers from 1 to 30 (corresponding to days of the month) can occur any day of the week. Don't forget about leap years.

D33. Answer: no.

Numbers obtained from each other by interchanging their digits have the same remainder when divided by 9. Consider the remainders in the division of powers of 2 by 9 and verify that the powers with the same remainder must be more than 10 times greater.

D34. Answer: two chocolates.

Suppose that N is the number of chocolates in the box, a is the number of chocolates on the plate for Piglet, b chocolates are on the plate for Pooh, m is Piglet's remainder and k is Pooh's remainder. Therefore, we have the system

$$6a + m = N, \quad 7b + k = N, \quad a + k = 16.$$

Let us add the first and third equations and then subtract the second, obtaining

$$7(a - b) + m = 16.$$

Thus, $16 - m \mathrel{\vdots} 7$. Since $m < 6$, we obtain $m = 2$. Note that the number of chocolates in the box may differ.

D35. Note that the same set of letters is repeated in both words. Therefore, the sum of the digits in both numbers is the same, and they have the same remainder when divided by 9. Therefore, their difference must be divisible by 9. However, the number $2013 \cdot 2014$ is not divisible by 9.

D36. Answer: $x = 1$, $y = 0$.

Consider the factorization of 198 into coprime factors: $198 = 11 \cdot 2 \cdot 9$. By the divisibility by 9 test, we find that $8+4+x+5+y = 17+x+y \,\vdots\, 9$. By the divisibility by 11 test, we find that $8-4+x-5+y = -1+x+y \,\vdots\, 11$. Only $x+y=1$ from the interval $0<x+y<18$ is suitable. Therefore, one of the numbers is 0 and the other is 1. Using the divisibility by 2 test, we see that the digit y must be even, that is, $y = 0$, and hence $x = 1$.

D37. To write a number in the positional number system with base q, the number is divided by q and the remainder is written as the last digit. Next, the incomplete quotient is divided by q and the remainder is written as the next-to-last digit, and so on.

D38. Answer: 689.

The sum of the digits must be at least 23, that is, the number must have more than two digits. Of three-digit numbers, the smallest with such a sum of digits is 599 (not suitable) and 689 (suitable).

D39. Answer: no.

Prove by enumerating the remainders of squares divided by 10 that a square cannot end with numbers 2, 3, 7, 8.

D40. Answer: a), b), c) are composite.

Let us use the shortened multiplication formulas:
a) $3999991 = 4000000 - 9 = 2000^2 - 3^2 = 1997 \cdot 2003$;
b) $1000027=1000000+27=100^3+3^3=103\cdot(100^2-100\cdot3+3^2)$;
c) $9^{10} + 6^{10} + 4^9 = (3^{10} + 2^9)^2$.

D41. Answer: a typo.

Think about what digit this number ends with. (In fact, the correct number is actually $2^{3021377} - 1$.)

D42. Answer: $p = 3$.

As in Problem 4.4, for $p > 3$, p is divided by 6 with remainders 1 or 5. If the remainder is 1, then $p + 14$ is composite, and if the remainder is 5, then $p + 10$ is composite.

D43. a) All primes from 2 to N will remain. The crossing-out removes all numbers that are multiple of the prime p, except p itself. This means that all composite numbers will be deleted.

b) Note that numbers can be crossed out beginning with the number p^2, because all composite numbers smaller than p^2 will already be crossed out by this time. And, accordingly, we can stop the algorithm when p^2 becomes greater than n. Compare this solution with that of Problem 4.2.

The sieve of Eratosthenes is the oldest fast method for obtaining the sequence of primes. In the era of Eratosthenes, numbers were written on wax tablets and, instead of crossing out, a hole was pierced, hence the name of the method.

D44. Answer: at $n = 2$.

The sum of two consecutive positive integers can be a prime: $2 + 3 = 5$. The sum of three cannot be prime, because it is divisible by 3 and is greater than 3. The sum of four also cannot be prime, because it is even and greater than 2. Let us prove that no further sum can be prime. Let the first number be k, then the last one will be $k + n - 1$. The sum of these numbers is the sum of the arithmetical progression

$$\frac{k + (k + n - 1)}{2} n = \frac{n}{2}(2k + n - 1).$$

Further, we consider this expression separately for even n and for odd n, and prove that, for $n > 2$, it can be expressed as the product of two integers greater than 1.

D45. Answer: 2, 3, 4, 5.

D46. Let the numbers $a < b < c < d$ satisfy the assumptions of the problem. By assumption, the quotients $\frac{b}{a}$, $\frac{c}{b}$, $\frac{d}{c}$ are various odd numbers greater than 1. Their product is not less than $3 \cdot 5 \cdot 7 = 105$, and hence $d = a \cdot \frac{b}{a} \cdot \frac{c}{b} \cdot \frac{d}{c} \geqslant 1 \cdot 105 > 100$.

We can prove in the same way that $c = a \cdot \frac{b}{a} \cdot \frac{c}{b} \geqslant 1 \times 3 \cdot 5 = 15$, $b \geqslant 3$ (and, of course, $a \geqslant 1$). Replacing all the non-strict inequalities by equalities, we obtain the four-tuple (1, 3, 15, 105) giving the answer and being, in a sense, minimal.

D47. Answer: no.

Examples:

$$2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19;$$
$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509.$$

The fact that a number is not divisible by the first few primes does not imply that it is not divisible by a prime greater than those primes.

D48. Answer: Yes, there are.

We will construct these numbers just as in the solution of Problem 4.9: consider a number N such that $N + 3$ is divisible by 3, $N + 5$ is divisible by 5, ..., $N + 21$ is divisible by 21. This is true, for example, for $N = 3 \cdot 5 \cdot \ldots \cdot 21$. However, the neighboring resulting numbers differ not by 1, but by 2. We then note that they are all even, and so we take $(N + 3)/2$, $(N + 5)/2$, ..., $(N + 21)/2$ as an example justifying the answer. (Here we have used the factor cancellation theorem; see Problem 6.11.)

D49. Answer: yes.

An example is constructed just as in problem 4.3.

D50. Answer: a) prime for $n = 1$ and composite for $n \geqslant 2$; b) prime for $n = 1; 3$ and composite for $n \geqslant 4$; c) prime for $n = 1$ and composite for $n \geqslant 2$; d) composite for all positive n.

Solution. c) Note that

$$\begin{aligned} n^4 + 4 &= (n^4 + 4n^2 + 4) - 4n^2 \\ &= (n^2 + 2)^2 - (2n)^2 = (n^2 + 2n + 2)(n^2 - 2n + 2). \end{aligned}$$

(Sometimes the sum of squares can also be decomposed into factors!) When substituting any number into this equality, we obtain a factorization of the number n^4+4. If both factors differ from ± 1, then the number is composite. For $n = 1$, we have $5 = 5 \cdot 1$, which is prime. For $n \geqslant 2$, both factors are greater than 1, and hence the number is composite.

d) Indeed,

$$2^{4n+2} + 1 = 4^{2n+1} + 1 = (4+1)(4^{2n} - 4^{2n-1} + \ldots - 4 + 1).$$

For the number to be composite, it suffices for the second factor to be greater than 1. This is achieved when $n \geqslant 1$.

D51. Answer: no.

Assume the converse and substitute $x = 1$ into the decomposition.

This polynomial is called a *cyclotomic polynomial*. It turns out that it cannot be factored into the product of polynomials with either integer or rational coefficients.

D52. Let x_1 and x_2 be the roots of the trinomial. Then, by Vieta's theorem, $x_1 + x_2 = -a$, $b = 1 - x_1 x_2$. Therefore,

$$a^2 + b^2 = x_1^2 + x_2^2 + 2x_1x_2 + x_1^2x_2^2 - 2x_1x_2 + 1 = (x_1^2 + 1)(x_2^2 + 1).$$

For non-zero values of x_1, x_2, this equality gives the factorisation of the number $a^2 + b^2$ into factors other than 1.

D53. Consider the rectangular parallelepiped with edges a, b, c.

D54. Answer: 1, 2, 3, 4, 6, 12.

Note that $(n, n+12) = (n, 12)$.

D55. Answer: The answer will not change.

Prove that

$$[1, 2, 3, \ldots, 2n-1, 2n] = [n+1, n+2, \ldots, 2n].$$

Take into account the fact that it suffices to keep the greatest of the numbers $2k$ and k.

D56.

$$[n, n+1, n+2] = [[n, n+1], n+2] = [n(n+1), n+2] = \frac{n(n+1)(n+2)}{(n(n+1), n+2)}.$$

Further,

$$(n(n+1), n+2) = (n^2+n, n+2) = (|n^2+n-(n^2+2n)|, n+2) = (n, n+2) = 1 \text{ or } 2,$$

depending on the parity of n. Therefore,

$$[n, n+1, n+2] = n(n+1)(n+2) \quad \text{for odd } n,$$
$$[n, n+1, n+2] = \frac{n(n+1)(n+2)}{2} \quad \text{for even } n.$$

D57. a) All pairs of the form $(2n-1; 2n+1)$, where n is an integer (see Problem 5.7).

b) All pairs of the form $(3n-1; 3n+2)$ and of the form $(3n-2; 3n+1)$, where n is an integer.

D58. $377 = 261 \cdot 1 + 116$, $261 = 116 \cdot 2 + \boxed{29}$, $116 = \boxed{29} \cdot 4 + 0$. Therefore, $\dfrac{377}{261} = \dfrac{29 \cdot 13}{29 \cdot 9} = \dfrac{13}{9}$.

D59. $(10n+2, 6n+1) = (4n+1, 6n+1) = (2n, 4n+1) = (2n, 2n+1) = 1$.

D60. **Answer:** $(a, b) = (a, a+b) = (a, a-b)$.

D61. **Answer:** 160 cm by 370 cm.

Let us write Euclid's algorithm from end to beginning: $5 \cdot 10 = 50$, $50 \cdot 3 + 10 = 160$, $160 \cdot 2 + 50 = 370$.

D62. Consider the value on the right side. By Euclid's algorithm,

$$\begin{aligned}(13a+8b, 5a+3b) &= (8a+5b, 5a+3b) = (5a+3b, 3a+2b)\\ &= (3a+2b, 2a+b) = (2a+b, a+b) = (a+b, a) = (a, b).\end{aligned}$$

We can also continue this chain in the increasing direction. The coefficients will be equal to the consecutive Fibonacci numbers.

D63. a) **Answer:** $2^{20}-1$.

Divide $2^{120}-1$ by $2^{100}-1$ with remainder:

$$2^{120}-1 = (2^{100}-1) \cdot 2^{20} + 2^{20} - 1.$$

Acting further in a similar way, we obtain:

$$\begin{aligned}&(2^{120}-1, 2^{100}-1) = (2^{100}-1, 2^{20}-1) = (2^{80}-1, 2^{20}-1)\\ &= (2^{60}-1, 2^{20}-1) = (2^{40}-1, 2^{20}-1) = (2^{20}-1, 2^{20}-1) = 2^{20}-1.\end{aligned}$$

Note that the exponents in this equality are also "divisible with remainder".

b) **Answer:** $(2^p-1, 2^q-1) = 2^{(p,q)}-1$.

Moreover, here the number 2 can be replaced by an arbitrary number.

D64. a) **Answer:** $\underbrace{111\ldots11}_{10\text{ ones}}$.

$$(\underbrace{111\ldots11}_{100\text{ ones}}, \underbrace{111\ldots11}_{90\text{ ones}}) = (\underbrace{111\ldots11}_{90\text{ ones}} \cdot 10^{10} + \underbrace{111\ldots11}_{10\text{ ones}}, \underbrace{111\ldots11}_{90\text{ ones}})$$
$$= (\underbrace{111\ldots11}_{10\text{ ones}}, \underbrace{111\ldots11}_{90\text{ ones}}) = \underbrace{111\ldots11}_{10\text{ ones}},$$

because the last number is divisible by the next-to-last one.

b) In general,

$$(\underbrace{111\ldots11}_{k\text{ ones }1}, \underbrace{111\ldots11}_{l\text{ ones }1}) = \underbrace{111\ldots111}_{(k,l)\text{ ones }1}.$$

D65. Answer: if the number n is prime, then the second player wins; otherwise, the first player wins.

After the first move, an isosceles trapezium[1] is formed. Let us see what figures are formed in subsequent moves. Suppose that, after some move, one of the players gets a piece of chocolate in the form of an isosceles trapezium with a smaller base a and a greater base b (the side length of such a trapezium is equal to $b-a$). If that player (let us call him A) breaks off a triangle whose side is less than $b-a$, then the other player can break off a triangle with side 1, and the other player wins (see Fig. 1).

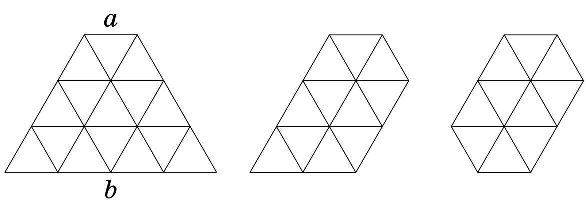


Fig. 1

[1]By a trapezium we mean a quadrilateral with two parallel sides of unequal length.

So, in this situation, A must break off a triangle with side $b - a$. After this move, there remains a parallelogram whose side lengths are a and $b - a$.

Now suppose one of the players got a piece of chocolate in the form of a parallelogram with sides a and b, $a < b$. Then, for similar reasons, that player must break off a triangle with side a. After that move, there remains an isosceles trapezium with bases $b - a$ and b.

Next, suppose one of the players was given a piece of chocolate in the form of a parallelogram with sides a and b ($a < b$), then, after two moves, that player will get a piece of chocolate in the form of a parallelogram with sides a and $b - a$.

Finally, suppose one of the players obtained a parallelogram with equal sides (that is, a rhombus), then that player has to move so that a triangle is formed after his move (see Fig. 2).

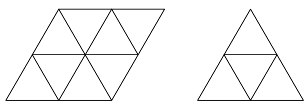


Fig. 2

Now let's outline the winning strategy for the second player for a prime n. For him, it suffices to break off the piece of largest size every time. Let us show that this strategy results in winning the contest. Let the first player break off a triangle with side k. After the second player's move, a parallelogram is formed with sides k and $n - k$. These numbers are coprime, because n is a prime. Further, after each move of the second player, a parallelogram will be formed (until eventually it becomes a rhombus). The side lengths of this parallelogram are coprime (if k and n are coprime, then k and $n - k$ are also coprime). Therefore, the side lengths of the rhombus (which are equal) are also coprime, but this means that the rhombus has side 1! From it, the first player will be forced to break off a triangle with side 1, after which the second player wins. If $n = 1$, then the first player has already won.

Now let the number n be composite. Denote by p any prime divisor of n. Let the first player first break off a triangle with side p, and then each time break off the largest piece. After a while, the second player will get a triangle with side p and, as discussed above, will lose in a few moves.

Note that the described process illustrates Euclid's algorithm.

D66. Answer: a) No, he couldn't, b) Yes, he could.

Note that when cutting a piece into 3 parts, 2 parts are added, and when cutting into 5 pieces, 4 parts are added. Therefore, the total number of parts is equal to $1 + 2x + 4y$, where x and y are the number of cuts of the sheet into the respective number of parts. Solving the Diophantine equation $1 + 2x + 4y = 60$ or 61, we obtain the answer.

D67. a) $x + y = 0$; b) $x + y = 1$; c) $x + y = n - 1$.

D68. Answer: $x = 4 + 43n, y = 6 + 65n$, where $n \geqslant 0$.

First, using the usual algorithm, we will find the following integer solutions: $x = 4 + 43n, y = 6 + 65n$, where n is an integer. Now let's select integer solutions from them. Solving the inequalities $x > 0$, $y > 0$, we obtain $n \geqslant 0$.

D69. a) **Answer:** $x = 1, y = 4, z = 7$.

There are 12 months in a year. One of them, February, consists of 28 days, four months (April, June, September, November) consist of 30 days each, the remaining 7 months consist of 31 days. Since there are 365 days in a year, we have

$$28 \cdot 1 + 30 \cdot 4 + 31 \cdot 7 = 365.$$

b) There is another solution in natural numbers, namely $x = 2, y = 1, z = 9$.

D70. Let us write the equation $73x = 1000y + 1$, that is, $73x - 1000y = 1$. Finding $(73, 1000)$ by Euclid's algorithm, we obtain the particular solution $x_0 = 137$, $y_0 = 10$. The general solution has the form $x = 137 + 1000n$, $y = 10 + 73n$, where n is an integer. Solve the inequality

$$1 \leqslant 73x \leqslant 100000 \Longleftrightarrow 1 \leqslant 10001 + 73000n \leqslant 100000$$
$$\Longleftrightarrow 0 \leqslant n \leqslant 1.$$

Calculating $73x$ for each of the two values of n, we obtain the answer: 10001 and 83001.

D71. Answer: 19 narrow boards and 7 wide ones or 6 narrow boards and 18 wide ones.

Suppose we have x boards 11 cm wide and y boards 13 cm wide. Then we have the equation $11x + 13y = 300$. A partial solution of that equation with 1 on the right-hand side is $(6; -5)$. Multiplying by 300, we obtain $x_0 = 1800$, $y_0 = -1500$. The general solution is $x = -13n + 1800$, $y = 11n - 1500$. Now we need to find a value of n such that both components are non-negative. From the inequality $x \geqslant 0$, we obtain $n \leqslant 138$ and, from the inequality $y \geqslant 0$, we get $n \geqslant 137$. Substituting $n = 137$, we obtain the answer: 19 narrow boards and 7 wide ones. Substituting $n = 138$, we obtain the other answer: 6 narrow boards and 18 wide ones.

D72. First, we guess a partial solution: $(1; 1; 1)$. Now we write out the homogeneous equation $2x + 3y + 5z = 0$. Let us rewrite that equation as $2(x + y + 2z) + y + z = 0$. Denoting the expression in parentheses by t (which is obviously an integer), we obtain the following system of equations: $2t + y + z = 0$ and $x + y + 2z = t$.

Let us express x and y in terms of z and t: $y = -2t - z$, $x = 3t - z$. To avoid confusion, let's put $z = u$, where u is a parameter. By letting t and u take arbitrary integer values, we obtain all possible tripes $(x; y; z) = (3t - u; -2t - u; u)$ satisfying the homogeneous equation. Adding together the particular solution of the inhomogeneous equation and the general solution of the homogeneous equation, we then obtain $x = 1 + 3t - u$, $y = 1 - 2t - u$, $z = 1 + u$.

Note that now the solution depends on two parameters! Generally speaking, an equation with two unknowns leaves one "degree of freedom", while an equation with three unknowns leaves two "degrees of freedom".

D73. Answer: 9 sparrows, 10 turtledoves, 11 pigeons.

D74. Answer: 498 dollars.

Note that $(300, 198) = 6$, that is, both operations change the amount of money outside the bank by a multiple of 6. And the largest number which is a multiple of 6 and does not exceed 500, is 498. Therefore it will not be possible to withdraw more than \$498.

One can withdraw \$498, in particular, as follows. The equation $300y - 198x = 6$ has the solution $x = 3$, $y = 2$. If we can withdraw, in some order, \$300 twice and put in \$198 three times, then we will withdraw exactly \$6. Suppose there are n dollars in the bank at some point. Remove \$300, put in \$198, remove \$300, and put in \$198 twice. It is easy to check that this sequence of operations is possible if $n \geqslant 402$. Repeating this 16 times, we will put \$404 in the bank. Now, having done the first three operations from the specified sequence, we will leave \$2 in the bank.

D75. Answer: 19.

It is necessary to choose a number k such that the Diophantine equation $3x + 4y = k$ will have two natural solutions. Solving this equation in integers and requiring that x and y be positive, we obtain the condition that there must be exactly two integer points in the interval $(k/4, k/3)$. The smallest such number is $k = 19$.

D76. Since the numbers 56 and 65 are coprime, by the factor cancellation theorem, we have $a = 65n$, and so $b = 56n$. Therefore, the number $a+b = 65n+56n = 121n$ is composite.

D77. a) **Answer:** $x = \pm 9, y = \pm 8$.

Factor the left and right sides and consider all possible options.

b) **Answer:** there are no solutions.

Let us rewrite the equation in the form

$$x^2 - y^2 = 2010 \iff (x-y)(x+y) = 2010.$$

Note that the right side is divisible by 2, but not by 4. However, the numbers in parentheses on the left side are both either even or odd.

D78. Note that all three automata preserve the common divisor of the numbers.

a) This is impossible, because the initial numbers are coprime, and the final numbers are multiples of 3.

b) Using the first and third automata, it is possible to implement Euclid's algorithm. Both the pair $\{20; 11\}$ and the pair $\{31; 13\}$ can be reduced to the pair $\{1; 1\}$, because they are both coprime. Since all the steps are reversible, the pair $\{20; 11\}$ can be reduced to the pair $\{31; 13\}$.

D79. Answer: a) This is true; b) This is true for composite numbers in which each prime factor occurs once, but not for other composite numbers.

D80. Answer: a) This is true for all prime n; b) false for any composite n.

a) Use the prime divisor theorem.

b) Let $n > 4$. Then n has a divisor greater than 2 and less than n; let's denote it by a. Then we can write $n = ab$, where $1 < b < n/2$. Let us place two $a \times b$ rectangles side by side so that they form the rectangle $a \times 2b$. This rectangle cannot be cut into rectangles $1 \times n$, because both sides of it are less than n.

For $n = 4$, let's take three tetramino figures: two of dimensions 1×4 and one of dimensions 2×2 and make a 2×6 rectangle out of them.

D81. Note that the prime 53 is not a divisor of the number 50!, because, otherwise, by the prime factor theorem, one of the factors of 50! would be divisible by 53, but this is impossible. On the other hand, it's clear that 50! is divisible by $3 \cdot 17 = 51$ and by $4 \cdot 13 = 52$ (because these pairs of numbers are coprime).

D82. Answer: The number is prime.

The number $(n-1)!$ is divisible by all numbers from 2 to $n-1$. Therefore, the number $(n-1)!+1$ is not divisible by any of these numbers. Thus, n is the smallest divisor other than 1 of the number $(n-1)!+1$. Hence, n cannot be composite (otherwise, there would exist prime divisors smaller than n).

It turns out that actually any prime n is suitable; indeed, if n is prime, then $(n-1)!+1$ is a multiple of n. This statement is called *Wilson's theorem* and is much more difficult to prove.

D83. Answer: 8, 9, as well as numbers of the form p and $2p$, where p is prime.

It is clear that, for a prime p, the numbers $n = p$ and $n = 2p$ satisfy the condition, because $(n-1)!$ is not divisible by p^2. It is also easy to see that 7! is not divisible by 8^2, nor 8!, by 9^2. Let us prove that, for the other valuies of n, the number $(n-1)!$ is divisible by n^2.

First case. Let n have at least two distinct divisors. Let us denote one of them by p. Then, among the numbers $1, 2, \ldots, n-1$, there exist at least $n/p-1$ numbers divisible by p. If n is divisible by p^k, but not by p^{k+1}, then we have

$$\frac{n}{p} - 1 \geqslant 2p^{k-1} - 1 \geqslant 2^k - 1 \geqslant 2k - 1.$$

If $n \neq 2p$, then at least one of the inequalities given above is strict. Hence, $n/p - 1 \geqslant 2k$, and $(n-1)!$ is divisible by p^{2k}. Since this is true for all p, it follows that $(n-1)!$ is divisible by n^2.

Second case. Let n be the power of a prime: $n = p^k$. Then $n/p - 1 = p^{k-1} - 1$. For $p \geqslant 5$, as well as for $p = 3$ and $k \geqslant 3$ or for $p = 2$ and $k \geqslant 5$, this number is not less than $2k$. Therefore, $(n-1)!$ is divisible by n^2. The case of $n = 2^4$ can be dealt with directly.

D84. Answer: No.

Among the prime factors of a composite two-digit number, there must exist single-digit numbers (the product of two non-one-digit numbers is at least a three-digit number).

Since there are only four one-digit primes (2, 3, 5, 7), then at least two of our two-digit numbers will have the same prime factor and they will not be coprime.

D85. a) If Paul ate and drank four times as much, then the sum of money would also be a multiple of 11, and it would have turned out to be 33 teas and 11 bagels more than Tom ate and drank. Therefore, Tom's portion also costs an integer number of dollars, a multiple of 11.

b) True. See item a).

D86. Answer: 19.

Let the first house from the corner of the block have the number p, and suppose the number of houses on one side of the block is equal to k. Then the sequence p, $p+2$, $p+4$, ..., $p+2(k-1)$ of numbers of these houses is an arithmetical progression. The sum of the first k terms of this progression is

$$\frac{p+p+2k-2}{2}k=(p+k-1)k.$$

By assumption, we have the equation $(p+k-1)k=247$. The prime factorization of the number 247 has the form $247=13\cdot 19$. Since $p\geqslant 1$, we have $p+k-1\geqslant k$, and hence $p+k-1=19$, while $k=13$, so that $p=7$. Consequently, there are 13 houses on one side of the block, and their numbering begins with 7. Thus, the seventh house (from any corner) has the number 19.

It is also possible to reason differently.

The sum of the numbers is odd, which means that there are odd numbers on the specified side of the block and the number of houses is odd. The sum of the numbers (the terms of the arithmetic progression) is equal to the product of the number of houses by the number of the middle house, and $247=13\cdot 19$. If the number of the middle house is 13, then 8 houses will not fit in front of it. Therefore, the number of the middle house is 19, and it is the seventh from the corner. (*The cases in which the average house number is* 1 *or* 247 *are discarded for obvious reasons*).

D87. Consider the factorization of the number 2007 into prime factors: $2007 = 3 \cdot 3 \cdot 223$. We could now conclude that Eddie's marks are two 2's and three 3's. But, in fact, it is still necessary to prove that there can be no other marks. Let us see how else we can factor 2007: $2007 = 9 \cdot 223 = 3 \cdot 669$.

Since there is no mark 9, these factorizations of the number 2007 could not have come from Eddie's marks. Since Eddie has more 3's than 2's, and the last mark, no matter how we rearrange the factors, is 3, we can expect that he will get the mark 3 at the end of the term.

D88. Answer: yes, we need to cross out 50!.

Let us see how many times each number from 2 to 100 occurs in our product. The number 2 occurs in all factorials beginning with the second, that is, 99 times; the number 3 occurs in all factorials beginning with the third, that is, 98 times, and so on; thus, the number n occurs $101 - n$ times in the product:

$$1! \cdot 2! \cdot \ldots \cdot 100! = 2^{99} \cdot 3^{98} \cdot 4^{97} \cdot \ldots \cdot 97^{4} \cdot 98^{3} \cdot 99^{2} \cdot 100.$$

In particular, all odd numbers in the product occur an even number of times and even numbers an odd number of times. Let us separate out the product of all even numbers with exponent 1:

$$\begin{aligned} 1! \cdot 2! \cdot \ldots \cdot 100! &= 2^{99} \cdot 3^{98} \cdot 4^{97} \cdot \ldots \cdot 97^{4} \cdot 98^{3} \cdot 99^{2} \cdot 100 \\ &= (2^{98} \cdot 3^{98} \cdot 4^{96} \cdot \ldots \cdot 97^{4} \cdot 98^{2} \cdot 99^{2}) \cdot (2 \cdot 4 \cdot 6 \cdot \ldots \cdot 98 \cdot 100). \end{aligned}$$

In the first parenthesis, all the exponents are even, which means that the product of the numbers in the first parenthesis is the square of an integer. The product of the numbers in the second parenthesis is $2 \cdot 4 \cdot 6 \cdot \ldots \cdot 98 \cdot 100 = 2^{50} \cdot 50!$. However, 2^{50} is the square of an integer. Therefore, if we delete 50!, then the remaining part of the product will be the square of an integer.

D89. b) The number N is equal to the product

$$(a+1)(b+1) \cdot \ldots \cdot (w+1),$$

where a, b, ..., w are the exponents of prime factors in the factorization. Therefore, to any factorization of the number N corresponds its own set of exponents in the factorization into primes.

D90. a) Let the number a be of the form 2^n. Then the divisors of the number a are of the form 1, 2, ..., 2^n and the divisors of the number $2a$ have the form1, 2, ..., 2^n, 2^{n+1}. Thus, there were $n+1$ divisors, but now there are $n+2$, that is, 1 more. We have

$$\frac{1}{n+1} = \frac{1}{5} \Rightarrow n = 4.$$

This implies the assertion of the problem.

Now let a be of the form $2^n b$, where b is an odd number with k divisors. Then a has $(n+1)k$ divisors, and $2a$ has $(n+2)k$ divisors (due to the multiplicativity of the number of divisors). Next, we argue just as in the previous paragraph.

We can also directly apply the formula for the number of divisors.

b) Answer: by 40%.

D91. Answer: $x = 6$, $y = 5$, $z = 4$.

D92. Answer: $2^6 \cdot 3$.

A number with 14 divisors has the form p^{13} or the form $p^6 q$, where p and q are prime. Since $12 = 2^2 \cdot 3$, it follows that only the second option is possible: the required number is $2^6 \cdot 3$.

D93. Answer: 8, 12.

Denote by n the desired number and by $\tau(x)$ the number of divisors of x. Note that, by assumption, n is a multiple of 2. Consider successively the cases $n = 2b$, $2^2 b$, $2^3 b$, $2^m b$, where b is odd. In each case, let's solve the equation $n = 2\tau(n)$. We will use the fact that, for the numbers 1 and 2, the number of divisors is equal to the number (1 or 2) itself and, for the numbers n greater than 2, the number of divisors is less than the number n itself. Also note that $\tau(ab) = \tau(a)\tau(b)$ for coprime a and b.

1. Let $n = 2b$. We have $2b = 2\tau(2b) \Leftrightarrow b = 2\tau(b)$, which is impossible, because b is odd.

2. Let $n = 2^2 b$. We have $2b = 3\tau(b)$. Note that $b = 3$ is a solution. Let us prove that there are no other solutions. It is clear that b is a multiple of 3. If $b = 3^k$, then we have $2{\cdot}3^k = 3{\cdot}(k+1)$, which is true only for $k=1$ (because, for $k>1$, the left side is greater than the right one). If $b = 3^k \cdot s$ (where s is not multiple of 3), then we have $2 \cdot 3^k s = 3 \cdot (k+1)\tau(s)$, and this equation also has no solutions, because $s > \tau(s)$ for $s > 2$.

3. Let $n = 2^3 b$. We have $b = \tau(b)$, which implies $b = 1$.

4. Let $n = 2^m b$, where $m > 3$. Then

$$2^m b = 2\tau(2^m b) = 2(m+1)\tau(b).$$

However, $2^m > 2(m+1)$ for $m > 3$. Also $b > \tau(b)$ for $b > 2$. Therefore, the equation has no solutions.

D94. b) In the factorization of $n!$, the number 2 occurs once for each even number in $n!$, also once for each number divisible by 4, and also once for each number divisible by 8, and so on.

c) **Answer:** $n!$ is not divisible for any n.

Use the inequality $[x] \leqslant x$ and the formula for the sum of an infinite arithmetic progression.

d) **Answer:** the product is divisible by 2^n, but not divisible by 2^{n+1}.

Find the exponents of the powers in which 2 occurs in the prime factorization of the numbers $n!$ and $2n!$.

e) Consider the product

$$(m+1)(m+2)\ldots(m+n) = \frac{(m+n)!}{m!}.$$

Express the power of each prime factor for $m!$, $n!$ and $(m+n)!$ and take into account the inequality

$$\left[\frac{a+b}{c}\right] \geqslant \left[\frac{a}{c}\right] + \left[\frac{b}{c}\right].$$

Another solution of problem D94, item e), can be obtained from the fact that the binomial coefficient

$$\binom{m+n}{n} = \frac{(m+n)!}{n!\,m!} = \frac{(m+1)(m+2)\ldots(m+n)}{n!}$$

is an integer by virtue of its combinatorial meaning.

D95. Answer: This is true.

Hints. 1. Let the selected number be m. Prove that m^{100} contains all the prime divisors of the remaining numbers, each with exponent not less than 100.

2. Prove that the exponent of any prime factor in any two-digit number does not exceed 6 (then, in the product of 16 numbers, it does not exceed 96).

D96. $p^{\alpha} \cdot p^{\beta} = p^{\min(\alpha,\beta)} \cdot p^{\max(\alpha,\beta)}$. And so with each prime factor.

D97. a) **Answer:** no.

For example, $(6, 10, 15)[6, 10, 15] = 1 \cdot 30 \neq 6 \cdot 10 \cdot 15$.

b) **Answer:** "$\leqslant$".

It suffices to study the case in which $a = p^{\alpha}$, $b = p^{\beta}$, $c = p^{\gamma}$, where $\alpha \leqslant \beta \leqslant \gamma$. Then $(a, b, c)[a, b, c] = p^{\alpha}p^{\gamma}$, and $abc = p^{\alpha+\beta+\gamma}$.

c), d)

$$(a, b, c) = \frac{abc[a, b, c]}{[a, b][b, c][a, c]}, \quad [a, b, c] = \frac{abc(a, b, c)}{(a, b)(b, c)(a, c)}.$$

Using the notation and assumptions of item b), we can verify these formulas by a direct substitutions.

D98. a) **Answer:** $\varphi(a)\varphi(b) < \varphi(ab)$.

b) **Answer:** $\tau(a)\tau(b) > \tau(ab)$.

D99. Answer: $\varphi(d)$.

D100. Use the result of the previous problem.

Appendix 1

Two Unsolved Problems about Primes

In number theory, there are problems with very simple formulations whose solutions are still unknown. It is useful to introduce students to such problems, in particular, so as to rid them of the illusion that “everything in mathematics is already discovered”.

1. Goldbach and Euler noticed that it is possible to represent any even number (except 2) as the sum of two primes. For example, $4 = 2 + 2$, $6 = 3 + 3$, $8 = 5 + 3$, $10 = 5 + 5$, $12 = 5 + 7$, $14 = 7 + 7$, $16 = 13 + 3$, $18 = 11 + 7$, ..., $100 = 97 + 3$, and so on. Goldbach’s conjecture has not yet been proved, although it has been verified up to $4 \cdot 10^{18}$. You can study experimentally (using a computer) the number of representations of the number $2n$ as the sum of two primes.

2. Prime numbers are often found in pairs (“twins”) p and $p + 2$. Such are 3 and 5, 11 and 13, 29 and 31, and so on. It follows from Problem 4.4 that all pairs of prime twins, except $(3; 5)$, have the form $(6n - 1; 6n + 1)$. Is there an infinite number of such “twins”? It follows from Problem 4.9 that, as primes increase, the gaps between them become wider, but it is still not known whether small gaps persist. In 2013, the mathematician Zhang Itan proved that there are infinitely many pairs of primes and the distance between which does not exceed 70 million. Over time, this distance was lowered down to 246. As of 2019, the largest known prime twins are $2996863034895 \cdot 2^{1290000} \pm 1$.

Find the error in the following “proof” of the existence of an infinite number of pairs of primes. Consider the numbers $2 \cdot 3 \cdot 5 \cdot ... \cdot P - 1$ and $2 \cdot 3 \cdot 5 \cdot ... \cdot P + 1$ (we take primes in increasing order up to P). As Euclid showed, they are not divisible by any prime from 2 to P, and hence they are prime (Problem 4.7). In addition, they differ by 2, so they are prime twins. Since there are infinitely many primes, then we can get as many prime twins as we wish in this way.

Appendix 2

Several Research Problems Related to Divisibility

Solvability of linear equations in non-negative integers

The fundamental lemma guarantees that the expression $ax + by$, where a and b are coprime, can take any integer value for an appropriate choice of the integers x and y. It is interesting to see what will happen if we limit ourselves to non-negative integers x and y. For example, in Problem **6.10**, it was proved that the equation $3x+5y = N$ iis solvable in non-negative integers for all $N > 7$. Let's generalize the problem.

Let coprime a and b be given; for what values of N is the equation $ax + by = N$ solvable?

It is convenient to organize the study as follows: having fixed a and b, we mark all the numbers representable as $ax+by$ on the integer axis in green and the unrepresentable ones in red, and search for patterns.

It is not difficult to notice that the equation is unsolvable only for finitely many right-hand sides, that is, there will always be such a boundary number N_0 that all larger numbers are expressed as $ax+by$ (just as in the special case of problem **6.10**, where $N_0 = 7$). To guess the dependence of N_0 on a and b, we can fix a and find the boundary number by increasing b step by step. (It is clear that a and b must appear in the formula symmetrically.) Next, it suffices to prove that N_0 cannot be expressed as $ax + by$, but all N greater than N_0 can.

A beautiful pattern (and the idea of a solution) can be seen by looking at the marked numerical axis. See [13, pp. 30–32].

Quadratic remainders

Remainders obtained in dividing the squares of positive integers by a number M are called *quadratic remainders* of the number M. The remaining numbers in the range from 0 to $M-1$ are called *quadratic non-remainders* of the number M. For example, the numbers 0 and 1 are quadratic remainders of the number 3, and the number 2 is a quadratic non-remainder of 3.

a) Find all quadratic remainders of the integers $M = 2$, 5, 7, 11. What can we say about the number of these remainders?

b) State a conjecture for all primes $M > 2$ and prove it.

c*) Do the same for M equal to the product of various primes.

d**) Solve the same problem for an arbitrary M.

See V. V. Ostrik and M. A. Tsfasman. *Algebraic Geometry and Number Theory*: *Rational and Elliptic Curves*. Moscow: MCCME, 2022 (pp. 11–12, 41–42).

Primitive roots

Let's take a prime such as $p = 7$ and look for the remainders resulting from the division of powers of 2 by 7: we see that 2 gives the remainder 2, 2^2 gives the remainder 4, 2^3 gives the remainder 1, 2^4 gives the remainder 2, ...

Now let's look at the remainders resulting from the division of powers of 3 by 7: we see that 3 gives the remainder 3, 3^2 gives the remainder 2, 3^3 gives the remainder 6, 3^4 gives the remainder 4, 3^5 gives the remainder 5, 3^6 gives the remainder 1, ...

It is not difficult to understand that the sequence will loop sooner or later. For $a = 3$, the remainder manages to run through all possible numbers 1, 2, ..., $p-1$. In this case, the number a is called a *primitive root modulo p*. For $a = 2$, the loop consists of only three numbers.

The following questions arise:

a) Does any prime p have a primitive root?

b) What length can the loop of powers of the number a modulo p have?

c) What is the number of primitive roots for a given prime p?

It is worthwhile to continue the experiment: choose a prime p and successively consider the powers of $a = 2, 3, \ldots, p - 2$ (for $a = 1, p - 1$, everything is clear). Conjectures and a proof for item b) are easy to find, but a proof for item a) is very difficult.

Easter

One of the main holidays of Christians, Easter, is moveable, that is, every year it falls on a new date. The orthodox Christians celebrate Easter on the first Sunday after the first full moon, which is after March 21[1]. The importance of knowing the date of Easter in the Middle Ages is shown, for example, by a Scottish fairy tale in which the inhabitants of Scotland send a messenger to the Vatican every year to find out the date of the next Easter. The hero of the fairy tale became famous for being able to find out not only the date, but also a method for calculating it.

Gauss found a simple algorithm for calculating the day of Orthodox Easter, which can be written in a few lines. Denote by a the remainder of the division of the number of the year by 19, by b the remainder of the division of it by 4, and by c the remainder of the division by 7. Further, denote the remainder in the division of $19a + 15$ by 30 by d, and denote the remainder in the division of $2b + 4c + 6d + 6$ by 7 by e. Easter Day will be the $(22 + d + e)$th day of March, or, equivalently, the $(d + e - 9)$th day of April (according to the Julian calendar!).

Following this algorithm, one can do a little research work guided by the following plan.

---

[1]According to the Julian calendar, which is now 13 days behind the Gregorian calendar by which we live.

a) Is the date of Easter periodic? If so, find the period (called the “great indiction”).

b) Check that the earliest Easter was in 2010. When will the next earliest Easter occur? When will the next latest Easter occur? How many times during one period one of the Easters occurs and how many times, the other?

c) Do all the intermediate dates occur? Which dates are most common and which are the least common?

d) Can Easter day fall on the same date two years in a row?

d*) (for amateurs of astronomy). Justify the Gauss algorithm.

You can use a computer to make an perpetual Easter calendar, that is, the dates for Easter over the entire period.

Appendix 3

An Alternative Outline of the Course

Let a and b be natural numbers. Consider the Diophantine equation $ay = bx$. The *minimal positive solution* (i.e., the solution with the smallest positive value of x) will be denoted by $(x_0; y_0)$. It exists because the set of positive solutions is nonempty (for example, $(a; b)$ is a solution) and is bounded below.

Lemma 1. *Any solution is a multiple of the minimal solution, i.e., if $ay = bx$, then x is divisible by x_0 and y is divisible by y_0.*

Proof by contradiction.

Suppose that there is a positive solution $(x_1; y_1)$ which is not a multiple of the minimal solution. Let us subtract the equality $ay_0 = bx_0$ from the equality $ay_1 = bx_1$, obtaining

$$a(y_1 - y_0) = b(x_1 - x_0).$$

Thus we see that $(x_1 - x_0; y_1 - y_0)$ is also a positive solution. If it is less than $(x_0; y_0)$, then we have obtained a contradiction. If not, then we subtract $(x_0; y_0)$ a few more times until we come to a positive solution which is less than $(x_0; y_0)$.

Lemma 2. *Let a and b be coprime numbers. Then the Diophantine equation $ay = bx$ has only the solutions $x = ka$, $y = kb$.*

Proof. Let us prove that $(a; b)$ is a minimal solution. Assume that the minimal solution $(x_0; y_0)$ is smaller. Then, by Lemma 1, we have $a = dx_0$, $b = dy_0$, where d is an integer. But, by the assumption that a and b are coprime, we have $d = 1$.

Problem (it is not required for what follows, but gives a beautiful geometric interpretation of the lemmas). A $a \times b$ rectangle, where a and b are positive integers is drawn on square-lined paper. Into how many parts do the nodes of the grid divide the diagonal of the rectangle?

All the key theorems are now easily deduced from Lemma 2.

Theorem on coprime divisors. *If n is divisible by the coprimes a and b, then n is also divisible by their product ab.*

Proof. By assumption, n can be represented as $n = ay = bx$. By Lemma 2, we have $y = kb$, and hence $n = k(ab)$.

The factor cancellation theorem. *Let a and b be coprime, and let bx be divisible by a. Then x is divisible by a.*

Proof. Since bx is divisible by a, it follows that $bx = ay$. By Lemma 2, we have $x = ka$.

The prime divisor theorem. *If the product ab is divisible by a prime p, then either a or b is divisible by p.*

Proof. If a is divisible by p, then everything is proved. If a is not divisible by p, then a is coprime to p. Therefore, by the factor cancellation theorem, b is divisible by p.

As we see, the proofs of the lemmas are quite clear (although there are some difficulties hidden in the proofs), and students can independently deduce all the necessary theorems from these lemmas. This exposition dramatically simplifies the proofs!

In this connection, an alternative course plan can be proposed:

— Lessons 1–4;

— Lesson 5, from which Problems 5.6 and 5.11 are removed, but the new lemmas are added and the theorem on coprime divisors is derived from them;

— Lesson 7, in which the theorems on the cancellation of factors and on prime divisors are proved using the new lemmas;

— Lesson 8;

— Lesson 6, in which we can now focus our attention on the study of Diophantine equations as such. This overloaded lesson will now be facilitated by the fact that the structure of the solution of homogeneous Diophantine equations will actually be described in the lemmas and in the necessary three theorems proved earlier. One can remove “conversational”

Problems 6.1 and 6.2 and add a couple of more serious problems on Diophantine equations, bearing in mind that this is now the last lesson.

This plan has a drawback. The point is that the proof of the fundamental theorem of arithmetic based on Euclid's algorithm and the fundamental lemma is almost literally transferred to polynomials and Gaussian numbers. In "higher mathematics", Euclid's algorithm is a very important construction that allows us to look at the fundamental theorem of arithmetic from a fairly general position. But the plan proposed here is difficult to generalise. This disadvantage can partially be compensated by also showing the "high road": in the last lesson (former Lesson 6) we can again derive the prime divisor theorem by using the fundamental lemma.

Handout Material

Lesson 1. Divisibility of numbers

Problem 1.1. Find all the divisors of the number 36.

Problem 1.2^{+}**.** The topmost row of the table indicates what is **given**. The left column, what is **asked**. Fill in the empty cells: if "yes", then write "+", if "no", write "–", and if there is not enough data, write "?". Justify your answers.

	$a \vdots m$ and $b \vdots m$	$a \vdots m$ and $b \not\vdots m$	$a \not\vdots m$ and $b \not\vdots m$
$a + b \vdots m$?			
$a - b \vdots m$?			
$a \cdot b \vdots m$?			

Problem 1.3. Find out, without performing the divisions, whether a) $18^2 - 7^2$ is divisible by 11; b) $45^3 + 55^3$ by 2500; c) $1^3 + 2^3 + ... + 82^3$ by 83.

Problem 1.4. Peter believes that if a^2 is divisible by $a - b$, then b^2 is divisible by $a - b$. Is he right?

Problem 1.5. a) Find the number of divisors of the integers 4, 9, 16, 36, 81. Do the results lead you to make a general conjecture? b) Is the statement converse to the conjecture valid?

Problem 1.6. Prove that: a) the product of two consecutive numbers is divisible by 2; b) the number $(n^2 + n)/2$ is an integer.

Problem 1.7. For what numbers a and b is a is divisible by b and b is divisible by a? (The numbers can also be negative!)

Problem 1.8^{+}**.** a) Is it true that if $a \vdots m$ and $b \vdots n$, then $ab \vdots mn$? b) Is it true that if $a \vdots b$ and $b \vdots c$, then $a \vdots c$?

Problem 1.9. Paul believes that if $ab + cd$ is divisible by $a - c$, then $ad + bc$ is also divisible by $a - c$. Is he right?

Problem 1.10. In the Triple Kingdom, only coins of 9 and 15 ducats are in circulation. Is it possible to assemble such coins to obtain a) 48 ducats, b) 50 ducats?

Problem 1.11. a) Mary demonstartes the following trick: given any three-digit number, she writes the given number twice, obtaining a six-digit number, and then, in a second, mentally divides this six-digit number by 1001. How does she do it?

b) Alex noticed that all of Mary's six-digit numbers are divisible by 7. How? By what other numbers are they divisible?

Problem 1.12. In an ancient kingdom, there was a prison with one inmate in each of its hundred cells. The prison cells are numbered from 1 to 100 and the locks in them were arranged so that the door opens when the key was turned once, but, at the next turn of the key, the door closes, and so on. At that time, the king was at war with the neighboring kinddom and, at some point, it seemed to him that he was winning.

Filled with joy, the king sent a messenger with instructions to unlock all the cell doors, but then the luck turned, and the king sent another messenger after the first, instructing him to turn the key in the lockin every second cell; then the next messenger was sent to turn the key in the lock of every third cell, and so on. In this way, 100 messengers arrived at the prison one after another and turned the locks in the cells in succession. How many prisoners were, as a result, set free and from what cells?

Lesson 2. Divisibility tests

Problem 2.1. a) Prove that a number is divisible by 2 if and only if its last digit is divisible by 2. b) Derive a divisibility test by 4 associated with the last two digits.

Problem 2.2. Peter noticed that if one subtracts the sum of its digits from a number, then one gets a number which is a multiple of 9. a) Prove this fact. b) On its basis, formulate divisibility tests by 9 and by 3.

Problem 2.3. Johnny found the number

$$100! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 99 \cdot 100.$$

He added all its digits, obtaining a new number, in which he again added all the digits, and so on until he got a one-digit number. What was it?

Problem 2.4. a) The digits of a positive integer are numbered from right to left (the first being the 1's digit, the second the 10's digit, and so on). After that, the sum of digits located at even places was added to the given number and, after that, the sum of the digits at the odd places was subtracted. Prove that the resulting number is divisible by 11.

b) Formulate a divisibility by 11 test.

Problem 2.5. Is it true that if a number n is divisible by two other numbers, then it is also divisible by their product? Check this by dividing the number n by the following numbers: a) 6 and 4, b) 3 and 2, c) 9 and 4.

Problem 2.6. In the number 65432789, cross out the least number of digits so that the remaining number is divisible by 36.

Problem 2.7. a) Prove the divisibility by 5 test.

b) Derive a divisibility by 25 test.

Problem 2.8. A machine prints the digit "4" one by one on a strip of paper. Is it be possible to stop it so that a multiple of 8 is printed?

Problem 2.9. Several digits in a number were interchanged, which resulted a number three times greater than the original one. Prove that the resulting number is divisible by 27.

Problem 2.10. Find the smallest natural number that contains only the digits 1 and 0 and is divisible by 225.

Problem 2.11. Professor Snape wrote a prescription containing numbers

EVILLIVE and LEVICORPUS

(the same letters are replaced by the same digits and different letters by different digits). Professor McGonagall claims that both of these numbers are composite. Is the professor right?

Problem 2.12. a) Prove that the product of three consecutive numbers is divisible by 6. b) Prove that the number $(n^3 - n)/6$ is an integer.

Lesson 3. Division with remainder

Problem 3.1^{+}**.** Mary was absent from the lesson due to sickness and worked out examples of division with remainder as follows: a) $20=3\cdot4+8$; b) $19=3\cdot5+4$; c) $-11=2\cdot(-5)-1$. Explain her mistakes.

Problem 3.2. What remainder will the number 123321 give when divided by 999?

Problem 3.3. The divisor and the dividend are increased threefold. How will the quotient and remainder change?

Problem 3.4. A number a is a multiple of 3. Can the remainder from the division of the number a by 12 equal 2?

Problem 3.5. a) Find the least integer (greater than one) that gives the remainder 1 under division by 2, by 3, by 5, and by 7.

b) Find *all* such integers.

Problem 3.6^{+}**.** Back to Problem 1.2. Fill in the table using the remainders: "0" if the number is divisible by m without remainder, and "not 0" if it is divisible with remainder.

Problem 3.7. Each of the numbers from 1 to 1,000,000 is replaced by the sum of its digits. Each of the resulting numbers is again replaced by the sum of its digits. We proceed in his way until one million single digits remain. Which numbers prevail: 1's or 2's?

Problem 3.8. Divide with remainder

a) 239 by 6;

b) -239 by 6;

c) -99 by 10;

d) -101 by 100.

Problem 3.9. When the Miserly Knight puts his coins in stacks of nine, he has eight coins left. How many coins will there be left when he puts the coins in stacks of 18?

Problem 3.10. The number a gives a remainder of 6 when divided by 12. Can it give a remainder of 12 when divided by 20?

Problem 3.11. Find the smallest natural number that gives the remainder 1 when divided by 2, the remainder 2 when divided by 3, the remainder 3 when divided by 4, the remainder 4 when divided by 5, and the remainder 5 when divided by 6.

Problem 3.12. A number a, when divided by b, gives the quotient q and the remainder r. What quotient and remainder will the number $-a$ give when divided by b?

Problem 3.13. The number 2 is written on the blackboard. Every second the sum of its digits is added to the number on the board. Can the number 123456 appear on the board after a while?

Lesson 4. Prime Numbers

Problem 4.1. a) A rectangle on square-lined paper consists of 31 squares of side 1. What is its perimeter equal to?

b) A rectangle on square-lined paper consists of n squares of side 1. What property must n have so that the rectangle's perimeter can be uniquely determined?

Problem 4.2. Find the largest a) two-digit; b) three-digit prime.

Problem 4.3. a) Give an example of three numbers that are not divisible by each other and such that the product of any two of them is divisible by the third.

b) The same question for numbers greater than one hundred.

Problem 4.4$^+$. Prove that a prime greater than 3 can be expressed either in the form $6n + 1$ or in the form $6n + 5$, where n is a natural number or 0.

Problem 4.5. Can the positive integers $n - 2012$, n, and $n + 2012$ be primes at the same time?

Problem 4.6$^+$. Two boys play the following game: Peter dictates to John a number (this is where his role ends), and John writes that number on the blackboard. Next, John represents the number as the product of two factors other than 1, and replaces it by the product of these two factors. Then John does the same with one of the factors, and so on.

Can Peter choose the original number so that John a) cannot even make the first move; b) John will perform the moves endlessly?

Problem 4.7$^+$. Consider the set of all primes. Denote them by $p_1, p_2, \dots, p_n$. Let's construct the number $p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$. Obviously, this number is not divisible by any prime. So it's also a prime. However, it is not included in our set of all primes, because it is greater than each of them. We arrived at a contradiction. Where is the mistake?

Problem 4.8. a) Let m and n be positive inetgers, and let $m^2 - n^2$ be a prime. Find $m - n$.

b) A smaller square in a large square on square-lined paper was painted green, and 79 unpainted cells remained. Can all the corners of the large square remain unpainted?

Problem 4.9. Is there a hundred consecutive composite numbers?

Problem 4.10. Let us call a number *simplified* if it is the product of exactly two primes (not necessarily different). What is the largest number of consecutive simplified numbers?

Problem 4.11. Can the remainder in the division of a prime by 30 be composite?

Problem 4.12. a) Find five primes such that the distance between any two adjacent primes is 6.

b) Are there six such primes?

Lesson 5. Common Divisors and Common Multiples. Euclid's Algorithm

Problem 5.1. Let's draw a rectangle of 8×12 little 1×1 squares on square-lined paper. What equal squares can the rectangle be partitioned into?

Problem 5.2. What squares can be constructed by putting together 4×6 rectangles (with the long sides of all rectangles being parallel)?

Problem 5.3$^+$**.** Find the common divisors of the numbers n and $n+1$.

Problem 5.4. Find $(846, 246)$.

Problem 5.5$^+$**.** Prove that, for any two positive integers a and b, the following equality $(a, b) \cdot [a, b] = ab$ holds.

Problem 5.6. Solve each of the following systems:

a) $\begin{cases} (x, y) = 5, \\ [x, y] = 10 \end{cases}$; b) $\begin{cases} (x, y) = 1, \\ [x, y] = 4 \end{cases}$; c) $\begin{cases} (x, y) = 5, \\ [x, y] = 31. \end{cases}$

Problem 5.7. Is it true that the following numbers are coprime:

a) two adjacent odd numbers;

b) an odd number and half the even number following it?

Problem 5.8. Find: a) $(1960, 588)$; b) $[1960, 588]$ by using Euclid's algorithm.

Problem 5.9. An automaton can cut off from any rectangle a square with a side equal to the smaller side of the rectangle. Find some pair of numbers a and b such that when cutting the $a \times b$ rectangle, the automaton obtains squares of six different sizes.

Problem 5.10. Find all values of m for which the fraction $\dfrac{11m+3}{13m+4}$ is cancellable.

Problem 5.11. Solve each of the two following systems:

a) $\begin{cases} (x, y) = 5, \\ [x, y] = 30 \end{cases}$; b) $\begin{cases} (x, y) = 1, \\ [x, y] = 30. \end{cases}$

Problem 5.12. The Fibonacci numbers 1, 1, 2, 3, 5, 8, 13, 21, 34, ... are defined by the equalities $\varphi_{n+2} = \varphi_{n+1} + \varphi_n$ (the next number is equal to the sum of the previous two) and $\varphi_1 = \varphi_2 = 1$. Find $(\varphi_{100}, \varphi_{101})$.

Lesson 6. Diophantine Equations

Problem 6.1. A grasshopper jumps along the number line. First, it takes one or more jumps of length 3 inches in one direction (right or left), and then one or more jumps of length 5 in the other direction. How can he get from point 0 to point 7? Find all the options.

Problem 6.2. A seller and a buyer have an unlimited number of coins of two denominations. The seller can give change. The buyer was able to pay 7 doublons. Can the buyer pay

a) 14 doublons;

b) 35 doublons;

c) 36 doublons?

Problem 6.3[+]. Find an integer solution of the equation a) $15x + 17y = 1$; b) $15x + 17y = 9$.

Problem 6.4. Using a blue felt-tip pen, a craftsman puts marks spaced 34 cm apart on a long ribbon starting from its beginning, while another craftsman puts marks on it with a red felt-tip pen every 27 cm. Can any blue mark be at the distance of 2 cm from any red one?

Problem 6.5. Do the following Diophantine equations have a solution:

a) $6x+8y = 9$; b) $5x+10y = 17$; c) $25x+10y = 55$; d) $12x + 15y = 22$; e) $24x + 18y = 2010$?

Problem 6.6. Prove the theorem on coprime divisors (Lesson 2). *If a number n is divisible by each of two coprime numbers a and b, then it is divisible by their product ab.*

Problem 6.7. Use arguments similar to Problem 6.5 in general form and prove the following statement:

Theorem (criterion for the solvability of Diophantine equations). a) *If c is divisible by (a, b), then equation*

$$ax + by = c, \tag{1}$$

has infinitely many solutions. b) *If c is not divisible by (a, b), then equation* (1) *has no solutions.*

Problem 6.8. n points are marked on the circle at equal distances from one another (as in the dial of a clock). One of these points is the starting point. It is connected by a segment to a point which is d arcs away from it clockwise.

We also connect this new point by a segment to a point which is d arcs away from it. We continue in this way until the last point coincides with the starting point. Thus, we will obtain a closed polygonal line (possibly, a self-intersecting one).

a) For what values of d will all of the n points turn out to be vertices of a polygonal line?

b) How many revolutions will the polygonal line perform before closing?

Problem 6.9. It is required to lay a gas pipeline on a 450 m long plot of land. There are pipes of length 9 and 13 m at the disposal of the builders. How many pipes of these lengths must be taken to lay the route so that the number of welds is minimal? The pipes must not be cut.

Problem 6.10. a) Prove that amounts of 8, 9, and 10 francs can be paid in three- and five-franc bills.

b) What are the largest amounts that can be paid in three- and five-franc bills?

Problem 6.11. Arguing as in Problem 6.6, prove the following statement that we used when solving homogeneous Diophantine equations.

> **Theorem on the cancellation of a factor.** *If the product of ac is divisible by b and the numbers a and b are coprime, then the number c is divisible by b.*

Problem 6.12.

Forty grey mice ran with forty grains of rice,
Two thinner ones strained, with a load of two grains,
A few ran all smiles, without any rice,
The big ones were serving, carrying seven,
Small mice, through the door, ran carrying four.
How many grey mice ran without any rice?

Lesson 7. Prime Divisor Theorem

Problem 7.1. Does the rebus $\mathrm{AB} \cdot \mathrm{CD} = \mathrm{EEFF}$ have a solution?

Problem 7.2. Prove that if an exact square is divisible by a prime p, then it is divisible by p^2.

Problem 7.3. Nick boasts that he can solve any problem. The teacher gives him one hundred cards with 0 written on it, one hundred cards with 1 on it, and one hundred cards with 2 on it and asks him to use all these cards to compose a number which is a complete square. Will Nick be able to solve this problem?

Problem 7.4. Let p be a prime. Prove that if the product of several numbers is divisible by p^2, then one of the factors is divisible by p^2 or there are at least two factors, each of which is divisible by p.

Problem 7.5. Three numbers have the same remainder when divided by 3. Prove that their product either is not divisible by 3 or is a multiple of 27.

Problem 7.6. For what values of n is the number $(n-1)!$ divisible by n without a remainder?

Problem 7.7. Can a number whose digits are one 1, two 2's, three 3's, ..., nine 9's be an exact square?

Problem 7.8. A prime was squared to give a ten-digit number. Can all the digits of the resulting number be different?

Problem 7.9. What is the smallest natural number n for which $n!$ is divisible by 100?

Problem 7.10. Let p_1, p_2, p_3, p_4 be different primes. Find prime common divisors of the numbers: a) p_1p_2 and p_3p_4, b) p_1p_2 and p_2p_4.

Problem 7.11. a) Write positive integers at the vertices of a square so that, at every pair of adjacent vertices, the integers will not be coprime, but, at every pair of non-adjacent vertices, they will be coprime.

b) The same problem for a cube (if the vertices are connected by an edge, then the integers must not be coprime, and if they are not connected by an edge, then they must be coprime).

Problem 7.12. The integers x, y, and z satisfy

$$(x-y)(y-z)(z-x) = x+y+z.$$

Prove that the number $x+y+z$ is divisible by 27.

Lesson 8. Factorization into Primes. The Fundamental Theorem of Arithmetic

Problem 8.1. Four natural numbers are written at the vertices of a square. On each side, the product of the numbers at its ends is written. The sum of these products is 77. Find the sum of the numbers written at the vertices.

Problem 8.2. Prove that, in the factorization into primes of an exact cube, all the exponents are multiples of 3.

Problem 8.3$^+$. Find the number of divisors of the following numbers: a) p^k; b) $p^k q^s$, where p and q are prime. c) Generalise the results obtained.

Problem 8.4. Let the factorizations into primes of the numbers a and b contain the prime factor p to the mth and nth power, respectively, and let $m \geqslant n$. Prove that p appears in the factorization into primes of the number $[a, b]$ raised to the mth power, and in the factorization into primes of the number (a, b) raised to the nth power.

Problem 8.5$^+$. A even positive integer is said to be *evenly-prime* if it cannot be represented as a product of two smaller even numbers. (For example, the numbers 2, 6, 10 are evenly-prime, and $4 = 2 \cdot 2$, $8 = 4 \cdot 2$ are not.) State an analogue of the fundamental theorem of arithmetic for even numbers, replacing the words "natural" by "even", and "prime" by "evenly-prime". Check both parts of the resulting statement.

Problem 8.6. Find a) $\varphi(p)$; b) $\varphi(p^2)$; c) $\varphi(p^k)$, where p is prime.

Problem 8.7. Is there an integer whose product of digits is a) 1990; b) 2000; c) 2010?

Problem 8.8. We are given two rectangular pieces of cardboard of dimensions 49×51 and 99×101. They are cut into identical rectangular, but not square, parts with integer sides. Find the dimensions of these parts.

Problem 8.9. Is there a set of a) two; b) ten natural numbers such that none of them is divisible by any of the others, and the square of each of them is divisible by each of the others?

Problem 8.10. Is there a positive integer whose product by 2 is a square, by 3 is a cube, and by 5 a fifth power?

Problem 8.11. Can a number having exactly 15 divisors be divisible by a) 100; b) 1000?

Problem 8.12. Your friend has chosen several arbitrary positive integers, and you want to guess all of them exactly in the order in which he chose those numbers. You are allowed to ask your friend to make an arbitrary calculation related to his numbers, for example, to find the product or sum of some of them, or a more complex combination and tell you the result. Let's call each such calculation a move. What is the smallest number of moves needed for you to be able to determine those numbers?

Problem 8.13. For coprime numbers a and b, consider the following table:

$$\begin{array}{ccccc}
1, & 2, & 3, & \ldots, & b; \\
b+1, & b+2, & b+3, & \ldots, & 2b; \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
(a-1)b+1, & (a-1)b+2, & (a-1)b+3, & \ldots, & ab.
\end{array}$$

a) Prove that there are exactly $\varphi(b)$ columns in which all numbers are coprime to b.

b) Prove that, in each column, all the remainders in the division by a are different.

c) Prove that, in each column, there are exactly $\varphi(a)$ numbers coprime to a.

d) Find $\varphi(ab)$ from $\varphi(a)$ and $\varphi(b)$.

References

1. V. G. Boltyansky and G. G. Levitas. *Divisibility of Numbers and Prime Numbers.* In the book: *Additional Chapters for a Course in Mathematics. Study Guide for an Optional Course for Students of Intermediate Forms.* — Moscow: Prosveshchenie, 1974.

2. N. B. Vasiliev, V. L. Gutenmacher, J. M. Rabbot, and A. L. Toom. *Mathematical Olympiads by Correspondence.* — Moscow: Nauka, 1986.

3. N. N. Vorobyov. *Divisibility Tests.* — Moscow: Nauka, 1988.

4. E. V. Galkin. *Non-Standard Mathematical Problems. Problems with Integers.* — Chelyabinsk: Vzglyad, 2005.

5. S. A. Genkin et al. *Leningrad Mathematical Circles.* — Kirov: ASA, 1994.

6. I. Ya. Depman. *History of Arithmetic.* — Moscow: URSS, 2007.

7. *Mathematical Problems Offered to the Students of the Mathematics Class of School* 57 (*graduation year* 2000). Edited by A. Shen. — Moscow: MTsNMO, 2000.

8. *Mathematical Problems Offered to the Students of the Mathematics Class of School* 57 (*graduation year* 2004). Edited by V. Dotsenko. — Moscow: MCCME, 2004.

9. L. I. Zvavich and A. R. Ryazanovsky. *Algebra for the* 8*th Form*: *A Problem Book for classes with in-Depth Study of Mathematics.* — Moscow: Mnemosyne, 2002.

10. R. Courant and H. Robbins. *What is Mathematics*? — Oxford University Press, New York, 1979.

11. *Moscow Mathematical Regattas. Part* 1. 1998–2006. Compilers: A. D. Blinkov, E. S. Gorskaya, and V. M. Gurovits. — Moscow: MCCME, 2014.

12. *Moscow Mathematical Regattas. Part* 2. 2006–2013. Compiler: A. D. Blinkov. — Moscow: MCCME, 2014.

13. A. V. Spivak. *Arithmetic*. — Moscow: Bureau Quantum, 2007.

14. A. Shen. *Prime and Composite Numbers*. — Moscow: MCCME, 2016.

Web Resources

1. `http://problems.ru` — mathematical problems database.