CHAPTER VI

EULER'S TOTIENT FUNCTION AND THE THEOREM OF EULER

§ 1. Euler's totient function. The number of natural numbers $\leqslant n$ that are relatively prime to n is denoted by $\varphi(n)$ (n being a natural number). The function $\varphi(n)$ thus obtained is called *Euler's totient function*. In fact, Euler was the first to investigate this function and its properties in the year 1760. The notation $\varphi(n)$, however, is due to Gauss (it was introduced by him in 1801) — this is the reason why some authors call the function $\varphi(n)$ *Gauss's function*.

It follows immediately from the definition of $\varphi(n)$ that $\varphi(1)=1$, $\varphi(2)=1$, $\varphi(3)=2$, $\varphi(4)=2$, $\varphi(5)=4$, $\varphi(6)=2$, $\varphi(7)=6$, $\varphi(8)=4$, $\varphi(9)=6$, $\varphi(10)=4$.

If n is a prime, then, of course, every natural number less than n is relatively prime to n; accordingly for prime n,

$$\varphi(n)=n-1. \tag{1}$$

If, however, a natural number n is composite, i.e. has a divisor d such that $1<d<n$, then in the set $1, 2, \ldots, n$ there are at least the two numbers, n and d, that are not relatively prime to n; therefore $\varphi(n) \leqslant n-2$. Finally, for $n=1$ we have $\varphi(n)=n>n-1$. We thus see that formula (1) holds only in the case where n is a prime.

This establishes the truth of the following theorem:

A natural number $n>1$ is a prime if and only if for every natural number $a<n$ the congruence $a^{n-1}\equiv 1 \pmod n$ holds.

In fact, the congruence implies that $(a, n)=1$, and so, if it is valid for any $a<n$, then $\varphi(n)=n-1$, and consequently n is a prime. The condition is thus sufficient. Its necessity follows immediately from the theorem of Fermat (theorem 5, Chapter V).

It is easy to evaluate $\varphi(n)$ for any prime power $n=p^k$, k being a natural number.

The only numbers in the set $1, 2, \ldots, p^k$ which are not relatively prime to p^k are those that are divisible by p. These are the numbers pt, where t is a natural number such that $pt \leqslant p^k$, that is, such that $t \leqslant p^{k-1}$. Clearly the number of the t's is p^{k-1}. Hence it follows that in the sequence

$1, 2, \ldots, p^k$ there are exactly p^{k-1} numbers which are not relatively prime to p^k; consequently, $\varphi(p^k)=p^k-p^{k-1}$. We have thus proved

THEOREM 1. *If p is a prime and k a natural number, then*

$$\varphi(p^k)=p^{k-1}(p-1).$$

In order to obtain a formula for $\varphi(n)$, where n is an arbitrary natural number, we prove the following

LEMMA. *Let m be a natural number, l a natural number relatively prime to m, and r an arbitrary integer. Then, dividing the numbers*

$$r,\ l+r,\ 2l+r,\ \ldots,\ (m-1)l+r \tag{2}$$

by m, we obtain the set of remainders

$$0,\ 1,\ 2,\ \ldots,\ m. \tag{3}$$

Proof. Suppose that for some integers k and h with $0 \leqslant k < h < m$ the numbers $kl+r$ and $hl+r$ yield the same remainder when divided by m. Then the difference between these numbers, equal to $(h-k)l$, is divisible by m, whence, in view of $(l, m)=1$, $m \mid h-k$, which is impossible since $0<h-k<m$. Thus we see that dividing numbers (2) by m we obtain different remainders. But the number of numbers (2) is m, and this is equal to the number of the residues mod m, i.e. to the number of numbers (3). The lemma is thus proved.

THEOREM 2. *If l and m are relatively prime natural numbers, then*

$$\varphi(lm)=\varphi(l)\varphi(m). \tag{4}$$

Proof. Since $\varphi(1)=1$, theorem 2 is valid if at least one of the numbers l, m is equal to 1. Suppose that $l>1$ and $m>1$. As we know, number $\varphi(lm)$ is equal to the number of all the terms of the table

$$\begin{array}{llll}
1, & 2, & \ldots, & r, \ldots, l \\
l+1, & l+2, & \ldots, & l+r, \ldots, 2l \\
2l+1, & 2l+2, & \ldots, & 2l+r, \ldots, 3l \\
\ldots & \ldots & \ldots & \ldots \\
(m-1)l+1, & (m-1)l+2, & \ldots, & (m-1)l+r, \ldots, ml
\end{array}$$

that are relatively prime to lm, i.e. to the number of terms which are relatively prime both to l and to m.

Let r be a given natural number $\leqslant l$. We consider the rth column of the table. If $(r, l)=1$, then all the numbers of the column are relatively prime to l; if $(r, l)>1$, none of the numbers of the column is relatively prime to l. The number of the natural numbers $r<l$ for which $(r, l)=1$ is of course $\varphi(l)$, this being the number of the columns in which all the

numbers are relatively prime to l. Let us consider one of these columns, say the rth. According to the lemma, the remainders obtained by dividing the numbers of the column by m fill up the set $0, 1, 2, \ldots, m-1$, whence the number of the numbers of the column, which are relatively prime to m, is $\varphi(m)$. This shows that in each of the $\varphi(l)$ columns, the terms of which are relatively prime to l, there are $\varphi(m)$ numbers relatively prime to m. Therefore the total number of the numbers of the table, which are relatively prime to m and to l, is $\varphi(l)\,\varphi(m)$. This completes the proof of the theorem.

From theorem 2, by an easy induction, we obtain the following

COROLLARY. *If $m_1, m_2, \ldots, m_k$ are natural numbers any two of which are relatively prime, then*

$$\varphi(m_1 m_2 \ldots m_k) = \varphi(m_1)\varphi(m_2)\ldots\varphi(m_k).$$

Now let n be a natural number >1 and $n = q_1^{a_1} q_2^{a_2} \ldots q_k^{a_k}$ its factorization into prime factors. Applying the formula, just proved, for $m_i = q_i^{a_i}$, $i = 1, 2, \ldots, k$, we obtain the formula

$$\varphi(n) = \varphi(q_1^{a_1})\,\varphi(q_2^{a_2})\ldots\varphi(q_k^{a_k}).$$

But since, by theorem 1, $\varphi(q_i^{a_i}) = q_i^{a_i-1}(q_i-1)$ holds for $i = 1, 2, \ldots, k$, the following theorem 3 is valid:

THEOREM 3. *If a natural number $n>1$ yields the factorization into prime factors $n = q_1^{a_1} q_2^{a_2} \ldots q_k^{a_k}$, then*

$$\varphi(n) = q_1^{a_1-1}(q_1-1)\,q_2^{a_2-1}(q_2-1)\ldots q_k^{a_k-1}(q_k-1). \tag{5}$$

This can be rewritten in the form

$$\varphi(n) = n\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\ldots\left(1-\frac{1}{q_k}\right). \tag{6}$$

From theorem 3 one can easily deduce that, if $(a, b) = 1$, then $\varphi(ab) > \varphi(a)\varphi(b)$ and that, if $m \mid n$, then $\varphi(m) \mid \varphi(n)$.

THEOREM 4. *We have*

$$\lim_{n\to\infty} \varphi(n) = +\infty.$$

Proof (due to J. Browkin). It is sufficient to show that the inequality $\varphi(n) \geqslant \frac{1}{2}\sqrt{n}$ holds for any natural number n. Clearly, the inequality is valid for $n = 1$. Suppose that $n>1$ and let $n = 2^{a_0} q_1^{a_1} q_2^{a_2} \ldots q_k^{a_k}$ be the factorization of number n into prime factors, a_0 being a non-negative integer and $a_1, a_2, \ldots, a_k$ natural numbers. For an arbitrary natural number $a>2$ we have $a-1 > \sqrt{a}$, and for any natural number b the inequality $b-\frac{1}{2} \geqslant \frac{1}{2}b$ holds. Hence, by theorem 3,

$$\varphi(n) = 2^{a_0-1} q_1^{a_1-1} q_2^{a_2-1} \ldots q_k^{a_k-1}(q_1-1)(q_2-1)\ldots(q_k-1)$$
$$\geqslant 2^{a_0-1} q_1^{a_1-\frac{1}{2}} q_2^{a_2-\frac{1}{2}} \ldots q_k^{a_k-\frac{1}{2}} \geqslant 2^{a_0-1} q_1^{\frac{1}{2}a_1} q_2^{\frac{1}{2}a_2} \ldots q_k^{\frac{1}{2}a_k} \geqslant \tfrac{1}{2}\sqrt{n}.$$

In connection with theorem 4 we note that there exist infinitely many natural numbers n such that $\varphi(n) > \varphi(n+1)$.

In order to show this we prove

THEOREM 5. *If n is a composite natural number, then*

$$\varphi(n) \leqslant n - \sqrt{n}. \tag{7}$$

Proof. Let n denote a composite number and p_1 the least prime divisor of it. As we know, $p_1 \leqslant \sqrt{n}$, so, by formula (6),

$$\varphi(n) \leqslant n\left(1-\frac{1}{p_1}\right) \leqslant n - \frac{n}{\sqrt{n}},$$

which proves inequality (7).

Now suppose that n is a prime number >7. Then $n+1$ is a composite number and $n+1 \geqslant 9$. Hence $\sqrt{n+1} \geqslant 3$ and, by (7), $\varphi(n+1) \leqslant n+1-\sqrt{n+1} \leqslant n-2$. But, since $\varphi(n) = n-1$, we have $\varphi(n) > \varphi(n+1)$. We see that this inequality is valid for any prime number $n>7$ (as is easy to prove, it holds for $n=5$ and also for $n=7$); consequently, it holds for infinitely many natural numbers n.

The equation $\varphi(n) = \varphi(n+1)$ in natural numbers n has been a subject of interest for several authors (cf. Klee [2], Moser [1]).

As has been verified, all the solutions of the equation in natural numbers $n \leqslant 10000$ are the numbers $n = 1$, 3, 15, 104, 164, 194, 255, 495, 584, 975, 2204, 2625, 2834, 3255, 3705, 5186, 5187. It follows that the least natural number n which satisfies the equation $\varphi(n) = \varphi(n+1) = \varphi(n+2)$ is the number 5186. (It is easy to verify that the number 5186 indeed satisfies the equation. This follows immediately from the factorization of the following numbers into prime factors: $5186 = 2\cdot2593$, $5187 = 3\cdot7\cdot13\cdot19$, $5188 = 2^2\cdot1297$ and $2592 = 2\cdot6\cdot12\cdot18 = 2\cdot1296$.)

We do not know whether there exist infinitely many natural numbers n for which $\varphi(n) = \varphi(n+1)$. As regards the equation $\varphi(n+2) = \varphi(n)$, we know that for $n \leqslant 10000$ it has 80 solutions (for $n \leqslant 100$ these are $n = 4$, 7, 8, 10, 26, 32, 70, 74). The equation $\varphi(n+3) = \varphi(n)$, however, has only two solutions, $n = 3$ and $n = 5$, for $n \leqslant 10000$.

It is easy to prove that for any given natural number k the equation $\varphi(n+k) = \varphi(n)$ has at least one solution in natural numbers n (cf. exercise 11 below). It follows from the conjecture H (cf. Chapter III, § 8)

that it has infinitely many solutions for any even natural numbers k (cf. Schinzel and Sierpiński [3], p. 195). A. Schinzel and Andrzej Wakulicz [1] have proved that for every natural number $k \leqslant 2 \cdot 10^{58}$ the equation $\varphi(n+k) = \varphi(n)$ has at least two solutions in natural numbers n (cf. also Schinzel [10]).

If each of the numbers n and $n+2$ is prime, then $\varphi(n+2) = \varphi(n)+2$. The equation, however, is satisfied also by composite numbers, for example $n = 12, 14, 20, 44$. L. Moser [1] has proved that there are no composite odd numbers $n < 10000$ that satisfy this equation. This suggests a conjecture that there are no odd numbers n, except for the pairs of twin primes $n, n+2$ for which the equality $\varphi(n+2) = \varphi(n)+2$ holds. In this connection A. Mąkowski [3] has raised the question whether there exist composite natural numbers n for which the equalities $\varphi(n+2) = \varphi(n)+2$ and $\sigma(n+2) = \sigma(n)+2$ hold simultaneously.

If n is a prime, then $\varphi(n) = n-1$, so $\varphi(n) \mid n-1$. We do not know whether there exist composite natural numbers n for which $\varphi(n) \mid n-1$ [1]. On the other hand, it is easy to find all the natural numbers n for which $\varphi(n) \mid n$. It has been proved that all the numbers with this property are the numbers $n = 2^\alpha$, $\alpha = 0, 1, 2, \ldots$, and $n = 2^\alpha 3^\beta$, where α, β are natural numbers (cf. Sierpiński [25], pp. 196-197).

It follows from (5) that if $n = 2^\alpha$, where α is a natural number > 1, then $\varphi(n) = 2^{\alpha-1}$. Consequently, $2 \mid \varphi(2^\alpha)$ for $\alpha = 2, 3, \ldots$ If, however, n has an odd prime divisor p, then number $p-1$ is even and therefore, by (5), $p-1 \mid \varphi(n)$ and so $2 \mid \varphi(n)$. Since any natural number > 2 either is the kth power of 2 with $k > 1$ or has an odd prime divisor, we see that for any natural number $n > 2$ the relation $2 \mid \varphi(n)$ holds.

Since $\varphi(1) = \varphi(2) = 1$, the equation $\varphi(x) = m$, m being odd, is solvable only in the case where $m = 1$. Thus it is shown that there exist infinitely many (odd) natural numbers m for which the equation $\varphi(x) = m$ is unsolvable in natural numbers x. On the other hand, it can be proved that there exist infinitely many even natural numbers m for which the equation $\varphi(x) = m$ has no solutions in natural numbers x. We show this by proving that this is the case for the numbers $m = 2 \cdot 5^{2k}$, where $k = 1, 2, \ldots$, for instance. It follows from (5) that if $\varphi(n) = 2 \cdot 5^{2k}$, where k is a natural number, then n must have precisely one odd prime divisor. The argument is that if q_1 and q_2 were two different odd prime divisors of the number n, then, by (5), $(q_1-1)(q_2-1) \mid \varphi(n) = 2 \cdot 5^{2k}$ and so $4 \mid \varphi(n)$, which is impossible. Therefore we must have $n = 2^\alpha p^\beta$, where α is an integer $\geqslant 0$ and β a natural number. Moreover, $\alpha \leqslant 1$, since otherwise, if $\alpha \geqslant 2$, $2^{\alpha-1}(p-1) \mid \varphi(n)$, and so $4 \mid \varphi(n)$, which is impossible. In the

[1] D. H. Lehmer [2] has conjectured that there are no such numbers, F. Schuh [1] has proved that if they exist, they must have at least eleven prime factors.

case of $\alpha = 0$ we have $n = p^\beta$ and, in the case of $\alpha = 1$, $n = 2p^\beta$; so in either case we have $\varphi(n) = p^{\beta-1}(p-1) = 2 \cdot 5^{2k}$. If β were > 1, then $p = 5$ and so $p-1 = 4$, which is impossible. Therefore $\beta = 1$, whence $p = 2 \cdot 5^{2k}+1$ which is impossible since the number $5^{2k} = (5^k)^2$ is congruent to 1 with respect to the modulus 3, whence $3 \mid p$, so $p = 3$ and this is clearly false. Thus we see that the equation $\varphi(n) = 2 \cdot 5^{2k}$, where $k = 1, 2, \ldots$, has no solutions in natural numbers.

By a similar method a stronger theorem has been proved by A. Schinzel [6]. The theorem states that for every natural number s there exists a natural number m divisible by s and such that the equation $\varphi(n) = m$ has no solutions in natural numbers n. This theorem in its turn is an immediate consequence of the following result of S. S. Pillai [2], obtained in quite a different way: if $g(x)$ denotes the number of natural numbers $m \leqslant x$ for which the equation $\varphi(n) = m$ is solvable, then

$$\lim_{x \to \infty} \frac{g(x)}{x} = 0.$$

It follows from theorem 4 that for every natural number m the number of solutions of the equation $\varphi(n) = m$ in natural numbers n is finite $\geqslant 0$. Conversely, theorem 4 is an immediate consequence of this fact. The theorem of Pillai implies the following:

THEOREM 6. *For every natural number s there exists a natural number m such that the equation $\varphi(n) = m$ has more than s different solutions in natural numbers n.*

Proof. We give an elementary proof of this theorem, due to A. Schinzel in paper [5]. Let s denote a natural number and let $m = (p_1-1)(p_2-1)\ldots(p_s-1)$. We are going to prove that each of the numbers $x_1, x_2, \ldots, x_{s+1}$, where $x_i = p_1 \ldots p_{i-1}(p_i-1)p_{i+1}\ldots p_s$, $i = 1, 2, \ldots$; $x_{s+1} = p_1 p_2 \ldots p_s$ is a solution of the equation $\varphi(n) = m$.

In fact, let i be one of the numbers $1, 2, \ldots, s$. The number p_i-1 is not divisible by any prime $> p_i$, and so $p_i-1 = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_{i-1}^{\gamma_{i-1}}$, where $\gamma_1, \gamma_2, \ldots, \gamma_{i-1}$ are non-negative integers. Hence $x_i = p_1^{\gamma_1+1} p_2^{\gamma_2+1} \ldots \cdot \ldots p_{i-1}^{\gamma_{i-1}+1} p_{i+1} p_{i+2} \ldots p_s$ and consequently

$$\varphi(x_i) = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_{i-1}^{\gamma_{i-1}} (p_1-1)(p_2-1)\ldots(p_{i-1}-1)(p_{i+1}-1)\ldots(p_s-1).$$

Hence, looking at the formula for p_i-1 and recalling the definition of m, we see that $\varphi(x_i) = m$ for $i = 1, 2, \ldots, s$. Plainly, we also have $\varphi(x_{s+1}) = m$. We see that the numbers $x_1, x_2, \ldots, x_{s+1}$ are different and that they are positive integers; the theorem is thus proved.

As has been shown by P. Erdös [3], there exists an infinite increasing sequence of natural numbers m_k ($k = 1, 2, \ldots$) such that the number of solutions of the equation $\varphi(n) = m_k$ for any $k = 1, 2, \ldots$ is greater than m_k^c, where c is a positive constant. A conjecture of P. Erdös is that

for any number $\varepsilon > 0$ constant in question can be taken greater than $1-\varepsilon$.

The question arises whether for every natural number s there exists a natural number m such that the equation $\varphi(n) = m$ has precisely s solutions in natural numbers. We do not know the answer to this question even in the simple case of $s = 1$. In fact, we do not know any natural number m such that the equation $\varphi(n) = m$ has precisely one solution in natural numbers n. A conjecture of Carmichael [5] is that there is no such natural number m. As was shown by V. L. Klee Jr. [3], there are no such numbers $m \leqslant 10^{400}$.

However, it can be proved that there exist infinitely many natural numbers m such that the equation $\varphi(n) = m$ has precisely two (or precisely three) solutions in natural numbers n (cf. exercise 12 below).

For a natural number $s > 1$ denote by m_s the least natural number m such that the equation $\varphi(n) = m$ has precisely s solutions in natural numbers n (provided the number m_s exists). It can be calculated that $m_2 = 1, m_3 = 2, m_4 = 4, m_5 = 8, m_6 = 12, m_7 = 32, m_8 = 36, m_9 = 40, m_{10} = 24, m_{11} = 48, m_{12} = 160, m_{13} = 396, m_{14} = 2268, m_{15} = 704$.

We conjecture that for every natural number $s > 1$ there exist infinitely many natural numbers m such that the equation $\varphi(n) = m$ has precisely s solutions in natural numbers n. This follows from the conjecture H (cf. Schinzel [15]). The main difficulty consists in proving the existence of the number m_s, since, as has been proved by P. Erdös [18], if for a given natural number s there exists a natural number m such that the equation $\varphi(n) = m$ has precisely s solutions (in natural numbers n), then there exist infinitely many natural numbers m with this property.

We do not know whether there exist infinitely many natural numbers which are not of the form $n-\varphi(n)$ where n is a natural number. (It can be proved that the numbers 10, 26, 34 and 50 are not of this form.) We do not know whether every odd number is of this form. (The answer is in the positive, provided any even natural number > 6 is the sum of two different prime numbers.)

EXERCISES. **1.** Prove the formula of N. C. Scholomiti [1]:

$$\varphi(n) = \sum_{k=1}^{n-1} \left[\frac{1}{(n,k)}\right] \quad \text{for natural numbers } n > 1.$$

The proof follows from the remark that if $n > 1$, $k < n$ and $(n,k) = 1$, then $\left[\frac{1}{(n,k)}\right] = 1$. On the other hand, if $(n,k) > 1$, then $\left[\frac{1}{(n,k)}\right] = 0$. Therefore the right-hand side of the formula is equal to the number of natural numbers $< n$ relatively prime to n, which, for $n > 1$, is the value of $\varphi(n)$.

2. Find the natural numbers n for which $\varphi(n)$ is not divisible by 4.

Solution. They are the numbers 1, 2, 4 and the numbers p^α and $2p^\alpha$, where p is a prime of the form $4t+3$. The proof is straightforward (cf. Carmichael [1], Klee [1]).

3. Prove that there exist infinitely many pairs of natural numbers x, y, $y > x$, such that $d(x) = d(y)$, $\varphi(x) = \varphi(y)$ and $\sigma(x) = \sigma(y)$.

Proof. As is easy to see, all the equations are satisfied by the numbers $x = 3^k \cdot 568$, $y = 3^k \cdot 638$, where $k = 0, 1, 2, \ldots$ (cf. Jankowska [1]).

4. Prove that there exist infinitely many systems x, y, z such that $x < y < z$ and $d(x) = d(y) = d(z)$, $\varphi(x) = \varphi(y) = \varphi(z)$, $\sigma(x) = \sigma(y) = \sigma(z)$.

Proof. We put $x = 5^k \cdot 2^3 \cdot 3^3 \cdot 71 \cdot 113$, $y = 5^k \cdot 2^3 \cdot 3 \cdot 29 \cdot 37 \cdot 71$, $z = 5^k \cdot 2 \cdot 3^3 \cdot 11 \cdot 29 \cdot 113$.

P. Erdös [19] has proved that for any natural number s there exist s different natural numbers $a_1, a_2, \ldots, a_s$ such that

$$d(a_i) = d(a_j), \quad \varphi(a_i) = \varphi(a_j), \quad \sigma(a_i) = \sigma(a_j)$$

hold for any $1 \leqslant i < j \leqslant s$. According to a conjecture of P. Erdös one may additionally assume that any two numbers of the sequence $a_1, a_2, \ldots, a_s$ are relatively prime (cf. Erdös [20]).

5. Prove that for any natural number m there exists a natural number n such that

$$\varphi(n) - \varphi(n-1) > m \quad \text{and} \quad \varphi(n) - \varphi(n+1) > m.$$

Proof. Let p be a prime of the form $4k+3$ that is greater than $2m+3$. Then, since $p = 4k+3$, we have $\varphi(p) = 4k+2$, $\varphi(p-1) = \varphi(4k+2) = \varphi(2k+1) \leqslant 2k+1$. Therefore $\varphi(p) - \varphi(p-1) \geqslant 2k+1 > m$. We also have $p+1 = 4(k+1) = 2^\alpha l$, where $\alpha \geqslant 2$ and l is an odd number. Hence

$$\varphi(p+1) = 2^{\alpha-1}\varphi(l) \leqslant 2^{\alpha-1} l = \tfrac{1}{2}(p+1),$$

and so

$$\varphi(p) - \varphi(p+1) \geqslant p - 1 - \tfrac{1}{2}(p+1) = \tfrac{1}{2}(p-3) > m.$$

Let us mention the following fact: there exists a natural number $n > 1$ such that $\varphi(n-1)/\varphi(n) > m$ and $\varphi(n+1)/\varphi(n) > m$, and similarly there exists a natural number $n > 1$ such that $\varphi(n)/\varphi(n-1) > m$ and $\varphi(n)/\varphi(n+1) > m$ (cf. Schinzel and Sierpiński [1]).

It can be also proved (cf. Erdös and Schinzel [1]) that for any two natural numbers m and $k > 1$ there exist a natural number n such that

$$\frac{\varphi(n+i)}{\varphi(n+i-1)} > m \quad \text{for} \quad i = 1, 2, \ldots, k$$

and a natural number n such that

$$\frac{\varphi(n+i-1)}{\varphi(n+i)} > m \quad \text{for} \quad i = 1, 2, \ldots, k.$$

6. Prove that for arbitrary natural numbers a, b there exist infinitely many pairs of natural numbers x, y such that

$$\varphi(x) : \varphi(y) = a : b.$$

Proof. Let a and b be two given natural numbers. Without loss of generality we may assume that they are relatively prime. Let c denote a natural number prime to ab (there are of course infinitely many such numbers; in particular all the numbers $kab+1$, where $k = 1, 2, \ldots$, have this property). Let $x = a^2bc$, $y = ab^2c$. Since any two of the numbers a, b, c are relatively prime, $\varphi(x) = \varphi(a^2)\varphi(b)\varphi(c)$ and $\varphi(y) = \varphi(a)\varphi(b^2)\varphi(c)$. As follows easily from theorem 3, for any natural number n we have $\varphi(n^2) = n\varphi(n)$, consequently $\varphi(a^2) = a\varphi(a)$, $\varphi(b^2) = b\varphi(b)$, whence $\varphi(x):\varphi(y) = a:b$, as required.

It is worth observing that conjecture H implies the existence of infinitely many primes x, y such that $\varphi(x):\varphi(y) = a:b$ for a given pair of natural numbers a, b (cf. Schinzel and Sierpiński [3], p. 192).

7. Prove that if n is a natural number > 1, then there exist infinitely many natural numbers m such that $\varphi(m)/m = \varphi(n)/n$.

Proof. Number n, being a natural number > 1, has a prime divisor p; so we may assume that $n = p^\alpha n_1$, where α is a natural number and $(n_1, p) = 1$. Hence

$$\frac{\varphi(n)}{n} = \frac{p^{\alpha-1}(p-1)\varphi(n_1)}{p^\alpha n_1} = \frac{p-1}{p}\cdot\frac{\varphi(n_1)}{n_1}.$$

Let $m = p^\beta n_1$, where β is a natural number. By a similar reasoning, we find

$$\frac{\varphi(m)}{m} = \frac{p-1}{p}\cdot\frac{\varphi(n_1)}{n_1}, \quad \text{so} \quad \frac{\varphi(m)}{m} = \frac{\varphi(n)}{n},$$

and hence the proof follows.

It can be proved that the numbers $\varphi(n)/n$, $n = 1, 2, \ldots$, form a dense subset in the unit interval $(0, 1)$. On the other hand, there exists a dense subset of the interval $(0, 1)$ consisting of rational numbers which are not of the form $\varphi(n)/n$ (cf. Schoenberg [1], Sierpiński [25], p. 210).

K. Zarankiewicz has raised a question whether the set of the numbers $\varphi(n+1)/\varphi(n)$, $n = 1, 2, \ldots$, is dense in the set of the real numbers. A. Schinzel [3] has proved that the answer to this question is affirmative (cf. Erdős and Schinzel [1]).

8. Find all the solutions of the equation $\varphi(n) = \varphi(2n)$ in natural numbers.

Answer. Those are all the odd numbers.

9. Find all the solutions of the equation $\varphi(2n) = \varphi(3n)$ in natural numbers.

Answer. They are those even natural numbers which are not divisible by 3.

10. Find all the solutions of the equation $\varphi(3n) = \varphi(4n)$ in natural numbers n.

Answer. They are all those natural numbers which are not divisible by 2 or by 3.

11. Prove that for any natural number k there exists at least one natural number n such that $\varphi(n+k) = \varphi(n)$.

Proof. If k is an odd number, then the assertion holds, since in this case $\varphi(2k) = \varphi(k)$ and we may put $n = k$. Suppose that k is even, and let p denote the least prime which is not a divisor of k. Consequently each prime number $< p$ is a divisor of the number k. Hence $\varphi((p-1)k) = (p-1)\varphi(k)$ (this follows at once from theorem 3 — in fact, if m is a natural number such that any prime divisor of it is a divisor of a natural number k, then $\varphi(mk) = m\varphi(k)$). But, since $(p, k) = 1$, we have $\varphi(pk) = \varphi(p)\varphi(k) = (p-1)\varphi(k) = \varphi((p-1)k)$, and so putting $n = (p-1)k$, we obtain $\varphi(n+k) = \varphi(n)$, as required (cf. Sierpiński [17], p. 184).

It has been proved by A. Schinzel that for any natural number m there exists a natural number k such that the equation $\varphi(n+k) = \varphi(n)$ has more than m solutions in natural numbers n (cf. ibid. pp. 184-185).

12. Prove that there exist infinitely many natural numbers m such that the equation $\varphi(n) = m$ has precisely two solutions in natural numbers n.

Proof. Such are for instance the numbers $m = 2\cdot 3^{6k+1}$, where $k = 1, 2, \ldots$ In fact, suppose that n is a natural number such that $\varphi(n) = 2\cdot 3^{6k+1}$. Of course, number n is not a power of number 2 (because $\varphi(2^\alpha) = 2^{\alpha-1}$); consequently it must have an odd prime divisor p, and moreover, it cannot have more than one such divisors, because $\varphi(n)$ is not divisible by 4.

If $p = 3$, then $n = 3^\beta$ or $n = 2^\alpha\cdot 3^\beta$, where α and β are natural numbers. Then, by $\varphi(n) = 2\cdot 3^{6k+1}$, we obtain $2\cdot 3^{\beta-1} = 2\cdot 3^{6k+1}$ or $2^\alpha\cdot 3^{\beta-1} = 2\cdot 3^{6k+1}$. Consequently, $\alpha = 1$ and, in either case, $\beta - 1 = 6k+1$. Therefore $n = 3^{6k+2}$ or $n = 2\cdot 3^{6k+2}$ and, as is easy to verify, in any case $\varphi(n) = 2\cdot 3^{6k+1} = m$.

If $p \neq 3$, that is if $p > 3$, then the number n cannot be divisible by p^2 because, if it were, $p \mid \varphi(n) = 2\cdot 3^{6k+1}$, which for $p > 3$ is impossible. Therefore $n = p$ or $n = 2^\alpha p$, where α is a natural number. Hence, by $\varphi(n) = 2\cdot 3^{6k+1}$ we find $p-1 = 2\cdot 3^{6k+1}$ or $2^{\alpha-1}(p-1) = 2\cdot 3^{6k+1}$. Consequently, since $p-1$ is even, $\alpha = 1$ and, in any case, $p = 2\cdot 3^{6k+1}+1$, which is impossible since, by $k \geqslant 1$, we have $p > 7$ and, in virtue of the theorem of Fermat, $3^6 \equiv 1 \pmod 7$, whence $p = 2\cdot 3^{6k+1}+1 \equiv 2\cdot 3+1 \equiv 0 \pmod 7$, so $7 \mid p$. Thus we see that the equation $\varphi(n) = 2\cdot 3^{6k+1}$, where k is a natural number, has precisely two solutions, $n = 3^{6k+1}$ and $n = 2\cdot 3^{6k+2}$. The equation $\varphi(n) = 2\cdot 3$, however, has four solutions: $n = 7, 9, 14, 18$, and the equation $\varphi(n) = 2\cdot 3^2$ also has four solutions: $n = 19, 27, 38, 54$.

Remark. A. Schinzel [6] has found infinitely many natural numbers m such that the equation $\varphi(n) = m$ has precisely three solutions in natural numbers n. Such are, for instance the numbers $m = 7^{12k+1}\cdot 12$, where $k = 0, 1, 2, \ldots$ We then have $\varphi(n) = m$ for $n = 7^{12k+2}\cdot 3$, $7^{12k+2}\cdot 4$ and $7^{12k+2}\cdot 6$. The proof that there are no other solutions, though elementary, is rather long.

13. Find all the solutions of the equation $\varphi(n) = 2^{10}$ in natural numbers n.

Solution. Suppose that n is an even number, and that $n = 2^\alpha q_1^{\alpha_1} q_2^{\alpha_2}\ldots q_{k-1}^{\alpha_{k-1}}$, where $q_1, q_2, \ldots, q_{k-1}$ are odd primes, is the factorization of n into prime factors. Let $q_1 < q_2 < \ldots < q_{k-1}$. (We do not exclude the case $k = 1$, i. e. $n = 2^\alpha$). Since $\varphi(n) = 2^\alpha$, we see that

$$2^{\alpha-1} q_1^{\alpha_1-1} q_2^{\alpha_2-1}\ldots q_{k-1}^{\alpha_{k-1}-1}(q_1-1)(q_2-1)\ldots(q_{k-1}-1) = 2^{10},$$

which proves that $\alpha_1 = \alpha_2 = \ldots = \alpha_{k-1} = 1$ and $q_i = 2^{\beta_i}+1$, $i = 1, 2, \ldots, k-1$, where β_i $(i = 1, 2, \ldots, k-1)$ are natural numbers, and, finally, $\alpha - 1+\beta_1+\beta_2+\ldots+\beta_{k-1} = 10$, and so $\beta_i \leqslant 10$ for $i = 1, 2, \ldots, k-1$.

Odd prime numbers of the form $2^\beta+1$, $\beta \leqslant 10$ are the numbers $2^\beta+1$ with $\beta = 1, 2, 4, 8$ only. Therefore $k \leqslant 5$.

If $k = 1$ that is if $n = 2^\alpha$, then $\alpha - 1 = 10$, whence $\alpha = 11$ and consequently $n = 2^{11} = 2048$.

If $k = 2$, then $\alpha - 1+\beta_1 = 10$ and for $\beta_1 = 1, 2, 4, 8$ we find $\alpha = 10, 9, 7, 3$, respectively. So the values for n are $2^{10}\cdot 3 = 3072$, $2^9\cdot 5 = 2560$, $2^7\cdot 17 = 2176$ or $2^3\cdot 257 = 2056$.

If $k = 3$, then $\alpha - 1+\beta_1+\beta_2 = 10$. Here β_1 cannot be > 2 because, if it were, β_1 would be greater than or equal to 4. But, since $\beta_1 < \beta_2$ (for $q_1 < q_2$), we would obtain $\beta_2 > 4$ so $\beta_2 \geqslant 8$ and $\beta_1+\beta_2 \geqslant 12$, which is impossible. Therefore β_1 is equal

either to 1 or to 2. If $\beta_1 = 1$, then $\alpha+\beta_2 = 10$ and $\beta_2 > \beta_1 = 1$; so $\beta_2 = 2, 4$ or 8, which implies $\alpha = 8, 6, 2$, and this gives the following values for n: $2^8\cdot 3\cdot 5$, $2^6\cdot 3\cdot 17$ or $2^2\cdot 3\cdot 257$. If $\beta_1 = 2$, then $\alpha+\beta_2 = 9$, $\beta_2 = 4$ or 8, whence $\alpha = 5$ or 1 and so $n = 2^5\cdot 5\cdot 17$ or $2\cdot 5\cdot 257$.

If $k = 4$, then $\alpha - 1+\beta_1+\beta_2+\beta_3 = 10$. Since $\beta_1 < \beta_2 < \beta_3$ (which holds because $q_1 < q_2 < q_3$), in virtue of the fact that $\beta_1, \beta_2, \beta_3$ can be chosen from the numbers 1, 2, 4, 8 only, we infer that $\beta_1 = 1$, $\beta_2 = 2$, $\beta_3 = 4$, which proves that $\alpha = 4$ and so $n = 2^4\cdot 3\cdot 5\cdot 17$.

Finally, we see that the case $k = 5$ is impossible. This is because the equality $k = 5$ implies $\beta_1 = 1$, $\beta_2 = 2$, $\beta_3 = 4$, $\beta_4 = 8$, which contradicts the equality $\alpha - 1+\beta_1+\beta_2+\beta_3+\beta_4 = 10$.

Now suppose that n is odd. Then $n = q_1^{\alpha_1}q_2^{\alpha_2}\dots q_{k-1}^{\alpha_{k-1}}$, where $q_1, q_2, \dots, q_{k-1}$ are odd prime numbers and $q_1 < q_2 < \dots < q_{k-1}$. By assumption, we have

$$q_1^{\alpha_1-1}q_2^{\alpha_2-1}\dots q_{k-1}^{\alpha_{k-1}-1}(q_1-1)(q_2-1)\dots(q_{k-1}-1) = 2^{10}.$$

Hence $\alpha_1 = \alpha_2 = \dots = \alpha_{k-1} = 1$ and $q_i = 2^{\beta_i}+1$ for $i = 1, 2, \dots, k-1$. Moreover, $\beta_1+\beta_2+\dots+\beta_{k-1} = 10$.

If $k = 2$, then $\beta_1 = 10$, which is impossible. If $k = 3$, then $\beta_1+\beta_2 = 10$, whence we easily infer that $\beta_1 = 2$, $\beta_2 = 8$, and this gives $n = 5\cdot 257$.

If $k = 4$, then $\beta_1+\beta_2+\beta_3 = 10$, which is impossible because $\beta_1, \beta_2, \beta_3$ are different numbers chosen out of the sequence 1, 2, 4, 8. Similarly, $k \geqslant 5$ is impossible.

Thus we reach the final conclusion that the equation $\varphi(n) = 2^{10}$ has 12 solutions in natural numbers n, namely:

$n = 2^{11}$, $2^{10}\cdot 3$, $2^9\cdot 5$, $2^7\cdot 17$, $2^3\cdot 257$, $2^8\cdot 3\cdot 5$, $2^6\cdot 3\cdot 17$, $2^2\cdot 3\cdot 257$, $2^5\cdot 5\cdot 17$, $5\cdot 257$, $2\cdot 5\cdot 257$, $2^3\cdot 3\cdot 5\cdot 17$.

Remark. It can be proved that for $0 \leqslant m \leqslant 31$ (m being an integer) the equation $\varphi(n) = 2^m$ has $m+2$ solutions in natural numbers n. For $31 < m < 2^{17}$ the equation has always precisely 32 solutions. The proof is based on the fact that the numbers $2^{2^n}+1$ ($5 \leqslant n < 17$) are composite [1].

14. Prove that there exist infinitely many natural numbers m such that the equation $\varphi(n) = m$ has at least one solution in natural numbers and such that any solution of the equation is even.

Proof. Let $m = 2^{32+2^s}$, where $s = 6, 7, \dots$ If there existed an odd natural number n such that $\varphi(n) = m$, then n would be the product of different odd prime factors which, in addition, would be of the form $F_h = 2^{2^h}+1$. (The argument is that if p is a prime and $p|n$, then $p-1|\varphi(n) = m$, whence it follows that $p-1$ is a natural power of 2, and so $p = F_h$). Suppose that they are the numbers $F_{h_1}, F_{h_2}, \dots, F_{h_k}$. Then $2^{h_1}+2^{h_2}+\dots+2^{h_k} = 2^5+2^s$, where $h_1, h_2, \dots, h_k$ are different natural numbers. The number 2^5+2^s, where $s > 5$, admits only one representation as the sum of different powers of the number 2. Therefore one of the numbers $F_{h_1}, F_{h_2}, \dots, F_{h_k}$ must be equal to F_5, which is impossible, since F_5 is a composite number. Thus we see that the equation $\varphi(n) = m$ has no solutions in odd natural numbers. If n is allowed to be even, a solution can be easily found, for example $\varphi(2^{33+2^s}) = m$.

15. Prove that, if $p > 2$ and $2p+1$ are prime numbers, then for $n = 4p$ the equality $\varphi(n+2) = \varphi(n)+2$ holds.

---

[1] Cf. Carmichael [1] for $m < 2^{10}$. For the numbers $2^{10} \leqslant m < 2^{17}$ the proof is analogous.

Proof. If the numbers $p > 2$ and $2p+1$ are prime, then $\varphi(4p) = \varphi(4)\varphi(p) = 2(p-1)$ and $\varphi(4p+2) = \varphi(2(2p+1)) = \varphi(2p+1) = 2p$, whence $\varphi(4p+2) = \varphi(4p)+2$.

Remark. It easily follows from conjecture H (cf. Chapter III, § 8) that there exist infinitely many pairs of twin prime numbers; similarly, it follows from this conjecture that there exist inifinitely many primes p for which the numbers $2p+1$ are also prime. Consequently, conjecture H implies that there exist infinitely many odd and infinitely many even numbers n which satisfy the equation $\varphi(n+2) = \varphi(n)+2$.

§ 2. Properties of Euler's totient function. Now for a given natural number n we are going to calculate the number of natural numbers $\leqslant n$ such that the greatest common divisor of any of them and n is equal to a number d (with $d \mid n$).

In order that the greatest common divisor of the numbers $m \leqslant n$ and n be d it is necessary and sufficient that $m = kd$, where k is a natural number $\leqslant n/d$ relatively prime to n/d. Consequently, the number of natural numbers $m \leqslant n$ which satisfy the condition $(m, n) = d$ is equal to the number of natural numbers $\leqslant n/d$ which are relatively prime to n/d, and so it is equal to $\varphi(n/d)$.

Thus we see that *in the sequence* $1, 2, \dots, n$ *for every natural divisor* d *of a natural number* n *there are precisely* $\varphi(n/d)$ *natural numbers* m *such that, for any* m, $(m, n) = d$.

Let $d_1, d_2, \dots, d_s$ be all the natural divisors of a natural number n. The numbers $1, 2, \dots, n$ can be divided into s classes by the rule that a number m belongs to the ith class if and only if $(n, m) = d_i$. The number of elements of the ith class is then $\varphi\left(\frac{n}{d_i}\right)$. Moreover, since the number of numbers in the sequence $1, 2, \dots, n$ is equal to n, we obtain the formula

$$\varphi\left(\frac{n}{d_1}\right)+\varphi\left(\frac{n}{d_2}\right)+\dots+\varphi\left(\frac{n}{d_s}\right) = n.$$

But, clearly, if d_i runs all over the set of natural divisors of number n, then $\frac{n}{d_i}$ runs all over the same set of natural divisors of n. Hence $\varphi(d_1)+\varphi(d_2)+\dots+\varphi(d_s) = n$, i.e.

$$\sum_{d|n}\varphi(d) = n. \tag{8}$$

We have thus proved the following

THEOREM 7. *The sum of the values of Euler's totient function over the set of natural divisors of a natural number* n *is equal to* n.

Applying Dirichlet's multiplication (cf. Chapter IV, § 3) to the series $a_1+a_2+\ldots$ and $b_1+b_2+\ldots$, where, for real $s>2$, $a_n=\varphi(n)/n^s$, $b_n=1/n^s$ $(n=1,2,\ldots)$, we obtain by (8)

$$c_n=\sum_{d\mid n}a_d b_{\frac{n}{d}}=\sum_{d\mid n}\frac{\varphi(d)}{d^s}\cdot\frac{d^s}{n^s}=\frac{1}{n^s}\sum_{d\mid n}\varphi(d)=\frac{n}{n^s}=\frac{1}{n^{s-1}}.$$

Hence $\sum_{n=1}^{\infty}c_n=\zeta(s-1)$ and so

$$\sum_{n=1}^{\infty}\frac{\varphi(n)}{n^s}=\frac{\zeta(s-1)}{\zeta(s)}\quad\text{for}\quad s>2.$$

By the use of (8) we can prove the identity of Liouville

$$\sum_{n=1}^{\infty}\frac{\varphi(n)x^n}{1-x^n}=\frac{x}{(1-x)^2}\quad\text{for}\quad |x|<1.$$

It follows from theorem 6 of § 10, Chapter IV, that Euler's totient function is the only function φ that satisfies theorem 7. Formulae (8) and (37) of Chapter IV give together the formula

$$\varphi(n)=n\sum_{d\mid n}\frac{\mu(d)}{d} \tag{9}$$

valid for all natural numbers n. Plainly, formula (9) can be rewritten in the form

$$\varphi(n)=\sum_{kl=n}l\mu(k) \tag{10}$$

where the summation extends all over the pairs of natural numbers k and l such that $kl=n$. For $x\geqslant 1$ formula (10) gives

$$\sum_{n=1}^{[x]}\varphi(n)=\sum_{kl\leqslant x}l\mu(k), \tag{11}$$

where $\sum_{kl\leqslant x}$ denotes the sum extended all over the pairs of natural numbers k,l such that $kl\leqslant x$. But, clearly,

$$\sum_{kl\leqslant x}l\mu(k)=\sum_{k=1}^{[x]}\Big(\mu(k)\sum_{l=1}^{[x/k]}l\Big)$$

and since

$$\sum_{l=1}^{[x/k]}l=\frac{1}{2}\left[\frac{x}{k}\right]\left(\left[\frac{x}{k}\right]+1\right),$$

in virtue of formula (33) of Chapter IV, formula (11) gives

$$\sum_{n=1}^{[x]}\varphi(n)=\frac{1}{2}+\frac{1}{2}\sum_{k=1}^{[x]}\left(\mu(k)\left[\frac{x}{k}\right]^2\right). \tag{12}$$

This formula can be used for calculating the sum of the consecutive values of the function φ as well as for finding the approximate value of that sum. Using the formula

$$\sum_{k=1}^{\infty}\frac{\mu(k)}{k^2}=\frac{6}{\pi^2},$$

proved in Chapter IV, § 10, one can prove that the ratio of number $\sum_{n=1}^{[x]}\varphi(n)$ to number $3x^2/\pi^2$ tends to 1, as x increases.

A generalization of the function $\varphi(n)$ is the function $\varphi_k(n)$, defined for pairs of natural numbers k, n as the number of the sequences $a_1, a_2, \ldots, a_k$ consisting of k natural numbers $\leqslant n$ such that $(a_1, a_2, \ldots, a_k, n)=1$.

It is easy to prove the theorem of C. Jordan [1] (pp. 95-97) stating that if $n=q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_s^{\alpha_s}$ is the factorization of the number n into prime factors, then

$$\varphi_k(n)=n^k\left(1-\frac{1}{q_1^k}\right)\left(1-\frac{1}{q_2^k}\right)\ldots\left(1-\frac{1}{q_s^k}\right)\quad\text{and}\quad\sum_{d\mid n}\varphi_k(d)=n^k.$$

Another generalization of the function φ is the function $\Phi_k(n)$ given by V. L. Klee, Jr. [4]. This is defined for natural numbers k and n as the number of numbers h that occur in the sequence $1, 2, \ldots, n$ and are such that number (h, n) is not divisible by the kth power of any number greater than 1.

It is easy to prove that if $n=q_1^{\alpha_1}q_2^{\alpha_2}\ldots q_s^{\alpha_s}$ is the factorization of the number n into prime factors, then

$$\Phi_k(n)=\prod_{\alpha_i<k}q_i^{\alpha_i}\prod_{\alpha_i\geqslant k}q_i^{\alpha_i-k}(q_i^k-1).$$

We also have

$$\Phi_k(n)=n\prod_{\substack{q^k\mid n\\ q\text{ prime}}}(1-q^{-k})\quad\text{and}\quad\sum_{d\mid n}\Phi_k(d^k)=n^k.$$

§ 3. The theorem of Euler. Let $m>1$ be a given natural number and let

$$r_1, r_2, \ldots, r_{\varphi(m)} \tag{13}$$

be the sequence of the natural numbers relatively prime to m less than m. Let a denote an arbitrary integer relatively prime to m. Denote by ϱ_k

the remainder obtained by dividing the number ar_k by m ($k = 1, 2, \ldots, \varphi(m)$). We then have

$$\varrho_k \equiv ar_k \pmod m \quad \text{for} \quad k = 1, 2, \ldots, \varphi(m) \tag{14}$$

and

$$\varrho_k = ar_k + mt_k, \tag{15}$$

where t_k ($k = 1, 2, \ldots, \varphi(m)$) are integers.

We are going to prove that the numbers

$$\varrho_1, \varrho_2, \ldots, \varrho_{\varphi(m)} \tag{16}$$

and numbers (13) are identical in certain order. For this purpose it is sufficient to prove that

1° any term of sequence (16) is a natural number relatively prime to m and less than m,

2° the elements of sequence (16) are different.

Let $d_k = (\varrho_k, m)$. In virtue of (15), we see that $ar_k = \varrho_k - mt_k$, whence it follows that $d_k \mid ar_k$. But, since $(a, m) = (r_k, m) = 1$, $(ar_k, m) = 1$. Therefore, in view of $d_k \mid m$ and $d_k \mid ar_k$, we must have $d_k = 1$, i.e. $(\varrho_k, m) = 1$. On the other hand, number ϱ_k, as the remainder obtained from division by m, satisfies the inequalities $0 \leqslant \varrho_k < m$. Moreover, since $(\varrho_k, m) = 1$ and $m > 1$, ϱ_k cannot be equal to 0. Thus we have proved that the terms of sequence (16) have property 1°.

Now, suppose that for certain two different indices i and j taken out of the sequence $1, 2, \ldots, \varphi(m)$ the equality $\varrho_i = \varrho_j$ holds. Then, in virtue of (14), we have $ar_i \equiv ar_j \pmod m$, and so $m \mid a(r_i - r_j)$ and, since $(a, m) = 1$, we have $m \mid r_i - r_j$, which is impossible because r_i and r_j, as two different terms of sequence (13), (since $i \neq j$) are different natural numbers $\leqslant m$. We have thus proved that the terms of sequence (16) have property 2°.

This proves that the elements of sequence (16) and those of sequence (13) are identical apart from the order. Therefore

$$\varrho_1 \varrho_2 \ldots \varrho_{\varphi(m)} = r_1 r_2 \ldots r_{\varphi(m)}.$$

Denote by P the common value of these products. The number P is relatively prime to m because anyone of its factors is relatively prime to m.

Multiplying the congruences obtained from (14) by substituting $1, 2, \ldots, \varphi(m)$ for k, we obtain

$$\varrho_1 \varrho_2 \ldots \varrho_{\varphi(m)} \equiv a^{\varphi(m)} r_1 r_2 \ldots r_{\varphi(m)} \pmod m,$$

that is, the congruence $P \equiv a^{\varphi(m)} P \pmod m$ which is, clearly, equivalent to $m \mid P(a^{\varphi(m)} - 1)$, whence, since $(P, m) = 1$, we obtain $m \mid a^{\varphi(m)} - 1$.

We have thus proved

THEOREM 8 (Euler). *For any integer a which is relatively prime to a natural number m the congruence*

$$a^{\varphi(m)} \equiv 1 \pmod m$$

holds.

If p is a prime, then $\varphi(p) = p - 1$; therefore the theorem of Euler can be regarded as a generalization of the theorem of Fermat (proved in Chapter V, § 5).

THEOREM 8ª (Rédei) (1). *For any natural number $m > 1$ and every integer a we have*

$$m \mid a^m - a^{m - \varphi(m)}. \tag{17}$$

Proof. Let $m = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_k^{\alpha_k}$ be the factorization of the number m into prime factors. Let i denote one of the numbers $1, 2, \ldots, k$. If $(a, q_i) = 1$, then, in view of theorem 8, we have $q_i \mid a^{\varphi(q_i^{\alpha_i})} - 1$, and, since by theorem 3 $\varphi(q_i^{\alpha_i}) \mid \varphi(m)$, we have $q_i^{\alpha_i} \mid a^{\varphi(m)} - 1$.

If a and $q \geqslant 2$ are natural numbers, then (as it is easy to prove by induction) $q^{a-1} \geqslant a$. On the other hand, for $i = 1, 2, \ldots, k$, we have $q_i^{\alpha_i - 1} \mid m$ and $q_i^{\alpha_i - 1} \mid \varphi(m)$, whence $q_i^{\alpha_i - 1} \mid m - \varphi(m)$. Since, moreover, $m - \varphi(m)$ is positive for m greater than 1, the last relation implies that $m - \varphi(m) \geqslant q_i^{\alpha_i - 1} \geqslant \alpha_i$. Hence, in the case where $(a, q_i) > 1$, that is, if $q_i \mid a$, we have $q_i^{\alpha_i} \mid q_i^{m - \varphi(m)} \mid a^{m - \varphi(m)}$.

Thus we see that for any integer a the relation $q_i^{\alpha_i} \mid a^{m - \varphi(m)}(a^{\varphi(m)} - 1)$ holds for every $i = 1, 2, \ldots, k$. This means that $q_i^{\alpha_i} \mid a^m - a^{m - \varphi(m)}$, whence, looking at the factorization of a into prime factors, we see that formula (17) holds. Theorem 8ª is thus proved.

The theorem of Euler is an easy consequence of theorem 8ª. In fact, in view of theorem 8ª, for any natural $m > 1$ and any integer a we have $m \mid a^{m - \varphi(m)}(a^{\varphi(m)} - 1)$. So, if in addition $(a, m) = 1$, then $(a^{m - \varphi(m)}, m) = 1$, whence $m \mid a^{\varphi(m)} - 1$, which gives the theorem of Euler.

EXERCISES. **1.** Prove that from any infinite arithmetical progression, whose terms are integers, a geometric progression can be selected.

Proof. Suppose we are given an infinite arithmetical progression

$$a, \ a + r, \ a + 2r, \ \ldots \tag{18}$$

the terms of which are integers. If $r = 0$, there is nothing to prove since then the whole sequence (18) can be regarded as a geometric progression.

If $r < 0$, the desired result follows provided it is proved for the arithmetical progression obtained from the original one by a simple change of the sign at each of the terms of the progression. Thus the problem reduces to the case where r is a natural number. Moreover, we may suppose that $(a, r) = 1$, since otherwise, that

(1) Cf. Szele [1], footnote 2.

is, if $d = (a, r) > 1$, we have $a = da'$, $r = dr'$ where $(a', r') = 1$, and so it is sufficient to prove the theorem for the arithmetical progression $a', a'+r', a'+2r', \ldots$

Finally, since $r > 0$, from a certain term onwards all the terms of (18) are greater than 1. Thus in order to prove the theorem we may remove some terms at the beginning and suppose $a > 1$. Since $(a, r) = 1$, then, by theorem 8, we have $a^{\varphi(r)} \equiv 1 (\mathrm{mod} r)$. Hence, for natural numbers n, $a^{n\varphi(r)} \equiv 1 (\mathrm{mod} r)$ and therefore the number $k_n = (aa^{n\varphi(r)} - a)/r$ is an integer for any $n = 1, 2, \ldots$ But $a + k_n r = a(a^{\varphi(r)})^n$ for $n = 1, 2, \ldots$, and so, since $a > 0$, $0 \leqslant k_1 < k_2 < \ldots$ and the numbers $a + k_n r$ $(n = 1, 2, \ldots)$ form a geometrical progression.

The theorem we have just proved implies that in any infinite arithmetical progression there are infinitely many terms which have the same prime factors (cf. Pólya and Szegö [1], p. 344). Another consequence of the theorem just proved is this: from any infinite arithmetical progression whose terms are rational numbers an infinite geometric progression can be selected.

2. Prove that if m, a, r are natural numbers with $(a, r) = 1$ and Z is any infinite set of terms of the arithmetical progression $a + kr$ $(k = 1, 2, \ldots)$, then the progression contains terms which are products of more than m different numbers of the set Z.

Proof. We take $s = m\varphi(r) + 1$ different numbers of the set Z. Denote them by $t_1, t_2, \ldots, t_s$. These numbers, being the terms of the arithmetical progression $a + kr$ $(k = 1, 2, \ldots)$, are congruent to $a (\mathrm{mod} r)$. So $t_1 t_2 \ldots t_s \equiv a^s \equiv a \cdot a^{m\varphi(r)} (\mathrm{mod} r)$, whence, in view of $(a, r) = 1$, by theorem 8, we infer that $a^{\varphi(r)} \equiv 1 (\mathrm{mod} r)$. Therefore $t_1 t_2 \ldots t_s \equiv a (\mathrm{mod} r)$, and consequently the number $t_1 t_2 \ldots t_s$ is a term of the arithmetical progression $a + kr$ $(k = 1, 2, \ldots)$ Moreover, $s = m\varphi(r) + 1 > m$, and so the proof follows.

3. Prove that every natural number which is not divisible by 2 or by 5 is a divisor of a natural number whose digits (in the scale of ten) are all equal to 1.

Proof. If $(n, 10) = 1$, then of course $(9n, 10) = 1$ and hence, by theorem 8, $10^{\varphi(9n)} \equiv 1 (\mathrm{mod} 9n)$. Therefore $10^{\varphi(9n)} - 1 = 9nk$, where k is a natural number. Hence $nk = (10^{\varphi(9n)} - 1)/9$ and thus we see that the digits (in the scale of ten) of this number are equal to 1.

4. Prove that every natural number has a multiple whose digits (in the scale of ten) are all equal to 1 or 0 and the digits equal to 1 precede those equal to 0.

Proof. Every natural number can be represented in the form $n = n_1 2^\alpha 5^\beta$, where $(n_1, 10) = 1$. In virtue of exercise 3, the number n_1 is a divisor of a number m whose digits (in the scale of ten) are equal to 1. On the other hand, $2^\alpha 5^\beta \mid 10^\gamma$, where $\gamma = \max(\alpha, \beta)$; consequently, $n \mid m \cdot 10^\gamma$.

5. Find all the solutions of the congruence $x^x \equiv 3 (\mathrm{mod} 10)$ in natural numbers x.

Solution. If a natural number x satisfies the congruence, then, since $(3, 10) = 1$, we must have $(x, 10) = 1$. Consequently $(x + 20k, 10) = 1$ for any $k = 0, 1, 2, \ldots$ Hence, by theorem 8, since $\varphi(10) = 4$, we find that $(x + 20k)^4 \equiv 1 (\mathrm{mod} 10)$ and, *a fortiori*, $(x + 20k)^{20k} \equiv 1 (\mathrm{mod} 10)$. On the other hand, the congruence $(x + 20k)^x \equiv x^x (\mathrm{mod} 10)$ holds for any natural number x. Therefore, multiplying the last two congruences, we obtain $(x + 20k)^{x+20k} \equiv x^x (\mathrm{mod} 10)$ for any $k = 0, 1, 2, \ldots$ If a natural number x satisfies the congruence $x^x \equiv 3 (\mathrm{mod} 10)$, then any of the terms of the arithmetical progression $x + 20k$ $(k = 0, 1, 2, \ldots)$ just obtained also satisfies it. It is easy to verify that among the integers x such that $0 \leqslant x < 20$ only numbers 7 and 13 satisfy the congruence. From this we infer that the solutions of the congruence $x^x \equiv 3 (\mathrm{mod} 10)$ in natural numbers x are precisely the numbers $7 + 20k$ and $13 + 20k$, where $k = 0, 1, 2, \ldots$

§ 4. Numbers which belong to a given exponent with respect to a given modulus. It follows from theorem 8 that if a is an integer relatively prime to a natural number m, then the congruence

$$a^x \equiv 1 (\mathrm{mod} m) \tag{19}$$

has infinitely many solutions in natural numbers x; for example an infinite set of solutions is formed by the numbers $x = k\varphi(m)$, where $k = 1, 2, \ldots$ On the other hand, it is clear that congruence (19) has natural solutions only in the case where $(a, m) = 1$.

If $x = \delta$ is the least natural solution of congruence (19), then we say that *number a belongs to exponent δ with respect to modulus m.*

It is clear that if two numbers are congruent with respect to modulus m, then they belong to the same exponent with respect to modulus m; for, if $a \equiv b (\mathrm{mod} m)$ and for some x formula (19) holds, then $b^x \equiv 1 (\mathrm{mod} m)$ (since, as we know, the congruence $a \equiv b (\mathrm{mod} m)$ implies the congruence $a^x \equiv b^x (\mathrm{mod} m)$ for any $x = 1, 2, \ldots$).

THEOREM 9. *If $(a, m) = 1$, then any solution of congruence* (19) *is divisible by the exponent δ to which a belongs with respect to modulus m.*

Proof. Suppose, to the contrary, that the solution x of congruence (19) is not divisible by δ. This means that x divided by δ leaves a positive remainder r. Accordingly, $x = k\delta + r$, where k is a non-negative integer. By (19) we have

$$a^{k\delta+r} \equiv 1 (\mathrm{mod} m) \quad \text{that is} \quad (a^\delta)^k a^r \equiv 1 (\mathrm{mod} m). \tag{20}$$

By the definition of δ the congruence $a^\delta \equiv 1 (\mathrm{mod} m)$ holds. Therefore, by (20), $a^r \equiv 1 (\mathrm{mod} m)$. Thus we see that our assumption leads us to the conclusion that there exists a solution r of congruence (19) less than δ, which contradicts the definition of δ. The theorem is thus proved.

Since, by theorem 8, $\varphi(m)$ is a solution of congruence (19), theorem 9 implies the following

COROLLARY. *The exponent to which an arbitrary number relatively prime to m belongs with respect to modulus m is a divisor of number $\varphi(m)$.*

In particular, numbers (relatively prime to m) which belong to exponent $\varphi(m)$ with respect to modulus m (that is numbers which belong to the maximum exponent with respect to modulus m), if they exist, are called *primitive roots of number m.*

For example, number 3 is a primitive root of number 10 because $3^1 \equiv 3$, $3^2 \equiv 9$, $3^3 \equiv 7$, $3^4 \equiv 1 (\mathrm{mod} 10)$ and $\varphi(10) = 4$. Number 10, however, is not a primitive root of number 3 because $10 \equiv 1 (\mathrm{mod} 3)$, which shows that 10 belongs to the exponent 1 with respect to modulus 3 and $\varphi(3) = 2$.

Number 7 is also a primitive root of number 10 since $7^1 \equiv 7$, $7^2 \equiv 9$, $7^3 \equiv 3$, $7^4 \equiv 1 \pmod{10}$. Equally, number 10 is a primitive root of the number 7 because $10 \equiv 3$, $10^2 \equiv 2$, $10^3 \equiv 6$, $10^4 \equiv 4$, $10^5 \equiv 5$, $10^6 \equiv 1 \pmod 7$ and $\varphi(7) = 6$.

It follows immediately from theorem 8 that for any natural number m there exists the least natural number $\lambda(m)$ such that $m \mid a^{\lambda(m)}-1$ for $(a, m) = 1$ [1]. Number $\lambda(m)$ is called the *minimum universal exponent* mod m. By theorem 8, the inequality $\lambda(m) \leqslant \varphi(m)$ holds for any natural m. It can be proved that $\lambda(2) = 1$, $\lambda(2^2) = 2 \cdot \lambda(2^a) = 2^{a-2}$, $a = 3, 4, \ldots$ It is also true that if $m = 2^a q_1^{a_1} q_2^{a_2} \ldots q_s^{a_s}$, $2 < q_1 < q_2 < \ldots < q_s$ is the factorization of number m into prime factors, then

$$\lambda(m) = [\lambda(2^{a_0}),\ \varphi(q_1^{a_1}),\ \ldots,\ \varphi(q_s^{a_s})],$$

and that for any natural number m there exist natural numbers that belong to the exponent $\lambda(m)$ with respect to modulus m (cf. Ore [2], pp. 292-293).

As announced in Mathematical Tables and other Aids to Computation 4 (1950), pp. 29-30, S. Whitten [1] has tabulated the function $\lambda(n)$ for $n \leqslant 1200$.

The accompanying table covers the values of the function $\lambda(m)$ for $m < 100$.

	0	1	2	3	4	5	6	7	8	9
			1	2	2	4	2	6	2	6
1	4	10	2	12	6	4	4	10	6	18
2	4	6	10	22	2	20	12	18	6	28
3	4	30	8	10	16	12	6	36	18	12
4	4	40	6	42	10	12	22	46	4	42
5	20	16	12	52	18	20	6	18	28	58
6	4	60	30	6	16	12	10	66	16	22
7	12	70	6	72	36	20	18	30	12	78
8	4	54	40	82	6	16	42	28	10	88
9	12	12	22	30	46	36	8	96	42	30

It can be proved that $\lambda(m) = \varphi(m)$ holds only for $m = 1, 2, 4, p^a$ and $2p^a$, where p is an odd prime and a a natural number. Another fact worth reporting is that there exists an increasing infinite sequence of natural numbers n_k $(k = 1, 2, \ldots)$ such that $\lim_{k=\infty} \lambda(n_k)/\varphi(n_k) = 0$. For example, such is the sequence $n_k = p_1 p_2 \ldots p_k$ $(k = 1, 2, \ldots)$. It can also be proved that in order that a number m be a composite number

[1] This function should not be mistaken for the function of Liouville considered in Chapter IV, § 11.

of Carmichael (and so absolutely pseudo-prime) it is necessary and sufficient that $\lambda(m) \mid m-1$ (cf. Carmichael [2], p. 237, formula (18)).

As announced by Carmichael (ibid., p. 236) the equation $\lambda(n) = 2$ has precisely six solutions, $n = 3, 4, 6, 8, 12, 24$, and the equation $\lambda(n) = 4$ has 12 solutions (the least of which is $n = 5$ and the greatest $n = 240$); the equation $\lambda(n) = 12$ has 84 solutions (the least of which is $n = 13$ and the greatest $n = 65520$). We have $\lambda(100) = 20$. For $n < 100$ the equality $\lambda(n+1) = \lambda(n)$ holds only for $n = 3$, 15 and 90.

For every natural number s there exists a natural number m_s such that the equation $\lambda(n) = m_s$ has more than s solutions in natural numbers n. The proof of this fact presented here is due to A. Schinzel. By theorem 11, which will be proved in the next section, for every natural number s there exists a natural number k such that $p = 2^s k+1$ is a prime number. For $j = 0, 1, 2, \ldots, s, s+1$ we have $\lambda(2^j(2^s k+1)) = 2^s k$, so putting $m_s = 2^s k$ we obtain the desired result.

It is easy to prove that for natural numbers $n > 2$ the numbers $\lambda(n)$ are even. There exist infinitely many even numbers which are not values of the function $\lambda(n)$. It can be proved that the numbers $2 \cdot 7^k$, where $k = 1, 2, \ldots$, have this property (cf. Sierpiński [25], pp. 191-192).

THEOREM 10. *If p is a prime > 2, then any natural divisor of the number 2^p-1 is of the form $2kp+1$, where k is an integer.*

Proof. Since the product of two (or more) numbers of the form $2kp+1$ is also of this form, and since number 1 is of this form (for $k = 0$), it is sufficient to prove that every prime divisor q of number 2^p-1 is of the form $2kp+1$. If $q \mid 2^p-1$, then $2^p \equiv 1 \pmod q$ and so, by theorem 9, $\delta \mid p$, where δ denotes the exponent to which number 2 belongs with respect to modulus q. We cannot have $\delta = 1$ because, in that case, $2 \equiv 1 \pmod q$ and so $q \mid 1$, which is impossible. Therefore, since $\delta \mid p$ and p is a prime, we infer that $\delta = p$. On the other hand, the corollary to theorem 9 gives $\delta \mid \varphi(q)$, i.e. $\delta \mid q-1$. Thus we see that $p \mid q-1$ and, since q is a divisor of an odd number and since $(p, 2) = 1$ (because p is a prime > 2), we conclude that $2p \mid q-1$, that is $q-1 = 2kp$, so $q = 2kp+1$, where k is an integer. The theorem is thus proved.

We note that in theorem 10 the assumption that p is a prime > 2 is essential; the divisors 3, 5 and 15 of number 2^4-1 are not of the form $8k+1$ and the divisor $7 = 2^3-1$ of number $2^{15}-1$ is not of the form $30k+1$.

EXERCISES. **1.** Prove the following theorem of Fermat:

If p is a prime > 3, then any natural divisor > 1 of number $(2^p+1)/3$ is of the form $2kp+1$, where k is a natural number.

Proof. Number $(2^p+1)/3$ is a natural number since, for odd p, $2+1 \mid 2^p+1$. Let d denote a divisor > 1 of number $(2^p+1)/3$ and let q be a divisor relatively prime to d. If $q = 3$, then $2^p+1 \equiv 0 \pmod 9$, whence $2^{2p} \equiv 1 \pmod 9$ and, by theorem 9,

number $2p$ is divisible by the exponent to which number 2 belongs with respect to modulus 9. But, as is easy to calculate, $\delta = 6$, so $6 \mid 2p$, whence $3 \mid p$, and this contradicts the assumption that $p > 3$. Therefore, necessarily, $q \neq 3$. Since $2^p + 1 \equiv 0 \pmod{q}$, we have $2^{2p} \equiv 1 \pmod{q}$. Now let δ denote the exponent to which number 2 belongs with respect to modulus q. We cannot have $\delta = 1$ or $\delta = 2$, because $q \neq 3$. Therefore $\delta > 2$. But, in virtue of theorem 9, $\delta \mid 2p$ and, by $2^{q-1} \equiv 1 \pmod{q}$, $\delta \mid q-1$. Thus we see that numbers $2p$ and $q-1$ have a common divisor $\delta > 2$, which, in turn, implies that numbers p and $q-1$ have a common divisor > 1. But, since p is a prime, this implies that $p \mid q-1$ and so $q = pt+1$, where t is an integer and, in view of the fact that the numbers p, q are odd, t is even. Thus we conclude that $q = 2kp+1$, where k is a natural number, and so we see that each divisor of the number d is of the form $2kp+1$. Consequently number d itself is of the form $2kp+1$. This completes the proof of the theorem.

2. Prove that if a, b and n are natural numbers such that $a > b$, $n > 1$, then each prime divisor of number $a^n - b^n$ is either of the form $nk+1$, where k is an integer, or a divisor of a number $a^{n_1} - b^{n_1}$, where $n_1 \mid n$ and $n_1 < n$.

Proof. Let $(a, b) = d$. Since $a > b$, we have $a = a_1 d$, $b = b_1 d$, where $(a_1, b_1) = 1$ and $a_1 > b_1$. Suppose that p is a prime divisor of number $a^n - b^n$. Then $p \mid a^n - b^n = d^n(a_1^n - b_1^n)$. If $p \mid d^n$, then $p \mid d$ and hence $p \mid a-b$, and the theorem is proved. Suppose that $p \mid a_1^n - b_1^n$. Then, since $(a_1, b_1) = 1$, we have $(a_1, p) = (b_1, p) = 1$. Let p be a primitive divisor of number $a_1^\delta - b_1^\delta$ (this means that $p \mid a_1^\delta - b_1^\delta$ and $p \nmid a_1^m - b_1^m$ for $0 < m < \delta$). We note that then $\delta \mid n$. In fact, suppose that n is not divisible by δ. Then $n = k\delta + r$, where k is an integer $\geqslant 0$ and $0 < r < \delta$. But $p \mid a_1^\delta - b_1^\delta$, and so $p \mid a_1^{k\delta} - b_1^{k\delta}$. In virtue of the identity

$$a_1^{k\delta+r} - b_1^{k\delta+r} = (a_1^{k\delta} - b_1^{k\delta})a^r + b_1^{k\delta}(a_1^r - b_1^r)$$

we have $p \mid b_1^{k\delta}(a_1^r - b_1^r)$, which, in view of $(b_1, p) = 1$, implies that $p \mid a_1^r - b_1^r$ for $0 < r < \delta$, contrary to the assumption that p is a primitive divisor of number $a_1^\delta - b_1^\delta$.

If $\delta < n$, then $\delta \mid n$ and $p \mid a_1^{n_1} - b_1^{n_1} \mid a^{n_1} - b^{n_1}$ for $n_1 = \delta$, $n_1 \mid n$ and $n_1 < n$. Let $\delta = n$. Then, in virtue of the theorem of Fermat, $p \mid a_1^{p-1} - 1$, $p \mid b_1^{p-1} - 1$, whence $p \mid a_1^{p-1} - b_1^{p-1}$. Consequently, $n = \delta \mid p-1$ and so p is of the form $nk+1$.

3. Prove that, if a, b, n are natural numbers $a > b$, $n > 1$, then every prime divisor of number $a^n + b^n$ is of the form $2nk+1$, where k is an integer, or is a divisor of number $a^{n_1} + b^{n_1}$, where n_1 is the quotient obtained by dividing the number n by an odd number greater than 1.

The proof is analogous to that in the preceding exercise.

§ 5. Proof of the existence of infinitely many primes in the arithmetical progression $nk+1$.

THEOREM 11. *If p is a prime and s a natural number, then there exist infinitely many primes of the form $2p^sk+1$, where k is a natural number.*

Proof. Let p be a prime and let s be a natural number. We set $a = 2^{p^{s-1}}$. Let q denote an arbitrary prime divisor of number $a^{p-1} + a^{p-2} + \ldots + a + 1$. If a were congruent to $1 \pmod{q}$, then $q \mid a^{p-1} + a^{p-2} + \ldots + a + 1 \equiv p \pmod{q}$; so $q \mid p$, which, in view of the fact that p and q are primes, would imply $q = p$, and so $a^p \equiv 1 \pmod{p}$, that is, $2^{p^s} \equiv 1 \pmod{p}$.

But, in virtue of theorem 5[a] of Chapter V, we have $2^p \equiv 2 \pmod{p}$, whence, by induction, $2^{p^s} \equiv 2 \pmod{p}$, and this would show that 1 is congruent to $2 \pmod{p}$; so $p \mid 1$, which is impossible. We have thus proved that $a \not\equiv 1 \pmod{q}$, i.e. that $2^{p^{s-1}} \not\equiv 1 \pmod{q}$. Let δ denote the exponent to which 2 belongs with respect to modulus q. Since $q \mid a^p - 1$, i.e. $2^{p^s} \equiv 1 \pmod{q}$, we see that $\delta \mid p^s$ and, since by $2^{p^{s-1}} \not\equiv 1 \pmod{q}$, the relation $\delta \mid p^{s-1}$ is impossible, δ must be equal to p^s. In virtue of the corollary to theorem 9, we have $\delta \mid \varphi(q)$, i.e. $p^s \mid q-1$. By $2^{p^s} \equiv 1 \pmod{q}$, we see that number q is odd and, consequently, $q-1$ is even. If p is a prime > 2, then $(p, 2) = 1$ and so, in view of $p^s \mid q-1$, we see that $2p^s \mid q-1$, which shows that $q = 2p^sk+1$ for a natural number k. If $p = 2$, then $2^s \mid q-1$, whence $q = 2^sk+1$, where k is a natural number.

Thus we have proved that if p is odd, then there exists at least one prime number of the form $2p^sk+1$; if $p = 2$, then there exists at least one prime of the form 2^sk+1. Since s is arbitrary, this proves theorem 11.

The proof of a more general theorem is slightly more difficult:

THEOREM 11[a]. *For any natural number n there exist infinitely many prime numbers of the form $nk+1$, where k is a natural number.*

Proof (due to A. Rotkiewicz [5]) (cf. Estermann [2]). First we note that in order to prove the theorem it is sufficient to show that for any natural number n there exists at least one prime number of the form $nk+1$, where k is a natural number; for this implies that for any two natural numbers n, m there exists at least one prime of the form $nmt+1$, where t is a natural number, and this prime is, clearly, $> m$ and of the form $nk+1$ (where k is a natural number).

It is also plain that without loss of generality we may suppose that $n > 2$ (for in the sequence of odd numbers there exist (as we know) infinitely many primes).

Let $n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}$ be the factorization of number n into prime factors with $q_1 < q_2 < \ldots < q_s$.

Suppose that for any prime divisor p of number $a^n - 1$ number n belongs to an exponent $< n$ with respect to the modulus p. Let

$$P_n = \prod_{d \mid n} (n^d - 1)^{\mu(n:d)}, \tag{21}$$

where μ is the Möbius function (cf. Chapter IV, § 10). We represent each of the factors $n^d - 1$ as the product of its prime factors. Then product (21) becomes the product of prime factors; the exponent of any of them is an integer, positive, negative, or zero. Let p be one of those prime factors. Then there exists a natural number $d \mid n$ such that $p \mid n^d - 1$. Since $d \mid n$, then, *a fortiori*, $p \mid n^n - 1$ and $(n, p) = 1$. Let δ denote the exponent to which n belongs with respect to modulus p. It follows from the assumption

that $\delta < n$. As an immediate consequence of theorem 9, we see that among the numbers n^d-1, where $d \mid n$, numbers divisible by p are precisely those for which $\delta \mid d$ holds, i.e. those for which $d = \delta k$, where k is a natural number such that $\delta k \mid n$, that is $k \mid \frac{n}{\delta}$. Since $p \mid n^n-1$, we have $\delta \mid n$, whence we infer that n/δ is a natural number >1 (because $\delta < n$).

Let λ be the greatest exponent for which p^λ divides $n^\delta-1$. We have $p^\lambda \mid n^\delta-1$ and $p^{\lambda+1} \nmid n^\delta-1$. If for a natural number $k \mid n/\delta$ we have $p^{\lambda+1} \mid n^{k\delta}-1$, then, by the identity

$$\frac{n^{\delta k}-1}{n^\delta-1} = \left((n^\delta)^{k-1}-1\right)+\left((n^\delta)^{k-2}-1\right)+\ldots+(n^\delta-1)+k,$$

$p \mid k$, which is impossible, since $k \mid n$ and $(n, p) = 1$. Therefore, for every natural number $k \mid n/\delta$, λ is the greatest exponent such that $p^\lambda \mid n^{\delta k}-1$. From this we infer that in the factorization of number (21) the exponent of the prime p is $\sum_{k \mid \frac{n}{\delta}} \lambda\mu\left(\frac{n}{\delta k}\right)$. But, since n/δ is a natural number >1, by formula (32) of Chapter IV, § 10, we see that $\sum_{k \mid \frac{n}{\delta}} \mu\left(\frac{n}{\delta k}\right) = \sum_{k \mid \frac{n}{\delta}} \mu(k) = 0$. Since this is valid for any prime factor p of number (21), we see that $P_n = 1$. But by (21) we have

$$P_n = \prod_{d \mid n} (n^{n/d}-1)^{\mu(d)} = \prod_{d \mid q_1 q_2 \ldots q_s} (a^{n/d}-1)^{\mu(d)} \tag{22}$$

because, as we know, $\mu(d) = 0$ whenever d is divisible by the square of a natural number >1. Let $b = n^{q_1^{\alpha_1-1} q_2^{\alpha_2-1} \ldots q_s^{\alpha_s-1}}$. We have $b \geqslant n > 2$ and $b^{q_1 q_2 \ldots q_s} = n^n$, thus, by (22)

$$P_n = \prod_{d \mid q_1 q_2 \ldots q_s} (b^{q_1 q_2 \ldots q_s/d}-1)^{\mu(d)}.$$

We see that P_n is the quotient of two polynomials in b with integral coefficients. Now we are going to find the least exponents of b that appear in the numerator and in the denominator of this quotient. We consider two cases separately: that of s being even and that of s being odd. In the former cases the least natural exponent of b in the numerator is obtained for $d = q_1 q_2 \ldots q_s$. Consequently the exponent is equal to 1. As it is easy to see, the numerator divided by b^2 leaves a remainder equal either to $b-1$ or to b^2-b+1. In the denominator, however, in virtue of the inequalities $q_1 < q_2 < \ldots < q_s$, the least exponent is obtained

for $d = q_2 q_3 \ldots q_s$. Consequently the exponent is equal to q_1. The denominator divided by b^2 yields the remainder 1 or b^2-1. But, since $P_n = 1$, this leads to a contradiction because, since $b > 2$, numbers $b-1$ and b^2-b+1 are different from numbers 1 and b^2-1. If s is odd, then the least exponent on b that appears in the numerator is obtained for $d = q_2 q_3 \ldots q_s$; the same for the denominator is obtained for $d = q_1 q_2 \ldots q_s$, which, as before, leads to a contradiction.

Thus, as we see, the assumption that for any prime divisor of the number n^n-1 number n belongs to an exponent less than n with respect to modulus p leads to a contradiction.

Therefore number n^n-1 has at least one prime divisor p such that n belongs to the exponent n with respect to the modulus p. But $(n, p) = 1$, and so, by the theorem of Fermat, $p \mid n^{p-1}-1$, whence, by theorem 9, $n \mid p-1$, i.e. $p = nk+1$, where k is a natural number.

We have thus shown that for every natural number $n > 1$ there exists at least one prime number of the form $nk+1$, where k is a natural number, whence, as we learned above, theorem 11[a] follows.

As an application of theorem 11[a] we give a proof of the following theorem of A. Mąkowski (cf. Chapter V, § 7):

For any natural number $k \geqslant 2$ there exist infinitely many composite natural numbers n such that the relation $n \mid a^{n-k}-1$ holds for any integer a with $(a, n) = 1$.

Proof. Let $k = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}$, where $q_1 < q_2 < \ldots < q_s$, be the factorization of a natural number $k \geqslant 2$ into prime factors. In view of theorem 11[a] there exist infinitely many prime numbers $p > k$ each of the form $(q_1-1)(q_2-1)\ldots(q_s-1)t+1$, where t is a natural number. We are going to prove that if p is any of those numbers, then number $n = kp$ is a composite number, whose existence thet heorem asserts.

In fact, we have

$$n-k = k(p-1) = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s}(q_1-1)(q_2-1)\ldots(q_s-1)t$$
$$= q_1 q_2 \ldots q_s \varphi(k) t,$$

whence, in virtue of the theorem of Euler and the theorem of Fermat, we infer that for $(a, n) = 1$ the number $a^{n-k}-1$ is divisible by k and p, and so it is divisible by $kp = n$.

Another application of theorem 11[a] is this. We call a sequence p, $p+2$, $p+6$ whose elements are all primes a *triplet of the first category* and a sequence $p, p+4, p+6$, whose elements are all prime numbers, a *triplet of the second category.*

We prove that if from the set of primes we remove those primes which belong to triplets of the first or of the second category, then infinitely many primes still remain in the set.

In fact, as follows from theorem 11[a], there exist infinitely many prime numbers q of the form $q = 15k+1$ where k is a natural number. Trivially, for any of the q's we have $3 \mid q+2$, $5 \mid q+4$, $3 \mid q-4$, $5 \mid q-6$. Therefore, since $q > 15$, the numbers $q+2$, $q+4$, $q-4$ and $q-6$ are composite. Hence it follows immediately that q cannot be any of the numbers which belong to any triplet of the first or of the second category. In fact, if q were any of those numbers, i.e. if either $q = p$ or $q = p+2$ or $q = p+6$ and the numbers $p, p+2, p+6$ were prime, then, in the first case, the number $p+2 = q+2$ would be composite, in the second case, the number $p+6 = q+4$ would be composite, and finally, in the third case the number $p = q-6$ would be composite. Thus we see that none of the cases is possible. Similarly, if the numbers p, $p+4$, $p+6$ are prime, then, if $p = q$, $p+4 = q+4$ is a composite number, if $q = p+4$, then $p+6 = q+2$ is composite, and, finally, if $q = p+6$, then $p = q-6$ is composite.

§ 6. Proof of the existence of the primitive root of a prime number. Let p denote a given prime number. By the corollary to theorem 9, the terms of the sequence

$$1, 2, 3, \ldots, p-1 \tag{23}$$

belong (mod p) to the exponents which are divisors of number $\varphi(p) = p-1$. For each natural divisor δ of number $p-1$ denote by $\psi(\delta)$ the number of those elements of sequence (23) which belong to exponent δ with respect to modulus p. Since each of the elements of sequence (23) is relatively prime to p, they must belong to an exponent δ which is a divisor of number $p-1$. Consequently,

$$\sum_{\delta \mid p-1} \psi(\delta) = p-1.$$

Since, in view of theorem 7, $\sum_{\delta \mid p-1} \varphi(\delta) = p-1$, we have

$$\sum_{\delta \mid p-1} \big(\varphi(\delta) - \psi(\delta)\big) = 0. \tag{24}$$

We are going to prove that $\psi(\delta) \leqslant \varphi(\delta)$ for $\delta \mid p-1$. Plainly this is true for $\psi(\delta) = 0$. Suppose that $\psi(\delta) > 0$, i.e. that sequence (23) contains at least one number a which belongs to exponent δ with respect to modulus p. We then have $a^\delta \equiv 1 (\mathrm{mod}\, p)$. Consequently, number a is one of the roots of the congruence

$$x^\delta - 1 \equiv 0 (\mathrm{mod}\, p). \tag{25}$$

Let

$$r_1, r_2, \ldots, r_\delta \tag{26}$$

be the remainders obtained by dividing the numbers a^k $(k = 1, 2, \ldots, \delta)$ by p. Numbers (26) are different because otherwise, if $r_k = r_{k+l}$, where k, l are natural numbers and $k+l \leqslant \delta$, then $p \mid a^{k+l} - a^k = a^k(a^l - 1)$, whence, taking into account the relation $(a, p) = 1$, we infer that $p \mid a^l - 1$, i.e. $a^l \equiv 1 (\mathrm{mod}\, p)$, which is impossible because a belongs to exponent δ with respect to modulus δ, and l is a natural number less than δ (in fact, $k+l \leqslant \delta$ and $k \geqslant 1$ give $l < \delta$). According to the definition of numbers (26), for $k = 1, 2, \ldots, \delta$ the relation $r_k \equiv a^k (\mathrm{mod}\, p)$ holds. Hence, in virtue of $a^\delta \equiv 1 (\mathrm{mod}\, p)$, we have $r_k^\delta \equiv (a^\delta)^k \equiv 1 (\mathrm{mod}\, p)$, which proves that numbers (26) are roots of congruence (25). Congruence (25), however, is of δth degree and satisfies the conditions of Lagrange's theorem (theorem 13, § 8, Chapter V), so it cannot have any other solution than that given by the δ numbers (26).

On the other hand, any of the numbers x that belongs to exponent δ with respect to modulus p satisfies congruence (25); so it is one of the numbers (26). Our aim is to find numbers r_k which belong to the exponent δ with respect to the modulus p. We prove that they are precisely the numbers r_k for which $(k, \delta) = 1$.

Suppose that $(k, \delta) = 1$. Then the number r_k, as a root of congruence (25), belongs to the exponent $\delta' \leqslant \delta$ with respect to the modulus p. Therefore $r_k^{\delta'} \equiv 1 (\mathrm{mod}\, p)$. But $r_k \equiv a^k (\mathrm{mod}\, p)$, whence $a^{k\delta'} \equiv 1 (\mathrm{mod}\, p)$. We see that number $k\delta'$ is one of the roots of the congruence $a^x \equiv 1 (\mathrm{mod}\, p)$. Hence, by theorem 9, $\delta \mid k\delta'$, which in virtue of the assumption $(k, \delta) = 1$, gives $\delta \mid \delta'$, and this, by $\delta' \leqslant \delta$, proves that $\delta' = \delta$. Thus we see that if $(k, \delta) = 1$, then r_k belongs to the exponent δ with respect to the modulus p.

Now, suppose the converse, i.e. that $(k, \delta) = d > 1$. Let $k = k_1 d$, $\delta = \delta_1 d$, where $\delta_1 < \delta$. Then $k\delta_1 = k_1 d \delta_1, = k_1 \delta$.

Consequently,

$$r_k^{\delta_1} \equiv a^{k\delta_1} \equiv a^{k_1 \delta} \equiv (a^\delta)^{k_1} \equiv 1 (\mathrm{mod}\, p).$$

This shows that $r_k^{\delta_1} \equiv 1 (\mathrm{mod}\, p)$, where $\delta_1 < \delta$, and so the number r_k cannot belong to the exponent δ with respect to the modulus p. We have thus proved that the condition $(k, \delta) = 1$ is both necessary and sufficient in order that number r_k should belong to the exponent δ with respect to the modulus p. In other words, it has turned out that numbers r_k of sequence (26) which belong to the exponent δ with respect to the modulus p are precisely those whose indices k are relatively prime to δ. The number of them is clearly $\varphi(\delta)$. Thus if (for a given natural divisor δ

of number $p-1$) $\psi(\delta) > 0$, then $\psi(\delta) = \varphi(\delta)$. It follows that all the summands of (24) are non-negative, which, in virtue of the fact that the sum is equal to zero, proves that each of the summands must be equal to zero. Hence, trivially, $\psi(\delta) = \varphi(\delta)$ for $\delta \mid p-1$.

We have thus proved the following

THEOREM 12. *Let p be a prime and δ a natural divisor of the number $p-1$. Then there are precisely $\varphi(\delta)$ different numbers of the sequence $1, 2, \ldots, p-1$ that belong to the exponent δ with respect to the modulus p.*

As an important special case, for $\delta = p-1$, we obtain

COROLLARY. *Every prime number p has $\varphi(p-1)$ primitive roots among the terms of the sequence $1, 2, \ldots, p-1$.*

A glance at the proof of the theorem shows that if g is a primitive root of a prime p, then all the primitive roots of p that belong to sequence (23) are to be found among the remainders yielded by the division by p of those terms of the sequence

$$g,\ g^2,\ g^3,\ \ldots,\ g^{p-1}$$

whose exponents are relatively prime to $p-1$.

Denote by $\gamma(p)$ the least primitive root of a prime p. The following table shows the values of the function $\gamma(p)$ for odd primes $p < 100$:

p	3	5	7	11	13	17	19	23	29	31	37	41
$\gamma(p)$	2	2	3	2	2	3	2	5	2	3	2	6

p	43	47	53	59	61	67	71	73	79	83	89	97
$\gamma(p)$	3	5	2	2	2	2	7	5	3	2	3	5

It has been proved that $\overline{\lim}\,\gamma(p) = \infty$ (Pillai [7]) and even that, for infinitely many p, $\gamma(p) > c \log p$ (cf. Turán [1]). On the other hand, we do not know whether there exist infinitely many primes for which number 2 is a primitive root. E. Artin has conjectured that every integer $g \neq -1$ which is not a square is a primitive root of infinitely many primes (cf. Hasse [1], p. 68). This can be deduced from the conjecture H (cf. Schinzel and Sierpiński [3], pp. 199-201).

The table presented above shows that $\gamma(p) \leqslant 7$ for any prime $p < 100$. For $p < 191$ we also have $\gamma(p) \leqslant 7$, but $\gamma(191) = 19$. If $p < 409$, then $\gamma(p) \leqslant 19$, but $\gamma(409) = 21$. For primes $p < 3361$ we have $\gamma(p) \leqslant 21$, but $\gamma(3361) = 22$. For $p < 5711$ we have $\gamma(p) \leqslant 22$, but $\gamma(5711) = 29$. If p is a prime < 5881, then $\gamma(p) \leqslant 29$, but $\gamma(5881) = 31$ (cf. Wertheim [1], pp. 406-409).

If g is a primitive root of a prime p, then the numbers $g^0, g^1, g^2, \ldots, g^{p-2}$ divided by p leave different remainders, each of them, in addition, being different from zero. Consequently, the number of the remainders is equal to the number of the numbers $g^0, g^1, g^2, \ldots, g^{p-2}$, i.e. it is equal to $p-1$. Therefore, for any number $x = g^0, g^1, \ldots, g^{p-2}$, there exists a number y of the sequence $0, 1, 2, \ldots, p-2$ such that $g^y \equiv x \pmod p$.

Now we are going to establish all the natural numbers $m > 1$ which have primitive roots. The situation is described by the following theorem:

A natural number $m > 1$ has primitive roots if and only if it is one of the numbers

$$2,\ 4,\ p^\alpha,\ 2p^\alpha$$

where p is an odd prime and α a natural number. The number of primitive roots of any number m of this form is $\varphi(\varphi(m))$ (cf. Sierpiński [12], p. 193).

As an application of the theorem on the existence of primitive roots of odd prime numbers, we shall find all the natural numbers m for which the congruences $a \equiv b \pmod m$ and $c \equiv d \pmod m$ imply the congruence $a^c \equiv b^d \pmod m$ for any positive integers a, b, c, d.

For simplicity, we call the above-mentioned property of number m property P. Suppose that a natural number m has property P. Let a denote a given integer. In virtue of the obvious relations $m \mid a-a$ and $m \mid (m+1)-1$ we then have $m \mid a^{m+1}-a$, i. e. $m \mid a(a^m-1)$. On the other hand, suppose that number m is such that for any integer a we have $m \mid a(a^m-1)$. Let a, b, c, d be integers such that $m \mid a-b$ and $m \mid c-d$. If $c = d$, then, by $m \mid a-b$, we have $m \mid a^c - b^d$. Suppose that $c \neq d$. Interchanging, if necessary, the roles of c and d, we assume that $c > d$. Then, since $m \mid c-d$, $c = d+mk$, where k is a natural number. We then have $a \mid a^d$ and $a^m-1 \mid a^{mk}-1$. Moreover, it follows from $m \mid a(a^m-1)$ that $m \mid a^d(a^{mk}-1) = a^c - a^d$. But, in virtue of $m \mid a-b$, we have $m \mid a^d - b^d$, which, by the formula $m \mid a^c - a^d$ gives $m \mid a^c - b^d$. We see that number m has property P. We have thus proved that a necessary and sufficient condition for a number m to have property P is that for any integer a, $m \mid a(a^m-1)$.

Now, our aim is to find all the numbers m that have property P. Trivially, numbers 1 and 2 have property P. Suppose that m is a natural number > 2. If m were divisible by a square of a prime number, then, for $a = p$, we would have $p^2 \mid p(p^m-1)$, which is impossible because $(p, p^m-1) = 1$. Consequently, number m must be a product of different prime factors; being greater than 2, the product must contain a prime odd factor p. Let g denote a primitive root of the prime p. Since $p \mid m \mid g(g^m-1)$ and $(p, g) = 1$, we find that $p \mid g^m-1$. But since g belongs to the exponent $p-1$ with respect to modulus p, we have $p-1 \mid m$. Therefore number m is even and is the product of at least two different prime factors 2, and p. If m is the product of precisely those two different prime factors, then $m = 2p$. Since $p-1 \mid m$ and $(p-1, p) = 1$, we have $p-1 \mid 2$; so, in view of $p \geqslant 3$ (since p is an odd prime), we conclude that $p = 3$ and consequently $m = 2 \cdot 3 = 6$. Number 6 indeed has property P because, as we know, for any integer a we have $6 \mid (a-1)a(a+1) = a(a^2-1)$ and $a^2-1 \mid a^6-1$, whence $6 \mid a(a^6-1)$.

We now suppose that m is a product of three (necessarily different) prime factors, i.e. $m = 2p_1p_2$, where $2 < p_1 < p_2$. As we know, $p_1-1 \mid m$ that is $p_1-1 \mid 2p_1p_2$. But $p_1-1 > 1$ (since $p_1 > 2$) and also $p_1-1 < p_1 < p_2$. The prime p_2 cannot be divisible by p_1-1 and therefore $p_1-1 \mid 2p_1$, whence, in analogy to the previous case, we infer that $p_1 = 3$, and so $m = 6p_2$. In virtue of the relations $p_2-1 \mid m = 6p_2$

and $(p_2-1, p_2) = 1$, one has $p_2 - 1 | 6$, which, by the fact that $p_2 > p_1$, i.e. that $p_2 > 3$ and so $p_2 - 1 \geqslant 2$, gives either $p_2 - 1 = 3$ or $p_2 - 1 = 6$. But $p_2 - 1 = 3$ is impossible because p_2 is a prime, so $p_2 - 1 = 6$ is valid, whence $p_2 = 7$ and consequently $m = 2 \cdot 3 \cdot 7 = 42$. As can easily be verified, number 42 indeed has property P. In fact, as is known, $6 | a(a^6 - 1)$ holds for any integer a, whence *a fortiori* $6 | a(a^{42} - 1)$. If a is not divisible by 7, then, in virtue of the theorem of Fermat, $7 | a^6 - 1$, whence again $7 | a(a^{42} - 1)$. Thus we see that for any integer a the relations $6 | a(a^{42} - 1)$ and $7 | a(a^{42} - 1)$ simultaneously hold, which, by $(6, 7) = 1$, gives $42 | a(a^{42} - 1)$, and this proves that number 42 has property P.

Further we suppose that m is a product of four prime factors. That is that $m = 2p_1p_2p_3$, where $2 < p_1 < p_2 < p_3$. Then, as in the above argument, we infer that $p_1 - 1 | 2$, whence $p_1 = 3$; similarly, $p_2 - 1 | 2p_1 = 6$, whence $p_2 = 7$; and finally, $p_3 - 1 | 2p_1p_2 = 42$. Therefore, since $p_3 > p_2 = 7$, it must be true that $p_3 - 1 = 7$, 14, 21 or 42, which, in virtue of the fact that p_3 is a prime, implies $p_3 - 1 = 42$, i.e. $p_3 = 43$, whence $m = 1806$. It is easy to see that number 1806 has property P because, as we have just proved, $42 | a(a^{42} - 1)$ for any integer a, whence *a fortiori* $42 | a(a^{1806} - 1)$. If a is divisible by 43, then we have $43 | a(a^{1806} - 1)$; if a is not divisible by 43, this relation is a simple consequence of the theorem of Fermat, because then $43 | a^{42} - 1$, whence *a fortiori* $43 | a^{1806} - 1$. The relations $42 | a(a^{1806} - 1)$ and $43 | a(a^{1806} - 1)$, valid for any integer a, give by $(42, 43) = 1$ and $1806 = 42 \cdot 43$ the required relation $1806 | a(a^{1806} - 1)$, which proves that number 1806 has property P.

Finally, we suppose that m is a product of more than four prime factors. That is $m = 2p_1p_2 \ldots p_k$, where $k \geqslant 4$, $2 < p_1 < p_2 < \ldots < p_k$. As we have seen above, $p_1 = 3$, $p_2 = 7$, $p_3 = 43$. Further, $p_4 - 1 | m$, whence, as can easily be found, $p_4 - 1 | 2p_1p_2p_3$, i.e. $p_4 - 1 | 1806$. On the other hand, $p_4 - 1 > p_3 - 1 = 42$, and, moreover, $p_4 - 1$ is even. Even divisors of the number $1806 = 2 \cdot 3 \cdot 7 \cdot 43$ which are greater than 42 are the numbers 86, 258, 602, 1806. Therefore p_4 must be one of the numbers 87, 259, 603, or 1807, but none of them is prime. We have $87 = 3 \cdot 29$, $259 = 7 \cdot 37$, $603 = 3^2 \cdot 67$, $1807 = 13 \cdot 139$. Thus we see that the assumption that a number m is a product of more than four prime factors leads to a contradiction.

We have thus proved the theorem of J. Dyer Bennet [1], stating that *the numbers* 1, 2, 6, 42, 1806 *are the only ones which have property* P. Consequently, they are the only moduli m for which the congruences $a \equiv b \pmod m$ and $c \equiv d \pmod m$ imply $a^c \equiv b^d \pmod m$ for any positive integers a, b, c, d.

As is easy to notice, numbers m which have property P are precisely those square-free integers m for which $\lambda(m) | m$, where $\lambda(m)$ is the minimum universal exponent with respect to the modulus m (cf. § 4).

EXERCISE. Prove that number 2 is not a primitive root of any prime number of the form $2^{2^n} + 1$, where n is a natural number > 1.

Proof. If p is a prime number and $p = 2^{2^n} + 1$, then $2^{2^{n+1}} \equiv 1 \pmod p$. But $p - 1 = 2^{2^n} > 2^{n+1}$ for $n > 1$ because, as can easily be proved by induction, $2^n > n + 1$ for $n = 2, 3, \ldots$ Consequently number 2 belongs to an exponent $< p - 1$ with respect to the modulus p and is not a primitive root of p.

§ 7. An *n*th power residue for a prime modulus *p*. If p is a prime, n a natural number > 1, then an integer a is called an *n-th power residue for the modulus* p whenever there exists an integer x such that $x^n \equiv a \pmod p$. Clearly, the number 0 is an nth residue for the modulus p for any prime p and integer n. Therefore we generally assume that any nth power residue we are concerned with is different from zero.

From the purely theoretical point of view, there exists a method for establishing whether a given natural number $a \neq 0$ is an nth power residue for a given modulus p. In fact, it is sufficient to check whether there exists a number x in the sequence $1, 2, \ldots, p-1$ which satisfies the congruence $x^n \equiv a \pmod p$.

In this connection, we have the following

THEOREM 13 (Euler). *An integer a which is not divisible by a prime p is an n-th power residue for a prime modulus p if and only if the relation*

$$a^{(p-1)/d} \equiv 1 \pmod p \quad \text{with} \quad d = (p-1, n) \tag{27}$$

holds.

Proof. Suppose that an integer a, which is not divisible by a prime p, is an nth power residue for the modulus p. Then there exists an integer x, of course not divisible by p, such that $a \equiv x^n \pmod p$. Hence

$$a^{(p-1)/d} \equiv (x^n)^{(p-1)/d} \equiv (x^{p-1})^{n/d}. \tag{28}$$

Since $d \mid n$ and, by the theorem of Fermat, $x^{p-1} \equiv 1 \pmod p$, from (28) we infer the truth of (27). Thus we see that the condition is necessary.

Suppose now that formula (27) holds. Let g be a primitive root of the prime p. As we learned in § 6, there exists an integer h such that $0 \leqslant h \leqslant p-2$ and $a \equiv g^h \pmod p$ which, in virtue of (27), proves that $g^{h(p-1)/d} \equiv 1 \pmod p$. Since g is a primitive root for the prime p, the last relation implies that $p - 1 \mid \frac{h(p-1)}{d}$, which gives $d | h$ and so $h = kd$, where k is a non-negative integer. According to the definition, $d = (p-1, n)$, which, by theorem 16 from Chapter I, proves that there exist two natural numbers u, v such that $d = nu - (p-1)v$, whence $kd = knu - k(p-1)v$. But, in virtue of the theorem of Fermat, $g^{k(p-1)v} \equiv 1 \pmod p$. Hence, using the relations $a \equiv g^h \equiv g^{kd} \pmod p$, we find $a \equiv ag^{k(p-1)v} \equiv g^{kd+k(p-1)v} \equiv g^{knu} \equiv (g^{ku})^n \pmod p$, which proves that a is an nth power residue for the prime p. This proves the sufficiency of the condition. Theorem 13 is thus proved.

If a is an nth power residue for a modulus p, then, clearly, every number a that is congruent to $a \pmod p$ is also an nth power residue for the modulus p. Therefore the number of nth power residues for a given modulus p is understood as the number of mutually non-congruent $\pmod p$ nth power residues for the modulus p.

The following theorem holds:

THEOREM 14. *If p is a prime, n a natural number and $d = (n, p-1)$, then the number of different n-th power residues for the modulus p (number 0 included) is $(p-1)/d + 1$.*

Proof. Let g be a primitive root for the modulus p. Let $d=(p-1, n)$, $n=dm$, $p-1=ds$, where m, s are natural numbers and $(m, s)=1$. Let k, l be any two numbers of the sequence $1, 2, \ldots, s$ such that $k>l$. If $g^{kn} \equiv g^{ln} \pmod p$, then $p \mid g^{kn}-g^{ln}=g^{ln}(g^{(k-l)n}-1)$, so, by $(p, g)=1$, $g^{(k-l)n} \equiv 1 \pmod p$. Hence, since g is a primitive root for the prime p, $p-1 \mid (k-l)^n$, which, in virtue of the relations $n=dm$, $p-1=ds$, gives $s \mid (k-l)m$; so, since $(m, s)=1$, $s \mid k-l$, which is impossible because k and l are two different numbers of the sequence $1, 2, \ldots, s$. Thus we conclude that the numbers $g^n, g^{2n}, \ldots, g^{sn}$ divided by p yield different remainders. Moreover, each of these numbers is an nth power residue for the modulus p (since the congruence $x^n \equiv g^{kn} \pmod p$ has an obvious solution $x=g^k$). Therefore there are at least s different nth power residues for the modulus p, each of them different from zero.

Now let a denote an arbitrary nth power residue for the modulus p different from zero. Then there exists an integer x (clearly not divisible by p) such that $x^n \equiv a \pmod p$. As we have learned, in the sequence $0, 1, \ldots, p-2$ there exists a number y such that $x \equiv g^y \pmod p$, whence $a \equiv g^{ny} \pmod p$. Let r denote the remainder obtained by dividing y by s. We then have $y=ks+r$, where k is a non-negative integer and $0 \leqslant r<s$. Hence $ny=nks+nr$. But, since $n=dm$, $p-1=ds$, we have $ns=(p-1)m$. Consequently, $ny=k(p-1)m+nr$, whence $a \equiv g^{ny} \equiv g^{nr} \pmod p$, and this shows that there are no nth power residues for the modulus p different from zero other than $1, g^n, g^{2n}, \ldots, g^{(s-1)n}$. Since $sn=(p-1)m$, residue 1 can be replaced by the residue g^{sn}. We have thus proved that for a given prime modulus p there exist precisely $\dfrac{p-1}{(n, p-1)}+1$ different nth power residues.

As an immediate corollary to theorem 14 we have the following proposition: *in order that for a given natural number n every integer be an n-th power residue for a given prime modulus p it is necessary and sufficient that n be relatively prime to $p-1$.*

Accordingly, in the case of $n=3$, in order that every integer be a third power residue for a prime modulus p it is necessary and sufficient that p should not be of the form $3k+1$, where k is a natural number, i.e. that it be either one of the numbers 2, 3 or of the form $3k+2$, where k is a natural number.

It is easy to prove that there are infinitely many primes of the form $3k+2$. In fact, let n denote an arbitrary natural number and let $N=6n!-1$. Clearly, N is a natural number >1. It is easy to see that any divisor of the number N is of the form $6k+1$ or $6k-1$. Not all prime divisors of N are of the form $6k+1$ since, if they were, their product would be of this form, which is trivially untrue since N is not of this form. Consequently, number N has at least one prime divisor $p=6k-1$, where k is a natural number. The relation $p \mid N=6n!-1$ implies that $p>n$. This, since n is arbitrary, shows that there exist arbitrarily large primes of the form $6k-1=3\big(2(k-1)+1\big)+2$, as was to be proved.

It can be proved that if n is a prime and m a natural number >1, then in order that every integer be an nth power residue for the modulus m it is necessary and sufficient that m be a product of different primes, none of the form $nk+1$ (where k is a natural number) (cf. Sierpiński [9]).

EXERCISE. Prove that if p is a prime, n a natural number and $d=(p-1, n)$, then the nth power residue for the prime p coincides with the dth power residue for the prime p.

Proof. By $d=(p-1, n)$ we have $d \mid p-1$, so $d=(p-1, d)$ and consequently, by theorem 13, a necessary and sufficient condition for an integer a, not divisible by p, to be an nth power residue for the modulus p is the same as that for a to be a dth power residue for the modulus p. Therefore the sets of nth power residues and dth power residues for the modulus p coincide.

In particular, it follows that if p is a prime of the form $4k+3$, where $k=0, 1, 2, \ldots$, then (since $2=(p-1, 4)$), the quadratic residues for the modulus p coincide with the 4th power residues for the modulus p.

§ 8. Indices, their properties and applications. In § 4 we defined a primitive root of a natural number m as an integer g which belongs to the exponent $\varphi(m)$ with respect to the modulus m. It follows that, as we know, the numbers $g^0, g^1, \ldots, g^{\varphi(m)-1}$ are all incongruent $(\mathrm{mod}\, m)$. Since the number of them is $\varphi(m)$, this being equal to the number of the numbers relatively prime to m which appear in the sequence $1, 2, \ldots, m$, then for any integer x relatively prime to m there exists precisely one number y in the sequence $0, 1, 2, \ldots, \varphi(m)-1$ such that $g^y \equiv x \pmod m$. We say that y is the *index* of x relative to the primitive root g. It is denoted by $\mathrm{ind}_g x$, or, if no confusion is likely to ensue, by $\mathrm{ind}\, x$. We call g the *base* of the index.

Now we fix a natural number $m>1$ which admits a primitive root g and consider the indices $\mathrm{ind}\, x$ of integers x relatively prime to the number m. We prove the following properties of indices:

I. *The indices of integers which are congruent* $(\mathrm{mod}\, m)$ *are equal.* (Needless to say, the primitive roots are assumed to be equal and the integers to be relatively prime to m.)

In fact, if $a \equiv b \pmod m$ and, $g^{\mathrm{ind}\, a} \equiv a \pmod m$, then $g^{\mathrm{ind}\, a} \equiv b \pmod m$. But, as we know, since $(b, m)=1$, the congruence $g^x \equiv b \pmod m$ has precisely one root among the numbers $0, 1, \ldots, \varphi(m)-1$, and this is $\mathrm{ind}\, b$; we conclude that $\mathrm{ind}\, a=\mathrm{ind}\, b$.

Therefore in the tables of indices the values of $\mathrm{ind}\, x$ are given only for natural numbers x less than the modulus (and relatively prime to it).

II. *The index of the product is congruent* $(\mathrm{mod}\,\varphi(m))$ *to the sum of the indices of the factors*, i.e.

$$\mathrm{ind}(ab) \equiv \mathrm{ind}\,a + \mathrm{ind}\,b \pmod{\varphi(m)}. \tag{29}$$

In fact, according to the definition of indices, we have $g^{\mathrm{ind}\,a} \equiv a \pmod m$, $g^{\mathrm{ind}\,b} \equiv b \pmod m$ (whenever a and b are relatively prime to m). Hence, multiplying the last two congruences, we obtain

$$g^{\mathrm{ind}\,a+\mathrm{ind}\,b} \equiv ab \pmod m.$$

But since $g^{\mathrm{ind}(ab)} \equiv ab \pmod m$, we infer that

$$g^{\mathrm{ind}(ab)} \equiv g^{\mathrm{ind}\,a+\mathrm{ind}\,b} \pmod m. \tag{30}$$

Suppose that for any non-negative integers μ, ν the congruence $g^\mu \equiv g^\nu \pmod m$ holds. If $\mu \geqslant \nu$, then $m \mid g^\nu(g^{\mu-\nu}-1)$, which, in virtue of the fact that $(g, m) = 1$, implies $g^{\mu-\nu} \equiv 1 \pmod m$. Number g, as a primitive root of m, belongs to the exponent $\varphi(m)$ with respect to the modulus m. Hence, by theorem 9, it follows that $\varphi(m) \mid \mu-\nu$.

The last relation remains true also in the case where $\mu \leqslant \nu$. Thus, from (30) congruence (29) follows.

The property just proved is easily generalized to any finite number of factors. Hence

III. *The index of the n-th power* (n *being a natural number*) *is congruent* $(\mathrm{mod}\,\varphi(m))$ *to the product of* n *multiplied by the index of the base. We have*

$$\mathrm{ind}\,a^n \equiv n\,\mathrm{ind}\,a \pmod{\varphi(m)}.$$

Now we are going to establish the relation between indices taken with respect to different primitive roots of a fixed number m. According to the definition of the index, we have

$$a \equiv g^{\mathrm{ind}_g a} \pmod m.$$

Hence, using properties I and III, we obtain

$$\mathrm{ind}_\gamma a \equiv \mathrm{ind}_g a \cdot \mathrm{ind}_\gamma g \pmod{\varphi(m)},$$

where γ is a primitive root of m. Hence

In order to change the base of indices it is sufficient to multiply each of them by a fixed number (*namely by the index of the former base relative to the new base*) *and find the residues for the modulus* $\varphi(m)$ *of the products.*

THEOREM 15. *In order that a number* a, *which is not divisible by* p, *be a quadratic residue for an odd prime* p, *it is necessary and sufficient that* $\mathrm{ind}\,a$ *be even.*

Proof. Suppose that $\mathrm{ind}_g a = 2k$, where k is a non-negative integer. We have $g^{2k} \equiv a \pmod p$, which shows that the congruence $x^2 \equiv a \pmod p$ has a root $x = g^k$. Therefore number a is a quadratic residue for the modulus p.

In the sequence $1, 2, \ldots, p-1$ there are, of course, $\frac{1}{2}(p-1)$ numbers whose indices are even. (The proof follows from the remark that the indices of the numbers of the sequence coincide with the numbers $0, 1, 2, \ldots, p-2$ in a certain order; among $0, 1, 2, \ldots, p-2$, however, there are precisely $\frac{1}{2}(p-1)$ even numbers.) Each of these numbers is then a quadratic residue for the prime p. But, by theorem 14 (with $d = (2, p-1) = 2$), there are only $\frac{1}{2}(p-1)$ quadratic residues in the sequence $1, 2, \ldots, p-1$. From this we infer that none of the numbers with odd indices can be a quadratic residue for the prime p. The theorem is thus proved.

It is an immediate consequence of theorem 15 that none of the primitive roots of an odd prime p can be a quadratic residue to p.

We note that an analogous theorem for an nth power residue with n greater than 2 is not true. For example, among the indices relative to the modulus 5 there are only two, 0 and 3, divisible by 3, and each of the numbers $1, 2, 3, 4$ is a 3rd power residue to 5. (In fact, $1 \equiv 1^3 \pmod 5$, $2 \equiv 3^3 \pmod 5$, $3 \equiv 2^3 \pmod 5$, $4 \equiv 4^3 \pmod 5$). For the modulus 7 the numbers $1 \equiv 1^4 \pmod 7$, $2 \equiv 2^4 \pmod 7$, $4 \equiv 3^4 \pmod 7$ are 4th power residues; among the indices relative to the modulus 7, however, there are only two, 0 and 4, divisible by 4.

Indices are applied in solving congruence.

Let p be a prime, and a, b numbers not divisible by p. Consider the congruence

$$ax \equiv b \pmod p.$$

By properties I and II

$$\mathrm{ind}\,a + \mathrm{ind}\,x \equiv \mathrm{ind}\,b \pmod{p-1},$$

whence

$$\mathrm{ind}\,x \equiv \mathrm{ind}\,b - \mathrm{ind}\,a \pmod{p-1}.$$

The number $\mathrm{ind}\,x$ is thus the remainder left by the difference $\mathrm{ind}\,b - \mathrm{ind}\,a$ divided by number $p-1$. Thus, knowing the value of $\mathrm{ind}\,x$, we find x by $x \equiv g^{\mathrm{ind}\,x} \pmod p$. Of course, to apply this method in practice one should have the tables of indices $(\mathrm{mod}\,p)$.

Now let a be an integer which is not divisible by p, and n a natural exponent. Consider the congruence

$$x^n \equiv a \pmod p.$$

By properties I and III it follows that the congruence is equivalent to the congruence

$$n\operatorname{ind} x \equiv \operatorname{ind} a \pmod{p-1}.$$

Thus the problem of solving binomial congruences reduces to that of solving linear congruences.

Consider an exponential congruence

$$a^x \equiv b \pmod{p},$$

where a, b are integers not divisible by the prime p. The congruence is equivalent to the linear congruence

$$x\operatorname{ind} a \equiv \operatorname{ind} b \pmod{p-1}.$$

EXAMPLES. We are going to tabulate the indices (mod13). Accordingly, first we have to establish a primitive root of 13. We begin with the least possible number 2.

We find the residue (mod13) of the consecutive powers of number 2. Clearly, it is not necessary to calculate number 2^n for every natural exponent n; for, if r_k is the remainder obtained by dividing 2^k by 13, then the remainder yielded by 2^{k+1} divided by 13 is equal to the remainder of $2r_k$. In this way we find $2 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 3$, $2^5 \equiv 6$, $2^6 \equiv 12$, $2^7 \equiv 11$, $2^8 \equiv 9$, $2^9 \equiv 5$, $2^{10} \equiv 10$, $2^{11} \equiv 7$, $2^{12} \equiv 1 \pmod{13}$.

This proves that 2 is a primitive root of 13. We tabulate the numbers x according to their indices $\operatorname{ind}_2 x \equiv k$ (where $k = 0, 1, \ldots, 11$) as follows:

$\operatorname{ind}_2 x$	0	1	2	3	4	5	6	7	8	9	10	11
x	1	2	4	8	3	6	12	11	9	5	10	7

By the use of this table we can tabulate the indices according to the numbers $x = 1, 2, \ldots, 12$ as follows:

x	1	2	3	4	5	6	7	8	9	10	11	12
$\operatorname{ind}_2 x$	0	1	4	2	9	5	11	3	8	10	7	6

Given a congruence

$$6x \equiv 5 \pmod{13}.$$

We have $\operatorname{ind}6 + \operatorname{ind}x \equiv \operatorname{ind}5 \pmod{12}$, whence $\operatorname{ind}x \equiv \operatorname{ind}5 - \operatorname{ind}6 \pmod{12}$. As we check in the second table, $\operatorname{ind}5 = 9$ and $\operatorname{ind}6 = 5$, thus we find $\operatorname{ind}x \equiv 9 - 5 \equiv 4 \pmod{12}$, and so $\operatorname{ind}x = 4$ and, using the first table, we infer that $x = 3$.

Consider the congruence

$$x^8 \equiv 3 \pmod{13}.$$

We have $8\operatorname{ind}x \equiv \operatorname{ind}3 \pmod{12}$. On the other hand, by the tables presented above, we see that $\operatorname{ind}3 = 4$, whence, putting $\operatorname{ind}x = y$, we obtain the congruence $8y \equiv 4 \pmod{12}$. This is equivalent to the relation $12 \mid 8y - 4$, which, in turn, is equivalent to $3 \mid 2y - 1$, i.e. to the congruence $2y \equiv 1 \pmod{3}$. Hence $4y \equiv 2 \pmod{3}$. But, since $4 \equiv 1 \pmod{3}$, $y \equiv 2 \pmod{3}$ and therefore $y = 2 + 3k$, where k is an integer. Numbers of this form that belong to the sequence $0, 1, 2, \ldots, 11$ are the numbers $2, 5, 8$ and 11. Consequently, they are the values of $y = \operatorname{ind}x$. Using the first table for x we find the values $4, 6, 9$ and 7. Thus we see that the congruence has precisely four solutions, $4, 6, 7, 9$.

Finally, consider the congruence

$$6^x \equiv 7 \pmod{13}.$$

We then have $x\operatorname{ind}6 \equiv \operatorname{ind}7 \pmod{12}$. As we check in the second table, $\operatorname{ind}6 = 5$, $\operatorname{ind}7 = 11$. Thus the congruence turns into the congruence $5x \equiv 11 \pmod{12}$, which is satisfied only for $x = 7$, provided the x's are taken out of the sequence $0, 1, \ldots, 11$. Consequently, all the solutions of the congruence are numbers of the form $7 + 12k$, where $k = 0, 1, 2, \ldots$

EXERCISES. **1.** Prove that for any odd prime modulus p relative to any primitive root of p,[1] the equalities $\operatorname{ind}(-1) = \operatorname{ind}(p-1) = \frac{1}{2}(p-1)$ hold.

Proof. In virtue of the theorem of Fermat, for any primitive root g of an odd prime p the relation $p \mid g^{p-1} - 1 = (g^{\frac{1}{2}(p-1)} - 1)(g^{\frac{1}{2}(p-1)} + 1)$ holds. But since $p \mid g^{\frac{1}{2}(p-1)} - 1$ is impossible (because g is a primitive root of p), $p \mid g^{\frac{1}{2}(p-1)} + 1$ is valid, i.e. $g^{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$, which shows that $\operatorname{ind}(-1) = \frac{1}{2}(p-1)$.

2. Prove that a necessary and sufficient condition for an integer g relatively prime to an odd prime p to be a primitive root of p is the validity of the relation $g^{(p-1)/q} \not\equiv 1 \pmod{p}$ for any prime divisor q of the number $p-1$.

Proof. If for a prime q the relations $q \mid p-1$ and $g^{(p-1)/q} \equiv 1 \pmod{p}$ hold, then q belongs to an exponent $\leqslant (p-1)/q < p-1$ and, consequently, g is not a primitive root of p. Thus the condition is necessary.

On the other hand, suppose that an integer g relatively prime to p is not a primitive root of p. Then the exponent δ to which g belongs with respect to modulus p is $< p-1$. As we know, δ must be a divisor of number $p-1$, whence number $(p-1)/\delta$ is a natural number > 1, and so it has a prime divisor q. We then have $q \mid (p-1)/\delta$, whence $\delta \mid (p-1)/q$ and, since $p \mid g^{\delta} - 1$ (because g belongs to the exponent δ with respect to the modulus p), then *a fortiori* $p \mid g^{(p-1)/q} - 1$, i.e. $g^{(p-1)/q} \equiv 1 \pmod{p}$. The condition is thus sufficient.