THE TEACHING OF MATHEMATICS
1998, Vol. I, pp. 1–22

SELECTED CHAPTERS FROM ALGEBRA

I. R. Shafarevich

Abstract. The aim of this publication (this paper together with several its continuations) is to present algebra as a branch of mathematics treating the contents close to the usual teaching matter. The whole exposition presupposes not a large frame of knowledge: operations with integers and fractions, square roots, removing of parentheses and other transformations of literal terms, properties of inequalities. The exposition clusters round a number of main themes: "Number", "Polynomial", "Set", each of which is treated in a series of chapters listed in Preface.

Preface

In the school mathematical education algebra has the role of Cinderella and geometry of Beloved Daughter. The extent of the geometrical knowledge, studied in school, coincides approximately with the development in this field attained in Ancient Greece and embodied in Euclid's "Elements" (III century B.C.). For long, geometry had been taught after Euclid and, only at a later time, some simplified versions appeared. In spite of all changes introduced into geometry course, the influence of Euclid and the spirit of the grandiose scientific revolution of Hellenic era continued to last. More than once I met people saying: "I have not chosen mathematics to be my profession, but I will remember forever all the beauty of logical construction of geometry with the precise derivations of more and more complex statements starting with the simplest".

Unfortunately, not even once I heard a similar reaction concerning algebra. The school course of algebra is a strange mixture of useful rules, logical reasonings, practices of how to use such auxilliary tools as tables of logarithms or a microcalculator. In its spirit, such a course is closer to the type of mathematical knowledge formed in Ancient Egypt or Babylon than to the direction of development which started in Ancient Greece and was continued in Western Europe, in the Renaissance period. None the less, algebra is a fundamental, deep and beautiful branch of mathematics as much as geometry is. Moreover, from the point of view of the contemporary classification of mathematics, the school course of algebra contains the elements of several subdivisions of mathematics: algebra, number theory, combinatorics and a small part of probability theory.

This paper is an English translation of: И. Р. Шафаревич, *Избранные главы алгебры*, Математическое образование, 1, 1, апр.--jун 1997, Москва, стр. 5--27. In the opinion of the editors, the paper merits wider circulation and we are thankful to the author for his kind permission to let us make this version.

The aim of this publication (this paper together with several its continuations) is to exhibit algebra as a branch of mathematics treating the contents close to the usual teaching matter. The whole exposition resupposes not a large frame of knowledge: operations with integers and fractions, square roots, cancellation of brackets and other transformations of literal terms, properties of inequalities. And all these practices are very well settled until the 9th class. The complexity of mathematical reasonings somewhat increases as we proceed with the matter. In order to help the reader digest the text with more ease, we also include some simple exercises.

The exposition clusters round a number of the main themes: "Number", "Polynomial", "Set", each of which is treated in more than one chapter, and the chapters related to different themes do not overlap. In the form of appendices, some more complex questions are selected, which are related to the rest of the text and which comprise no new facts besides those already in the reader's mind. In the first chapters they do not appear.

An expected list of chapters:

Chapter 1. Number.

(Irrationality of $\sqrt{2}$ and other radicals. Unique factorization of a positive integer as the product of primes.)

Chapter 2. Polynomial.

(Roots and linear factors. Common roots. Interpolation. Multiple roots. Derivative of a polynomial. Newton's binomial.)

Chapter 3. Set.

(Finite sets and their subsets. Combinatorics. Some concepts from probability theory.)

Chapter 4. Number (continued).

(Axioms of real numbers. Properties of polynomials as continuous functions.)

Chapter 5. Polynomial (continued).

(Separation of roots of a polynomial. Sturm's theorem.)

Chapter 6. Set (continued).

(Infinite sets, countable and uncountable sets.)

Chapter 7. Number (continued).

(Infinite set of prime numbers. Density of the set of prime numbers.)

Appendix I.

(Chebyshev's estimations of the number of primes less than the given bound.)

Chapter 8. Number (continued).

(Complex numbers.)

Chapter 9. Polynomial (continued).

(The existence of complex root of a polynomial with complex coefficients.)

CHAPTER I. NUMBER

1. Irrational numbers

Natural numbers arose as a result of counting. The cognition of the fact that two eyes, two men walking side by side and two oars of a boat have something in common, expressed by the abstract concept "two", was an important step in the logical development of mankind. The step to follow was not made so easily. Consonance, in many languages, of the word "three" and the words "many" (orig. " много") or "much" (orig. " слишком") bears a record to it. And only step by step, the idea of infinite series of natural numbers arose.

Gradually, the concept of number was related not only to counting, but also to measuring of length, area, weight etc. To be more concrete, we will only consider the length of line segments in the following. First of all, we have to choose a unit of length: cm, mm, km, light-year, ... Thus, a segment E is fixed and may be used for measuring of another segment A. If E is contained in A exactly n times, then we say that the length of segment A is equal to n (Fig. 1,a). But, as a rule, it will not happen (Fig. 1,b).

a) b)

Fig. 1

Then, the unit lessens, breaking up E into m equal segments E'. If E' is contained in A exactly n times, then we say that the length of A is equal to $\frac{n}{m}$ (relative to the unit E). Thousands of years, men, in different parts of the world, had applied this procedure in a variety of situations until the question: *is this breaking really possible?*, arose. This completely new setting of question already belongs to the historical epoch—Pythagoras' School, in the period of VI or V century B.C. The segments A and E are called *commensurable* if there exists a segment E' exactly m times contained in E and n times in A. Thus the above question modifies to the following: *are each two segments commensurable?* Or further: *is the length of each segment* (a unit being fixed) *equal to a rational number* $\frac{n}{m}$? The answer is *negative* and an example of a pair of incommensurable segments is simple. Consider a square, its side being E and its diagonal A.

Theorem 1. *The side of the square is incommensurable with its diagonal.*

Before we proceed with the proof, we give this theorem another form. According to the famous Pythagorean theorem, the area of the square over the hypotenuse of a right triangle is equal to the sum of areas of the squares over the other two sides. Or, in other words, the square of the length of the hypotenuse is equal to the sum of squares of the lengths of the other two sides. However, the diagonal A of our square is the hypotenuse of the isosceles triangle whose other two sides coincide with the sides E of the square (Fig. 2) and hence in our case $A^2 = 2E^2$, and if $A = nE'$, $E = mE'$, then $\left(\frac{n}{m}\right)^2 = 2$ or $\frac{n}{m} = \sqrt{2}$. Therefore, Theorem 1 can be reformulated as

Theorem 2. $\sqrt{2}$ *is not a rational number.*

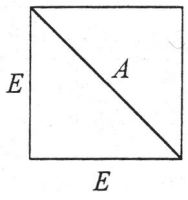

Fig. 2

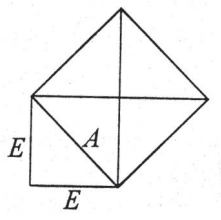

Fig. 3

We shall give a proof of this form of the theorem, but first we make the following remark. Although we have leaned on the Pythagorean theorem, we have

actually used it only for the case of an isosceles right triangle, when the conclusion is evident. Namely, it is enough to complete the Fig. 2 by constructing the square over the side A (Fig. 3). From known criterions of congruency it follows that all five small right isosceles triangles in Fig. 3 are congruent. Hence they have the same area S. But the square whose side is E consists of two such triangles and its area is E^2. Thus, $E^2 = 2S$. Similarly, $A^2 = 4S$. Hence, $A^2 = 2E^2$, i.e. $(A/E)^2 = 2$, which is all we need.

We can now proceed with the proof of Theorem 2. Since our task is to prove the *impossibility* of representing $\sqrt{2}$ in the form $\sqrt{2} = \dfrac{n}{m}$, it is natural to start with the converse, i.e. to suppose that $\sqrt{2} = \dfrac{n}{m}$, where n and m are positive integers. We also suppose that they are relatively prime, for if they have a common factor, it can be cancelled without changing the ratio $\dfrac{n}{m}$. By definition of the square root, the equality $\sqrt{2} = \dfrac{n}{m}$ means that $2 = \left(\dfrac{n}{m}\right)^2 = \dfrac{n^2}{m^2}$. Multiplying both sides by m^2 we obtain the equality

$$2m^2 = n^2, \tag{1}$$

where m and n are relatively prime positive integers, and it remains to prove that it is impossible.

Since there is a factor 2 on the left-hand side of (1), the question is naturally related to the possibility of dividing positive integers by 2. Numbers divisible by 2 are said to be *even*, and those indivisible by 2 to be *odd*. Therefore, every even number k can be written in the form $k = 2l$, where l is a positive integer, i.e. we have an explicit expression for even numbers, whereas odd numbers are defined only by a negative statement—that such an expression does not hold for them. But it is easy to obtain an explicit expression for odd numbers.

Lemma 1. *Every odd number r can be written in the form $r = 2s + 1$, where s is a natural number or 0. Conversely, all such numbers are odd.*

The last statement is evident: if $r = 2s + 1$ were even, it would be of the form $r = 2l$, which implies $2l = 2s + 1$, i.e. $2(l - s) = 1$, which is a contradiction.

In order to prove the first statement, notice that if the odd number $r \leqslant 2$, then $r = 1$ and the representation is true with $s = 0$. If the odd number $r > 1$, then $r \geqslant 3$. Subtracting 2 from it, we obtain the number $r_1 = r - 2 \geqslant 1$, and r_1 is again odd. If it is greater then 1, we again subtract 2 and put $r_2 = r_1 - 2$. In this way we obtain a decreasing sequence of numbers r, r_1, r_2, ... , where each member is less than its predecessor by 2. We continue this procedure as long as $r_i \geqslant 1$, and since positive integers cannot decrease indefinitely, we shall arrive at the situation when we cannot further subtract the number 2, i.e. when $r_i = 1$. We obtain that $r_i = r_{i-1} - 2 = r_{i-2} - 2 - 2 = \cdots = r - 2 - 2 \cdots - 2 = r - 2i = 1$. Hence $r = 2i + 1$, as stated.

We can now prove the basic property of even and odd numbers.

Lemma 2. *The product of two even numbers is even, the product of an even and an odd number is even and the product of two odd numbers is odd.*

The first two statements follow directly from the definition of even numbers: if $k = 2l$, then no matter whether m is even or odd, we always have $km = 2lm$ which is an even number. However, the proof of the last statement requires Lemma 1. Let k_1 and k_2 be two odd numbers. By Lemma 1 we can write them in the form $k_1 = 2s_1 + 1$, $k_2 = 2s_2 + 1$, where s_1 and s_2 are natural numbers or 0. Then $k_1k_2 = (2s_1+1)(2s_2+1) = 4s_1s_2+2s_1+2s_2+1 = 2s+1$ where $s = 2s_1s_2+s_1+s_2$. As we know, any number of the form $2s + 1$ is odd and so k_1k_2 is odd.

Notice the following particular case of Lemma 2: the square of an odd number is odd.

Now we can easily finish the proof of Theorem 2. Suppose that the equality (1) is true where m and n are positive integers, relatively prime. If n is odd, then by Lemma 2, n^2 is also odd, whereas from (1) follows that n^2 is even. Hence, n is even and can be written in the form $n = 2s$. But m and n are relatively prime, and so m must be odd (otherwise they would have common factor 2). Substituting the expression for n into (1) and cancelling by 2, we obtain

$$m^2 = 2s^2,$$

i.e. the square of the odd number m is even, which is in contradiction with Lemma 2. Theorem 2, and hence Theorem 1, are proved.

Under the supposition that the result of measuring the length of a segment (with respect to a given unit segment) is a number and that the square root of a positive number is a number, we can look at Theorems 1 and 2 from a different point of view. These theorems assert that in the case of the diagonal of a square or in the case of $\sqrt{2}$, these numbers are not rational, that is to say they are irrational. This is the simplest example of an irrational number. All the numbers, rational and irrational, comprise real numbers. In one of the following chapters we shall give a more precise logical approach to the concept of a real number, and we shall use it in accordance with the school teaching of mathematics, that is to say we shall not insist too much on the logical foundations.

Why did such a simple and at the same time important fact, the existence of irrational numbers, have to wait so long to be discovered? The answer is simple—because for all practical purposes, we can take, for instance, $\sqrt{2}$ to be a rational number. In fact, we have

Theorem 3. *No matter how small is a given number ε, it is possible to find a rational number $a = \dfrac{m}{n}$, such that $a < \sqrt{2}$ and $\sqrt{2} - a < \varepsilon$.*

All practical measurements can necessarily be carried out only up to a certain degree of accuracy, and up to that degree of accuracy we may take $\sqrt{2}$ to be rational. Hence, we can say that our measurements give us $\sqrt{2}$ as a rational number.

In order to prove Theorem 3 it is enough to write our arbitrarily small number ε in the form $\dfrac{1}{10^n}$ for sufficiently large n, and to find a positive integer k such that

$$\frac{k}{10^n} \leqslant \sqrt{2} < \frac{k+1}{10^n}. \tag{2}$$

Then we may take $a = \dfrac{k}{10^n}$, for $\sqrt{2} - \dfrac{k}{10^n} < \dfrac{1}{10^n}$. The inequalities (2) are equivalent to $\dfrac{k^2}{10^{2n}} \leqslant 2 < \dfrac{(k+1)^2}{10^{2n}}$ or $k^2 \leqslant 2 \cdot 10^{2n} < (k+1)^2$. Since the number n, and so $2 \cdot 10^n$, is given, there exists the largest positive integer k whose square is not greater than $2 \cdot 10^n$. This is the number we want.

Obviously, the conclusion of Theorem 3 holds not only for the number $\sqrt{2}$, but also for any positive (for simplicity's sake we confine ourselves to them) real number x. This becomes evident if we represent x by a point of the number axis, if we divide the unit length E into small segments $\dfrac{1}{10^n} E$ and cover the entire line by these segments (Fig. 4).

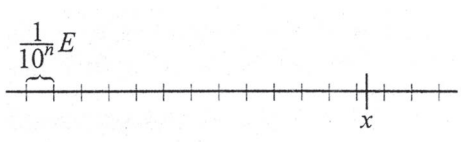

Fig. 4

Then the last of those points which is not right from x gives the required rational number: if it is the k-th point, then $a = \dfrac{k}{10^n} \leqslant x$ and $x - a < \dfrac{1}{10^n}$.

Now please consider the depth of the assertion contained in Theorems 1 and 2. This assertion can *never* be verified by an experiment, since an experiment can be carried out up to a certain degree of accuracy, and $\sqrt{2}$ can be expressed as a rational number with any given degree of accuracy. It is an accomplishment of *pure reasoning* which could not be achieved even as a result of thousands of years of experience. It had to wait for the revolution in mathematics carried out in Ancient Greece in VII–V centuries B.C. No wonder that in the Pythagorean School those facts were considered to be holy, secret knowledge, not to be shared with ordinary people. The legend says that Hyppas, a Pythagorean, died in a shipwreck as a punisment for revealing this secret. A hundred years later Plato in his book "Laws" narrates how he was astonished when he found that it is not always possible "to measure a length by a length". He speaks of his "shameful ignorance": "It seemed to me that it is not appropriate for men, but rather for swine. And I was ashamed not only for myself, but for all Greeks."

The Theorems 1 and 2 may throw some light onto the question often posed to mathematics: why prove theorems? The answer that first comes to mind is: in order to be sure that a statement is true. But sometimes a statement has been verified in so many particular cases that no one doubts its truth (and physicists often snigger at mathematicians who prove undoubted truths). But we have seen that a proof sometimes leads mathematicians into a completely new world of mathematical ideas and concepts, which would not be discovered otherwise.

Problems

1. Prove that the numbers $\sqrt{6}$ and $\sqrt[3]{2}$ are irrational.

2. Prove that the number $\sqrt{2} + \sqrt{3}$ is irrational.

3. Prove that the number $\sqrt[3]{3}+\sqrt{2}$ is irrational.

4. Determine $\sqrt{2}$ with accuracy not less than $\dfrac{1}{100}$.

5. Prove that every positive integer can be written as a sum of terms of the form 2^k, where all the terms are different. Prove that for each number this representation is unique.

2. Irrationality of other square roots

It would be interesting to generalize the results of the preceding section. For example, is it possible to prove in the same way that $\sqrt{3}$ is irrational? Clearly, we have to adapt the reasoning from the previous section to the new situation.

We want to prove the impossibility of the equality $3=\left(\dfrac{n}{m}\right)^2$, or

$$3m^2=n^2, \tag{3}$$

where, as in section **1**, we may take that the fraction $\dfrac{n}{m}$ cannot be further cancelled, i.e. that the positive integers m, n are relatively prime. Since in (3) we have the number 3, it is natural to examine the properties of division by 3. We adapt Lemmas 1 and 2 to the new case.

Lemma 3. *Every positive integer r is either divisible by 3 or it can be represented in one of the following forms: $r=3s+1$ or $r=3s+2$, where s is a natural numbers or 0. The numbers $3s+1$ and $3s+2$ are not divisible by 3.*

The last statement is evident. If, for example, $n=3s+1$ were divisible by 3, we would have $3s+1=3m$, i.e. $3(m-s)=1$, which is a contradiction. If $n=3s+2$ were divisible by 3 we would have $3s+2=m$. i.e. $3(m-s)=2$, again a contradiction. We prove the first statement of Lemma 3 by the same procedure used to prove Lemma 1. If r is not divisible by 3 and is less than 3, then $r=1$ or $r=2$ and the given representation holds with $s=0$. If $r>3$, then subtracting 3 from it we get $r_1=r-3>0$ and r_1 is again not divisible by 3. We continue to subtract the number 3 and we obtain the sequence r, $r_1=r-3$, $r_2=r-3-3$, $\dots$, $r_s=r-3-3-\cdots-3$, where we cannot subtract 3 any more, since as noticed above, $r_s=1$ or $r_s=2$. As a result we have two possibilities: $r-3s=1$, i.e. $r=3s+1$ or $r-3s=2$, i.e. $r=3s+2$, as stated.

In the formulation of the following lemma we take from the formulation of Lemma 2 only that part which we shall use later.

Lemma 4. *The product of two positive integers not divisible by 3 is itself not divisible by 3.*

Let r_1 and r_2 be two positive integers not divisible by 3. According to Lemma 3 for each one there are two possibilities: the number can be written in the form $3s+1$ or in the form $3s+2$. Hence, there are altogether four possibilities:

1) $r_1=3s_1+1,\ r_2=3s_2+1$; 2) $r_1=3s_1+1,\ r_2=3s_2+2$;

3) $r_1=3s_1+2,\ r_2=3s_2+1$; 4) $r_1=3s_1+2,\ r_2=3s_2+2$;

The cases 2) and 3) differ only in the numerations r_1 and r_2 and it is enough to consider only one of them (for instance, 2). For the remaining three cases we multiply out:

$$1)\ r_1r_2 = 9s_1s_2 + 3s_1 + 3s_2 + 1 = 3t_1 + 1,\ \ t_1 = 3s_1s_2 + s_1 + s_2;$$
$$2)\ r_1r_2 = 9s_1s_2 + 6s_1 + 3s_2 + 2 = 3t_2 + 2,\ \ t_2 = 3s_1s_2 + 2s_1 + s_2;$$
$$3)\ r_1r_2 = 9s_1s_2 + 6s_1 + 6s_2 + 4 = 3t_3 + 1,\ \ t_3 = 3s_1s_2 + 2s_1 + 2s_2 + 1$$

(in the last formula we put $4 = 3+1$, and group 3 with the numbers divisible by 3). As a result we obtain numbers of the form $3t+1$ and $3t+2$ which are not divisible by 3 (Lemma 3).

Now we can easily carry over Theorem 2 to our case.

Theorem 3. *$\sqrt{3}$ is not a rational number.*

The proof follows closely the lines of the proof of Theorem 2. We have to establish a contradiction starting with the equality (3): $3m^2 = n^2$, where m and n are relatively prime. If the number n is not divisible by 3, according to Lemma 4 its square is also not divisible by 3. But it is equal to $3m^2$, which means that n is divisible by 3: $n = 3s$. Substituting this into (3) and cancelling by 3 we get $m^2 = 3s^2$. But since n and m are relatively prime and n is divisible by 3, m cannot be divisible by 3. In view of Lemma 4 its square is also not divisible by 3, but it is equal to $3s^2$. This contradiction proves the theorem.

The close parallel between the reasonings used in the two cases we proved leads us to think that we can carry on. Of course, we do not consider $\sqrt{4}$, since $\sqrt{4} = 2$, but we may apply the same line of reasoning to $\sqrt{5}$. Clearly, we shall have to prove a lemma analogous to Lemmas 2 and 4, but the number of products which have to be evaluated will increase. We can verify all of them and conclude that $\sqrt{5}$ is irrational. We can continue and consider $\sqrt{6}$, $\sqrt{7}$, etc. In each new case the number of checkings in the proof of the lemma which corresponds to Lemmas 2 and 4 will increase. Considering all natural numbers n, for instance up to 20, we can conclude that $\sqrt{n}$ is irrational, except in those cases when n is the square of an integer ($n = 4$, 9 and 16). In this way, having to do more and more calculations, we can infer that $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{7}$, $\sqrt{8}$, $\sqrt{10}$, $\sqrt{11}$, $\sqrt{12}$, $\sqrt{13}$, $\sqrt{14}$, $\sqrt{15}$, $\sqrt{17}$, $\sqrt{18}$ and $\sqrt{19}$ are irrational numbers. This leads to the following conjecture: $\sqrt{n}$ is irrational for all positive integers n which are not squares of positive integers. But we cannot prove this general conjecture by the reasoning applied up to now, since in one step of the proof we have to analyse all possible cases.

It is interesting that the road covered by our reasoning was actually covered by mankind. As we have said, the irrationality of $\sqrt{2}$ was proved by the Pythagoreans. Later on irrationality of $\sqrt{n}$ was proved for some relatively small numbers n, until the general problem was formulated. About its solution we read in Plato's dialogue "Theaetetus", written in about 400 B.C. The author narrates how the famous philosopher Socrates met with Theodor, mathematician from Cyrene and his young, very talented pupil by the name of Theaetetus. Theaetetus had the age of today's schoolboy, between 14 and 15 years. Theodor's comment on his abilities reads: "he

approaches studying and research with such ease, fluency, eagerness and peace as oil flows form a pot and I wonder how can one achieve so much at that age". Further on, Theaetetus himself informs Socrates about the work he did with a friend, also called Socrates, a namesake of the philosopher. He says that Theodor informed them about the incommensurability (to use contemporary terms) of the side of a square with the unit segment if the area of the square is an integer, but not the square of an integer. If this area is n, this means that $\sqrt{n}$ is irrational. Theodor proved this for $n = 2, 3, 5$, and "solving one case after the other, he came up to 17". Theaetetus became intersted in the problem and, together with his friend Socrates, solved it, as it is recorded at the end of the dialogue. We shall not go into the reasoning of Theodor (there are several hypotheses), but we shall give the proof of the general statement, following the exposition of Euclid which is, very probably analogous to the proof of Theaetetus (with a simplification given by Gauss 2000 years later).

We first prove an analog of Lemmas 1 and 3.

Theorem 4. *For any two positive integers n and m there exist integers t and r, positive or 0, such that $r < m$ and*

$$n = mt + r. \tag{4}$$

For given n and m this representation is unique.

Representation (4) is called *division with remainder of n by m*, the number t is the *quotient* and r is the *remainder*.

The proof follows the known line of reasoning. If $m > n$, the equality (4) holds with $t = 0$, $r = n$. If $n \geqslant m$, then put $n_1 = n - m$. Clearly, $n_1 \geqslant 0$. If $n_1 \geqslant m$, put $n_2 = n_1 - m$. We keep on subtracting m until we arrive at the number $n_t = n - m - \cdots - m = r$, where $r \geqslant 0$ but $< m$. Thus we obtain the required representation $n - mt = r$, i.e. $n = mt + r$.

We now prove its uniqueness for given n and m. Let

$$n = mt_1 + r_1, \quad n = mt_2 + r_2.$$

Let $t_1 \neq t_2$, e.g. $t_1 > t_2$. Subtracting the second equality from the first we get: $m(t_1 - t_2) + r_1 - r_2 = 0$, i.e. $m(t_1 - t_2) = r_2 - r_1$. Since $r_1 < r_2$ on the right-hand side we have a positive number which is less than m, and on the left-hand side a number divisible by m. This is impossible.

Before we prove an analog of Lemmas 2 and 4 we have to introduce (or rather to recall) an important concept.

A positive integer, different from 1, is said to be *prime* if it is divisible only by itself and by 1. For example, among the first twenty numbers the following are prime: 2, 3, 5, 7, 11, 13, 17, 19.

Although obvious, the following property is important: *every positive integer, different from 1, has at least one prime divisor*. Indeed, if the number n has no divisors except itself and 1, it is by definition prime and is its own prime divisor. If n has other divisors, then $n = ab$, where $a < n$, $b < n$. Consider a which again can

be prime (and hence a prime divisor of n) or it has two factors: $a = a_1 b_1$. Then $n = a_1(b_1 b)$ where $a_1 < a$, i.e. a_1 is a divisor of n. Continuing this procedure we obtain a decreasing sequence of divisors of n: $a_r < \cdots < a_1 < n$. This sequence has to end somewhere. If it ends at a_r, then a_r is a prime divisor of n.

We are now able to prove an analog of Lemmas 2 and 4.

Theorem 5. *If the product of two positive integers is divisible by a prime, then at least one of them is divisible by that prime.*

Suppose that we want to prove the theorem for a prime p. We will prove it for all primes in the increasing order (as, in fact, we did it in the case of Lemma 2 for $p = 2$ and Lemma 4 for $p = 3$). Therefore, when we arrive at p, we can suppose the theorem has already been proved for all primes q smaller than p. Let $n_1 \cdot n_2$ be divisible by p and neither n_1 nor n_2 is divisible by p. Then

$$n_1 \cdot n_2 = pa. \tag{5}$$

Applying Theorem 4 to the pairs n_1, p and n_2, p, we get

$$n_1 = pt_1 + r_1, \quad n_2 = pt_2 + r_2,$$

where r_1 and r_2 are naturals less than p (and different from 0, for, otherwise, one of them would be divisible by p). Substituting in (5) and grouping the numbers divisible by p, we obtain

$$r_1 r_2 = p(a - t_1 r_2 - t_2 r_1 - p t_1 t_2),$$

or

$$r_1 r_2 = pb, \quad b = a - t_1 r_2 - t_2 r_1 - p t_1 t_2 \tag{6}$$

where, now, not alike in (5), $r_1 < p$ and $r_2 < p$. If $r_1 = 1$ and $r_2 = 1$, the contradiction $1 = pb$ is obtained. Let $r_1 > 1$. We know that r_1 has a prime factor q not greater than r_1 and, by that, less than p. Let $r_1 = qa_1$. The equality (6), now, implies

$$q(a_1 r_1) = pb. \tag{7}$$

As already said, the theorem can be considered proved for all primes less than p and, in particular, for q. Being pb divisible by q, one of its factors must also be divisible by q. Since p is prime, b is divisible by q: $b = qb_1$. Substituting in (7) and after cancellation, we obtain

$$a_1 r_2 = pb_1$$

and $a_1 < r_1$, $b_1 < b$. If $a_1 \neq 1$, proceeding again in the same way, another prime will be cancelled in the last equality. As the sequence a, a_1, ... of so obtained numbers is decreasing, we eventually come to an end, finishing with the number 1. Then, we have $r_2 = pb'$, which is impossible, being $r_2 < p$ (and $r_2 > 0$). Thus, the theorem has been proved.

You have noticed that the above reasoning is similar to the proofs of Lemmas 2 and 4: the statement reduces to the case when in (5), n_1 and n_2 (or better to

say r_1 and r_2) are less than p. But here, consideration of all possible cases and direct checking are replaced by an elegant reasoning, by which, the theorem can be taken to be true for smaller values than p. (Euclid proved Theorem 5 somewhat differently. Most probably, the here presented reasoning belongs to Gauss.)

Now, to prove irrationality in general, no new ideas are needed.

Theorem 6. *If c is a positive integer which is not the square of any positive integer, then c is not the square of any rational number, i.e. $\sqrt{c}$ is irrational.*

We may again verify our statement, going from a positive integer to the bigger one, and thus, we can suppose the theorem has been proved for all smaller c's. In that case, we can assume that c is not divisible by the square of any positive integer greater than 1. Indeed, if $c = d^2 f$, $d > 1$, then $f < c$ and f is not the square of positive integer, since $f = g^2$ would imply $c = (dg)^2$ which contradicts the assumption of the theorem. Thus we can assume the theorem has already been proved for f, and accordingly, take that $\sqrt{f}$ is irrational. But then $\sqrt{c}$ is not rational, either. In fact, the equality $\sqrt{c} = \dfrac{n}{m}$, in view of $\sqrt{c} = d\sqrt{f}$, yields $\dfrac{n}{m} = d\sqrt{f}$, $\sqrt{f} = \dfrac{n}{dm}$, which would mean $\sqrt{f}$ is rational.

Now we proceed to the main part of the proof. Suppose $\sqrt{c}$ is rational and $\sqrt{c} = \dfrac{n}{m}$, where n and m are taken, as we already did it before, to be relatively prime. Then $m^2 c = n^2$. Let p be a prime factor of c. Put $c = pd$ and d is not divisible by p, otherwise c would be divisible by p^2 and now we consider the case when c is not divisible by a square. From $m^2 c = n^2$, it follows that n^2 is divisible by p and, according to Theorem 5, n is divisible by p. Let $n = pn_1$. Using $n = pn_1$ and $c = pd$ and substituting in the relation $m^2 c = n^2$, we get $m^2 d = pn_1^2$. Being m and n relatively prime and n divisible by p, m is not divisible by p. Then, according to Theorem 5, m^2 is not divisible by p, either. And, as we have seen it, d is not divisible by p because it would imply that c is divisible by p^2. Now, the equation $m^2 d = pn_1^2$ is contradictory to Theorem 5.

Notice that, in this section, we have more than once derived this or that property of positive integers taking them one after the other and, first, checking the property for $n = 1$ and, then, after supposing its validity for numbers less than n, we proved it for n.

Here we lean upon a statement which has to be considered as an axiom of arithmetic.

If a property of positive integers is valid for $n = 1$ (or $n = 2$) and if from its validity for all positive integers less than n, the validity for n follows, then the property is valid for all positive integers. This statement is called the Principle of Mathematical Induction or of Total Induction. Sometimes, instead of supposing the validity for all numbers less than n, only the validity for $n - 1$ is supposed. A statement which corresponds to the case $n = 1$ or $n = 2$, with which the reasoning starts (sometimes $n = 0$ is more convinient) is called the *basis of induction* and the statement corresponding to $n - 1$, the *inductive hypothesis*. The Principle of Mathematical Induction is also used to produce a type of definitions, when a

concept involving a positive integer n is defined by supposing that it has already been defined for $n-1$. For example, when we define an arithmetic progression using the property that each term is obtained from the preceding one by adding a constant d, called the common difference, then we have the type of a definition by induction. To express the definition symbolically, we write

$$a_n = a_{n-1} + d.$$

And to determine the entire progression we only need to know the initial term: a_1 or a_0.

In one of his treatise, French mathematician and physicist H. Poincaré considers the question: how is it possible that mathematics, which is founded on proofs containing syllogisms, that is statements expressed in a finite number of words, does lead to theorems related to infinite collections (for example, Theorem 6 holds for infinite set of numbers c; Theorem 2 asserts that $2n^2 \neq m^2$ for all positive integers n and m, the number of which is also infinite). Possibilities for it, Poincaré sees in the Principle of Mathematical Induction, which, in his words, "contains an infinite number of syllogisms condensed in a single formula".

Problems

1. Prove the irrationality of $\sqrt{5}$ by the same method used in the proofs of Theorems 2 and 3.

2. Prove that the number of positive integers divisible by m and less than n is equal to the integer part of the quotient, when n is divided by m.

3. Prove that if a positive integer c is not the cube of any positive integer, then $\sqrt[3]{c}$ is irrational.

4. Replace the reasoning, connected with succesive subtracting of the number m in the proof of Theorem 4, by a reference to the Principle of Mathematical Induction.

5. Using the Principle of Mathematical Induction, prove the formula

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

6. Using the Principle of Mathematical Induction, prove the inequality $n \leqslant 2^n$.

3. The prime factorization

In the previous section we have seen that every natural number has a prime divisor. Starting with this, we can get much more:

Theorem 7. *Every natural number greater than* 1 *can be expressed as a product of prime numbers.*

If the number p is itself prime, then the equality $p = p$ is considered as a prime factorization containing only one factor. If the number $n > 1$ is not prime, it has

a prime divisor, different from itself: $n = p_1 \cdot n_1$ and (since by definition $p_1 \neq 1$), $n_1 < n$. Now we can apply the same reasoning to n_1 and continue. We obtain the factorization $n = p_1 \cdot \ldots \cdot p_k \cdot n_k$, where $p_1, \ldots, p_k$ are primes and the quotients n_k decrease: $n > n_1 > n_2 > \cdots$. Since our process must come to an end, we obtain $n_r = 1$ for some r and the factorization is $n = p_1 \cdot \ldots \cdot p_r$. Of course, the reader can easily formulate this proof in a more "scientific" way—using the method of mathematical induction.

The process used in the proof of Theorem 7 is not uniquely determined: if the number n has several prime factors, then any of them could be the first one. For example, 30 can be expressed first as $2 \cdot 15$ and then as $2 \cdot 3 \cdot 5$ and it is also possible to express it first as $3 \cdot 10$ and then as $3 \cdot 2 \cdot 5$. The fact that two resulting factorizations differ only by the order of their factors, was unpredictable. If for number 30 we could easily foresee all possibilities, is it so simple to convince oneself that the number

$$740037721 = 23623 \cdot 31327$$

has no other prime factorizations?

In school curricula it is usually assumed, as a self-evident fact, that every given natural number has only one prime factorization. However, this claim has to be proved, as the following example shows. Suppose that we know only even numbers and do not know how to use odd numbers. (It is possible that this is a reflection of the real historical situation, since in English the term "odd" has also the meaning "strange"). Repeating literally the definition of the prime number, we should call "prime" all even numbers which do not factorize into product of two *even* factors. For instance, the "prime" numbers would be 2, 6, 10, 14, 18, 22, 26, 30, ... Then a given number may have two different "prime" factorizations, for example

$$60 = 2 \cdot 30 = 6 \cdot 10.$$

It is also possible to find numbers with more different factorizations, such as

$$420 = 2 \cdot 210 = 6 \cdot 70 = 10 \cdot 42 = 14 \cdot 30.$$

Therefore, if the prime factorization is indeed unique, then in the proof of this statement we must use some properties which express that we are dealing with all natural numbers and not, say, with even numbers.

Since we are convinced that the uniqueness of the prime factorization is not self-evident, let us prove it.

Theorem 8. *Any two prime factorizations of a given natural number differ only by the order of their factors.*

The proof of the theorem is not really slef-evident, but all the difficulties have been already overcome in the proof of Theorem 5. From this theorem everything follows easily.

First, let us note an obvious generalization of Theorem 5.

If a product of any number of factors is divisible by a prime number p, then at least one of them is divisible by p.

Let

$$n_1 \cdot n_2 \cdot \ldots \cdot n_r = p \cdot a.$$

We shall prove our statement by induction on the number of factors r. When $r = 2$, it coincides with Theorem 5. If $r > 2$, write the equality in the form

$$n_1(n_2 \cdot \ldots \cdot n_r) = p \cdot a.$$

According to Theorem 5, either n_1 is divisible by p—and then the statement is proved—or $n_2 \cdot \ldots \cdot n_r$ is divisible by p—and then the statement is again true by the induction hypothesis.

We now prove Theorem 8. Suppose that a number n has two prime factorizations:

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s. \tag{8}$$

We see that p_1 didvides the product $q_1 \cdot \ldots \cdot q_s$. By the generalization of Theorem 5, proved earlier, p_1 divides one of the numbers $q_1, \ldots, q_s$. But q_i is a prime number and its only prime divisor is itself. Hence, p_1 coincides with one of the q_i's. Changing their numeration we can take $p_1 = q_1$. Cancelling the equality (8) by p_1 we get

$$n' = \frac{n}{p_1} = p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s. \tag{9}$$

This is a statement concerning a smaller number n' and using mathematical induction we can take it to be true. Hence the number of factors in the two factorizations is the same, i.e. $r-1 = s-1$, implying $r = s$. Besides, the factors $q_2, \ldots, q_s$ can be written in such an order that $p_2 = q_2$, $p_3 = q_3, \ldots, p_r = q_r$. Since we have already established that $p_1 = q_1$, the theorem is proved.

The theorem we just proved can be found in Euclid. Although simple, it was always considered to be an abstract mathematical theorem. However, in the last two decades it found an unexpected practical application which we shall shortly comment. The application is connected with *coding*, i.e. writing an information in such a form that it cannot be understood by a person who does not know some additional information (the key of the code). Namely, it turns out that the problem of prime factorization of large numbers requests an enormous amount of operations; this problem is much more involved than the "inverse" problem—multiplication of prime numbers. For example, it is possible, though tedious, to multiply two prime numbers, each one having tens of digits (30 or 40 digits, say) in a day and to write down the result (which will have about 70 digits) in the evening. But factorization of this number into two primes would take more time, even if we use the best contemporary computer, than the time which elapsed since the formation of the Earth. Hence, a pair of large numbers p and q on one hand, and their product $n = pq$ on the other, give, in view of Theorem 8, the same information, written in

two different ways, but the transition from the pair p, q to the number $n = pq$ is easy, whereas the transition from n to the pair p, q is practically impossible. This is the underlying idea of coding; we omit technical descripiton.

In the prime factorization of a number, certain primes may appear several times, for insatnce, $90 = 2 \cdot 3 \cdot 3 \cdot 5$. We can group together the equal factors and write $90 = 2 \cdot 3^2 \cdot 5$. Hence, for each positive integer n we have the factorization

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}, \tag{10}$$

where all the primes $p_1, \ldots, p_r$ differ from one another and the exponents $\alpha_i \geqslant 1$. This factorization is said to be *canonical*. Of course, such a factorization is unique for every n.

Knowing the canonical factorization of a number n, we can find out whatever we want about its divisors. First, if the canonical factorization has the form (10), then it is obvious that the numbers

$$m = p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}, \tag{11}$$

where $\beta_1 \leqslant \alpha_1$, $\beta_2 \leqslant \alpha_2$, $\ldots$, $\beta_r \leqslant \alpha_r$, are divisors of n, where β_i may have the value 0 (i.e. some of the p_i's which are divisors of n need not be divisors of m). Conversely, any divisor of n has the form (11). Indeed, if $n = mk$, then k is a divisor of n, i.e. it has the form (11): $k = p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$. Multiplying the canonical factorizations of m and k and grouping together the powers of equal primes, we have to arrive at the factorization (10), since this factorization is, by Theorem 8, unique. When two powers of a prime number are multiplied, their exponents add up which implies that $\beta_1 + \gamma_1 = \alpha_1$, i.e. $\beta_1 \leqslant \alpha_1$ and similarly $\beta_2 \leqslant \alpha_2$, $\ldots$, $\beta_r \leqslant \alpha_r$.

For example, we can find the sum of the divisors of n. We also take the number itself, n and also 1 to be its divisors. For instance, $n = 30$ has the divisors 1, 2, 3, 5, 6, 10, 15, 30 and their sum is 72. Consider first the simplest case when n is a power of a prime number: $n = p^\alpha$. Then its divisors are the numbers p^β where $0 \leqslant \beta \leqslant \alpha$, i.e. the numbers 1, p, p^2, $\ldots$, p^α. We therefore have to find the sum $1 + p + p^2 + \cdots + p^\alpha$. There is a general formula (which you may already know) which gives the sum of consecutive powers of a number:

$$s = 1 + a + \cdots + a^r.$$

The derivation of the formula is quite simple: we multiply both sides of the above equality by a:

$$sa = a + a^2 + \cdots + a^{r+1}.$$

We see that the expressions for s and sa consist of almost the same terms, but in s we have 1 which does not figure in sa, whereas in sa we have a^{r+1} which does not figure in s. Hence, after subtracting s from sa, all the terms cancel out, except those two:

$$sa - s = a^{r+1} - 1,$$

i.e. $s(a-1) = a^{r+1} - 1$, and

$$s = 1 + a + a^2 + \cdots + a^r = \frac{a^{r+1} - 1}{a - 1}. \tag{12}$$

Since we have divided by $a - 1$, we must suppose that $a \neq 1$.

Therefore, if $n = p^\alpha$ the sum of its divisors is $1 + p + \cdots + p^\alpha = \dfrac{p^{\alpha+1} - 1}{p - 1}$. Consider now the next case when n has two prime divisors p_1 and p_2. Its canonical factorization has the form $n = p_1^{\alpha_1} p_2^{\alpha_2}$. In view of formula (11), the divisors of n are $p_1^{\beta_1} p_2^{\beta_2}$, where $0 \leqslant \beta_1 \leqslant \alpha_1$, $0 \leqslant \beta_2 \leqslant \alpha_2$. Split them up into groups, one group for each value of β_2. So, for $\beta_2 = 0$ we obtain the divisors 1, p_1, p_1^2, $\ldots$, $p_1^{\alpha_1}$ whose sum is $\dfrac{p_1^{\alpha_1+1} - 1}{p_1 - 1}$. For $\beta_2 = 1$ we obtain the group p_2, $p_1 p_2$, $p_1^2 p_2$, $\ldots$, $p_1^{\alpha_1} p_2$. In order to find the sum of those divisors, we notice that it is equal to $(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) p_2 = \dfrac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\, p_2$. Similarly, for any value of β_2 we obtain the sum $(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}) p_2^{\beta_2} = \dfrac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\, p_2^{\beta_2}$. Hence, the total sum of divisors is

$$\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} + \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\, p_2 + \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\, p_2^2 + \cdots + \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\, p_2^{\alpha_2}$$
$$= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}).$$

We evaluate the sum in the parentheses by another application of the formula (12). As a result we conclude that the sum of all divisors of $n = p_1^{\alpha_1} p_2^{\alpha_2}$ is $\dfrac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \dfrac{p_2^{\alpha_2+1} - 1}{p_2 - 1}$.

We now pass on to the general case. Consider the product

$$S' = (1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1})(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}) \cdot \ldots \cdot (1 + p_r + p_r^2 + \cdots + p_r^{\alpha_r})$$

and remove the parentheses. How do we do that? If we have one pair of parentheses, i.e. an expression of the form $(a + b + \cdots)k$, we multiply each of the summands a, b, etc. by k and the result is the sum of ak, bk, etc. If we have two pairs of parentheses $(a_1 + b_1 + c_1 + \cdots)(a_2 + b_2 + c_2 + \cdots)$ we multiply each term from one parentheses by each term from the other and the result is the sum of all terms a_1a_2, a_1b_2, a_1c_2, b_1a_2, b_1b_2, etc. Finally, for any number of parentheses $(a_1 + b_1 + c_1 + \cdots)(a_2 + b_2 + c_2 + \cdots) \cdot \ldots \cdot (a_r + b_r + c_r + \cdots)$ we take one term from each, multiply them and then evaluate the sum of all such products. Apply this rule to our sum S'. The terms in the parentheses have the form $p_1^{\beta_1}$, $p_2^{\beta_2}$, $\ldots$, $p_r^{\beta_r}$ $(0 \leqslant \beta_i \leqslant \alpha_i)$. Multiplying them we get $p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}$, which is, in view of (11), a divisor of n, and according to Theorem 8, each one appears only once. Hence the sum S' is equal to the sum of the divisors of n. On the other hand, the

i-th parentheses, according to (12), is equal to $\dfrac{p_i^{\alpha_i+1}-1}{p_i-1}$, and the product of all parentheses is

$$S=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdot\ldots\cdot\frac{p_r^{\alpha_r+1}-1}{p_r-1}.$$

This is the formula for the sum of all divisors. But we have also found the *number* of divisors. Indeed, in order to determine the number of divisors we have to replace each summand in the sum of divisors by 1. Returning to the previous proof, we see that it is enough to replace each summand in each parentheses of the product S' by 1. The first parentheses is then equal to α_1+1, the second to α_2+1, $\ldots$, the r-th to α_r+1. Hence, the number of divisors is $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)$. For example, the number of divisors of the number whose canonical factorization is $p^\alpha q^\beta$ is equal to $(\alpha+1)(\beta+1)$.

In the same way we can derive the formula for the sum of squares or cubes or generally k-th powers of the divisors of n. The reasoning is the same as the one applied for finding the sum of the divisors. Verify that the formula for the sum of k-th powers of all divisors of the number n with the canonical factorization (10) is

$$S=\frac{p_1^{k(\alpha_1+1)}-1}{p_1^k-1}\cdot\frac{p_2^{k(\alpha_2+1)}-1}{p_2^k-1}\cdot\ldots\cdot\frac{p_r^{k(\alpha_r+1)}-1}{p_r^k-1}. \tag{13}$$

We can also investigate common divisors of two positive integers m and n. Let their canonical factorizations be

$$n=p_1^{\alpha_1}\cdot\ldots\cdot p_r^{\alpha_r},\qquad m=p_1^{\beta_1}\cdot\ldots\cdot p_r^{\beta_r}, \tag{14}$$

where in any pair of numbers (α_i,β_i) one of them may have the value 0—this is the case when a prime number divides one of the numbers m, n, but not the other. Then on the basis of what we know about divisors we can say that the number k is a common factor of m and n if and only if it has the form

$$k=p_1^{\gamma_1}\cdot\ldots\cdot p_r^{\gamma_r},$$

where $\gamma_1\leqslant\alpha_1$, $\gamma_1\leqslant\beta_1$, $\gamma_2\leqslant\alpha_2$, $\gamma_2\leqslant\beta_2$, $\ldots$, $\gamma_r\leqslant\alpha_r$, $\gamma_r\leqslant\beta_r$. In other words if σ_i denotes the smaller of the numbers α_i, β_i, these conditions become $\gamma_1\leqslant\sigma_1$, $\gamma_2\leqslant\sigma_2$, $\ldots$, $\gamma_r\leqslant\sigma_r$. Put

$$d=p_1^{\sigma_1}\cdot\ldots\cdot p_r^{\sigma_r}. \tag{15}$$

The above reasoning proves that the following theorem is true.

Theorem 9. *For any two numbers with canonical factorization* (14)*, the number d, defined by* (15)*, divides both n and m, and any common factor of n and m divides d.*

The number d is called the *greatest common divisor* of n and m and is denoted by $\mathrm{g.c.d.}(n,m)$. It is clear that among all divisors of n and m, d is the greatest, but it is not obvious that all other common divisors divide it. This follows from

Theorem 8 (about the uniqueness of prime factorization). That is why we proved those properties which are usually given in school courses without proof.

As we said earlier, finding the prime factorization of a number is a very difficult task. Hence we give a different method for finding the greatest common divisor which does not use prime factorization—this method is often taught at schools. It is based on Theorem 4. Let n and m be two positive integers and let $n = mt + r$, $0 \leqslant r < m$ be the representation eastablished in Theorem 4.

Lemma 5. *If* $r \neq 0$, *then* $\text{g. c. d.}(n, m) = \text{g. c. d.}(m, r)$.

More than that: all common divisors of the pairs (n, m) and (m, r) are equal, and so are the greatest which are divisible by the others. Indeed, any common divisor d of numbers n and m is a divisor of m and of r, because $r = n - mt$, and a common divisor d' of m and r is a divisor of m and of n, because $n = mt + r$.

The transition from the pair (n, m) to the pair (m, r) is fruitful since $r < m$. We can now apply the same reasoning to the pair (m, r). Let $m = rt_1 + r_1$, $0 \leqslant r_1 < r$. If $r_1 \neq 0$, then $\text{g. c. d.}(m, r) = \text{g. c. d.}(r, r_1)$. We continue this process as long as we can. But the process ends when we get the remainder 0, for example $r_i = r_{i+1}t_{i+2} + 0$ ($r_{i+2} = 0$). But then r_{i+1} divides r_i and clearly $\text{g. c. d.}(r_i, r_{i+1}) = r_{i+1}$. Therefore, the last nonzero remainder in the process of dividing n by m, m by r, r by r_1, etc. is equal to $\text{g. c. d.}(n, m)$. This method of finding the g. c. d. is called *Euclid's algorithm*, and it can be found in Euclid. For instance, in order to find $\text{g. c. d.}(8891, 2329)$ we make the following divisions:

$$8891 = 2329 \cdot 3 + 1904; \qquad 2329 = 1904 \cdot 1 + 425;$$
$$1904 = 425 \cdot 4 + 204; \qquad 425 = 204 \cdot 2 + 17; \qquad 204 = 17 \cdot 12 + 0,$$

and conclude: $\text{g. c. d.}(8891, 2329) = 17$.

The numbers n and m are said to be *relatively prime* if they have no common divisor other than 1. This means that $\text{g. c. d.}(n, m) = 1$. Hence, using Euclid's algorithm we can find whether two numbers are relatively prime, without knowing their prime factorizations.

At the end of this chapter we return to the question with which we started: the question of irrationality. We shall prove a very wide generalization of our first assertion regarding the irrationality of $\sqrt{2}$. It is in connection with the concept to which we devote the next chapter and so this can be treated as a kind of introduction to that chapter.

An expression of the form ax^k, where a is a number, x is unknown and k a natural number or 0 (in which case we simply write a), is called *monomial*. The number k is its *degree*, and a is its *coefficient*. In general, we can consider monomials in several unknowns, such as ax^2y^8, but at the moment we are concerned only with monomials in one unknown. A sum of monomials is a *polynomial*. If a polynomial contains several monomials of the same degree, for example ax^k and bx^k, we can replace them by one monomial, namely $(a + b)x^k$. Having this in mind, we shall always assume that a polynomial contains only one member of a given degree k and we write it in the form a_kx^k; for $k = 0$ we simply have the number a_0. The

greatest degree of all monomials which comprise a polynomial is the *degree* of the polynomial. For example, the degree of the polynomial $2x^3 - 3x + 7$ is 3 and its coefficients are $a_0 = 7$, $a_1 = -3$, $a_2 = 0$, $a_3 = 2$. Thus, a polynomial of degree n can be written in the form

$$f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n,$$

where some of a_k's can be zero, but $a_n \neq 0$, because otherwise the degree of the polynomial would be less than n. The term a_0 is called the *constant term* of the polynomial, a_n is its *leading coefficient*. The equation $f(x) = 0$ is called an *algebraic equation* with one unknown. A number α is called its *root* if $f(\alpha) = 0$. A root of the equation $f(x) = 0$ is also called a *root of the polynomial* $f(x)$. Degree of the polynomial $f(x)$ is the *degree of the equation*. Obviuosly, the equations $f(x) = 0$ and $cf(x) = 0$, where c is a number, distinct from 0, are equivalent.

Now we shall treat such equations $f(x) = 0$ whose coefficients a_0, a_1, ... , a_n are rational numbers, some of which may be equal to 0 or negative. If c is the common denominator of all, distinct from 0, coefficients, we can pass from the equation $f(x) = 0$ to the equation $cf(x) = 0$ having integer coefficients. In the sequel we shall treat only such equations. In this connection we shall have to deal with the divisibility of (not only nonnegative) integers. Recall that an integer a is, by definition, divisible by an integer b if $a = bc$ for some integer c.

Theorem 10. *Let $f(x)$ be a polynomial with integer coefficients and with leading coefficient equal to* 1. *If the equation $f(x) = 0$ has a rational root α, then α is an integer and it is a divisor of the constant term of the polynomial $f(x)$.*

Let us represent α in the form $\alpha = \pm\dfrac{a}{b}$, where the fraction $\dfrac{a}{b}$ is irreducible, i.e. positive integers a and b are relatively prime. By the condition, the polynomial $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1} + x^n$ has integer coefficients a_i. Let us substitute α into the equation $f(x) = 0$. By the assumption,

$$a_0 + a_1\left(\pm\frac{a}{b}\right) + \cdots + a_{n-1}\left(\pm\frac{a}{b}\right)^{n-1} + \left(\pm\frac{a}{b}\right)^n = 0. \tag{16}$$

Multiply the equation by b^n and transfer $(\pm a)^n$ to the right-hand side. All the terms remaining on the left-hand side will be divisible by b:

$$(a_0b^{n-1} + a_1(\pm a)b^{n-2} + \cdots + a_{n-1}(\pm a)^{n-1}b^{n-2})b = (\pm 1)^{n-1}a^n.$$

We see that b divides a^n. If α were not an integer, b would be > 1. Let p be some of its prime divisors. Then it has to divide a^n, and by Theorem 5, p divides a, too. However, by the assumption, a and b are relatively prime and we have obtained a contradiction. Hence, $b = 1$ and $\alpha = a$.

In order to obtain the second assertion of the theorem, let us leave just a_0 on the right-hand side, and transfer all the other terms to the right-hand side (recall that $b = 1$). All the terms on the right-hand side are divisible by a:

$$a_0 = a(\mp a_1 - a_2(\pm a) - \cdots - a_{n-1}(\pm a)^{n-2} - (\pm a)^{n-1}).$$

Obviously, it follows that a devides a_0.

Theorem 10 allows us to find rational roots of equations of the given form: in order to do that we have to list all the divisors of the constant term (with signs + and −) and check whether they are roots. For example, for the equation $x^5 - 13x + 6 = 0$ we have to check the numbers ± 1, ± 2, ± 3, ± 6. Only $x = -2$ is a root.

In such a way, all the roots of a polynomial $f(x)$ with integer coefficients and the leading coefficinet equal to 1 are irrational, except integer roots which are included as divisors of the constant term. That is just what we have proved in the beginning of this Chapter: firstly for $f(x) = x^2 - 2$ (Theorem 2), then for $f(x) = x^2 - 3$ (Theorem 3) and finally for $f(x) = x^2 - c$, where c is an integer (Theorem 6). Now we have obtained the widest generalization of all these assertions. It has a lot of other geometrical applications, besides Theorems 1, 2, 3, 6.

Consider, e.g., the equation

$$x^3 - 7x^2 + 14x - 7 = 0. \tag{17}$$

By Theorem 10, its integer roots can be just divisors of the number -7, i.e. one of the numbers 1, -1, 7, -7. Substitutions show that neither of these numbers satisfies the equation. We can conclude that the roots of the equation are irrational numbers. As a matter of fact, we do not know whether the equation (17) has roots at all. But, we shall show later that it has roots and even very interesting ones. One of its roots appears to be the square of the side of the regular heptagon, inscribed in the circle of radius 1.

Moreover, the equation (17) has three roots, lying: between 0 and 1, between 2 and 3 and between 3 and 4. They are the squares of the *diagonals* of the regular heptagon, inscribed into the unit circle. Here by a diagonal we mean an *arbitrary* segment, joining two vertices of a polygon, so that sides are included as diagonals. The regular heptagon has three diagonals of different length— AB, AC and AD (fig. 5). In such a way, all these lengths are irrational numbers.

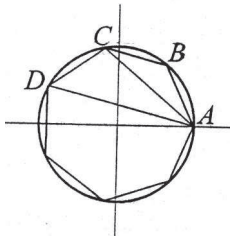

Fig. 5

Problems

1. Show that Theorem 5 is not valid if concepts of a number and a "prime" are understood as applied just to even numbers as has been discussed in the beginning of this section. Which part of the proof of Theorem 5 appears to be wrong in that case?

2. Prove that if integers m and n are relatively prime, then divisors of mn are obtained multiplying divisors of m by divisors of n, and each divisor of mn can be obtained in this way exactly once. Deduce that if $S(N)$ denote the sum of k-th powers of all divisors of N, m and n are relatively prime and $N = mn$, then $S(N) = S(m)S(n)$. Derive the formula (14) in that way.

3. A positive integer n is called *perfect* if it is equal to the sum of its proper divisors (i.e. the number itself is *excluded* from the set of its divisors). E.g. numbers 6 and 28 are perfect. Prove that if for some r the number $p = 2^r - 1$ is prime, then $2^{r-1}p$ is a perfect number (but recall that the formula on the sum of divisors S we have deduced, includes the number n itself). This proposition was already known to Euclid. Nearly 2000 years later Euler proved the inverse assertion: each even perfect number is of the form $2^{r-1}p$, where $p = 2^r - 1$ is a prime. Proof does not use any facts other than the ones presented previously, but is by no means easy. Try to rediscover this proof! By now, it is not known whether there exist *odd* perfect numbers.

4. If for two positive integers m and n there exist such integers a and b so that $ma + nb = 1$, then obviously m and n are relatively prime: each of their common divisors is divisible by 1. Prove the converse: for relatively prime numbers m and n there always exist integers a and b such that $ma + nb = 1$. Use the division algorithm and mathematical induction.

5. Using the result of problem 4 prove Lemmas 6 and 7 without using the theorem on uniqueness of prime factorization. Show that in such a way a new proof of this theorem (Theorem 8) can be obtained. This was just the way Euclid proved it.

6. Find integer values of a such that the polynomial $x^n + ax + 1$ has rational roots.

7. Let $f(x)$ be a polynomial with integer coefficients. Prove that if a reduced fraction $\alpha = \pm\frac{a}{b}$ is a root of the equation $f(x) = 0$, then b divides the leading coefficient and a divides the constant term. This is a generalization of Theorem 10 to the case of a polynomial with integer coefficients where the leading coefficient need not be equal to 1.

I. R. Shafarevich,
Russian Academy of Sciences,
Moscow, Russia