CHAPTER I

DIVISIBILITY AND INDETERMINATE EQUATIONS OF FIRST DEGREE

§ 1. Divisibility. By *natural numbers* we mean the numbers $1, 2, \ldots$, by *integers* we mean the natural numbers, the number zero and the negative numbers $-1, -2, -3, \ldots$

We say that an integer a is *divisible* by an integer b if there is an integer c such that $a = bc$. We then write

$$b \mid a.$$

We call b a *divisor* of a and a a *multiple* of b.

We write $b \nmid a$ if b does not divide a.

Since for each integer b we have $0 = 0 \cdot b$, every integer is a divisor of zero. Since for each integer a we have $a = a \cdot 1$, we see that 1 is a divisor of every integer.

Suppose now that x, y, z are integers such that

$$x \mid y \quad \text{and} \quad y \mid z. \tag{1}$$

Then there exist integers t and u such that $y = xt$ and $z = yu$. The number $v = tu$ is an integer (as the product of two integers). Thus, since $z = xv$, we obtain $x \mid z$. This proves that relations (1) imply the relation $x \mid z$ which means that a divisor of a divisor of an integer is a divisor of that integer. We express this by saying that the relation of divisibility of integers is *transitive*. It follows that if $x \mid y$, then $x \mid ky$ for every integer k.

It is easy to prove that a divisor of each of two given integers is a divisor of their sum and their difference. Moreover, if $d \mid a$ and $d \mid b$, then, for arbitrary integers x and y, $d \mid ax + by$.

In fact, the relations $d \mid a$ and $d \mid b$ imply that there exist integers k and l such that $a = kd$, $b = ld$, whence $ax + by = (kx + ly)d$ and consequently, since $kx + ly$ is an integer, $d \mid ax + by$.

Any two of the formulae $a = bc$, $-a = b(-c)$, $a = (-b)(-c)$, $-a = (-b)c$ are equivalent. Hence also any two of the formulae

$$b \mid a, \quad b \mid -a, \quad -b \mid a, \quad -b \mid -a$$

are equivalent. Consequently while examining divisibility of integers we can restrict ourselves to the investigation of divisibility of natural numbers.

It follows from the definition of the relation $b|a$ that if $0|a$, then $a=0$. If, however, $a\neq 0$, then every divisor b of the integer a is different from zero and, consequently, $-b$ is also a divisor of a. Thus for an integer a, $a\neq 0$, the divisors b of a can be arranged in pairs $(b,-b)$. Therefore, in order to find all the divisors of an integer, it is sufficient to find the natural ones and then join to each of them the negative divisor of the same absolute value.

It seems at first sight that the notions of divisor and multiple are, in a sense, dual. It is much easier, however, to find the multiples of an integer than the divisors of it. In fact, the multiples of an integer a are, clearly, all the integers of the form ka, where k is an arbitrary integer. Consequently, the multiples of a form the sequence

$$\ldots,\ -2a,\ -a,\ 0,\ a,\ 2a,\ \ldots,$$

which is infinite in both directions. On the other hand, the task of finding the set of the divisors of a is by no means simple. This might seem strange, since the set of the divisors is finite and the set of the multiples is infinite.

If a natural number a is divisible by a natural number d, then $d\leqslant a$. Thus, in order to find all the positive divisors of an integer a, it suffices to divide a by the natural numbers $1,2,\ldots,a$ successively and select those for which the quotient is an integer. Since for each natural number a the number of those quotients is finite, there exists a method, theoretically at least, for finding all the divisors of a given integer. The difficulty is, then, of a practical nature, and indeed for some natural numbers we are unable to find all the divisors. For instance, we cannot do this, for the time being at least, for the number $a=2^{101}-1$, which has 31 digits. This turns out to be much too tedious a task even with the aid of computing machines. It may seem interesting that we can prove (cf. Chapter X, § 3) that there exist exactly two divisors of the number a, different from the trivial ones: 1 and $2^{101}-1$, but we cannot find either of them. For the number 2^{101}, however, which is greater than a, we can, clearly, find all the natural divisors. They are 102 in number and form a geometric progression $1,2,2^2,2^3,\ldots,2^{101}$. We cannot find any of the non-trivial divisors of the number $2^{128}+1$ either. We do not even know the exact number of them, which is, as we know greater than three (compare Chapter X).

Sometimes the divisors of a natural number have been found by the use of electronic computers. This was the case with the number $(18!-1)$: $:59=108514808571661$. With the aid of the computer SWAC, D. H. Lehmer discovered that the number has exactly four natural divisors. They are 1, the number itself, 22663 and 478749547 (cf. Gabard [3], pp. 218-220).

To the divisors of natural numbers and the number of them we shall return in Chapter IV.

The solution of the problem whether a given integer is divisible by another one may involve serious difficulties, which sometimes can be overcome by the use of electronic computers. For example, the fact that the number $a=2^{65536}+1$ is divisible by the number $m=825753601$ has been found in this way. The reason why this particular fact has been of special interest will be given later (Chapter X, § 4). The number a has 19729 digits, and so it would be a very tedious task even to write it down. However, the problem was not to divide a by m but to decide whether a is divisible by m or not, and the computations necessary for that could be simplified to the extent accessible to a computer.

We present here another example of the solution of a similar problem. This is the problem of divisibility of the number $2^{2^{1945}}+1$ by the number $5\cdot 2^{1947}+1$. The first number has more than 10^{580} digits and it is clearly impossible to write down all of them; the second one has 587 digits. Here again, owing to the special form of the first number, the necessary computations could be simplified to such an extent that electronic computers could be used. We return to this problem in Chapter X, § 4.

EXERCISES. **1.** Prove that if a and b are natural numbers, then $a!b!|(a+b)!$.

Proof. The theorem is true if at least one of the numbers a and b is equal to 1, since for each natural b we have $(b+1)!=b!(b+1)$, whence $1!b!|(1+b)!$. Thus the theorem is true for $a+b=2$, since in this case $a=1$ and $b=1$. Suppose that n is a natural number greater than 2 and that the theorem is true for all natural numbers whose sum is equal to n. Let a and b be two natural numbers for which $a+b=n+1$. We already know that the theorem is true if at least one of the numbers a and b is equal to 1, and thus we may assume that $a>1$ and $b>1$. From the assumption that the theorem is true for the natural numbers whose sum is equal to n and from the equalities $(a-1)+b=n$, $a+(b-1)=n$ we infer that $(a-1)!b!|$ $|(a+b-1)!$ and $a!(b-1)!|(a+b-1)!$. But $(a+b)!=(a+b-1)!(a+b)=(a+b-1)!a$ $+(a+b-1)!b$, and since $(a-1)!b!|(a+b-1)!$ and $(a-1)!a=a!$, $a!b!|(a+b-1)!a$. Similarly, by $a!(b-1)!|(a+b-1)!$, we deduce that $a!b!|(a+b-1)!b$. Hence, by the identity for $(a+b)!$, we conclude that $a!b!|(a+b)!$, which proves the theorem for natural numbers whose sum is equal to $n+1$. From this by induction the theorem follows for all natural a and b.

2. Prove that, for a natural number k, the product $P=(a+1)(a+2)\ldots(a+k)$ is divisible by $k!$.

Proof. Plainly, $P=(a+k)!/a!$. Hence, in virtue of exercise 1 (for $b=k$), the theorem follows.

3. Prove that if $a_1,a_2,\ldots,a_m$ are natural numbers $(m\geqslant 2)$, then $a_1!a_2!\ldots a_m!|$ $|(a_1+a_2+\ldots+a_m)!$

Proof. As follows from exercise 1 the theorem is true for $m=2$. Suppose it is true for a given natural number m and let $a_1,a_2,\ldots,a_m,a_{m+1}$ be natural numbers. We then have

$$(a_1+a_2+\ldots+a_m)!\,a_{m+1}!\,|\,(a_1+a_2+\ldots+a_m+a_{m+1})!,$$

which, by the assumption that the theorem is true for the number m, implies the theorem for $m+1$. Thus, by induction, the theorem follows.

In particular, for $m = 3$, $a_1 = n$, $a_2 = 2n$, $a_3 = 3n$, with $n = 1, 2, \ldots$, we obtain

$$n!\,(2n)!\,(3n)!\,|\,(6n)!, \qquad n = 1, 2, \ldots$$

4. Prove that if S is a set of natural numbers such that for any two numbers of the set S their difference and their sum belong to S and d is the least natural number belonging to the set S, then S is the set of the natural multiples of the number d.

Proof. By hypothesis, the sum of any two numbers belonging to the set S belongs to S. Hence, by an easy induction we infer that the sum of any finitely many numbers of the set S belongs to S. Accordingly, in the case of equal numbers, the numbers nd, with $n = 1, 2, \ldots$ belong to S. In other words each natural multiple of the number d belongs to S.

On the other hand, suppose that k belongs to the set S and that k is not a multiple of d. Consequently, dividing k by d we obtain the positive reminder $r < d$. We have $k = qd+r$, where q is a natural number, for if $q = 0$, we would have $k \leqslant r < d$ and hence $k < d$, contrary to the assumption that d was the least number belonging to the set S. The number qd is then a natural multiple of the number d and as such belongs to the set S. Consequently, the natural number $r = k - qd$, as the difference of two numbers of the set S, belongs to S, which is impossible, since $r < d$. This proves that each number of the set S is a natural multiple of the number d, and this completes the proof of the theorem.

§ 2. Least common multiple. Let $a_1, a_2, \ldots, a_n$ be a finite sequence of integers. Every integer which is divisible by each of the integers a_i $(i = 1, 2, \ldots, n)$ is called a *common multiple* of the integers $a_1, \ldots, a_n$. Such is the product of the integers $a_1, a_2, \ldots, a_n$, for instance. If at least one of the integers $a_1, a_2, \ldots, a_n$ is zero, then clearly only the integer 0 is their common multiple. If, however, none of the integers a_i $(i = 1, 2, \ldots, n)$ is zero, there are infinitely many common multiples of these integers, e.g. all integers of the form $ka_1a_2\ldots a_n$, k being an integer. In this case there exist also common multiples which are natural numbers; for instance $|a_1a_2\ldots a_n|$, where $|x|$ denotes the module of the number x. In every set of natural numbers there exists the smallest number; consequently, the set of the common multiples of integers $a_1, a_2, \ldots, a_n$, which are natural numbers, contains the smallest one; it is called the *least common multiple* of the integers $a_1, a_2, \ldots, a_n$ and denoted by $[a_1, a_2, \ldots, a_n]$.

THEOREM 1. *Every common multiple of natural numbers $a_1, a_2, \ldots, a_n$ is divisible by their least common multiple.*

Proof. Suppose, contrary to theorem 1, that there exists a common multiple M of the integers $a_1, a_2, \ldots, a_n$ which is not divisible by their least common multiple N. Let

$$M = qN+r,$$

where r is a natural number $< N$. Hence $r = M - qN$. Let i be any of the numbers $1, 2, \ldots, n$. Since M and N are multiples of the integer a_i,

there exist integers x_i and y_i such that $M = x_ia_i$ and $N = y_ia_i$. Therefore $r = M - qN = (x_i - qy_i)a_i$, whence $a_i | r$ for all $i = 1, 2, \ldots, n$, which implies that the natural number r is a common multiple of the integers $a_1, a_2, \ldots, a_n$ and is smaller than their least common multiple N; this is clearly impossible.

§ 3. Greatest common divisor. Let S be a given (finite or infinite) set of natural numbers, such that at least one of them, for instance a_0, is different from zero. Every integer d which is a divisor of each of the integers of the set S is called a *common divisor* of the integers of the set S. Clearly, the integer 1 is an example of a common divisor of the integers of S.

Every integer d which is a common divisor of the integers of the set S is, clearly, a divisor of the natural number $|a_0|$, and so its module is less than $|a_0|$. It follows that the number of common divisors of the integers of the set S is finite, and therefore there exists the greatest one among them; that number is called the *greatest common divisor* of the integers of the set S, and is denoted by d_S. d_S is plainly a natural number. Now, let d denote an arbitrary common divisor of the integers of the set S and let $N = [d, d_S]$. Further, let a be an integer of the set S. We have $d | a$ and $d_S | a$, which proves that a is a common multiple of the divisors d and d_S, whence, by theorem 1, $[d, d_S] | a$. The number $N = [d, d_S]$ is then a divisor of the integers of the set S and, since d_S is the greatest common divisor of those integers, $N \leqslant d_S$. But the natural number N, as the least common multiple of the numbers d and d_S, is divisible by d_S, whence $N \geqslant d_S$. Thus $N = d_S$, and so $d | d_S$. This proves the following

THEOREM 2. *If S is a set (finite or infinite) of integers among which at least one is different from zero, then there exists the greatest common divisor of the integers of the set S. Moreover, the greatest common divisor is divisible by any other common divisor of the integers of the set S.*

It can be proved (cf. Schinzel [7]) that if $f(x)$ is a polynomial of degree n with integer coefficients and k is an arbitrary integer, then the greatest common divisor of the numbers $f(x)$, x running over the set of integers, is equal to the greatest common divisor of the following $n+1$ integers: $f(k), f(k+1), f(k+2), \ldots, f(k+n)$. Thus, for instance, if $f(x) = x^3 - x$, then, in virtue of what we have stated above, the greatest common divisor of the integers $f(x)$, x being an integer, is equal to the greatest common divisor of the integers $f(-1) = 0$, $f(0) = 0$, $f(1) = 0$, $f(2) = 6$, i.e. it is equal to 6.

§ 4. Relatively prime numbers. Two integers a and b whose greatest common divisor is equal to 1 are called *relatively prime.*

THEOREM 3. *Dividing each of two integers a and b by their greatest common divisor we obtain relatively prime numbers.*

Proof. Let a and b be two integers, d their greatest common divisor and $a_1 = a/d$, $b_1 = b/d$. If the integers a_1 and b_1 were not relatively prime, their greatest common divisor d_1 would be greater than 1, and then we should have $a_2 = a_1/d_1$ and $b_2 = b_1/d_1$, a_2 and b_2 being integers. But then we would obtain the equalities $a = dd_1a_2$, $b = dd_1b_2$, implying that the integer dd_1 is a common divisor of the integers a and b, whence $dd_1 \leqslant d$, which is impossible, since $d_1 > 1$. This shows that the integers a_1 and b_1 must be relatively prime, which completes the proof of theorem 3.

The greatest common divisor of integers $a_1, a_2, \ldots, a_n$ is denoted by $(a_1, a_2, \ldots, a_n)$.

The argument used to prove theorem 3 will also prove the following

THEOREM 3[a]. *Dividing each of the integers $a_1, a_2, \ldots, a_n$ by their greatest common divisor we obtain integers whose greatest common divisor is equal to* 1.

Let r be a rational number (i.e. the ratio a/b of two integers a and b with $b \neq 0$). Multiplying, if necessary, the denominator of r by -1, we may assume that $b > 0$. If $(a, b) = d$, then putting $a/d = a_1$, $b/d = b_1$ we obtain, by theorem 3, relatively prime numbers a_1 and b_1 with $b_1 > 0$, since b has been assumed to be > 0. We then have $r = a/b = a_1/b_1$. Thus every rational number can be written as a fraction whose numerator is an integer and denominator a natural number, the numerator and the denominator being relatively prime.

Now we prove that *if* $(a, b) = 1$ *and* $c \mid a$, *then* $(c, b) = 1$.

In fact, if $(c, b) = d$, then $d \mid b$ and $d \mid c$, whence, in virtue of $c \mid a$, we obtain $d \mid a$. Consequently, d is a common divisor of the integers a and b, thus, by theorem 2, it is a divisor of their greatest common divisor $= 1$, whence $d = 1$, which proves that $(c, b) = 1$.

For every finite sequence of natural numbers $a_1, a_2, \ldots, a_n$ we can easily find a natural number a which is relatively prime to every number of the sequence. Such is, for instance, the number $a = a_1a_2 \ldots a_n + 1$; for, every common divisor d_i of the integers a and a_i, where i is any number of the numbers $1, 2, \ldots, n$, is also a divisor of the number $a_1a_2 \ldots a_n$ and hence a divisor of the difference $a - a_1a_2 \ldots a_n = 1$, so it is equal to 1.

From this we can easily conclude that there exists an infinite sequence of natural numbers such that any two different elements of it are relatively prime. But the formula obtained in this way for the nth term of this sequence would not be simple. A much simpler example of a sequence F_k whose any two different terms are relatively prime is obtained by setting $F_k = 2^{2^k} + 1$ $(k = 0, 1, 2, \ldots)$. In fact, let m and n be

two integers, with $m > n \geqslant 0$. As is well known for each integer x and natural number k we have $x-1 \mid x^k-1$ (since $x^k - 1 = (x-1) \times (x^{k-1} + x^{k-2} + \ldots + x + 1)$). Applying this to $x = 2^{2^{n+1}}$, $k = 2^{m-n-1}$ we obtain that $2^{2^{n+1}} - 1 \mid 2^{2^m} - 1$. Since $F_n = 2^{2^n} + 1 \mid 2^{2^{n+1}} - 1$ and $2^{2^m} - 1 = F_m - 2$, we have $F_n \mid F_m - 2$. Hence if $d \mid F_n$ and $d \mid F_m$, then $d \mid F_m - 2$, which implies $d \mid 2$. But d, as a divisor of an odd number F_m, is an odd number, and thus the relation $d \mid 2$ implies $d \mid 1$, which proves that $(F_m, F_n) = 1$ for $m > n \geqslant 0$, as required.

It is worth-while noting that the following generalization of the above is also true. If a and b are two relatively prime integers and if $2 \mid ab$, then any two different numbers in the sequence $a^{2^k} + b^{2^k}$ $(k = 0, 1, 2, \ldots)$ are relatively prime.

One can prove that if k is a natural number $\leqslant 16$, then among every k consecutive natural numbers there exists at least one number relatively prime to each of the remaining $k-1$ numbers. On the other hand, one can prove that for each natural number $k \geqslant 17$ there exists a sequence of k consecutive natural numbers $m, m+1, \ldots, m+k-1$ such that none of the numbers of the sequence is relatively prime to each of the others (cf. Pillai [4] and Brauer [2]). Here we prove this statement for $k = 17$. We claim that in this case the number $m = 2184$ satisfies our conditions. In other words, we assert that none of the consecutive natural numbers 2184, 2185, ..., 2200 is relatively prime to each of the other numbers of the sequence.

None of the numbers of the sequence which is divisible by anyone of the numbers 2, 3, 5, 7, is relatively prime to each of the other numbers of the sequence, since for each $n = 2, 3, 5, 7$ there are at least two numbers in the sequence divisible by n. There are only two other numbers in the sequence, 2189 and 2197, but the first of them as well as the number 2200, is divisible by 11 and the second one, as well as the number 2184, is divisible by 13.

EXERCISES. **1.** Prove that if m and n are natural numbers and m is odd, then $(2^m - 1, 2^n + 1) = 1$.

Proof (J. Browkin). Let d be the greatest common divisor of the numbers $2^m - 1$ and $2^n + 1$. d is an odd number and $2^m - 1 = kd$, $2^n + 1 = ld$, where k and l are natural numbers. Hence $2^m = kd + 1$, $2^n = ld - 1$, whence $2^{mn} = (kd+1)^n = td + 1$, $2^{mn} = (ld-1)^m = ud - 1$, where t and u are natural numbers.

Consequently, since $td + 1 = ud - 1$, we have $d \mid 2$, and this in view of d being odd, implies that $d = 1$.

2. Prove that for each natural number n we have $(n! + 1, (n+1)! + 1) = 1$.

Proof. If $d \mid n! + 1$ and $d \mid (n+1)! + 1$, then using the equality $(n! + 1)(n+1) = (n+1)! + n + 1$, we see that $d \mid (n+1)! + n + 1$, whence $d \mid n$ and, since $d \mid n! + 1$, we have $d \mid 1$.

§ 5. Relation between the greatest common divisor and the least common multiple.

THEOREM 4. *The product of two natural numbers is equal to the product of their least common multiple and their greatest common divisor.*

Proof. Let a and b be two natural numbers, and let $N = [a, b]$. Since ab is clearly a common multiple of the numbers a and b, theorem 1 implies that $N \mid ab$. Let $ab = dN$, where d is a natural number. Since N is a common multiple of a and b, we have $N = ka = lb$, where k and l are natural numbers. From this we obtain $ab = dN = dka = dlb$, and hence $a = dl$ and $b = dk$, which proves that d is a common divisor of the numbers a and b.

Now, let t denote an arbitrary common divisor of the numbers a and b. We have $a = ta_1$, $b = tb_1$, which implies that the number ta_1b_1 is a common multiple of the numbers a and b. Therefore, by theorem 1, we have $N \mid ta_1b_1$. Hence, for an integer u, we obtain $ta_1b_1 = Nu$. But $dN = ab = t^2a_1b_1$, whence $tNu = dN$. Consequently, $d = tu$ and $t \mid d$. Thus the natural number d is a common divisor of the numbers a and b and, moreover, every common divisor of these numbers divides d; this proves that d is the greatest common divisor of the numbers a and b, which, in view of the formula $ab = dN$, completes the proof of theorem 4.

An important special case of theorem 4 is obtained when the natural numbers a and b are relatively prime, i.e. when $d = (a, b) = 1$. Then the formula $ab = Nd$ implies $N = ab$. This proves the following

COROLLARY. *The least common multiple of two relatively prime natural numbers is equal to their product.*

§ 6. Fundamental theorem of arithmetic. Let a and b be two relatively prime natural numbers and c a natural number such that $b \mid ac$. The number ac is divisible by each of the numbers a and b, therefore, by theorem 1, it is also divisible by their least common multiple, which, in virtue of the corollary to theorem 4, is equal to ab. Thus $ac = tab$, where t is an integer, whence $c = tb$, and therefore $b \mid c$. Thus we have proved the following

THEOREM 5. *A natural number which divides the product of two natural numbers and is relatively prime to one of them is a divisor of the other.*

Theorem 5 is sometimes called the *fundamental theorem of arithmetic.* We have proved it for natural numbers, but, clearly, it remains true for all integers since the change of the sign does not affect divisibility of the numbers.

COROLLARY. *If a, b, c are integers such that $a \mid c$, $b \mid c$ and $(a, b) = 1$, then $ab \mid c$.*

Proof. If $a \mid c$, then $c = at$, where t is an integer. Since $b \mid c$, we have $b \mid at$ and hence using both the assumption that $(a, b) = 1$ and theorem 5 we obtain $b \mid t$, i.e. $t = bu$, where u is an integer; hence $c = at = abu$, and thus $ab \mid c$, as required.

As an easy corollary to theorem 5 we prove

THEOREM 6. *If a, b, c are integers such that $(a, b) = (a, c) = 1$, then $(a, bc) = 1$.*

Proof. Let $d = (a, bc)$ and $d_1 = (b, d)$. We then have $d_1 \mid b$ and $d_1 \mid d$. Since $d \mid a$, $d_1 \mid a$; we see, in virtue of the fact that $d_1 \mid a$, $d_1 \mid b$ and $(a, b) = 1$ hold, that $d_1 = 1$. Thus $(b, d) = 1$. But, since $d = (a, bc)$, $d \mid bc$, which by theorem 5 implies that $d \mid c$. In view of $d \mid a$ and by $(a, c) = 1$ we conclude that $d = 1$, i.e. $(a, bc) = 1$, as required.

From this, by an easy induction, we derive

THEOREM 6^a. *Let n be a natural number $\geqslant 2$. If $a_1, a_2, \ldots, a_n$ and a are integers such that $(a_i, a) = 1$ holds for every $i = 1, 2, \ldots, n$, then $(a_1a_2 \ldots a_n, a) = 1$.*

In other words, theorem 6^a states that an integer, which is relatively prime to each of the given integers is relatively prime to their product.

Returning to theorem 5 we see that the argument used for its proof will also prove the following generalization of it.

If a, b and c are integers such that $b \mid ac$, then $b \mid (a, b)(b, c)$.

Theorem 6^a has the following

COROLLARY 1. *If $(a, b) = 1$ and n is a natural number, then $(a^n, b^n) = 1$.*

Proof. If $(a, b) = 1$, then, by theorem 6^a (for $a_1 = a_2 = \ldots = a_n = a$), we have $(a^n, b) = 1$, whence, again by theorem 6^a (for $a_1 = a_2 = \ldots = a_n = b$), we conclude that $(a^n, b^n) = 1$.

From corollary 1 we derive

COROLLARY 2. *For natural numbers a, b, n, the relation $a^n \mid b^n$ implies the relation $a \mid b$.*

Proof. Let $(a, b) = d$. We then have $a = da_1$, $b = db_1$, where $(a_1, b_1) = 1$. Hence, in view of corollary 1, $(a_1^n, b_1^n) = 1$. Since $a^n \mid b^n$, or equivalently $a_1^n d^n \mid b_1^n d^n$, we have $a_1^n \mid b_1^n$ and $a_1^n \mid (a_1^n, b_1^n)$, which proves that $a_1^n \mid 1$, whence $a_1 = 1$, $a = d$, and consequently, by $b = db_1 = ab_1$, $a \mid b$, as required.

We note that for two natural numbers a and b the relation $a^a \mid b^b$ does not necessarily imply $a \mid b$. For instance it is easy to check that $4^4 \mid 10^{10}$, but $4 \nmid 10$; similarly $9^9 \mid 21^{21}$, but $9 \nmid 21$.

Remark. The notion of divisibility of one number by another can be extended to real numbers in the following manner. Given two real numbers α and β we say that α divides β and write $\alpha \mid \beta$ if there exists

an integer k such that $\beta = k\alpha$. In the case of this extended notion of divisibility, however, the relation $\alpha^2 \mid \beta^2$ does not necessarily imply the relation $\alpha \mid \beta$. For instance, $2 \mid 6$, but it is not true that $\sqrt{2} \mid \sqrt{6}$, since if it were, the latter relation would imply the existence of an integer k such that $\sqrt{6} = k\sqrt{2}$, which would give $k = \sqrt{3}$, whence $3 = k^2$ and thus $k > 1$, i.e. $k \geqslant 2$, and then $3 = k^2 \geqslant 4$, which, clearly, is untrue.

COROLLARY 3. *For natural numbers a, b and $n > 1$, the relation $a^n \mid 2b^n$ implies $a \mid b$.*

Proof. Let $(a, b) = d$. Consequently, $a = da_1$, $b = db_1$, where $(a_1, b_1) = 1$. Hence, by corollary 1, $(a_1^n, b_1^n) = 1$ and, in virtue of the relation $a^n \mid 2b^n$, we have $d^n a_1^n \mid 2d^n b_1^n$, whence $a_1^n \mid 2b_1^n$ and by the use of $(a_1^n, b_1^n) = 1$ and theorem 5 we have $a_1^n \mid 2$, which, since $n > 1$, implies $a_1 = 1$, and consequently $a = d$, which gives $a \mid b$.

THEOREM 7. *If a natural number is the m-th power of a rational number and m is natural, then it is the m-th power of a natural number.*

Proof. Suppose that a natural number n is the mth power of a rational number p/q. As we know from § 4, we may assume that p and q are natural numbers and that $(p, q) = 1$. Hence, by theorem 6^a, we infer that $(p^m, q) = 1$. On the other hand, by $n = (p/q)^m$, we have $nq^m = p^m$, whence $q \mid p^m$ and therefore $q \mid (p^m, q) = 1$. Thus $q = 1$ (since q is a natural number), and consequently, $n = p^m$, which means that n is the mth power of a natural number.

As an immediate consequence of theorem 7 we have the following

COROLLARY. *The m-th root of a natural number which is not the m-th power of a natural number is an irrational number.*

In particular, the numbers $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{6}$, $\sqrt{7}$, $\sqrt{8}$, $\sqrt{10}$, $\sqrt[3]{2}$, $\sqrt[3]{3}$, $\sqrt[3]{4}$ are irrational.

EXERCISES. **1.** Prove that if a, b, d are integers such that $(a, b) = 1$ and $d \mid a+b$, then $(d, a) = 1$ and $(d, b) = 1$.

Proof. Suppose that $(a, b) = 1$ and $d \mid a+b$. If $(d, a) = \delta$, then $\delta \mid d$ and $\delta \mid a$, whence, since $d \mid a+b$, $\delta \mid a+b$ and consequently $\delta \mid (a+b)-a$, which gives $\delta \mid b$. Thus $\delta \mid (a, b)$. Hence $\delta = (d, a) = 1$. The proof of the equality $(d, b) = 1$ is analogous.

2. Prove that if n, n_1 and n_2 are natural numbers, $n \mid n_1 n_2$ and none of the numbers n_1, n_2 is divisible by n, then the number

$$(*) \qquad d = \frac{n_1}{\left(n_1, \dfrac{n_1 n_2}{n}\right)}$$

is a divisor of the number n, and moreover $1 < d < n$.

Proof. In virtue of (*) we have $\dfrac{n_1}{d} = \left(n_1, \dfrac{n_1 n_2}{n}\right)$. Thus the number $\dfrac{n_1}{d}$ is natural and, consequently $n_1 = \dfrac{n_1}{d}k$, $\dfrac{n_1 n_2}{n} = \dfrac{n_1}{d}l$, where k and l are relatively prime natural numbers. We also have $k = d$, $n_2 d = nl$ and, since $(d, l) = 1$, $d \mid n$. Thus d is a divisor of the number n. If $d = 1$, then we would have $n_2 = nl$ and consequently $n \mid n_2$, contrary to the assumption. If $d = n$, then, since, by (*), $d \mid n_1$, we have $n \mid n_1$, which also contradicts the assumption. Thus d is a divisor of n for which $1 < d < n$, as required.

3. Prove that if a and b are two relatively prime natural numbers and m is and arbitrary natural number, then in the arithmetical progression $a+bk$ ($k = 0, 1, 2, \ldots$) there are infinitely many numbers relatively prime to m.

Proof. Suppose $(a, b) = 1$ and m is an arbitrary natural number. The number m is, clearly, divisible by some divisors that are relatively prime to a, e.g. the number 1. Let c denote the greatest one of them. We are going to prove that the number $a+bc$ is relatively prime to m. We have $(a, b) = 1$, and, according to the definition of c, $(a, c) = 1$. Hence $(a, bc) = 1$. From exercise 1 it follows that if $d \mid a+bc$, then $(d, a) = 1$ and $(d, bc) = 1$; thus, a fortiori, $(d, c) = 1$. On the other hand, if also $d \mid m$, then since $c \mid m$ and $(d, c) = 1$, by the corollary to theorem 5 we have $dc \mid m$. Further, since $(d, a) = 1$ and $(a, c) = 1$, the equality $(a, dc) = 1$ holds. Thus the number dc is a divisor of the number m and is relatively prime to a, but, since c is the greatest divisor having these properties, $d = 1$. So far we have proved that if d is a common divisor of the numbers $a+bc$ and m, then $d = 1$; this proves that $(a+bc, m) = 1$. From this relation we conclude that if l is an arbitrary natural number, then for $k = c+lm$ the numbers $a+bk$ and m are relatively prime, and this is what we had to prove.

4. Prove that if a and b are relatively prime natural numbers then the arithmetical progression $a+kb$ ($k = 0, 1, 2, \ldots$) contains an infinite subsequence such that any two numbers of the subsequence are relatively prime.

Proof. We define the required subsequence $u_1, u_2, \ldots$ inductively. Let $u_1 = a$. Now, let n be an arbitrary natural number. Suppose we have already defined the numbers $u_1, u_2, \ldots, u_n$ and that any two of them are relatively prime. In virtue of exercise 3, for the natural number $u_1 u_2 \ldots u_n$ there is an term of the progression $a+kb$ ($k = 0, 1, 2, \ldots$) which is relatively prime to $u_1 u_2 \ldots u_n$. Let us denote it by u_{n+1}. It is readily shown that the sequence $u_1, u_2, \ldots$ defined in this way has the desired properties.

THEOREM 8. *Suppose that a and b are two relatively prime natural numbers such that the product of them is the n-th power of a natural number, i.e. $ab = c^n$, where n is a natural number. Then the numbers a and b are themselves the n-th powers of natural numbers.*

Proof. Let $(a, c) = d$. Then $a = da_1$, $c = dc_1$, where $(a_1, c_1) = 1$. By the assumption that $ab = c^n$, we have $da_1 b = d^n c_1^n$, whence $a_1 b = d^{n-1} c^n$. But in view of $d \mid a$ and $(a, b) = 1$, we obtain $(d, b) = 1$, whence, by theorem 6^a, we obtain $(d^{n-1}, b) = 1$. The equality $a_1 b = d^{n-1} c_1^n$ implies the relation $b \mid d^{n-1} c_1^n$. Therefore, by theorem 5, $b \mid c_1^n$. On the other hand, since $(a_1, c_1) = 1$, theorem 6^a implies that $(a_1, c_1^n) = 1$ and, since the equality $a_1 b = d^{n-1} c_1^n$ gives the relation $c_1^n \mid a_1 b$, then, by theorem 5,

we obtain $c_1^n \mid b$. The relations $b \mid c_1^n$ and $c_1^n \mid b$ together imply the equality $b = c_1^n$, whence $a_1 = d^{n-1}$ and $a = da_1 = d^n$. Thus we arrive at the final conclusion that each of the numbers a and b is the nth power of a natural number.

COROLLARY. *Suppose that k, c and n are natural numbers, that $a_1, a_2, \ldots, a_k$ is a sequence of natural numbers such that any two of them are relatively prime and that $a_1 a_2 \ldots a_k = c^n$. Then every number of the sequence $a_1, a_2, \ldots, a_k$ is the n-th power of a natural number.*

§ 7. Proof of the formulae

$$(a_1, a_2, \ldots, a_{n+1}) = \big((a_1, a_2, \ldots, a_n), a_{n+1}\big) \tag{2}$$

and

$$[a_1, a_2, \ldots, a_{n+1}] = \big[[a_1, a_2, \ldots, a_n], a_{n+1}\big]. \tag{3}$$

THEOREM 9. *For natural numbers $n > 2$ and $a_1, a_2, \ldots, a_{n+1}$ formula* (2) *holds.*

Proof. Let $d = \big((a_1, a_2, \ldots, a_n), a_{n+1}\big)$. Then d is a common divisor of the numbers $(a_1, a_2, \ldots, a_n)$ and a_{n+1}. Since $(a_1, a_2, \ldots, a_n)$ is a divisor of each of the numbers $a_1, a_2, \ldots, a_n$, d must be a divisor of each of the numbers $a_1, a_2, \ldots, a_n, a_{n+1}$. Now let d' denote an arbitrary divisor of the numbers $a_1, a_2, \ldots, a_{n+1}$. In virtue of theorem 2, we have $d' \mid |(a_1, a_2, \ldots, a_n)$. Since also $d' \mid a_{n+1}$, we have, by the definition of the number d and again by theorem 2, $d' \mid d$. Thus d is a common divisor of the numbers $a_1, a_2, \ldots, a_n, a_{n+1}$, which is divisible by every common divisor of these numbers. Consequently, d is the greatest common divisor of $a_1, a_2, \ldots, a_{n+1}$. Formula (2) is thus proved.

It follows that in order to find the number $(a_1, a_2, \ldots, a_n)$ we may calculate the divisors $d_2 = (a_1, a_2)$, $d_3 = (d_2, a_3)$, $d_4 = (d_3, a_4)$, $\ldots$, $d_{n-1} = (d_{n-2}, a_{n-1})$, and $(a_1, a_2, \ldots, a_n) = (d_{n-1}, a_n)$, successively.

Thus the calculation of the greatest common divisor of arbitrarily many numbers reduces to the successive calculation of the greatest common divisor of two numbers.

THEOREM 10. *For natural numbers $n \geqslant 2$ and $a_1, a_2, \ldots, a_{n+1}$ formula* (3) *holds.*

Proof. Let $N = \big[[a_1, a_2, \ldots, a_n], a_{n+1}\big]$. Then N is a common multiple of the numbers $[a_1, a_2, \ldots, a_n]$ and a_{n+1}. Since $[a_1, a_2, \ldots, a_n]$ is a multiple of each of the numbers $a_1, a_2, \ldots, a_n$, the number N is a multiple of each of the numbers $a_1, a_2, \ldots, a_n, a_{n+1}$. Let M denote an arbitrary common multiple of the numbers $a_1, a_2, \ldots, a_n, a_{n+1}$. In virtue of theorem 1, we have $[a_1, a_2, \ldots, a_n] \mid M$. Since also $a_{n+1} \mid M$, we have again by theorem 1, $\big[[a_1, a_2, \ldots, a_n], a_{n+1}\big] \mid M$ or, equally, $N \mid M$. Thus N is a common multiple of the numbers $a_1, a_2, \ldots, a_n, a_{n+1}$

which is a divisor of every common multiple of these numbers. Consequently, N is their least common multiple. This completes the proof of formula (3).

It follows that in order to find the number $[a_1, a_2, \ldots, a_n]$ we may calculate $N_2 = [a_1, a_2]$, $N_3 = [N_2, a_3], \ldots, N_{n-1} = [N_{n-2}, a_{n-1}]$ and $[a_1, a_2, \ldots, a_n] = [N_{n-1}, a_n]$ successively.

THEOREM 11. *If n is a natural number $\geqslant 2$ and if any two of the natural numbers $a_1, a_2, \ldots, a_n$ are relatively prime, then $[a_1, a_2, \ldots, a_n] = a_1 a_2 \ldots a_n$.*

Proof. In virtue of the corollary to theorem 4, theorem 11 is true for $n = 2$. Now, let n be an arbitrary natural number $\geqslant 2$. Suppose that the theorem is true for the natural number n and that $a_1, a_2, \ldots, a_n$, a_{n+1} are natural numbers such that any two of them are relatively prime. Consequently, $(a_i, a_{n+1}) = 1$ for all $i = 1, 2, \ldots, n$. Hence, by theorem 6[a] and corollary to theorem 4, $[a_1 a_2 \ldots a_n, a_{n+1}] = a_1 a_2 \ldots a_n a_{n+1}$. But by the hypothesis, theorem 11 is true for the number n; hence $a_1 a_2 \ldots a_n = [a_1, a_2, \ldots, a_n]$, and in virtue of (3), $a_1 a_2 \ldots a_n a_{n+1} = \big[[a_1, a_2, \ldots, a_n], a_{n+1}\big] = [a_1, a_2, \ldots, a_n, a_{n+1}]$, which proves the theorem for the number $n+1$, and thus, by induction, the theorem holds for all natural numbers.

It is worth-while to note that the implication stated by theorem 11 could be reversed: if for $n \geqslant 2$ and natural numbers $a_1, a_2, \ldots, a_n$ the formula $[a_1, a_2, \ldots, a_n] = a_1 a_2 \ldots a_n$ holds, then any two of the numbers $a_1, a_2, \ldots, a_n$ are relatively prime.

One can also prove the following statement: In order that the product of $n > 2$ natural numbers be equal to the product of their greatest common divisor and their least common multiple it is necessary and sufficient that any two of those numbers be relatively prime.

This statement, however, is not true for $n = 2$, since for instance the numbers 2 and 4 are not relatively prime and $2 \cdot 4 = (2, 4) \cdot [2, 4]$.

§ 8. Rules for calculating the greatest common divisor of two numbers.

Let a and b be two given natural numbers. The process of dividing the number a by b yields the quotient q and the remainder r less than b. We have

$$a = qb + r.$$

It follows immediately from this equality that every common divisor of the numbers a and b is a divisor of the remainder $r = a - qb$, and that every common divisor of the numbers b and r is a divisor of the number a. Therefore the common divisors of a and b are the same as the common divisors of b and r. So

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

We adopt the notation $a = n_0$, $b = n_1$, $r = n_2$, and write the above equality as

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

If $n_2 = 0$, then clearly, $(n_0, n_1) = n_1$. If, however, $n_2 \neq 0$, then we can divide n_1 by n_2 and denote the remainder by n_3; again

$$(n_1, n_2) = (n_2, n_3).$$

Proceeding in this way we obtain the following sequence of equalities:

$$\begin{aligned}
&(n_0, n_1) = (n_1, n_2),\\
&(n_1, n_2) = (n_2, n_3),\\
&(n_2, n_3) = (n_3, n_4),\\
&\cdots\cdots\cdots\cdots\\
&(n_{k-2}, n_{k-1}) = (n_{k-1}, n_k),\\
&(n_{k-1}, n_k) = (n_k, n_{k+1}).
\end{aligned} \tag{4}$$

Since n_{i+1} denotes here the remainder given by the division of n_{i-1} by n_i $(i = 1, 2, \ldots, k)$, we have $n_{i+1} < n_i$ for $i = 1, 2, \ldots, k$. Therefore the n_i's are continually decreasing, i.e.

$$n_1 > n_2 > n_3 > \ldots \geqslant 0.$$

This sequence cannot be infinite, since there are only n different non-negative integers less than n. Hence in the sequence of equalities (4) there exists a last one, say $(n_{k-1}, n_k) = (n_k, n_{k+1})$. If we could have $n_{k+1} \neq 0$, then we would divide n_k by n_{k+1} and obtain another equality, $(n_k, n_{k+1}) = (n_{k+1}, n_{k+2})$, contrary to the assumption that there are only k equalities in sequence (4). Thus $n_{k+1} = 0$, and consequently $(n_{k-1}, n_k) = n_k$. Accordingly, equalities (4) imply

$$(n_0, n_1) = (n_1, n_2) = (n_2, n_3) = \ldots = (n_{k-1}, n_k) = n_k,$$

whence

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

From the above reasoning we may deduce the following rule for finding the greatest common divisor of two given natural numbers:

In order to find the greatest common divisor of two given natural numbers n_0 and n_1 we divide n_0 by n_1 and find the remainder n_2. Then we divide n_1 by n_2 and again find the remainder n_3. Continuing, we divide n_2 by n_3 and so on. At the final step we obtain a remainder which is equal to zero. The remainder obtained in the last but one step is the greatest common divisor of the numbers n_0 and n_1.

The rule we have just presented is called either the *division algorithm*, the *Euclidean algorithm*, or the *algorithm of continued fractions*. The last name will find its justification in § 9.

It follows from the Euclidean algorithm that the greatest common divisor of two given natural numbers can be obtained in finitely many divisions.

The number of the divisions, however, can be arbitrarily large for suitably chosen natural numbers a and b. As a matter of fact, *for each natural number n there exist natural numbers a_n and b_n such that in order to find their greatest common divisor by means of the Euclidean algorithm n divisions are needed.*

We prove this by providing ourselves with the sequence

$$u_1 = u_2 = 1, \quad u_n = u_{n-1} + u_{n-2}, \quad \text{where} \quad n = 3, 4, \ldots \tag{5}$$

We have

$$u_1 = 1, \quad u_2 = 1, \quad u_3 = 2, \quad u_4 = 3, \quad u_5 = 5, \quad u_6 = 8, \quad u_7 = 13, \tag{6}$$
$$u_8 = 21, \quad u_9 = 34, \quad \ldots$$

This is the *Fibonacci sequence*: its first two terms are equal to 1 and each of the following terms is the sum of the preceding two.

Let $a_n = u_{n+2}$, $b_n = u_{n+1}$. We apply the Euclidean algorithm to find the number $(a_n, b_n) = (u_{n+2}, u_{n+1})$. We obtain the following sequence of divisions:

$$\begin{aligned}
u_{n+2} &= 1 \cdot u_{n+1} + u_n,\\
u_{n+1} &= 1 \cdot u_n + u_{n-1},\\
&\cdots\cdots\cdots\cdots\\
u_4 &= 1 \cdot u_3 + u_2,\\
u_3 &= 2 \cdot u_2.
\end{aligned}$$

Evidently the number of necessary divisions is n. For example, in order to find the greatest common divisor of the numbers $u_{12} = 144$ and $u_{11} = 89$ by means of the Euclidean algorithm one needs 10 divisions.

It can easily be proved that the least numbers for which one needs exactly n divisions to find their greatest common divisor by means of the Euclidean algorithm are the numbers u_{n+2} and u_{n+1}.

We now prove the following

THEOREM 12. *The number of divisions necessary to find the greatest common divisor of two natural numbers by means of the Euclidean algorithm is not greater than 5 multiplied by the number of digits in the decimal expansion of the smaller of the numbers* (Lamé [1]).

Proof. First we prove the following property of the Fibonacci sequence u_n $(n = 1, 2, \ldots)$ defined above:

$$u_{n+5} > 10u_n \quad \text{for} \quad n = 2, 3, \ldots \tag{7}$$

A straightforward computation shows that for $n = 2$ formula (7) holds (for, $u_7 = 13 > 10u_2 = 10$). Further, let $n \geqslant 3$. In virtue of (5) we have

$$u_{n+5} = u_{n+4} + u_{n+3} = 2u_{n+3} + u_{n+2} = 3u_{n+2} + 2u_{n+1}$$
$$= 5u_{n+1} + 3u_n = 8u_n + 5u_{n-1}.$$

Since the sequence (6) is not decreasing, $u_n = u_{n-1} + u_{n-2} \leqslant 2 \cdot u_{n-1}$, whence $2u_n \leqslant 4u_{n-1}$ and therefore $u_{n+5} = 8u_n + 5u_{n-1} > 8u_n + 4u_{n-1} \geqslant 10u_n$, which implies $u_{n+5} > 10u_n$, as required.

From (7), by a simple induction, we obtain

$$u_{n+5l} > 10^l u_n, \quad n = 2, 3, \ldots; \; l = 1, 2, \ldots \tag{8}$$

Now, let n_0 and $n_1 < n_0$ be two given natural numbers. Suppose that in order to find the greatest common divisor (n_0, n_1) by means of the Euclidean algorithm the following k divisions are necessary:

$$\begin{aligned} n_0 &= q_1 n_1 + n_2, \\ n_1 &= q_2 n_2 + n_3, \\ &\cdots\cdots\cdots\cdots \\ n_{k-2} &= q_{k-1} n_{k-1} + n_k, \\ n_{k-1} &= q_k n_k. \end{aligned} \tag{9}$$

We have, of course $q_k \geqslant 2$, since for $q_k = 1$ we would have $n_k = n_{k-1}$, which is impossible because n_k is the remainder obtained by dividing n_{k-2} by n_{k-1}. Thus $n_{k-1} = q_k n_k \geqslant 2n_k \geqslant 2 = u_3$. Hence $n_{k-2} \geqslant n_{k-1} + n_k \geqslant u_3 + u_2 = u_4$, $n_{k-3} \geqslant n_{k-2} + n_{k-1} \geqslant u_4 + u_3 = u_5, \ldots, n_1 \geqslant u_{k+1}$. So, if $k > 5l$ or equivalently, $k \geqslant 5l+1$, then $n_1 \geqslant u_{5l+2}$ and, by (8) (with $n = 2$), $n_1 > 10^l$. This means, however, that n_1 has at least $l+1$ digits in the scale of ten. Thus if n_1 has l digits, then $k \leqslant l$, which shows the truth of theorem 12.

It follows from theorem 12 that in order to find by means of the Euclidean algorithm the greatest common divisor of two natural numbers the smaller of which has at most 6 digits at most 30 divisions are needed. We note that in theorem 12 the number 5 cannot be replaced by the number 4 since, as we have seen, we need 10 divisions in order to find the greatest common divisor of 144 and 89.

§ 9. Representation of rationals as simple continued fractions. Let n_0, n_1 be two given natural numbers, and (9) the sequence of equalities obtained by the repeated application of the Euclidean algorithm to the numbers n_0 and n_1. For all $i = 1, 2, \ldots, k-1$ we have

$$\frac{n_{i-1}}{n_i} = q_i + \cfrac{1}{\cfrac{n_i}{n_{i+1}}} \quad \text{and} \quad \frac{n_{k-1}}{n_k} = q_k,$$

whence

$$\frac{n_0}{n_1} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{q_4 + \ddots + \cfrac{1}{q_{k-1} + \cfrac{1}{q_k}}}}}, \tag{10}$$

which we write in the abbreviated form

$$\frac{n_0}{n_1} = q_1 + \frac{1}{|q_2} + \frac{1}{|q_3} + \frac{1}{|q_4} + \ldots + \frac{1}{|q_{k-1}} + \frac{1}{|q_k}.$$

In formulae (9) q_1 is a positive integer which is the quotient obtained by dividing the natural number n_0 by the natural number n_1, the numbers q_i, for $i = 2, 3, \ldots, k$, are natural numbers, since $n_{i-1} > n_i$. The expression on the right-hand side of formula (10), q_1 being an integer and $q_2, q_3, \ldots, q_n$ being natural numbers, is called a *simple continued fraction*.

Thus we may say that by the use of the Euclidean algorithm every rational number can be represented as a simple continued fraction.

EXAMPLES. Consider the number 314159/100000. The successive application of the Euclidean algorithm gives

$$\begin{aligned} 314159 &= 3 \cdot 100000 + 14159, \\ 100000 &= 7 \cdot 14159 + 887, \\ 14159 &= 15 \cdot 887 + 854, \\ 887 &= 1 \cdot 854 + 33, \\ 854 &= 25 \cdot 33 + 29, \\ 33 &= 1 \cdot 29 + 4, \\ 29 &= 7 \cdot 4 + 1, \\ 4 &= 4 \cdot 1. \end{aligned}$$

Thus

$$\frac{314159}{100000} = 3 + \frac{1}{|7} + \frac{1}{|15} + \frac{1}{|1} + \frac{1}{|25} + \frac{1}{|1} + \frac{1}{|7} + \frac{1}{|4}.$$

To take another example, consider the number u_{n+1}/u_n, where u_k $(k=1, 2, \ldots)$ denotes the Fibonacci sequence (cf. § 8). It follows immediately from (10) that for all natural numbers n we have

$$\frac{u_{n+1}}{u_n} = 1+\cfrac{1}{\left|1\right.}+\cfrac{1}{\left|1\right.}+\cfrac{1}{\left|1\right.}+\ldots+\cfrac{1}{\left|1\right.},$$

where the sign $\left|\right.$ appears $n-1$ times. Thus, e.g.

$$\frac{u_2}{u_1}=1, \quad \frac{u_3}{u_2}=1+\cfrac{1}{\left|1\right.}, \quad \frac{u_4}{u_3}=1+\cfrac{1}{\left|1\right.}+\cfrac{1}{\left|1\right.}$$

and so on. We could, of course, have also written

$$\frac{u_4}{u_3}=1+\cfrac{1}{\left|2\right.}.$$

We shall go into some more details concerning continued fractions in Chapter VIII.

§ 10. Linear form of the greatest common divisor.

THEOREM 13. *If $a_1, a_2, \ldots, a_m$ are $m>1$ integers such that at least one of them is different from zero, then there exist integers $t_1, t_2, \ldots, t_m$ such that*

$$(a_1, a_2, \ldots, a_m) = a_1t_1+a_2t_2+\ldots+a_mt_m. \tag{11}$$

Proof. Denote by D the set of the natural numbers defined by the rule: a number n belongs to the set D if and only if there exist integers $x_1, x_2, \ldots, x_m$ such that

$$n = a_1x_1+a_2x_2+\ldots+a_mx_m. \tag{12}$$

In other words, D is the set of all natural numbers of the form $a_1x_1+a_2x_2+\ldots+a_mx_m$, where $x_1, x_2, \ldots, x_m$ are integers.

The set D is non-empty (i.e. it contains at least one number) since if, say, $a_k \neq 0$ (where $1 \leqslant k \leqslant m$) then $|a_k|$ belongs to D because it is plainly of the form $a_1x_1+a_2x_2+\ldots+a_mx_m$, where $x_i=0$ for $i \neq k$ and x_k equals $+1$ or -1 depending on whether $a_k>0$ or $a_k<0$.

Denote by d the least natural number belonging to the set D. (The number d does exist since every set of natural numbers contains the least one.) If d belongs to the set D, then, by definition, there exist integers $t_1, t_2, \ldots, t_m$ such that

$$d = a_1t_1+a_2t_2+\ldots+a_mt_m. \tag{13}$$

But since d is the least number of the set D, for every natural number n of the form (12), where $x_1, x_2, \ldots, x_m$ are integers, the inequality $n \geqslant d$ holds.

We are going to prove that for each of the integers $x_1, x_2, \ldots, x_m$ the number $a_1x_1+a_2x_2+\ldots+a_mx_m$ is divisible by d. Suppose that this is not the case. Then, for some integers $y_1, y_2, \ldots, y_m$ the division of the number $a_1y_1+a_2y_2+\ldots+a_my_m$ by d yields a quotient q and a positive remainder r. We have $a_1y_1+a_2y_2+\ldots+a_my_m = qd+r$, whence, by (13), $r = a_1y_1+a_2y_2+\ldots+a_my_m-q(a_1t_1+a_2t_2+\ldots+a_mt_m) = a_1x_1+a_2x_2+\ldots+a_mx_m$, where $x_i = y_i-qt_i$ are, of course, integers for all $i=1, 2, \ldots, m$. Thus the natural number r is of the form (12), which implies that r belongs to the set D. But, on the other hand, r, as the remainder obtained by dividing an integer by d, is less than d, contrary to the assumption that d was the least number belonging to the set D.

We have thus proved that for arbitrary integers $x_1, x_2, \ldots, x_m$ the number $a_1x_1+a_2x_2+\ldots+a_mx_m$ is divisible by d. Hence, in particular, $d \mid a_1x_1+a_2x_2+\ldots+a_mx_m$, where $x_k=1$ and $x_i=0$ for $i \neq k$. Hence, for each $k=1, 2, \ldots, m$, $d \mid a_k$, which means that d is a common divisor of the numbers $a_1, a_2, \ldots, a_m$.

Now, let δ denote an arbitrary common divisor of the numbers $a_1, a_2, \ldots, a_m$, and let $z_1, z_2, \ldots, z_m$ be the integer for which $a_k = \delta z_k$ $(k=1, 2, \ldots, m)$. Hence, by (13), we have

$$d = a_1t_1+a_2t_2+\ldots+a_mt_m = (a_1z_1+a_2z_2+\ldots+a_mz_m)\,\delta,$$

whence $\delta \mid d$. From this we conclude that the common divisor d is equal to $(a_1, a_2, \ldots, a_m)$ because it is divisible by every common divisor of the numbers $a_1, a_2, \ldots, a_m$. Thus (12) implies (13), and this completes the proof of the theorem.

Let $a_1, a_2, \ldots, a_m$ be $m>1$ integers such that $(a_1, a_2, \ldots, a_m)=1$. By theorem 13 there exist integers $t_1, t_2, \ldots, t_m$ such that

$$a_1t_1+a_2t_2+\ldots+a_mt_m = 1. \tag{14}$$

Conversely, suppose that for given integers $a_1, a_2, \ldots, a_m$ there exist integers $t_1, t_2, \ldots, t_m$ such that equation (14) holds. The left-hand side of the equation is clearly divisible by every common divisor of the numbers $a_1, a_2, \ldots, a_m$. But, since the right-hand side of the equation is 1, we see that $(a_1, a_2, \ldots, a_m)=1$, and this proves the following theorem.

THEOREM 14. *For $m>1$ the relation $(a_1, a_2, \ldots, a_m)=1$ holds if and only if there exist integers $t_1, t_2, \ldots, t_m$ such that $a_1t_1+a_2t_2+\ldots+a_mt_m=1$.*

COROLLARY. *If for integers d, k and $a_1, a_2, \ldots, a_m$ with $m>1$ we have $(a_1, a_2, \ldots, a_m)=1$ and $d \mid ka_i$ with $i=1, 2, \ldots, m$, then $d \mid k$.*

Proof. By theorem 14, since $(a_1, a_2, \ldots, a_m) = 1$, there exist integers $t_1, t_2, \ldots, t_m$ such that $a_1t_1+a_2t_2+\ldots+a_mt_m = 1$. But since $d \mid ka_i$ for all $i = 1, 2, \ldots, m$, $d \mid ka_it_i$ for $i = 1, 2, \ldots, m$, whence we infer that $d \mid k(a_1t_1+a_2t_2+\ldots+a_mt_m)$ and, consequently, $d \mid k$, as required.

We note that theorems analogous to theorem 13 and 14 are valid for polynomials of one variable, and fail for polynomials of several variables. In fact, if $f(x, y) = x$ and $g(x, y) = y$, then the greatest common divisor of the polynomials $f(x, y)$ and $g(x, y)$ is a constant. The expression $xp(x, y)+yq(x, y)$, however, cannot be a constant different from zero whichever polynomials $p(x, y)$, $q(x, y)$ are taken (Bochner [1]).

Let us return for a while to theorem 13. It would be of some interest to find for given numbers $a_1, a_2, \ldots, a_m$ the numbers $t_1, t_2, \ldots, t_m$ for which (11) holds. The proof of the theorem does not contain any hint what to do this. (We say that it is *purely an existential proof.*) We can do this, however, with the aid of the Euclidean algorithm. We start with the case $m = 2$. Then, apart from the trivial case when one of the numbers is equal to zero, we change, if necessary, the signs of t_1 and t_2 and assume that a_1 and a_2 are natural numbers, which we denote by n_0 and n_1, respectively. Applying the Euclidean algorithm to them we obtain formulae (9). As we know, $n_k = (n_0, n_1)$. The last but one equality of (9) is equivalent to

$$n_k = n_{k-2} - q_{k-1}n_{k-1}. \tag{15}$$

Substituting here the value of n_{k-1} obtained from the last but two equality of (9), we have

$$n_k = n_{k-2} - q_{k-1}(n_{k-3} - q_{k-2}n_{k-2}) = -q_{k-1}n_{k-3} + (1 + q_{k-1}q_{k-2})n_{k-2}.$$

Further, we substitute in the last equality the value of n_{k-2} obtained from the equality last but three of (9) and so on. Proceeding in this way, we arrive after $k-2$ substitutions at the equality $n_k = n_0x+n_1y$, where x and y are integers. It is obvious that this process leads us to an effective calculation of the numbers $x = t_1$ and $y = t_2$.

In the general case, when m is an arbitrary natural number >1, we proceed by induction. Suppose that for all integers $a_1, a_2, \ldots, a_m$ we have a rule for finding the numbers $t_1, t_2, \ldots, t_m$ satisfying equality (1). Let $a_1, a_2, \ldots, a_m, a_{m+1}$ be given integers. By theorem 9 we have $(a_1, a_2, \ldots, a_{m+1}) = \big((a_1, a_2, \ldots, a_m), a_{m+1}\big)$. As we know from the reasoning above, there is a rule for finding the numbers x and y satisfying the equality

$$\big((a_1, a_2, \ldots, a_m), a_{m+1}\big) = (a_1, a_2, \ldots, a_m)x + a_{m+1}y. \tag{16}$$

We set $x_i = t_ix$ for $i = 1, 2, \ldots, m$ and $x_{m+1} = y$. In virtue of (16) and (11) we have

$$(a_1, a_2, \ldots, a_{m+1}) = a_1x_1+a_2x_2+\ldots+a_mx_m+a_{m+1}x_{m+1}, \tag{17}$$

where $x_1, x_2, \ldots, x_{m+1}$ are integers. Thus we have established a rule for finding integers $x_1, x_2, \ldots, x_{m+1}$ satisfying equation (17) provided that a rule for finding integers $t_1, t_2, \ldots, t_m$ is given.

This, by induction, completes the proof of the following assertion: *for every $m > 1$ and integers $a_1, a_2, \ldots, a_m$ such that at least one of them is different from zero there exists a rule for finding integers $t_1, t_2, \ldots, t_m$ satisfying equation* (11).

§ 11. Indeterminate equations of m variables and degree 1.

THEOREM 15. *Given $m > 1$ integers $a_1, a_2, \ldots, a_m$ at least one of which is different from zero. The equation*

$$a_1x_1+a_2x_2+\ldots+a_mx_m = b, \tag{18}$$

is solvable in integers $x_1, x_2, \ldots, x_m$ if and only if $(a_1, a_2, \ldots, a_m) \mid b$.

Proof. Suppose that there exist integers $x_1, x_2, \ldots, x_m$ satisfying equation (18). It follows immediately from (18) that every common divisor of the numbers $a_1, a_2, \ldots, a_m$ is a divisor of the number b. Thus $(a_1, a_2, \ldots, a_m) \mid b$, and this proves the necessity of the condition.

On the other hand, suppose that $d = (a_1, a_2, \ldots, a_m) \mid b$. Then there exists an integer k such that $b = kd$. Since at least one of the numbers $a_1, a_2, \ldots, a_m$ is different from zero, then, by theorem 13, there exist integers $t_1, t_2, \ldots, t_m$ satisfying equation (11). Set $x_i = kt_i$ for all $i = 1, 2, \ldots, m$. Hence, since $d = (a_1, a_2, \ldots, a_m)$, in virtue of formula (11), we have

$$a_1x_1+a_2x_2+\ldots+a_mx_m = k(a_1t_1+a_2t_2+\ldots+a_mt_m) = kd = b.$$

Thus the condition of theorem 15 is sufficient.

Theorem 15 can also be expressed in the following form:

In order that an equation of degree 1 with integral coefficients and $m > 1$ variables be solvable in integers, it is necessary and sufficient that the constant term of the equation be divisible by the greatest common divisor of the coefficients at the variables.

From the proof of theorem 15 and the fact that for given integers $a_1, a_2, \ldots, a_m$ we can effectively find integers $t_1, t_2, \ldots, t_m$ satisfying equation (11), it follows that if equation (11) is solvable in integers, then also we can effectively find integers $x_1, x_2, \ldots, x_m$ satisfying equation (11), i.e. we have a rule for finding at least one of the integral solutions of equation (18). The question arises what is the rule for finding all the integral solutions of equation (18).

We start with the case $m = 2$. Consider an equation

$$ax+by = c, \tag{19}$$

where a, b, c are integers and $(a, b) \mid c$. We may assume that both a and b are different from zero, since otherwise we would have an equation in one variable, for which we could easily find the solution. Since $(a, b) \mid c$, we can find integers x_0, y_0 such that

$$ax_0+by_0 = c. \tag{20}$$

Suppose now that x and y are arbitrary integers satisfying equation (19). From equalities (19) and (20) we derive

$$a(x-x_0) = b(y_0-y). \tag{21}$$

Since $d = (a, b)$ is the greatest common divisor of the numbers a and b, we have $a = da_1$, $b = db_1$, where a_1 and b_1 are relatively prime integers. From (21) we have

$$a_1(x-x_0) = b_1(y_0-y). \tag{22}$$

Hence, by $(a_1, b_1) = 1$ and theorem 6, we have $b_1 \mid x-x_0$, whence $x-x_0 = b_1t$, where t is an integer. By (22), $a_1b_1t = b_1(y_0-y)$, whence, since $b_1 \neq 0$, we obtain $y_0-y = a_1t$. The equalities $x-x_0 = b_1t$, $y_0-y = a_1t$ imply

$$x = x_0+b_1t, \quad y = y_0-a_1t. \tag{23}$$

We have thus proved that if x, y form integral solution of equation (19), then they can be written in the form (23), where t is an integer.

Now, let t denote an arbitrary integer. We find x and y from (23) and calculate the value of

$$ax+by = a(x_0+b_1t)+b(y_0-a_1t) = ax_0+by_0+(ab_1-ba_1)t.$$

Hence, in virtue of (20) and the identity $ab_1-ba_1 = da_1b_1-db_1a_1 = 0$ we obtain equality (19). Thus,

In order that integers x and y constitute a solution of equation (19) *it is necessary and sufficient that for some natural t formulae* (23) *hold.*

It follows that for $t = 0, \pm1, \pm2, \ldots$ formulae (23) give all the integral solutions of equation (19). Since at least one of the numbers a_1, b_1 is different from zero, if equation (19) has at least one integral solution, then it has infinitely many of them.

We now prove the following

THEOREM 16. *If a and b are relatively prime natural numbers, then there exist natural numbers u and v such that $au-bv = 1$.*

Proof. In virtue of theorem 15 there exist integers x_0 and y_0 such that $ax_0+by_0 = 1$. We choose an integer t_0 such that $t_0 > x_0/b$ and $t_0 > y_0/a$, and put $u = x_0+bt_0 > 0$ and $v = -(y_0-at_0) > 0$. Plainly, u and v are natural numbers and $au-bv = ax_0+by_0 = 1$.

From theorem 16 we derive the following three corollaries.

COROLLARY 1. *If natural numbers a, b, l, m satisfy the conditions*

$$(l, m) = 1 \quad \text{and} \quad a^l = b^m,$$

then there exists a natural number n such that $a = n^m$ and $b = n^l$.

Proof. Since $(l, m) = 1$, then, in virtue of theorem 16, there exist natural numbers r and s such that $lr-ms = 1$. Hence, since $a^l = b^m$, we have $a = a^{lr-ms} = a^{lr}/a^{ms} = (b^r/a^s)^m$. The number a is then the mth power of a rational number b^r/a^s, which, in virtue of theorem 7, implies that it is the m-th power of a natural number $n = b^r/a^s$. Thus $a = n^m$, whence $b^m = a^l = n^{ml}$, which shows that $b = n^l$. This gives $a = n^m$ and $b = n^l$, where n is a natural number as required.

COROLLARY 2. *If a and b are two relatively prime natural numbers, then every natural number $n > ab$ can be written in the form $n = ax+by$, where x, y are natural numbers.*

Proof. Let a and b be two relatively prime natural numbers, and u, v natural numbers satisfying theorem 16. We then have $au-bv = 1$, whence, for $n > ab$, $anu-bnv = n > ab$ and, consequently, $nu/b-nv/a > 1$. Therefore there exists an integer t such that $nv/a < t < nu/b$. (Such is the greatest integer less that nu/b.) Let $x = nu-bt$, $y = at-nv$. We have $x > 0$ and $y > 0$ and also $ax+by = a(nu-bt)+b(at-nv) = n$, which completes the proof of corollary 2.

We notice that in corollary 2 the number ab cannot be replaced by a smaller number. The reason is that if $(a, b) = 1$, the number ab itself does not have a representation in the form $ax+by = ab$ where x, y are natural numbers. In fact, suppose $ab = ax+by$, then $ax = (a-y)b$, whence, since $(a, b) = 1$, $b \mid x$, whence $x \geqslant b$ and then $ab = ax+by \geqslant ab+by > ab$, which is impossible.

COROLLARY 3. *Given natural numbers $a > 1, m, n$. Then*

$$(a^m-1, a^n-1) = a^{(m,n)}-1.$$

Proof. Let $\delta = (m, n)$. Then $m = \delta m_1$, $n = \delta n_1$, where m_1 and n_1 are relatively prime natural numbers. In virtue of theorem 16 there exist natural numbers u, v such that $m_1u-n_1v = 1$, hence $\delta = mu-nv$. Let $d = (a^m-1, a^n-1)$. Clearly, $a^{(m,n)}-1 \mid a^m-1$ and $a^{(m,n)}-1 \mid a^n-1$, which implies that $a^{(m,n)}-1 \mid d$. On the other hand, we have $d \mid a^m-1$, whence $d \mid a^{mu}-1$ and $d \mid a^n-1$, and this implies $d \mid a^{nv}-1$. Hence $d \mid a^{mu}-a^{nv} = a^{nv}(a^{mu-nv}-1) = a^{nv}(a^\delta-1)$. Since $d \mid a^m-1$ and $a > 1$,

we have $(d, a) = 1$ and hence $d \mid a^{\delta}-1$, consequently $d \mid a^{(m,n)}-1$, which, by the formula $a^{(m,n)}-1 \mid d$, gives $a^{(m,n)}-1 = d = (a^m-1, a^n-1)$, as required.

So far we have proved that for a linear equation of the type (19) the integral solutions are given by formulae (23). Now we are going to consider the general case of linear equation (18) with arbitrarily many variables m. The following proof of the fact that there is a method for finding the solution of equation (18) seems the simplest and easiest to remember.

We note first that we may confine ourselves to considering only equations (18) where a_i's, $i = 1, 2, \ldots, m$, are natural numbers. This is because coefficients equal to zero do not affect the solutions and if any of the a_i's is negative we may replace it by $-a_i$ and change the sign at the variable.

If any two of the coefficients a_i, $i = 1, 2, \ldots, m$ are equal, for instance $a_1 = a_2$, then setting $x_1+x_2 = x$ we obtain the equation

$$a_1 x + a_3 x_3 + a_4 x_4 + \ldots + a_m x_m = b. \tag{24}$$

From every integral solution $x_1, x_2, \ldots, x_m$ of equation (18) we can derive a solution $x, x_3, x_4, \ldots, x_m$ of equation (24) putting $x = x_1+x_2$. Conversely, from every integral solution $x, x_3, x_4, \ldots$ of (24) we can derive a solution of (18) letting x_1 be an arbitrary integer, $x_2 = x-x_1$. Thus, the problem of finding all integral solutions of equation (18) in the case where two of its coefficients are equal is equivalent to the analogous problem for equation (24) in which less number of variables occurs. If any two coefficients of equation (24) are equal we can proceed in the same way, decreasing further the number of variables. Thus, we may suppose that the coefficients of equation (18) are all different natural numbers. Let, a_1 say, be the greatest of them. Then, in particular $a_1 > a_2$. Suppose that the division of a_1 by a_2 yields the quotient k and the remainder a_2'. We then have $a_1 = a_2 k + a_2'$, where k is a natural number and a_2' is an integer such that $0 < a_2' < a_2$. Set $x_1' = kx_1+x_2$, $x_2' = x_1$, $a_1' = a_2$. We have $a_1x_1+a_2x_2 = a_2(kx_1+x_2)+a_2'x_1 = a_1'x_1'+a_2'x_2'$. Thus equation (24) can be written in the form

$$a_1' x_1' + a_2' x_2' + a_3 x_3 + \ldots + a_m x_m = b. \tag{25}$$

From every integral solution $x_1, x_2, \ldots, x_m$ of equation (24) we derive an integral solution $x_1', x_2', x_3, \ldots, x_m$ of equation (25) putting $x_1' = kx_1+x_2$, $x_2' = x_1$. Conversely, from every integral solution $x_1', x_2', x_3, \ldots, x_m$ of equation (25) we derive an integral solution of (18) putting $x_1 = x_2'$, $x_2 = x_1'-kx_2'$.

Thus the problem of finding the integral solutions of equation (18) reduces to that of solving equation (25) in which the greatest of the coefficients at the variables is less than the corresponding one in equation (18). Continuing, from equation (25) we can similarly obtain an equation in which the greatest of the coefficients at the variables is less than the corresponding one in (25). This process leads to an equation in one variable, which, if solvable, of course, can be easily solved.

Thus we have proved that for a linear equation with integral coefficients there exists a method for finding all the integral solutions. The method we have presented here is far from being the most convenient rule for finding integral solution of a linear equation in practice, it is just simple enough to present it as a proof of the existence of the solutions. The question of finding the method which is most convenient in practice is not of our interest now.

It is worth-while to note that if in (18) one of the coefficients $a_1, a_2, \ldots, a_m$, for instance a_1, equals 1, then all the integral solutions of (18) are simply obtained by taking arbitrary integers for $x_2, x_3, \ldots, x_m$ and putting

$$x_1 = b - a_2x_2 - a_3x_3 - \ldots - a_mx_m.$$

It is easy to see that if equation (18) is solvable in integers and $m > 1$, then it necessarily has infinitely many integral solutions. In fact, if $y_1, y_2, \ldots, y_m$ are integers such that $a_1y_1+a_2y_2+\ldots+a_my_m = b$, then putting $x_i = y_i+a_mt_i$ for $i = 1, 2, \ldots, m-1$ and $x_m = y_m-a_1t_1-\ldots-a_{m-1}t_{m-1}$, where $t_1, t_2, \ldots, t_{m-1}$ are arbitrary integers, we obtain integers $x_1, x_2, \ldots, x_m$ satisfying equation (18).

It is also easy to prove that if equation (18) has an integral solution $x_1, x_2, \ldots, x_m$, then the integers $x_1, x_2, \ldots, x_m$ can be written as linear combinations of $m-1$ integral parameters.

This property enables us to find the integral solutions of the systems of n linear equations of m variables. In order to do this we express each of the variables of the first equations as a linear combination with integral coefficients of $m-1$ parameters and substitute them for the variables in the remaining $n-1$ equations. Thus, regarding the parameters as variables we obtain a system of $n-1$ equations of $m-1$ variables. Proceeding in this way we finally arrive either at one equation (of one or more variables), which we have already learned how to solve, or to one or more equations with one variable.

§ 12. Chinese Remainder Theorem.

THEOREM 17. *Suppose that m is a natural number $\geqslant 2$, $a_1, a_2, \ldots, a_m$ are natural numbers such that any two of them are relatively prime, and $r_1, r_2, \ldots, r_m$ are arbitrary integers. Then there exist integers $x_1, x_2, \ldots, x_m$ such that*

$$a_1x_1+r_1 = a_2x_2+r_2 = \ldots = a_mx_m+r_m. \tag{26}$$

Proof. The theorem is true for $m = 2$, since if a_1, a_2 are relatively prime, the equation $a_1x - a_2y = r_2 - r_1$ has an integral solution in x and y.

Now let m be an arbitrary natural number $\geqslant 2$. Suppose that theorem 17 is true for the number m. Let $a_1, a_2, \ldots, a_m, a_{m+1}$ be natural numbers such that any two of them are relatively prime and let $r_1, r_2, \ldots, r_m, r_{m+1}$ be arbitrary integers. From the assumption that the theorem is true for the number m we infer that there exist integers $x_1, x_2, \ldots, x_m$ satisfying equation (26). Since each of the numbers $a_1, a_2, \ldots, a_m$ is relatively prime to the number a_{m+1}, then, by theorem 6[a], the number $a_1a_2\ldots a_m$ is also relatively prime to a_{m+1} and therefore, as we know, there exist integers t and u such that

$$a_1a_2\ldots a_mt - a_{m+1}u = r_{m+1} - a_1x_1 - r_1.$$

We set

$$x_i' = \frac{a_1a_2\ldots a_m}{a_i}t + x_i, \quad \text{where} \quad i = 1, 2, \ldots, m \text{ and } x_{m+1}' = u.$$

Plainly the numbers $x_1', x_2', \ldots, x_{m+1}'$ are integers and, as is easy to check,

$$a_1x_1' + r_1 = a_2x_2' + r_2 = \ldots = a_{m+1}x_{m+1}' + r_{m+1},$$

which by induction, completes the proof of the theorem.

It follows from theorem 17 that if any two of $m \geqslant 2$ natural numbers $a_1, a_2, \ldots, a_m$ are relatively prime and $r_1, r_2, \ldots, r_m$ are arbitrary integers, then there exists an integer k such that dividing k by $a_1, a_2, \ldots, a_m$ we obtain the remainders $r_1, r_2, \ldots, r_m$, respectively. This, by the way, is the reason why the theorem is called the remainder theorem.

It is obvious that adding to k an arbitrary multiple of the number $a_1a_2\ldots a_m$, we obtain an integer which divided by $a_1, a_2, \ldots, a_m$ gives also the remainders $r_1, r_2, \ldots, r_m$ respectively. It follows that there exist infinitely many integers which have this property.

We present here a simple application of theorem 17. Let m and s be two given natural numbers. We proved in § 4 that any two different terms of the sequence $F_k = 2^{2^k}+1$ $(k = 0, 1, 2, \ldots)$ are relatively prime. Put $a_i = F_i^s$ and $r_i = -i$ for all $i = 1, 2, \ldots, m$. For $c = a_1x_1 + r_1$ formulae (26) imply that $F_i^s x_i = a_ix_i = a_1x_1 + r_1 - r_i = c + i$, whence $F_i^s \mid c+i$ for all $i = 1, 2, \ldots, m$. Since $F_i > 1$ for $i = 1, 2, \ldots$, each of the numbers $c+1, c+2, \ldots, c+m$ is divisible by the sth power of a natural number greater than 1. Thus we have proved the following assertion:

For each natural number s there exist arbitrarily long sequences of consecutive natural numbers, each of them divisible by the s-th power of a natural number greater than 1.

§ 13. Thue Theorem.

THEOREM 18 (Thue [1]). *If m is a natural number and a an integer relatively prime to m, then there exist natural numbers x and y both less than $\sqrt{m}$ and such that the number $ax \pm y$ is divisible by m for a suitable choice of the ambigous sign $\pm$.*

Proof. The theorem is, of course, true for $m = 1$, since in this case we may set $x = y = 1$. Suppose that m is a natural number greater than 1. Let q denote the greatest natural number less than or equal to $\sqrt{m}$. Then, clearly, $q+1 > \sqrt{m}$ and hence $(q+1)^2 > m$. Consider the expressions $ax - y$, for x, y taking the values $0, 1, 2, \ldots, q$. There are $(q+1)^2 > m$ of them and, since there are only m different remainders obtained from division by m, for two different pairs x_1, y_1 and x_2, y_2, where, for instance, $x_1 \geqslant x_2$, one obtains the same remainders from division of $ax - y$ by m. Consequently the number $ax_1 - y_1 - (ax_2 - y_2) = a(x_1 - x_2) - (y_k - y_2)$ is divisible by m. We cannot have $x_1 = x_2$, since then the number $y_1 - y_2$ would be divisible by m, which, in view of the fact that $0 \leqslant y_1 \leqslant q \leqslant \sqrt{m} < m$ (since $m > 1$) and similarly $0 \leqslant y_2 < m$, is impossible because the pairs x_1, y_1 and x_2, y_2 were different. The equality $y_1 = y_2$ is also impossible, since then the number $a(x_1 - x_2)$ would be divisible by m, which, in view of the fact that the number a is relatively prime to m, would imply that $m \mid (x_1 - x_2)$, and this, in virtue of the inequalities $0 \leqslant x_1 \leqslant q < m$, $0 \leqslant x_2 \leqslant q$ and $x_1 \neq x_2$, is impossible. Thus we have both $x_1 \neq x_2$ and $y_1 \neq y_2$. Since $x_1 \geqslant x_2$, $x = x_1 - x_2$ is a natural number. The number $y_1 - y_2$ can be a negative integer, but certainly it is different from zero, so $y = |y_1 - y_2|$ is a natural number. We see that $x = x_1 - x_2 \leqslant x_1 \leqslant q \leqslant \sqrt{m}$, $y \leqslant q \leqslant \sqrt{m}$ and that for the appropriate sign $+$ or $-$ the number $a(x_1 - x_2) - (y_1 - y_2) = ax \pm y$ is divisible by m, and this is what the Thue theorem states.

By a slight modification of the proof given above we could have the following generalization of the theorem (Scholz and Schoenberg proved [1], p. 44):

If m, e and f are natural numbers such that $e \leqslant m$, $f \leqslant m < ef$, then for each integer a with $(a, m) = 1$ there exist integers x and y such that for the appropriate sign $+$ or $-$ we have

$$m \mid ax \pm y \quad \text{and} \quad 0 \leqslant x \leqslant f, \quad 0 \leqslant y \leqslant e.$$

For other generalizations of the Thue theorem, see Brauer and Reynolds [1], Mordell [6] and Nagell [6].

§ 14. Square-free numbers. An integer is called *square-free* if it is not divisible by the square of any natural number > 1. The square-free natural numbers $\leqslant 20$ are the following: 1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19.

It follows from the assertion proved at the end of § 12 that there exist arbitrarily long sequences of consecutive natural numbers such that none of them is square-free. Among every four consecutive natural numbers at least one is not square-free (since at least one of them is divisible by $4 = 2^2$). One can prove that there exist infinitely many triples of consecutive natural numbers such that each of the numbers is square-free.

It can be proved that each natural number >1 is the sum of two square-free natural numbers and in infinitely many ways a difference of such numbers (cf. Sierpiński [36]). It is also true that each sufficiently large natural number is the sum of the square-free number and the square of a natural number (Esterman [1]; cf. Nagell [1], Erdös [13]).

We prove

THEOREM 19. *Each natural number n can be uniquely represented in the form $n = k^2 l$, where k and l are natural numbers and l is square-free.*

Proof. For a given natural number n, let k denote the greatest natural number such that $k^2 \mid n$. We have $n = k^2 l$, where l is a natural number. If l were be not square-free, then we would have $l = r^2 s$, where r, s are natural numbers and $r > 1$. Thus $n = (kr)^2 s$ and consequently $(kr)^2 \mid n$, where $kr > k$, contrary to the definition of k.

Now suppose that $n = k_1^2 l_1$, where k_1, l_1 are natural numbers and l_1 is square-free. Let $d = (k, k_1)$. We have $k = dh$, $k_1 = dh_1$, where h, h_1 are natural numbers and $(h, h_1) = 1$. Since $n = d^2 h^2 l = d^2 h_1^2 l_1$, we have $h^2 l = h_1^2 l_1$ and, since $(h^2, h_1^2) = 1$, by theorem 5, we obtain $h^2 \mid l_1$, which proves that $h = 1$, since l_1 is square-free. This implies that $k = dh = d$. But since $d \mid k_1$, we have $k \mid k_1$, whence $k \leqslant k_1$ which, in virtue of the definition of k and the equality $n = k_1^2 l_1$, implies $k = k_1$, whence also $l = l_1$.

CHAPTER II

DIOPHANTINE ANALYSIS OF SECOND AND HIGHER DEGREES

§ 1. Diophantine equations of arbitrary degree and one unknown. The name of Diophantine analysis bears a branch of the theory of numbers concerning equations which are to be solved in integers. The equations themselves are called *Diophantine*. They are named after a Greek mathematician Diophantus who lived in Alexandria in the third century A. D. and occupied himself with problems reducible to the equations of the above-mentioned type.

We start with the equations of arbitrary degree and one unknown.

Suppose that the left-hand side of an equation is a polynomial with integral coefficients, i.e. let the equation be of the form

$$a_0 x^m + a_1 x^{m-1} + \ldots + a_{m-1} x + a_m = 0, \tag{1}$$

where m is a given natural number and $a_0, a_1, \ldots, a_m$ are integers with $a_0 \neq 0$ and $a_m \neq 0$.

If there is an integer x satisfying equation (1), then

$$(a_0 x^{m-1} + a_1 x^{m-2} + \ldots + a_{m-1}) x = -a_m.$$

It follows that the integer x must be a divisor of the integer a_m, therefore, since the integer a_m, being different from zero, has finitely many divisors, all the integral solutions of equation (1) can be found in finitely many trials. We just substitute the divisors (positive and negative as well) of a_m successively in equation (1) and select those which satisfy the equation. If $a_m = 0$, then clearly $x = 0$ is a solution of the equation. The other solutions are obtained by considering the equation

$$a_0 x^{m-1} + a_1 x^{m-2} + \ldots + a_{m-2} x + a_{m-1} = 0,$$

whose solutions are found in analogy to the previous case whenever $a_{m-1} \neq 0$. If $a_{m-1} = 0$, then the equation turns into an equation of degree $m-2$ and we repeat the same reasoning.

As an example we consider the equation

$$x^7 + x + 2 = 0.$$