Preface

I wish that algebra would be the Cinderella of our story. In the mathematics program in schools, geometry has often been the favorite daughter. The amount of geometric knowledge studied in schools is approximately equal to the level achieved in ancient Greece and summarized by Euclid in his *Elements* (third century B.C.). For a long time, geometry was taught according to Euclid; simplified variants have recently appeared. In spite of all the changes introduced in geometry courses, geometry retains the influence of Euclid and the inclination of the grandiose scientific revolution that occurred in Greece. More than once I have met a person who said, "I didn't choose math as my profession, but I'll never forget the beauty of the elegant edifice built in geometry with its strict deduction of more and more complicated propositions, all beginning from the very simplest, most obvious statements!"

Unfortunately, I have never heard a similar assessment concerning algebra. Algebra courses in schools comprise a strange mixture of useful rules, logical judgments, and exercises in using aids such as tables of logarithms and pocket calculators. Such a course is closer in spirit to the brand of mathematics developed in ancient Egypt and Babylon than to the line of development that appeared in ancient Greece and then continued from the Renaissance in western Europe. Nevertheless, algebra is just as fundamental, just as deep, and just as beautiful as geometry. Moreover, from the standpoint of the modern division of mathematics into branches, the algebra courses in schools include elements from *several* branches: algebra, number theory, combinatorics, and a bit of probability theory.

The task of this book is to show algebra as a branch of mathematics based on materials closely bordering the course in schools. The book does not claim to be a textbook, although it is addressed to students and teachers. The development presumes a rather small base of knowledge: operations with integers and fractions, square roots, opening parentheses and other operations on expressions involving letter symbols, the properties of inequalities. All these skills are learned by the 9th grade. The complexity of the mathematical considerations increases somewhat as we move through the book. To help the reader grasp the material, simple problems are given to be solved.

The material is grouped into three basic themes—**Numbers**, **Polynomials**, and **Sets**—each of which is developed in several chapters that alternate with the chapters devoted to the other themes.

Certain matters related to the basic text, although they do not use more ideas than are already present, are more complicated and require that the reader keep more facts and definitions in mind. These matters are placed in supplements to the chapters and are not used in subsequent chapters.

For the proofs of assertions given in the book, I chose not the shortest but the most "understandable." They are understandable in the sense that they connect the assertion to be proved with a larger number of concepts and other assertions; they thus clarify the position of the assertion to be proved within the structure of the presented area of mathematics. A shorter proof often appears later, sometimes as a problem to be solved.

At the first acquaintance with mathematics, the history of its development usually retreats into second place. Sometimes it even seems that mathematics was born in the form of a perfected textbook. In fact, mathematics has arisen as the result of the work of uncounted scholars throughout many milleniums. To give some attention to that aspect of mathematics, the dates of the lives of the mathematicians (and physicists) mentioned in the text are listed at the end of the book.

There are quite many formulas. For convenience in referring to them, they are numbered. If I only give the formula number when referring to it, then the formula is in the current chapter. For example, if "multiplying equality (16), we obtain ... " is said in Chap. 2, then the formula with the number (16) in Chap. 2 is meant. If a formula in a different chapter is intended, then the number of the chapter is also given, for example, "using formula (12) in Chap. 1." To help find the necessary chapter, the chapter numbers are printed at the top of every left-hand page. Theorems and lemmas are numbered in order throughout the entire book.

The Foundation for Mathematical Education and Enlightenment and especially S. I. Komarov and V. M. Imaikin helped me greatly in preparing the manuscript. S. P. Demushkin took upon himself the labor of reading the manuscript and made many important comments. I convey my heartfelt gratitude to all of them.

I. R. Shafarevich Moscow, 2000

Added to the English edition:

Finally, I express my cordial gratitude to Bill Everett, who translated this book into English. As far as I can judge, this is beautiful English. However, I am not an expert in this. But certainly, he greatly improved the text as he showed me several mistakes and urged me by his questions to clarify the exposition in some places.

I. R. S. Moscow, 2002

4
Prime Numbers

Topic: Numbers

11. The Number of Prime Numbers is Infinite

In this chapter, we return to a question examined in Chap. 1. It was shown there that a natural number has a unique decomposition into prime factors. From the standpoint of the operation of multiplying, therefore, prime numbers are the simplest elements from which we can obtain all natural numbers, similar to how we obtain them all from the number 1 using the operation of adding. From this standpoint, the interest in the collection of prime numbers is understandable. Four prime numbers are found in the first decade of natural numbers: 2, 3, 5, 7. Further, we can find prime numbers, in turn dividing each number by all previously found smaller primes to determine if it is prime. We thus find 25 prime numbers in the first century:

$$2, 3, 5, 7,\ 11, 13, 17, 19,\ 23, 29,\ 31, 37,\ 41, 43, 47,$$
$$53, 59,\ 61, 67,\ 71, 73, 79,\ 83, 89,\ 97.$$

How far does this sequence continue?

This question already arose in antiquity. We find the answer to this question in Euclid. It is formulated in Theorem 24.

Theorem 24. *The number of prime numbers is infinite.*

We present several proofs of this theorem. The *first proof* is the one contained in Euclid's *Elements*. Suppose we have found n primes in all: $p_1, p_2, \ldots, p_n$. We consider the number $N = p_1 p_2 \cdots p_n + 1$. As we saw in Sec. 2, each number has at least one prime divisor. In particular, N

has a prime divisor. But it cannot be one of the numbers $p_1, \dots, p_n$. Indeed, suppose it were p_i. Then $N - p_1 \cdots p_n$ must be divisible by p_i, and because $N - p_1 \cdots p_n = 1$, this is impossible. Therefore, the prime divisor of N is different from p_i, $i = 1, \dots, n$. This means that for each n prime numbers, there follows one more prime number. This proves the theorem. □

Second proof. It was proved in Sec. 9 (see formula (25)) that the number of numbers less than a given number N and relatively prime to it is given by the formula

$$N\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_n}\right), \tag{1}$$

where $p_1, \dots, p_n$ are all the prime divisors of the number N.

Again suppose we have found n prime numbers $p_1, \dots, p_n$. We set $N = p_1 \cdots p_n$. Substituting this expression in formula (1), we obtain the simple factor $p_i - 1$ from each factor $p_i(1 - 1/p_i)$, and we thus obtain the expression $(p_1 - 1)(p_2 - 1) \cdots (p_n - 1)$ for the whole of formula (1). Because we know that there exists a prime number greater than 2 (for example, 3), this expression must be a number *greater than* 1. Therefore, there exists a number a less than N and relatively prime to it that is different from 1. But a has at least one prime divisor that cannot be contained among the numbers $p_1, \dots, p_n$, because a is relatively prime to N. We have obtained one more prime number, and this proves the theorem. □

The endless sequence of prime numbers is rather sparsely distributed among the natural numbers. For example, there is a “gap” in it however large you want, that is, we can find any given number of consecutive numbers (sufficiently far out) that are not prime. For example, the n numbers

$$(n+1)! + 2, \quad (n+1)! + 3, \quad \dots, \quad (n+1)! + n + 1$$

are obviously not prime: the first is divisible by 2, the second is divisible by 3, and the last is divisible by $n + 1$. For some time, people tried to find a formula expressing prime numbers. Euler found the remarkable polynomial $x^2 + x + 41$, which has a prime value for 40 values of x from 0 to 39. It is obvious, however, that for $x = 40$, it takes the nonprime value 41^2. It is easy to verify that there cannot exist a polynomial $f(x)$ that would yield prime values for all integer values $x = 0, 1, 2, \dots$ (not to speak of it yielding *all* prime numbers). We demonstrate this with the example of a second-degree polynomial $ax^2 + bx + c$ with the integer coefficients a, b, c.

We suppose that the value c, which the polynomial yields for $x = 0$, is prime. Then for an arbitrary positive integer k, we take $x = kc$ and find that the polynomial yields the value $ak^2c^2 + bkc + c$, which is obviously divisible by c. This value is either not prime or is exactly c. You can easily verify that for given a and b, there is at least one positive integer k for which $ak^2c^2 + bkc + c$ is equal to c. Therefore, all such values except possibly two are not prime.

Furthermore, there does not exist a polynomial $f(x)$ of arbitrary degree with integer coefficients such that all its values for integer x are prime numbers, *beginning from some boundary.* Indeed, suppose that the values of the polynomial $f(x) = a_0 + a_1x + \cdots + a_nx^n$ are prime for all integers $x \geq m$, where m is some natural number. We set $x = y + m$, $f(y + m) = g(y)$. The polynomial $g(y) = a_0 + a_1(y + m) + \cdots + a_n(y + m)^n = b_o + b_1y + \cdots + b_ny^n$ is obtained by opening parentheses and combining like terms. Therefore, its coefficients b_i are again integers, but it already yields prime values for all $y \geq 0$. In particular, $g(0) = b_0 = p$ is a prime number. Then for any integer k, the value $g(kp) = p + b_1kp + \cdots + b_n(kp)^n$ is divisible by p. They can coincide with p only if $p + b_1kp + \cdots + b_n(kp)^n = p$, that is,

$$b_1 + b_2kp + \cdots + b_n(kp)^{n-1} = 0.$$

This is a polynomial of degree $n - 1$ in k. According to Theorem 14, it has at most $n - 1$ roots. For all other values of k, the number $g(kp)$ is divisible by p and is different from p, that is, it is not prime.

It can be proved that for any number k of unknowns, there cannot exist a polynomial in k unknowns with integer coefficients such that all its values for all natural values of the unknowns are prime numbers. Nevertheless, it turns out that there exists a 25th-degree polynomial in 26 unknowns that has the following property: if we select the values it yields for nonnegative integer values of the unknowns such that the values themselves are positive, then their set coincides with the set of prime numbers. Because 26 is equal to the number of letters in the English alphabet, the unknowns can be denoted by those letters: $a, b, c, \ldots, x, y, z$. Then the polynomial has the form

$$\begin{aligned}
&F(a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p,q,r,s,t,u,v,w,x,y,z) = \\
&\quad = (k+2)\Big\{1 - \big[wz+h+j-q\big]^2 - \big[(gk+2g+k+1)(h+j)+h\big]^2 \\
&\qquad - \big[2n+p+q+z-e\big]^2 - \big[16(k+1)^2(k+2)(n+1)^2+1-f^2\big]^2 \\
&\qquad - \big[e^3(t+2)(a+1)^2+1-o^2\big]^2 - \big[(a^2-1)y^2+1-x^2\big]^2 \\
&\qquad - \big[16r^2y^4(a^2-1)+1-u^2\big]^2 \\
&\qquad - \big[\big(a+u^2(u^2-a^2)-1\big)(n+4dy)^2+1-(x-cu)^2\big]^2 \\
&\qquad - \big[n+l+v-y\big]^2 - \big[(a-1)l^2+1-m^2\big]^2 - \big[ai+k+1-l-i\big]^2 \\
&\qquad - \big[p+l(a-n-1)+b(2an+2a-n^2-2n-2)-m^2\big] \\
&\qquad - \big[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x\big]^2 \\
&\qquad - \big[z+pl(a-p)+t(2ap-p^2-1)-pm\big]^2\Big\}.
\end{aligned}$$

This polynomial is written here only to make the reader's eyes pop. The number of variables in it is very large. It can be proved that it also yields negative values $-m$, where m is not prime. Therefore, it does not give us a representation of the sequence of prime numbers.

Long efforts inclined the majority of mathematicians to the conviction that more or less simple formulas describing the sequence of prime numbers do not exist. "Explicit formulas" describing prime numbers exist, but they use objects about which we know less than about prime numbers. The mathematicians' attention therefore focused on characteristics of prime numbers "collectively" and not "individually." We clarify this posing of the question in the next section.

Problems:

1. Prove that number of prime numbers of the form $3s+2$ is infinite.
2. Prove that number of prime numbers of the form $4s+3$ is infinite.
3. Prove that any two numbers $2^{2^n}+1$ and $2^{2^m}+1$, where $n \neq m$, are relatively prime. From this, once more deduce the infiniteness of the number of prime numbers. *Hint*: Suppose that p is a common divisor of two such numbers and find the remainder from dividing 2^{2^n} and 2^{2^m} by p.
4. Let $f(x)$ be a polynomial with integer coefficients. Prove that among the prime divisors of its values $f(1), f(2), \ldots$, there exist an infinite number of different ones. (If the problem is not solved quickly, solve it first for first-degree polynomials $f(x)$, then second-degree.)
5. Let p_n denote the nth prime in ascending order. Prove that $p_{n+1} < p_n^n + 1$.
6. In the notation in Problem 5, prove that $p_n < 2^{2^n}$. Deduce the close inequality $p_{n+1} \le 2^{2^n}+1$ from the result of Problem 3.
7. In the notation in Problem 5, prove that $p_{n+1} < p_1 p_2 \cdots p_n$.

12. Euler's Proof That the Number of Prime Numbers is Infinite

We give yet another proof, belonging to Euler, of the infiniteness of the number of prime numbers, which elucidates certain general properties of this sequence.

We begin with the "prehistory," that is, with certain simple facts that were known before Euler began to study the question of prime numbers. The matter concerns the magnitude of the sums

$$1, \quad 1+\frac{1}{2}, \quad 1+\frac{1}{2}+\frac{1}{3}, \quad \ldots, \quad 1+\frac{1}{2}+\cdots+\frac{1}{n}, \quad \ldots.$$

In the notation in Sec. 6, these are the sums $(Sa)_n$, where a is the sequence of inverse natural numbers $1, 1/2, 1/3, \ldots$. Because the sums of the mth power of the natural numbers from 1 to n is denoted by $S_m(n)$ in our notation (see formula (29) in Chap. 2), our sums here are naturally denoted by $S_{-1}(n)$.

We come upon a concept here that we meet often in what follows. We therefore discuss it in more detail. It generally relates to properties of an *infinite* sequence of positive numbers $s_1, s_2, \ldots, s_n, \ldots$ (for us, it arose as the sequence of sums of another sequence, but this is not important now). One type of sequence is called an *bounded* sequence. This means that there exists a single number C for the whole sequence such that $s_n < C$ for all $n = 1, 2, 3, \ldots$. If the sequence does not have this property, then it is said to be *unbounded*. This means that no number C has that property, that is, for any number C, an index n can be found such that $s_n \geq C$. Finally, it can happen that for any number C, an index n can be found such that *all* $s_m \geq C$ for all $m = n, n+1, \ldots$. In other words, the number s_n becomes however large we want for sufficiently large n. In this case, the sequence is said to *increase without limit*. For example, the sequence $1, 1, 1, 2, 1, 3, \ldots$, in which the odd positions contain 1 and the even positions contain the sequence of natural numbers, is unbounded but does not increase without limit, because we can still find the number 1 no matter how far out we go.

If a sequence $a = a_1, a_2, \ldots, a_n, \ldots$ of positive numbers is given and $s = Sa$, then $s_{n+1} > s_n$ (because $s_{n+1} = s_n + a_{n+1}$, $a_{n+1} > 0$), and, more generally, $s_m > s_n$ for all $m > n$. Therefore, such a sequence increases without limit if it is not bounded. For example, if all $a_i = 1$, then $s_n = n$, and the sequence $s_1, s_2, \ldots$ is unbounded. But it might be bounded in other cases. An example is illustrated in Fig. 21, where we first divide the segment from 0 to 1 in half and set $a_1 = 1/2$, then divide

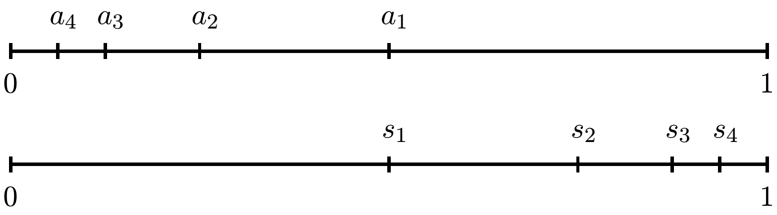

Fig. 21

the segment from 0 to 1/2 in half and set $a_2 = 1/4$, and so on. Thus, $a_n = 1/2^n$. The result of adding these numbers is shown in Fig. 21: we can see that their sums s_n always stay inside our segment because s_2 is the middle of the segment from s_1 to 1, s_3 is the middle of the segment from s_2 to 1, and so on. That is, $s_n < 1$. This is easily verified by calculating. If $a_n = 1/2^n$, then

$$(Sa)_n = \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n} = \frac{1}{2}\left(1 + \frac{1}{2} + \cdots + \frac{1}{2^n}\right),$$

and by formula (12) in Chap. 1,

$$(Sa)_n = \frac{1}{2}\frac{1/2^n - 1}{1/2 - 1} = 1 - \frac{1}{2^n}.$$

It follows that $(Sa)_n < 1$ for any n.

We show that the *first* case holds for the sequence $1, 1/2, 1/3, \ldots$. Although the terms of the sequence decrease, they do not decrease sufficiently rapidly, and their sum (i.e., $S_{-1}(n)$) increases without limit.

Lemma 8. *For sufficiently large n, the sum $S_{-1}(n)$ is greater than any fixed number given in advance.*

Let the number k be given. We show that for some n (and this means for all indices following it also), $S_{-1}(n) > k$. We take n such that $n = 2^m$ for some m. We subdivide the sum

$$S_{-1}(n) = 1 + \left(\frac{1}{2}\right) + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \cdots + \left(\frac{1}{2^{m-1}+1} + \cdots + \frac{1}{2^m}\right)$$

into subtotals enclosed in parentheses as shown in the formula. Each set of parentheses encloses a sum of the general form

$$\frac{1}{2^{k-1}+1} + \frac{1}{2^{k-1}+2} + \cdots + \frac{1}{2^k},$$

and there are m sets of parentheses. Within each set of parentheses, we replace each term with the least term, that is, the last. Because the number of terms in each set of parentheses is equal to $2^k - 2^{k-1} = 2^{k-1}$, we find that the sum in the kth set of parentheses is greater than $2^{k-1}/2^k = 1/2$. As a result, we obtain $S_{-1}(n) > 1+m/2$. This inequality holds for any n if $n = 2^m$. It remains for us to set $1 + m/2 = k$, that is, $m = 2k - 1$. Then we take $n = 2^{2k-1}$; it follows that $S_{-1}(n) > k$. □

We now turn to Euler's proof. His idea is connected with the method for calculating the sums of powers of divisors of a natural number described in Sec. 3 (see formula (13) in Chap. 1). The sum of the kth powers of all divisors (including 1 and n) of the natural number n is denoted by $\sigma_k(n)$. According to formula (13) in Chap. 1,

$$\sigma_k(n) = \frac{p_1^{k(\alpha_1+1)-1}}{p_1^k - 1} \frac{p_2^{k(\alpha_2+1)-1}}{p_2^k - 1} \cdots \frac{p_r^{k(\alpha_r+1)-1}}{p_r^k - 1} \tag{2}$$

for the number n with the canonical decomposition $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$. Formula (2) was already known from the time of antiquity, but it was tacitly assumed that k is a positive number in it. It finally fell into Euler's circle of interests, and he posed the question "what if k is an integer, but negative." The answer, of course, is that there is no difference; the deduction of formula (2) is perfectly formal and works equally for negative just as for positive numbers k. In particular, it holds for $k = -1$. Retaining the previous notation, we write the sum of the (-1)th powers (i.e., the inverse values) of the divisors of a given number n as $\sigma_{-1}(n)$. Formula (2) then yields

$$\sigma_{-1}(n) = \frac{1 - 1/p_1^{\alpha_1+1}}{1 - 1/p_1} \cdots \frac{1 - 1/p_r^{\alpha_r+1}}{1 - 1/p_r}$$

(we change the order of the terms in the numerator and denominator of each fraction). Hence (because all expressions in the numerators are less than 1),

$$\sigma_{-1}(n) < \frac{1}{(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_r)}. \tag{3}$$

We now replace n with $n!$ in this formula ($p_1, \ldots, p_r$ are now the prime divisors of $n!$, that is, simply speaking, all the prime numbers not exceeding n). Among the divisors of $n!$, we must certainly have $1, 2, \ldots, n$. We must therefore find the terms $1, 1/2, 1/3, \ldots, 1/n$ included in the sum $\sigma_{-1}(n!)$, and the sum of these terms is equal to $S_{-1}(n)$. According to Lemma 8, for sufficiently large n, the sum $S_{-1}(n)$ is already greater than any fixed number k given in advance. Because the other terms in $\sigma_{-1}(n!)$ are also positive, this assertion is still more applicable to the full sum. If the number of prime numbers were finite and if $p_1, \ldots, p_r$ were the complete list of them, then we would have

$$\frac{1}{(1-1/p_1)(1-1/p_2)\cdots(1-1/p_r)} > k,$$

where k is any number. This, of course, is a contradiction. □

In giving this proof, it is valuable that the proposition that the number of prime numbers is finite not only leads to a contradiction but also yields a certain quantitative characteristic of the sequence of prime numbers. Namely, rephrasing the result obtained, we can now state that if $p_1, p_2, \ldots, p_n, \ldots$ is the infinite sequence of all prime numbers, then the expression

$$\frac{1}{(1-1/p_1)(1-1/p_2)\cdots(1-1/p_r)}$$

for a sufficiently large n becomes greater than any number given in advance. Finally, this is equivalent to the fact that the denominator of this fraction for sufficiently large n becomes *less than* any number given in advance. We have proved Theorem 25.

Theorem 25. *If $p_1, p_2, \ldots, p_n, \ldots$ is the sequence of all prime numbers, then the product $(1-1/p_1)(1-1/p_2)\cdots(1-1/p_n)$ for sufficiently large n becomes less than any positive number given in advance.*

This is a first approximation to our goal. We now try to give the result obtained a more customary form.

Theorem 26. *If $p_1, p_2, \ldots, p_n, \ldots$ is the sequence of all prime numbers, then the sequence of sums $1/p_1 + 1/p_2 + \cdots + 1/p_n$ increases without limit.*

The deduction of Theorem 26 from Theorem 25 is purely formal. It does not depend on $p_1, p_2, \ldots, p_n, \ldots$ being the sequence of *prime* numbers; it could be any sequence of natural numbers for which the conclusion in Theorem 25 holds.

Lemma 9. *The inequality*

$$1 - \frac{1}{n} \geq \frac{1}{4^{1/n}} \tag{4}$$

holds for any natural number $n > 1$.

Because both sides of inequality (4) are positive, we raise them to the power n and obtain the *equivalent* inequality

$$\left(1-\frac{1}{n}\right)^n \geq \frac{1}{4}, \tag{5}$$

which we prove. Expanding the left-hand side of inequality (5) in accordance with the binomial formula, we obtain

$$\begin{aligned}\left(1-\frac{1}{n}\right)^n &= 1 - n\frac{1}{n} + \frac{n(n-1)}{2!}\frac{1}{n^2} - \\ &\quad - \frac{n(n-1)(n-2)}{3!}\frac{1}{n^3} + \cdots + (-1)^n\frac{1}{n^n}.\end{aligned} \tag{6}$$

The absolute value of the terms in the right-hand side of equality (6) form the sequence C_n^k/n^k. We examined such a sequence of numbers in connection with the Bernoulli scheme in Sec. 10 (formula (7) in Chap. 3). More precisely, if we set $p = 1/(n+1)$ and $q = 1-1/(n+1) = n/(n+1)$ in those formulas, then we obtain $p + q = 1$ and $p^k q^{n-k} = (n+1)^{-n} n^{n-k}$, that is, the numbers we obtain differ from those in formula (6) only in the factor $\big(n/(n+1)\big)^n$ that is common to all. In our case, the expression $(n+1)p - 1$ is equal to zero. We proved in Sec. 10 that if $k > (n+1)p - 1$ (if $k > 0$ in our case), then the $(k+1)$th term is less than the kth. This means that all numbers in the sequence C_n^k/n^k for $k = 1, 2, \ldots, n$ decrease monotonically. (We here refer to Chap. 3 to show how the questions we consider are connected with each other. It would be easy to write the ratio of the $(k+1)$th term to the kth term directly and verify that it is less than one.)

We see that the first two terms in the right-hand side of formula (6) cancel. The second two terms (after a reduction that you can easily perform) yield $1/3 - 1/(3n^2)$. This number is not less than $1/4$ for $n \geq 2$ (verify this!). And the remaining terms group into pairs in which the first term is positive and the second term is negative. But as we saw, the absolute value of the second term in each pair is less than the first. Therefore, each pair yields a positive contribution to sum (6). If n is odd, then the number of terms in the right-hand side of formula (6) is even (it is equal to $n + 1$), and the sum exactly subdivides into $(n + 1)/2$ pairs. And if n is even, then one positive term $1/n^n$ remains after pairing the terms. In either case, the right-hand side thus consists of a term that is not less than $1/4$ plus some additional positive terms. This proves inequality (5) and consequently proves the lemma. □

Theorem 26 is now almost obvious. For any p_i, we have

$$1 - \frac{1}{p_i} \geq \frac{1}{4^{1/p_i}}$$

according to the lemma. Multiplying these inequalities for $i = 1, \ldots, n$, we obtain

$$\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_n}\right) \geq \frac{1}{4^{1/p_1+1/p_2+\cdots+1/p_n}}.$$

If the sum $1/p_1 + \cdots + 1/p^n$ did not exceed a certain value k for all n, then it would follow that

$$\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_n}\right) \geq \frac{1}{4^k}.$$

This contradicts Theorem 25. □

According to Theorem 26, the sum $1/p_1 + 1/p_2 + \cdots + 1/p_n$ will be greater than any previously specified number C if we take all prime numbers less than a certain number N whose choice depends on the number C. However, calculations show that the sequence of sums $1/p_1 + 1/p_2 + \cdots + 1/p_n$ grows exceptionally slowly, that is, N must be chosen very large for the sum to be greater than even a fairly small number C. For example, the first term yields the value $1/2$. The sum of three terms, corresponding to the prime numbers 2, 3, and 5, is already equal to $31/30$, that is, already greater than 1. But the sum first becomes greater than 2 only when we add the values $1/p$ for all prime numbers not exceeding 277. However, for $N = 10\,000$, that is, when we include $1/p$ for all prime numbers $p < 10\,000$, we obtain a value less than 3. For $N = 10^7$ (that is, ten million), this sum is still less than 3, and for the enormous value $N = 10^{18}$ (a million trillion), it is less than 4. Nevertheless, Theorem 26 confirms that the sum becomes greater than any, even extremely large, given number C, but then the number N must be chosen to be simply humongous! This is a curious example showing that numerical experiments can suggest a totally wrong answer—and the situation is obviously the same with a physical experiment.

In connection with Theorem 26, we come upon a new type of question. If N is a subset of a finite set S, then we can say how much less than S N is by comparing the numbers of their elements, for example, calculating the ratio $n(N)/n(S)$. But now we have two infinite subsets: the set of natural numbers and the set of prime numbers contained within it. How to compare them? Theorem 26 offers one possibility of comparison, not very simple at first glance. It can be applied to any sequence of natural numbers $a = a_1, a_2, \ldots, a_n, \ldots$. According to Lemma 8, the sums of the inverse values for the sequence of all natural numbers (that is, the sums

$S_{-1}(n)$) increase without limit. We can consider a sequence a "densely" distributed among the natural numbers if the same property is preserved for it, that is, the sums

$$\frac{1}{a_1}, \quad \frac{1}{a_1}+\frac{1}{a_2}, \quad \ldots, \quad \frac{1}{a_1}+\frac{1}{a_2}+\cdots+\frac{1}{a_n}, \quad \ldots$$

increase without limit. This means that sufficiently many natural numbers are retained in the sequence a for the sums of the inverses of its terms to be not much less than the sums $S_{-1}(n)$ of the inverses of all natural numbers. But if the sums of the inverse values of a sequence a remain bounded, then we can consider it "sparsely" distributed in the ranks of the natural numbers. Theorem 26 confirms that the sequence of prime numbers is "dense." The most extreme "sparse" case is where the sequence a consists of only a finite number of terms.

But there do exist intermediate cases. For example, the sequence of squares: $1, 4, 9, \ldots, n^2, \ldots$. The corresponding sums $1+1/4+1/9+\cdots+1/n^2$ are naturally denoted by $S_{-2}(n)$. We prove that it is bounded, irrespective of n. For this, we use the same approach used to prove Lemma 8. Let m be such that $2^m \geq n$. Then $S_{-2}(n) \leq S_{-2}(2^m)$. We subdivide the sum $S_{-2}(2^m) = 1 + 1/2^2 + 1/3^2 + \cdots + 1/2^{2m}$ into parts:

$$(1) + \left(\frac{1}{2^2}\right) + \left(\frac{1}{3^2}+\frac{1}{4^2}\right) + \cdots + \left(\frac{1}{(2^{m-1}+1)^2} + \cdots + \frac{1}{2^{2m}}\right).$$

Each part

$$\frac{1}{(2^{k-1}+1)^2} + \cdots + \frac{1}{2^{2k}}$$

again contains 2^{k-1} terms, and the first term here is the largest. Therefore, each such part does not exceed $2^{k-1}/(2^{k-1}+1)^2 < 2^{k-1}/(2^{k-1})^2 = 1/2^{k-1}$. Hence,

$$S_{-2}(2^m) \leq 1+1+\frac{1}{2}+\frac{1}{2^2}+\cdots+\frac{1}{2^{m-1}} = 1+\frac{1-1/2^m}{1-1/2} \leq 1+\frac{1}{1-1/2} = 3,$$

that is, $S_{-2}(n)$ does not exceed 3.

Theorem 26 thus shows that the prime numbers, for example, are more densely distributed among the natural numbers than the squares.

Problems:

1. Prove that for any $k > 1$ and all natural numbers n, the sums $S_{-k}(n) = 1/1^k + 1/2^k + \cdots + 1/n^k$ are bounded.
2. Let the sequence a be an arithmetic progression: $a_0 = p$, $a_1 = p+q$, $a_2 = p+2q, \ldots, a_n = p+nq, \ldots$ for some natural numbers p and q. Prove that the sums $1/a_1$, $1/a_1+1/a_2, \ldots, 1/a_1+1/a_2+\cdots+1/a_n, \ldots$ increase without limit.

3. Let the sequence a be a geometric progression: $a_0 = c$, $a_1 = cq$, $a_2 = cq^2$, $\ldots$, $a_n = cq^n$, $\ldots$, where c and q are some natural numbers. Is it "dense" or "sparse" in the sequence of natural numbers?
4. Let $p_1, \ldots, p_n, \ldots$ be the sequence of all prime numbers. Prove that the expression
$$\frac{1}{\left(1-\frac{1}{p_1^2}\right)\left(1-\frac{1}{p_2^2}\right)\cdots\left(1-\frac{1}{p_n^2}\right)}$$
is bounded for all n.

13. Distribution of Prime Numbers

In this section, we again attempt to estimate how much the sequence of prime numbers differs from the entire sequence of natural numbers. For this, we replace the more elaborate method of comparing "dense" and "sparse" sequences, which arose by itself from Euler's proof in the preceding section, with a more naive method that first comes to mind. Namely, we try to answer the naive question "what portion of the natural numbers consists of prime numbers" by determining how many prime numbers there are that are less than 10, how many less than 100, how many less than 1000, and so on. For any natural number n, the number of prime numbers not exceeding n is denoted by $\pi(n)$: $\pi(1) = 0$, $\pi(2) = 1$, $\pi(4) = 2, \ldots$. What can we say about the ratio $\pi(n)/n$ when n increases without limit?

We first consider what a table can tell us. Any assertion or question about natural numbers can be checked for all natural numbers not exceeding a certain limit N. Such a situation plays a role in number theory (the study of the properties of natural numbers) that is played by the possibility of an actual experiment in physics. In particular, we can calculate the value of $\pi(n)$ for $n = 10^k$, $k = 1, 2, \ldots, 10$. We obtain the table on the next page.

We see that the ratio $n/\pi(n)$ constantly increases, and this means that $\pi(n)/n$ constantly decreases. That is, the portion of natural numbers that are prime numbers comes closer and closer to zero as n increases. According to the table, we can say that "prime numbers comprise a zero portion of all natural numbers." Euler thus formulated it, although his considerations did not include a complete proof. We formulate this assertion precisely and then prove it.

Theorem 27. *For sufficiently large n, the ratio $\pi(n)/n$ is less than any positive number given in advance.*

n	$\pi(n)$	$\dfrac{n}{\pi(n)}$
10	4	2.5
100	25	4.0
1 000	168	6.0
10 000	1 229	8.1
100 000	9 592	10.4
1 000 000	78 498	12.7
10 000 000	664 579	15.0
100 000 000	5 761 455	17.4
1 000 000 000	50 847 534	19.7
10 000 000 000	455 059 512	22.0

To prove the theorem, we must somehow estimate the value of the expression $\pi(n)$. For actual calculation of its value, we begin with the prime number 2 and cross out all other numbers divisible by 2 and not exceeding n. We then take the first remaining number—in this case, 3—and cross out all other numbers divisible by 3 and not exceeding n. We repeat this process until all numbers not exceeding n have been crossed out or used. The numbers not crossed out (2, 3, and so on) are all the prime numbers not exceeding n. This approach was already used in antiquity and is called the *sieve of Eratosthenes*.

We apply this approach to our problem. Suppose we have already found r prime numbers: $p_1, p_2, \dots, p_r$. Then the next prime numbers not exceeding n are contained among the numbers not exceeding n that are "not crossed out," that is, among those numbers $m \le n$ that are not divisible by one of the numbers $p_1, p_2, \dots, p_r$. But we investigated the number of numbers not exceeding n and not divisible by one of the prime numbers $p_1, p_2, \dots, p_r$ in Chap. 3—it is given by formula (25) in Sec. 9. The expression in that formula can be replaced with the simpler expression $n(1-1/p_1)\cdots(1-1/p_n)$, as was proved there, and the resulting error does not exceed 2^r (formula (28) in Chap. 3). Therefore, the number s of numbers $m \le n$ not divisible by one of the prime numbers $p_1, p_2, \dots, p_r$ satisfies the inequality

$$s \le n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)+2^r. \tag{7}$$

All the $\pi(n)$ prime numbers not exceeding n are included either among the r prime numbers $p_1, p_2, \dots, p_r$ or among the s numbers covered by inequality (7). Hence, $\pi(n) \le s + r$, and this means that

$$\pi(n) \leq n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)+2^r+r. \qquad (8)$$

That inequality (8) contains the product $(1-1/p_1)\cdots(1-1/p_r)$ is remarkable, and Theorem 25 already gives us information about its magnitude.

We can now turn directly to the proof of Theorem 27. Let an arbitrarily small positive number ε be given. We must find a number N such that $\pi(n)/n < \varepsilon$ for all $n > N$. In inequality (8), we replace r with the larger value 2^r (see Problem 6 in Sec. 2) to obtain the simpler inequality

$$\pi(n) \leq n\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)+2^{r+1}. \qquad (9)$$

There are two terms in the right-hand side of inequality (9), and we choose N such that each term does not exceed $\varepsilon n/2$ for $n \geq N$. It then follows from inequality (9) that $\pi(n) < \varepsilon n$ and hence $\pi(n)/n < \varepsilon$. But we recall that the number r has so far been arbitrary in our considerations. We first choose r such that the first term does not exceed $\varepsilon n/2$ and then choose N such that the second term does not exceed $\varepsilon n/2$. The first choice is possible by virtue of Theorem 25. It states that for sufficiently large r, the product $(1-1/p_1)\cdots(1-1/p_r)$ is less than any positive number given in advance. We can take $\varepsilon/2$ for such a positive number. Then the first term in inequality (9) does not exceed $\varepsilon n/2$. The matter is even simpler for the second term. Now, we have already chosen r. We choose N such that $2^{r+1} < \varepsilon N/2$. For this, we must choose $N > 2^{r+2}/\varepsilon$. Then $2^{r+1} < \varepsilon N/2 \leq \varepsilon n/2$ for any $n \geq N$. Theorem 27 is proved. □

We note that if we take an arithmetic progression $am+b$, even with a very large difference a, that is, appearing very rarely, then the number of terms in this progression not exceeding n coincides with the number of integers m for which $am \leq n-b$, that is, $\big[(n-b)/a\big]$. In Sec. 9, we saw that $\big[(n-b)/a\big]$ differs from $(n-b)/a$ by not more than 1. Therefore, the number of terms in the progression not exceeding n is not less than $(n-b)/a-1$. Its ratio to n is not less than

$$\frac{1}{n}\left(\frac{n-b}{a}-1\right)=\frac{1}{a}-\frac{1}{n}\frac{b}{a}-\frac{1}{n}.$$

As n increases, this number approaches $1/a$ and does not become arbitrarily small. Therefore, Theorem 27 would not be true if we took any arithmetic progression for the sequence. This shows that the prime numbers are distributed more sparsely than any arithmetic progression.

Problems:

1. Let p_n denote the nth prime number. Prove that for any arbitrarily large positive number C, the inequality $p_n > Cn$ holds for sufficiently large n. *Hint*: Use the fact that $\pi(p_n) = n$.
2. Consider the natural numbers with the property that their representation in the decimal system does not contain a specified digit (for instance, 0). Let $q_1, q_2, \dots, q_n, \dots$ be these numbers written in ascending order, and let $\pi_1(n)$ denote the number of such numbers not exceeding n. Prove that for sufficiently large n, the ratio $\pi_1(n)/n$ is less than any positive number given in advance. Prove that the sums

$$\frac{1}{q_1}, \quad \frac{1}{q_1} + \frac{1}{q_2}, \quad \dots, \quad \frac{1}{q_1} + \dots + \frac{1}{q_n}, \quad \dots$$

are bounded. *Hint*: Do not try to copy the proof of Theorem 27. Subdivide the sum into parts with the denominator ranging from 10^k to 10^{k+1}. Find the number of numbers q_i in such an interval. The answer depends on the digit chosen for exclusion: $r = 0$ or $r \neq 0$.

Supplement: The Chebyshev Inequality for $\pi(n)$

We place this material in a supplement first for a formal reason: we must use logarithms here, and the rest of the text does not assume familiarity with them. We recall that the *logarithm of a number x to the base a* is a number y such that

$$a^y = x.$$

This is written as

$$y = \log_a x.$$

Always in what follows, we assume that $a > 1$, and we consider positive numbers x. The basic properties of logarithms follow directly from the definition:

$$\log_a(xy) = \log_a x + \log_a y, \qquad \log_a c^n = n \log_a c, \qquad \log_a a = 1.$$

We have $\log_a x > 0$ if and only if $x > 1$. The logarithm function is monotonic, that is, $\log_a x \leq \log_a y$ if and only if $x \leq y$.

If the base of the logarithm is not shown here, then we assume that it is 2: $\log x$ means $\log_2 x$.

The second reason for segregating the following considerations in a supplement consists in the following. In the other parts of the book, the logic of the arguments is clear, why we go along namely that path (so I hope, at least). We here encounter a case, not rare in mathematical research, where some new thought seems to fall out the blue sky, as it were, and even the author is often unable to explain where it came from. About such situations, Euler said, "It sometimes seems to me that my pencil is smarter than I." Understandably, it is the result of uncounted trials, much cogitation, and the working of the subconscious mind.

We continue to study the question of the ratio $\pi(n)/n$ as n increases without limit. We once more examine the table on page 129, which shows the values of $\pi(n)$ for $n = 10^k$, $k = 1, 2, \ldots, 10$. We focus on the last column of the table, which gives the ratios $n/\pi(n)$ for certain values of n. We notice that when passing from $n = 10^k$ to $n = 10^{k+1}$, that is, when dropping down one line in the table, the values $n/\pi(n)$ change by almost the same amount. Namely, the first number is equal to 2.5; the second differs from it by 1.5; and the differences are equal to 2, 2.1, 2.3, 2.3, 2.3, 2.4, 2.3, and 2.3. We see that all these numbers are very close to one value: 2.3. Not trying to solve the riddle of why this value for the time being, we propose that even further beyond the bounds of our table, the number $n/\pi(n)$ when passing from $n = 10^k$ to $n = 10^{k+1}$ will increase by an amount even closer to a certain fixed constant α. This would mean that $n/\pi(n)$ for $n = 10^k$ would be very close to αk. But if $n = 10^k$, then $k = \log_{10} n$ by definition. Then it is natural to propose that for other values of n, the value of $n/\pi(n)$ is very close to $\alpha \log_{10} n$. This means that $\pi(n)$ is very close to $cn/\log_{10} n$, where $c = \alpha^{-1}$.

Many mathematicians were fascinated by the secret of the distribution of prime numbers and tried to discover it based on tables. In particular, Gauss was interested in this question almost in childhood. His interest in mathematics evidently began with a childhood interest in numbers and constructing tables. In general, great mathematicians were virtuosos of calculation and were able to perform enormous calculations, sometimes mentally. (Euler even struggled with insomnia in this way!) When Gauss was 14 years old, he constructed a table of prime numbers (true, less comprehensive than our table on page 129) and came to the same proposition we just formulated. It was later considered by many mathematicians. But the first result was proved more than half a century later, by Chebyshev in 1850.

Theorem 28. *There exist constants c and C such that for all $n > 1$*

$$c\frac{n}{\log n} \leq \pi(n) \leq C\frac{n}{\log n}. \tag{10}$$

We present a proof that is a result of simplications of Chebyshev's original proof subsequently given by many mathematicians. The principal idea of the proof is unchanged. Before turning to the proof, we make a few remarks concerning the formulation of the theorem. What is the base of the logarithm considered here? Answer: any base. It follows immediately from the definition of a logarithm that $\log_b x = \log_b a \log_a x$ (we need only replace a with $b^{\log_b a}$ in the relation $a^{\log_a x} = x$, and we obtain $b^{\log_b a \log_a x} = x$, which shows that $\log_b x = \log_b a \log_a x$). Therefore, if inequality (10) is proved for $\log_a n$, then it also holds for $\log_b n$ with c replaced with $c/\log_b a$ and C replaced with $C/\log_b a$.

Inequality (10) indeed expresses the thought suggested by the table that $\pi(n)$ is "close" to $cn/\log n$ for some constant c. Why are there two constants in the theorem (c and C) when there was only one constant c in our hypothetical considerations? Is it impossible to replace the two constants in the theorem with one in some sense? We consider these questions after proving the theorem.

The secret key to the proof of the Chebyshev theorem is properties of the binomial coefficients C_n^k: primarily the fact that they are integers and some properties of their divisibility by prime numbers. We list the properties that we need in the proof.

First is the assertion (proved in Sec. 6) that the sum of all binomial coefficients C_n^k for $k = 0, 1, \ldots, n$ is equal to 2^n. Because the sum of positive terms is not less than each term, we obtain

$$C_n^k \leq 2^n. \tag{11}$$

Large binomial coefficients will be especially useful for us. We saw in Chap. 2 that for even $n = 2m$, the coeeficient C_{2m}^m is larger than the others. For odd $n = 2m + 1$, there are two equal coefficients C_{2m+1}^m and C_{2m+1}^{m+1} that are larger than the others. We pay special attention to them. In particular,

$$C_{2n}^n = \frac{2n(2n-1)\cdots(n+1)}{1 \cdot 2 \cdots n}. \tag{12}$$

If we group the factors of the numerator with the factors of the denominator in reverse order, then we obtain

$$C_{2n}^n = \frac{2n}{n}\,\frac{2n-1}{n-1}\cdots\frac{n+1}{1}.$$

Obviously, each factor in this formula is not less than 2; therefore,

$$C_{2n}^n \geq 2^n. \tag{13}$$

We now consider properties of the divisibility of binomial coefficients by prime numbers. In expression (12), the factors in the numerator are obviously divisible by all prime numbers not exceeding $2n$ and greater than n. Such prime numbers cannot divide the factors of the denominator. Therefore, they do not cancel and are divisors of C_{2n}^n. The number of prime numbers distributed between $2n$ and n is equal to $\pi(2n)-\pi(n)$, and all of them are greater than n. Therefore,

$$C_{2n}^{n} \geq n^{\pi(2n)-\pi(n)}. \tag{14}$$

An analogous assertion holds, of course, for the "middle" coefficients $C_{2n+1}^{n} = C_{2n+1}^{n+1}$ with an odd lower index. Writing them in the form

$$C_{2n+1}^{n} = \frac{(2n+1)\cdots(n+2)}{1\cdot 2\cdots n},$$

we see that $\pi(2n+1)-\pi(n+1)$ prime numbers not exceeding $2n+1$ and greater than $n+1$ divide the numerator and cannot be canceled with the denominator. Because they are greater than $n+1$, we have

$$C_{2n+1}^{n} > (n+1)^{\pi(2n+1)-\pi(n+1)}. \tag{15}$$

A remarkable connection between binomial coefficients and prime numbers is already revealed in inequalities (14) and (15).

Finally, we introduce the last property of binomial coefficients needed for the proof. Although it is entirely simple, in contrast to the previous properties, it is not entirely obvious.

Lemma 10. *For any binomial coefficient C_n^k, the power of a prime number dividing it does not exceed n.*

We stress that we are speaking not of the *degree* but of the *power itself.* That is, we assert that if p^r divides C_n^k, where p is a prime number, then $p^r \leq n$. For example, $C_9^2 = 9\cdot 4$ is divisible by 9 and by 4, and both numbers do not exceed 9.

We write the binomial coefficient in the form

$$C_n^k = \frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k}. \tag{16}$$

The prime number p we are considering must divide the numerator of this fraction. We let m denote the factor containing the maximum power of p (or one of them if there are several) and let p^r denote that maximum power. It is obvious that $n \geq m \geq n-k+1$ for $k \geq 1$. We set $n-m=a$ and $m-(n-k+1)=b$. Then $a+b=k-1$, and C_n^k can be written as

$$C_n^k = \frac{(m+a)(m+a-1)\cdots(m+1)m(m-1)\cdots(m-b)}{k!}. \tag{17}$$

The factor m is now fundamental for us, and we write the product in the numerator with a factors to the left of it and b factors to the right. We transform the denominator analogously:

$$k! = (1 \cdot 2 \cdots a)(a+1) \cdots (a+b)(a+b+1).$$

Because $(a+1)(a+2)\cdots(a+b)$ as a product of b consecutive natural numbers is divisible by $b!$, this product can be written as $a!b!l$, where l is an integer.

We can now write C_n^k in the convenient form

$$C_n^k = \frac{m+a}{a}\,\frac{m+a-1}{a-1}\cdots\frac{m+1}{1}\,\frac{m-1}{1}\cdots\frac{m-b}{b}\,\frac{m}{l}, \qquad (18)$$

where we move the factor m/l to the end.

We note that in each of the factors $(m+i)/i$ or $(m-j)/j$, where $i = 1, \dots, a$ and $j = 1, \dots, b$, the power of p in the numerator completely cancels with the denominator; therefore, after canceling the common factor in the numerator and denominator, only the denominator can be divisible by p (although it can also be relatively prime to p). Indeed, we consider the fraction $(m+i)/i$ as an example (the fraction $(m-j)/j$ is treated in exactly the same way). Let i by exactly divided by p^s, that is, $i = p^s u$, where u is relatively prime to p. If $s < r$, then $m+i$ is also exactly divisible by p^s: setting $m = p^r v$ (we recall that m is divisible by p^r), we obtain $m + i = p^s(u + p^{r-s}v)$. And if $s \geq r$, then in exactly the same way, $m+i$ is divisible by p^r. Recalling the choice of m (it is divisible by the largest power of p among all numbers from n to $n-k+1$, and this power is p^r), we conclude that a larger power of p than the rth power cannot divide $m+i$. Therefore, p^r cancels in the numerator and denominator, and a number remains in the numerator that is not divisible by p. As a result, we see that of all the factors in expression (18), p can be retained only in the numerator of the last one, that is, in m. But the power of p dividing m is p^r, and this means that product (18) cannot be divided by a larger power of p than p^r. Because p^r divides m and $m \leq n$, we have $p^r \leq n$. The lemma is proved. □

We consider what this tells us about the canonical decomposition $C_n^k = p_1^{\alpha_1} \cdots p_m^{\alpha_m}$. First, the prime numbers $p_1, \dots, p_m$ can appear only from the numerator of expression (16), which means that all $p_i \leq n$ and the number of them m is therefore less than $\pi(n)$. According to the lemma, $p_i^{\alpha_i} \leq n$ for $i = 1, \dots, m$. As a result, we obtain

$$C_n^k \leq n^{\pi(n)}. \qquad (19)$$

We can now begin the actual proof of the Chebyshev theorem, that is, inequality (10). We note that it is sufficient for us to prove the satisfaction of the inequality just for all n beginning from some fixed boundary n_0. For all $n < n_0$, satisfaction of the inequality can be achieved by decreasing the constant c and increasing the constant C. If you want to obtain the explicit value of these constants most economically, then you can verify that inequality (10) is satisfied for $n \le n_0$ by constructing a table of prime numbers (in our considerations here, n_0 turns out to be not very large).

We begin by combining inequalities (13) and (20) for the binomial coefficient C_{2n}^n. We obtain $2^n \le C_{2n}^n \le (2n)^{\pi(2n)}$ and consequently

$$2^n \le (2n)^{\pi(2n)}. \tag{20}$$

Taking the logarithm to the base 2 of both sides (we recall that we write $\log_2 x = \log x$) and using the monotonicity of logarithms, we obtain $n \le \pi(2n) \log 2n$, which means

$$\pi(2n) \ge \frac{n}{\log 2n} = \frac{1}{2} \frac{2n}{\log 2n},$$

that is, the left inequality in (10) with the constant $c = 1/2$. But so far, it is proved only for even values n. For odd values of the form $2n+1$, we use the monotonicity of logarithms and the function $\pi(n)$. It follows that

$$\pi(2n+1)\log(2n+1) \ge \pi(2n)\log 2n.$$

Substituting the inequality obtained for $\pi(2n)$ in this expression, we see that

$$\pi(2n+1) \ge \frac{n}{\log 2n} \frac{\log 2n}{\log(2n+1)} = \frac{n}{\log(2n+1)}.$$

Because always $n \ge (2n+1)/3$, it follows that

$$\pi(2n+1) \ge \frac{1}{3} \frac{2n+1}{\log(2n+1)}.$$

The left inequality in (10) is thus proved for odd n and $c = 1/3$. This means that the left inequality in (10) holds for all n and $c = 1/3$.

We turn to the proof of the right inequality in (10). We prove it by induction on n. First let n be even. Instead of n, we write $2n$. We combine inequality (11) for the coefficient C_{2n}^n (that is, we replace n with $2n$ and k with n) with inequality (14). As a result, we obtain

$$n^{\pi(2n)-\pi(n)} \le 2^{2n}.$$

Passing to logarithms, we have

$$\begin{aligned} \pi(2n) - \pi(n) &\le \frac{2n}{\log n}, \\ \pi(2n) &\le \pi(n) + \frac{2n}{\log n}. \end{aligned} \tag{21}$$

In accordance with the induction assumption, we can consider the inequality we need already proved: $\pi(n) \le Cn/\log n$ with a constant C, whose value we later determine more precisely. Substituting in formula (21), we obtain

$$\pi(2n) \le C\frac{n}{\log n} + \frac{2n}{\log n} = \frac{(C+2)n}{\log n}.$$

But we wanted to prove the inequality $\pi(2n) \le C \cdot 2n/\log 2n$. For this, it remains to select a constant C such that the inequality

$$\frac{(C+2)n}{\log n} \le \frac{2Cn}{\log 2n} \tag{22}$$

is satisfied for all n beginning from some point.

This is already a simple school exercise, not connected with the properties of prime numbers. We cancel n on both sides of the inequality, and noting that $\log 2n = \log 2 + \log n = 1 + \log n$, we let x denote $\log n$. Then inequality (22) becomes

$$\frac{C+2}{x} \le \frac{2C}{1+x}.$$

Multiplying both sides by $x(1+x)$ (because $x > 0$) and combining like terms, we write it in the form

$$(C-2)x \ge C+2.$$

Obviously, we must choose C such that $C - 2 > 0$. Taking $C = 3$, for example, we find that the inequality is satisfied for $C = 3$ and all $x \ge 5$. Because x denotes $\log n$, this means that the needed inequality is satisfied for $n \ge 2^5 = 32$, $2n \ge 64$.

It only remains to consider the case with an odd value having the form $2n + 1$. For this, we combine inequality (11) (replacing n with $2n + 1$ and k with n) with inequality (15). We obtain the inequality

$$2^{2n+1} \ge (n+1)^{\pi(2n+1)-\pi(n+1)}.$$

Taking the logarithms, we obtain the inequality

$$2n+1 \ge \bigl(\pi(2n+1) - \pi(n+1)\bigr)\log(n+1).$$

From this, we use the induction assumption about $\pi(n+1)$ as previously to obtain

$$\pi(2n+1) \le C\frac{n+1}{\log(n+1)} + \frac{2n+1}{\log(n+1)}.$$

The needed inequality $\pi(2n+1) \leq C(2n+1)/\log(2n+1)$ will be proved if we verify that

$$C\frac{n+1}{\log(n+1)} + \frac{2n+1}{\log(n+1)} \leq C\frac{2n+1}{\log(2n+1)} \tag{23}$$

for an appropriate choice of the constant C and for all n beginning from some point. This is again a school exercise, although slightly more complicated than the previous one. To make it easier to compare the two sides, we replace $2n+1$ in the left-hand side with the larger value $2(n+1)$:

$$C\frac{n+1}{\log(n+1)} + \frac{2n+1}{\log(n+1)} \leq \frac{(C+2)(n+1)}{\log(n+1)}. \tag{24}$$

To transform the right-hand side, we note that $2n+1 \geq (3/2)(n+1)$ for $n \geq 1$ and that $\log(2n+1) \leq \log(2n+2) = 1+\log(n+1)$. Therefore,

$$\frac{2n+1}{\log(2n+1)} \geq \frac{(3/2)(n+1)}{1+\log(n+1)}. \tag{25}$$

Combining inequalities (24) and (25), we see that inequality (23) will be proved if we prove that

$$\frac{(C+2)(n+1)}{\log(n+1)} \leq \frac{(3/2)C(n+1)}{1+\log(n+1)}.$$

We cancel $n+1$ in both sides and set $\log(n+1) = x$. We obtain the inequality

$$\frac{C+2}{x} \leq \frac{(3/2)C}{1+x},$$

which is solved in exactly the same way as the previously analyzed case. We must multiply both sides by $x(1+x)$ and combine like terms. We obtain the inequality $(C+2)x + C + 2 \leq (3/2)Cx$ or

$$\left(\frac{1}{2}C - 2\right)x \geq C + 2.$$

Setting $C = 6$, we see that the inequality holds for $x \geq 8$, that is, $n+1 \geq 2^8$, $2n+1 \geq 511$. The right inequality in (10) is thus proved for the constant $C = 6$ and all values of n beginning with 511. The theorem is proved. □

We note that Theorem 27 is a very simple consequence of the theorem just proved. Indeed, if $\pi(n) \leq Cn/\log n$, then $\pi(n)/n \leq C/\log n$.

And because logarithms change monotonically and increase without limit ($\log 2^k = k$), $\pi(n)/n$ becomes less than any positive number. On the other hand, the proof of the Chebyshev theorem is based on completely different ideas than those used to prove Theorem 27.

In conclusion, we return once more to the propositions that can be made from examining the table on page 129. From it, we guessed that $n/\pi(n)$ is close to $C \log_{10} n$ with some definite constant C: the first two digits in the decimal representation of C^{-1} have the form 2.3. Hence, we can conclude that $\pi(n)$ is close to $C^{-1}n/\log_{10} n$. This expression can be given the simpler form $n/\log_e n$ if a new logarithm base e is chosen such that $C \log_{10} n = \log_e n$. But as was mentioned previously, always $\log_b x = \log_b a \log_a x$, and our relation is therefore satisfied if $C = \log_e 10$. Substituting the value $x = b$ in the relation $\log_b x = \log_b a \log_a x$, we obtain $\log_b a \log_a b = 1$, and the relation $C = \log_e 10$ that interests us can be rewritten as $C^{-1} = \log_{10} e$.

Fourteen-year-old Gauss certainly paid attention to these relations and guessed what the number e is for which $\log_{10} e$ is close to $(2.3)^{-1}$. Such a number was well known by that time specifically because logarithms to such a base have many useful properties (e is its conventionally accepted symbol). Logarithms to the base e are called *natural* logarithms and are denoted by ln: $\log_e x = \ln x$. Here, we are compelled to assume that the reader is familiar with natural logarithms.

The natural proposition following from studying the table is thus that $\pi(n)$ becomes ever closer to $n/\ln n$. The proved Chebyshev theorem (if natural logarithms are used) confirms the existence of two constants c and C such that $cn/\ln n \leq \pi(n) \leq Cn/\ln n$ beginning from some n. That hypothetical sharpening, which can be obtained from the table, asserts that the inequality $cn/\ln n \leq \pi(n) \leq Cn/\ln n$ is satisfied beginning with some n *whatever* constants $c < 1$ and $C > 1$ we might choose. This assertion is called the asymptotic law of the distribution of prime numbers. It was stated by Gauss and other mathematicians at the end of the 18th and beginning of the 19th century. After the proof of the Chebyshev theorem in 1850, the matter seemed to be only determining the constants c and C more precisely and bringing them closer together. However, the asymptotic law of the distribution of prime numbers was proved only half a century later, at the very end of the 19th century, on the basis of completely new ideas proposed by Riemann.

Problems:

1. Prove that $p_n > an \log n$ for some constant $a > 0$. *Hint*: Use the fact that $\pi(p_n) = n$.
2. Prove that $\log n < \sqrt{n}$ beginning from some point (determine it). *Hint*: Reduce the problem to proving that the inequality $2^x > x^2$ holds for real x beginning

from some point. Let $n \leq x \leq n+1$, where n is an integer. Reduce it to proving the inequality $2^n \geq (n+1)^2$ and use induction.

3. Prove that $p_n < Cn^2$ for some constant C. *Hint*: Apply the inequality in the preceding problem, and use the fact that $n = \pi(p_n)$.
4. Prove that $p_n < An \log n$ for some constant A.
5. Prove that the degree a of the highest power p^a that divides $n!$ is equal to

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

   Here, $[r/s]$ denotes the integer quotient of r divided by s, the sum includes all k for which $p^k \leq n$, p denotes an arbitrary prime number, and n denotes an arbitrary natural number.
6. Using the result of Problem 5, give a different proof of Lemma 10 in the supplement.
7. Prove that if $p_1, \ldots, p_r$ are prime numbers included between m and $2m+1$, then their product does not exceed 2^{2m}.
8. Determine the constants c and C for which inequality (10) is satisfied for all n.
9. Try to find the largest possible c and the smallest possible C for which inequality (10) is satisfied for all n beginning from some point. (Chebyshev himself used a very ingenious sharpening of his arguments to prove that it is possible to set $c = 0.694$ and $C = 1.594$.)