CHAPTER V

CONGRUENCES

§ 1. Congruences and their simplest properties. Let a and b be two integers. We say that a *is congruent to* b *with respect to the modulus* m if the difference of a and b is divisible by m. Using the notation introduced by Gauss, we write

$$a \equiv b \pmod{m}. \tag{1}$$

Thus formula (1) is equivalent to the formula

$$m \mid a-b.$$

It is clear that, if two integers are congruent with respect to the modulus m, then the division of either of them by m gives the same remainder and *vice versa*.

There is an analogy between congruence and *equality* (this justifies the use of the symbol $\equiv$, similar to the symbol of equality). We list here some of the more important properties which illustrate this analogy:

I. *Reflexivity* means that every integer is congruent to itself with respect to any modulus; i.e.

$$a \equiv a \pmod{m}$$

for any integer a and any natural number m. To prove this it is sufficient to observe that the number $a-a = 0$ is divisible by every natural number m.

II. *Symmetry* means that congruence (1) is equivalent to the congruence $b \equiv a \pmod{m}$. To prove this it is sufficient to note that the numbers $a-b$ and $b-a$ are either both divisible or both not divisible by a natural number m.

III. *Transitivity* means that, if

$$a \equiv b \pmod{m} \quad \text{and} \quad b \equiv c \pmod{m},$$

then

$$a \equiv c \pmod{m}.$$

To prove this we apply the identity

$$a-c = (a-b)+(b-c)$$

and recall the fact that the sum of two numbers, each of them divisible by m, is divisible by m.

Similarly, it is very easy to prove some other properties of congruence.

We prove that *two congruences can be added or subtracted from each other provided both have the same modulus.*

Let

$$a \equiv b \pmod{m} \quad \text{and} \quad c \equiv d \pmod{m}. \tag{2}$$

In order to prove that $a+c \equiv b+d \pmod{m}$ and $a-c \equiv b-d \pmod{m}$ it is sufficient to apply the identities

$$a+c-(b+d) = (a-b)+(c-d) \quad \text{and} \quad (a-c)-(b-d) = (a-b)-(c-d).$$

Similarly, using the identity

$$ac-bd = (a-b)c+(c-d)b,$$

we prove that congruences (2) imply the congruence

$$ac \equiv bd \pmod{m}.$$

Consequently, we see that *two congruences having the same modulus can be multiplied by each other.*

The theorem on the addition, subtraction and multiplication of two congruences can easily be extended to the case of any finite number of congruences.

The theorem on addition of congruences implies that *the summands can be transferred, with the opposite sign,* in just the same way as in equations, *from one side of a congruence to the other*. This is because that operation is equivalent to the subtraction of the transferred summand from each side of the congruence.

It follows from the theorem on the multiplication of congruences that *a congruence can always be multiplied throughout by any integer and that each side of a congruence can be raised to the same natural power.*

But it is not always legitimate to divide one congruence by another (even if the quotients are integers). For example the congruences $48 \equiv 18 \pmod{10}$ and $12 \equiv 2 \pmod{10}$ do not imply the congruence $4 \equiv 9 \pmod{10}$.

It follows immediately from the theorem stating that a divisor of a divisor of an integer is a divisor of that integer that, if $d \mid m$, then *the congruence* $a \equiv b \pmod{m}$ *implies the congruence* $a \equiv b \pmod{d}$.

The law of transitivity of congruences together with the theorem on the addition and multiplication of congruences implies that *in* *a given congruence we can replace any summand or factor by any other, congruent to it.*

This rule is not valid for the exponents. For example the congruence $2^6 \equiv 4 \pmod 5$ cannot be replaced by the congruence $2^1 = 4 \pmod 5$ though $6 \equiv 1 \pmod 5$.

Now, let

$$f(x) = A_0x^n + A_1x^{n-1} + \ldots + A_{n-1}x + A_n$$

be a polynomial of the nth degree with integral coefficients. Let m be a natural modulus and a, b integers such that $a \equiv b \pmod m$. The theorems on the natural powers and on the multiplication of congruences justify the following sequence of congruences:

$$\begin{aligned} A_0a^n &\equiv A_0b^n \pmod m, \\ A_1a^{n-1} &\equiv A_1b^{n-1} \pmod m, \\ &\ldots\ldots\ldots\ldots\ldots \\ A_{n-1}a &\equiv A_{n-1}b \pmod m, \\ A_n &\equiv A_n \pmod m. \end{aligned}$$

Adding them up, we obtain

$$A_0a^n + A_1a^{n-1} + \ldots + A_{n-1}a + A_n \\ \equiv A_0b^n + A_1b^{n-1} + \ldots + A_{n-1}b + A_n \pmod m,$$

i.e. $f(a) \equiv f(b) \pmod m$. We have thus proved the following

THEOREM 1. *If $f(x)$ is a polynomial in x with integral coefficients, then the congruence $a \equiv b \pmod m$ implies the congruence $f(a) \equiv f(b) \pmod m$.*

An illustration of the use of theorem 1 is provided by the rules of divisibility of a number by 9, 7, 11, 13, 27, 37.

Let N be a natural number. The usual representation of the number N by its digits in the scale of 10 is in fact a representation of N in the form

$$N = c_1 10^{n-1} + c_2 10^{n-2} + \ldots + c_{n-1}10 + c_n.$$

Let

$$f(x) = c_1x^{n-1} + c_2x^{n-2} + \ldots + c_{n-1}x + c_n. \tag{3}$$

Then $f(x)$ is a polynomial with integral coefficients and

$$f(10) = N. \tag{4}$$

In virtue of theorem 1, since $10 \equiv 1 \pmod 9$, we have

$$f(10) \equiv f(1) \pmod 9. \tag{5}$$

But $f(1) = c_1 + c_2 + \ldots + c_n$ and, consequently, by (4) and (5),

$$N \equiv c_1 + c_2 + \ldots + c_n \pmod 9,$$

which proves that any natural number N differs from the sum of its digits (in the scale of 10) by a multiple of 9. In particular, *N is divisible by 9 if and only if the sum of its digits is divisible by 9.*

In general, if s_N denotes the sum of the digits of N (in the scale of 10), then for natural numbers N and N' we have

$$N \equiv s_N \pmod 9, \qquad N' \equiv s_{N'} \pmod 9,$$

whence $NN' \equiv s_N s_{N'} \pmod 9$. Since also $NN' \equiv s_{NN'} \pmod 9$, then $s_{NN'} \equiv s_N s_{N'} \pmod 9$. This relation between the sums of the digits of the factors and the sum of the digits of the product serves as the basis for the well-known *test of multiplication by the use of* 9.

By (3) and by the congruence $10 \equiv -1 \pmod{11}$, theorem 1 implies that $f(10) \equiv f(-1) \pmod{11}$, whence, by (4) and (3), we obtain

$$N \equiv c_1 - c_2 + c_3 - c_4 + \ldots \pmod{11}.$$

This gives the rule of divisibility by 11.

Now we are going to find the rules of divisibility by 7 or 13. Denote by $(c_1c_2\ldots c_n)_{10}$ the number whose digits, in the scale of 10, are $c_1, c_2, \ldots, c_n$; this notation is really necessary in order to distinguish a number from the product of its digits $c_1c_2\ldots c_n$. Every natural number can be represented in the form

$$N = (c_{n-2}c_{n-1}c_n)_{10} + (c_{n-5}c_{n-4}c_{n-3})_{10} \cdot 1000 + (c_{n-8}c_{n-7}c_{n-6})_{10} \cdot 1000^2 + \ldots$$

Since $1000 \equiv -1 \pmod 7$ and $1000 \equiv -1 \pmod{13}$, we obtain the congruence

$$N \equiv (c_{n-2}c_{n-1}c_n)_{10} - (c_{n-5}c_{n-4}c_{n-3})_{10} + (c_{n-8}c_{n-7}c_{n-6})_{10} - \ldots \pmod 7$$

and a congruence identical to the above with the modulus 7 replaced by 13. These congruences give the rules of divisibility by 7 or 13. For example,

$$N = 8589879056 \equiv 56 - 879 + 589 - 8 \pmod 7 \text{ and } \pmod{13}.$$

Since the number on the right-hand side of these congruences, equal to -242, is divisible neither by 7 nor by 13, we see that the number N is not divisible by 7 or by 13.

The rules for 27 and 37 are based on the fact that

$$1000 \equiv 1 \pmod{27} \text{ and } \pmod{37}.$$

From this the rules are obtained in a complete analogy with the previous ones. For example, we have

$$N = 24540509 \equiv 509+540+24 (\mathrm{mod}\, 27) \text{ and } (\mathrm{mod}\, 37).$$

The number on the right-hand side of this congruence is 1073. So we may write again $1073 \equiv 73+1 (\mathrm{mod}\, 27)$ and $(\mathrm{mod}\, 37)$. Number 74 is divisible by 37 but it is not divisible by 27, consequently the same is true about number N.

EXERCISES. **1.** Find the last two digits of the number 2^{1000}.

Solution. We have $2^{10} = 1024 \equiv 24 (\mathrm{mod}\, 100)$. Hence $2^{20} \equiv 24^2 \equiv 76 (\mathrm{mod}\, 100)$. But $76^2 \equiv 76 (\mathrm{mod}\, 100)$, whence, by induction, $76^k \equiv 76 (\mathrm{mod}\, 100)$, $k = 1, 2, \ldots$ Therefore $2^{1000} = 2^{20\cdot 50} \equiv 76^{50} \equiv 76 (\mathrm{mod}\, 100)$. Thus we see that the last two digits of number 2^{1000} are 7 and 6.

2. Prove that for an integer x at least one of the following six congruences is valid (cf. Erdös [11]): 1) $x \equiv 0 (\mathrm{mod}\, 2)$, 2) $x \equiv 0 (\mathrm{mod}\, 3)$, 3) $x \equiv 1 (\mathrm{mod}\, 4)$, 4) $x \equiv 3 (\mathrm{mod}\, 8)$, 5) $x \equiv 7 (\mathrm{mod}\, 12)$, 6) $x \equiv 23 (\mathrm{mod}\, 24)$.

Proof. If an integer x satisfy neither 1) nor 2), then it is not divisible by 2 or by 3, and thus it is of the form $24t+r$, where t is an integer and r is one of the numbers 1, 5, 7, 11, 13, 17, 19, 23. Then, as can easily be verified, the number $x = 24t+r$ satisfies one of the congruences 3), 3), 5), 3), 4), 3), 4), 6).

Remark. P. Erdös [11] has proposed the following problem: given any natural number n, does there exist a finite set of congruences which uses only different moduli greater than n and such that every integer satisfies at least one of them? H. Davenport [1] conjectures that the answer is positive but, he says, it is not easy to see how to give a proof. P. Erdös himself has proved this for $n = 2$ (he has given the set of such congruences, the moduli being various factors of 120). D. Swift has given the proof for $n = 3$ (he has found the set of such congruences, the moduli being various factors of 2880).

3. Find the last two digits of number 9^{9^9}.

Solution. We easily find that with respect to the modulus 100 the following congruences hold

$$9^2 \equiv 81,\quad 9^4 \equiv 81^2 \equiv 61,\quad 9^8 \equiv 61^2 \equiv 21,\quad 9^9 \equiv 21\cdot 9 \equiv 89,\quad 9^{10} \equiv 89\cdot 9 \equiv 1.$$

We then have $9^9 \equiv 9 (\mathrm{mod}\, 10)$, whence $9^9 = 10k+9$, where k is a natural number. Hence, since $9^{10} \equiv 1 (\mathrm{mod}\, 100)$, it follows that $9^{9^9} = 9^{10k+9} \equiv 9^9 \equiv 89 (\mathrm{mod}\, 100)$, which proves that the last digit of number 9^{9^9} is 9 and the last but one is 8.

4. Find the last two digits of number $9^{9^{9^9}}$.

Solution. It follows from exercise 3 that $9^{9^9} \equiv 9 (\mathrm{mod}\, 10)$. Consequently $9^{9^9} = 10t+9$, where t is a natural number, whence $9^{9^{9^9}} = 9^{10t+9} \equiv 9^9 \equiv 89 (\mathrm{mod}\, 100)$. Thus we see that the last two digits of number $9^{9^{9^9}}$ are identical with those of 9^{9^9}.

Remark. According to W. Lietzmann [1], p. 118, the number of digits of this number has more than a quarter of a million digits.

Gauss is said to have called this number "a measurable infinity".

§ 2. Roots of congruences. Complete set of residues. Let $f(x)$ be a polynomial of the nth degree with integral coefficients and let m be a given modulus. Any number $x = a$ for which $f(a) \equiv 0 (\mathrm{mod}\, m)$ is called a *root of the congruence*

$$f(x) \equiv 0 \ (\mathrm{mod}\, m). \tag{6}$$

If follows from theorem 1 that if a is a root of congruence (6), then any number which is congruent to a with respect to the modulus m is also a root of (6). Therefore it is justified to regard the whole class of such roots as a single root of the congruence. This root can of course be represented by any number of this class.

Every integer is congruent with respect to modulus m to precisely one number of the sequence

$$0,\ 1,\ 2,\ \ldots,\ m-1. \tag{7}$$

In fact, let a be a given integer and let $r = a - m\left[\dfrac{a}{m}\right]$. Number r is an integer congruent to a with respect to m. Since $t-1 < [t] \leqslant t$ for real numbers t we have $\dfrac{a}{m} - 1 < \left[\dfrac{a}{m}\right] \leqslant \dfrac{a}{m}$, whence $0 \leqslant r < m$. Thus we see that number r belongs to sequence (7), and consequently every natural number a is congruent (with respect to m) to at least one of the numbers of sequence (7). Since, on the other hand, any two of the numbers of (7) give different remainders while divided by m, every integer a is congruent precisely to one of the numbers of (7). This number is called the *remainder* of number a with respect to modulus m.

All integers which are congruent to the same remainder r with respect to modulus m are of course of the form $mk+r$, where k is an integer and *vice versa*.

In order to solve congruence (6) (where $f(x)$ is a polynomial with integral coefficients) it is sufficient to find which of the numbers of sequence (7) are roots of the congruence. Thus we see that (6) can be solved by finitely many trials. This shows that, apart from the difficulties of a purely technical nature, we are able either to solve congruence (6) (where $f(x)$ is a polynomial with integral coefficients) or to prove that $f(x)$ has no roots.

EXAMPLES. 1. We solve the congruence

$$x^5 - 3x^2 + 2 \equiv 0 (\mathrm{mod}\, 7). \tag{8}$$

We have to find which of the numbers 0, 1, 2, 3, 4, 5, 6 satisfies (8). Substituting 0 and 1 in (8), successively, we see that 1 is and 0 is not a solution of (8). Similarly, substituting 2, we see that 2 is not a solution of (8). For number 3 we may proceed as follows. We see that $3^2 \equiv 2 (\mathrm{mod}\, 7)$, whence $3^4 \equiv 4 (\mathrm{mod}\, 7)$ and $3^5 \equiv 12 \equiv 5 (\mathrm{mod}\, 7)$. Therefore $3^5 - 3\cdot 3^2 + 2 \equiv 5 - 3\cdot 2 + 2 \equiv 1 (\mathrm{mod}\, 7)$, and thus number 3 is not a solution of (8). For number 4 we have $4 \equiv -3 (\mathrm{mod}\, 7)$, whence $4^5 \equiv -3^5 \equiv -5 (\mathrm{mod}\, 7)$ and so $4^5 - 3\cdot 4^2 + 2 \equiv -5 - 3\cdot 2 + 2 \equiv 3 (\mathrm{mod}\, 7)$; consequently the number 4 is not a solution of (8) either. For number 5 we have $5 \equiv -2 (\mathrm{mod}\, 7)$, whence $5^5 \equiv -2^5 \equiv 3 (\mathrm{mod}\, 7)$ and $5^5 - 3\cdot 5^2 + 2 \equiv 3 - 3\cdot 4 + 2 \equiv 0 (\mathrm{mod}\, 7)$, and so number 5 is a solution of (8). For number 6 we have $6 \equiv -1 (\mathrm{mod}\, 7)$, whence $6^5 - 3\cdot 6^2 + 2 \equiv -1 - 3 + 2 \equiv 5 (\mathrm{mod}\, 7)$, and so 6 is not a solution of (8). We have thus shown that congruence (8) has two roots, 1 and 5. Therefore every integer x which satisfies congruence (8) is of the form $7k+1$ or $7k+5$, where k is an arbitrary integer.

2. We now solve the congruence

$$x^2 + x \equiv 0 (\mathrm{mod}\, 2). \tag{9}$$

Here the only thing that we have to do is to verify whether (9) is satisfied by numbers 0 and 1. We see that both of them satisfy the congruence (9), which proves that every integer x is a solution of (9). This also follows from the remark that numbers x^2 and x are always either both odd or both even, and so their sum is always even.

We say that a congruence which holds for every integer holds identically. The example presented above shows that for a congruence which holds identically the coefficients not necessarily all are divisible by the modulus.

Another example of a congruence which holds identically is the congruence $x^3 - x \equiv 0 (\mathrm{mod}\, 3)$. In fact, $x^3 - x = (x-1)x(x+1)$, whence, since of three consecutive integers one is divisible by 3, we deduce that $x^3 - x \equiv 0$ (mod 3) for any integers x.

3. The fact that (9) holds identically implies that the congruence $x^2 + x + 1 \equiv 0 (\mathrm{mod}\, 2)$ has no solution. Similarly, the congruence $x^2 \equiv 3 (\mathrm{mod}\, 8)$ does not hold for any integer x, since the square of an odd integer yields the remainder 1, when divided by 8 while the remainder obtained from the division of the square of an even number by 8 is 0 or 4.

Let m denote a given modulus, k a given natural number $< m$ and $a_1, a_2, \ldots, a_k$ different non-negative integers $< m$. We ask whether there exists a polynomial $f(x)$ with integral coefficients such that the roots of the congruence $f(x) \equiv 0 (\mathrm{mod}\, m)$ are precisely the numbers $a_1, a_2, \ldots, a_k$ (or numbers congruent to any of them with respect to m).

If m is a prime, then, clearly, the required function is $f(x) = (x-a_1)\times \times(x-a_2)\ldots(x-a_k)$. If $m = 4$ and $a_1, a_2, \ldots, a_k$, $k \leqslant 4$, are given non-negative different integers < 4, then, as can easily be verified, the roots of the congruence $(x-a_1)(x-a_2)\ldots(x-a_k) \equiv 0 (\mathrm{mod}\, 4)$ are the numbers $a_1, a_2, \ldots, a_k$ (or numbers congruent to any of them with respect to 4). However, as has been proved by M. Chojnacka-Pniewska [1], there is no polynomial $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ for which the congruence $f(x) \equiv 0$(mod 6) is satisfied by numbers 2 and 3 and not satisfied by any other integer < 6.

In fact, suppose that $f(x)$ is such a polynomial. Then $f(2) \equiv f(3) \equiv 0 (\mathrm{mod}\, 6)$, whence $3f(2) - 2f(3) \equiv 0 (\mathrm{mod}\, 6)$. We have $3\cdot 2^k \equiv 2\cdot 3^k \equiv 0 (\mathrm{mod}\, 6)$ for any $k = = 1, 2, \ldots$ Hence $3f(2) \equiv 3a_n (\mathrm{mod}\, 6)$ and $2f(3) \equiv 2a_n (\mathrm{mod}\, 6)$. Therefore $3f(2) - - 2f(3) \equiv a_n (\mathrm{mod}\, 6)$, whence $a_n \equiv 0 (\mathrm{mod}\, 6)$, so $f(0) \equiv 0 (\mathrm{mod}\, 6)$. We have thus proved that the congruence $f(x) \equiv 0 (\mathrm{mod}\, 6)$ has a root $x = 0$, contrary to the assumption that 2 and 3 are its only roots.

It can be proved (cf. Sierpiński [15]) that if m is a composite number $\neq 4$, then there exist two integers a and b which, divided by m, give a remainder different from zero and such that if $f(x)$ is a polynomial with integral coefficients, then the congruences $f(a) \equiv f(b) \equiv 0 (\mathrm{mod}\, m)$ imply the congruence $f(0) \equiv 0 (\mathrm{mod}\, m)$.

From this we easily deduce that if m is a composite number $\neq 4$, then there exists a polynomial of the second degree $f(x) = x^2 + a_1x + a_2$ with integral coefficients for which the congruence $f(x) \equiv 0 (\mathrm{mod}\, m)$ has more than two roots.

There is a close connection between congruences and a type of the Diophantine equations, namely equations which are linear with respect to one of the unknowns. In fact, in order that an integer x may satisfy congruence (6) it is necessary and sufficient that there should exist an integer y such that $f(x) = my$. Thus congruence $f(x)$ is equivalent to the Diophantine equation

$$f(x) - my = 0.$$

An argument analogous to that which we used in the case of the algebraic congruence of one unknown shows that if the left-hand side of a congruence is a polynomial in several variables with integral coefficients, then, if we do not take into account the difficulties of a purely technical nature, we are able to solve the congruence.

For example, in order to solve the congruence in two variables

$$f(x, y) \equiv 0 \ (\mathrm{mod}\, m)$$

where $f(x, y)$ is a polynomial in variables x, y, it is sufficient to find which of the m^2 systems x, y with x and y ranging over the set of integers $0, 1, 2, \ldots, m-1$, satisfy the congruence. (In fact, this follows easily from the remark that if $a \equiv c (\mathrm{mod}\, m)$ and $b \equiv d (\mathrm{mod}\, m)$, then $f(a, b) \equiv f(c, d) (\mathrm{mod}\, m)$).

A simple numerical example of what we have just said is provided by the congruence

$$x^4 + y^4 \equiv 1 (\mathrm{mod}\, 5).$$

As we can verify directly it has 8 solutions: $(x, y) = (0, 1), (0, 2), (0, 3), (0, 4), (1, 0), (2, 0), (3, 0), (4, 0)$. Thus all the solutions of this congruence are the integers x, y such that one of them is divisible by 5 and the other is not.

It is also easy to see that the congruence

$$x^3 + y^3 + z^3 \equiv 4 (\mathrm{mod}\, 9)$$

is insolvable. This is because the cube of an integer is congruent with respect to the modulus 9 to one of the numbers $0, 1, -1$, and so the sum of three cubes cannot be congruent to 4.

§ 3. Roots of polynomials and roots of congruences. If an equation $f(x, y) = 0$, where $f(x, y)$ is a polynomial with the integral coefficients, has a solution in integers x, y, then, of course, for every natural number m there exist integers x, y such that the number $f(x, y)$ is divisible by m, i.e. such that the congruence $f(x, y) \equiv 0 (\mathrm{mod}\, m)$ is solvable for each natural number m. Hence it follows that if there exists a modulus m such that the congruence $f(x, y) \equiv 0 (\mathrm{mod}\, m)$ is not solvable in integers, then the equation $f(x, y) = 0$ has no solutions in integers.

For example the proof that for natural numbers n the equation $x^2+1-3y^n = 0$ is insolvable in integers follows from the fact that the congruence $x^2+1-3y^n \equiv 0 (\mathrm{mod}\, 3)$ has no solutions, this being a simple consequence of the fact that the square of an integer differs from the multiple of 3 either by 0 or by 1, whence the left-hand side of the congruence divided by 3 yields the remainder 1 or 2 but not 0.

It is not true, however, that for any polynomial $f(x, y)$ with integral coefficients for which the equation $f(x, y) = 0$ has no solutions in integers x, y there exists a modulus m such that the congruence $f(x, y) \equiv 0 (\mathrm{mod}\, m)$ is insolvable.

For instance the equation

$$(2x-1)(3y-1) = 0$$

has no solutions in integers x, y; the congruence

$$(2x-1)(3y-1) \equiv 0 (\mathrm{mod}\, m),$$

however, is solvable for any natural number m. To see this we recall the well-known fact that a natural number m can be written in the form $m = 2^{k-1}(2x-1)$, where k, x are natural numbers. Number $2^{2k+1}+1$ is, as we know, divisible by $2+1 = 3$, and so there exists a natural number y such that $2^{2k+1}+1 = 3y$. Consequently $(2x-1)(3y-1) = 2^{k+2}m$, which proves that the congruence under consideration is solvable.

It is easy to prove a stronger and more general assertion. If a_1, a_2 are two natural numbers such that $(a_1, a_2) = 1$, b_1, b_2 are arbitrary integers, then the congruence

$$(a_1x+b_1)(a_2x+b_2) \equiv 0 (\mathrm{mod}\, m)$$

is solvable for every natural number m (cf. Skolem [1]).

It is easy to prove that the equation $2x^2-219y^2 = 1$ has no solution in integers x, y. This is because the cogruence $2x^2-219y^2 \equiv 1 (\mathrm{mod}\, 3)$ is insolvable. (In fact, if x is an integer, x^2 divided by 3 gives the remainder 0 or 1, and so, since $219 = 3\cdot 73$, number $2x^2-219y^2$ differs from a multiple of 3 by 0 or 2, and consequently it cannot be congruent to 1 with respect to modulus 3.)

It is a little more difficult to prove that the equation $2x^2-219y^2 = -1$ is insolvable in integers. T. Nagell [7] has deduced this from a more general theorem, the proof of which is difficult. However, the congruence $2x^2-219y^2 \equiv -1 (\mathrm{mod}\, m)$ is, as he says (ibid. p. 62), easily proved to be solvable for any natural number m.

We present here the proof of the fact that the equation $2x^2-219y^2 = -1$ is insolvable in integers x, y due to A. Schinzel.

Suppose, to the contrary, that the equation is solvable in integers x, y. Then, of course, neither of the numbers x, y can be zero, consequently, we may assume that x, y are positive integers. Moreover, we assume that the solution x, y is chosen in such a way that y is the least among the corresponding numbers in all the solutions of the equation in natural numbers. Let

$$x_1 = |293x-3066y|, \qquad y_1 = -28x+293y.$$

As is easy to verify, we have $2x_1^2-219y_1^2 = 2x^2-219y^2$. Consequently, the numbers x_1, y_1 satisfy the equation. We cannot have $x_1 = 0$, and so x_1 is a natural number. We cannot have $y_1 \leqslant 0$ either, since if we had, we would have $x \geqslant \frac{293}{28} y$, whence $x^2 \geqslant \frac{85849}{784} y^2$, and so $2x^2-219y^2 \geqslant \frac{y^2}{392}$, whence $-1 \geqslant \frac{y^2}{392}$, which is impossible. Thus we see that x_1, y_1 are natural numbers. By assumption, $y \leqslant y_1$, so $-28x+$ $+293y \geqslant y$, whence $x \leqslant \frac{292}{28} y = \frac{73}{7} y$, therefore $x^2 \leqslant \frac{5329}{49} y^2$ and $2x^2-219y^2$ $\leqslant \frac{-73}{49} y^2 \leqslant -\frac{73}{49} < -1$, contrary to the assumption that x, y is a solution of the equation. We have thus proved that the equation has no solutions in integers x, y.

We now prove that the congruence

$$2x^2-219y^2 \equiv -1 (\mathrm{mod}\, m)$$

is solvable for any natural number m.

Let m be a natural number. We put $m = m_1m_2$, where $m_1 = 11^\alpha$ (α is an integer $\geqslant 0$) and $(m_2, 11) = 1$. Let $x_1 = 5\cdot 13^{\varphi(m_1)-1}$, $y_1 = 13^{\varphi(m_1)-1}$. Since $(13, m_1) = 1$, by the theorem of Euler (see Chapter VI, p. 243) $13^{\varphi(m_1)} \equiv 1 (\mathrm{mod}\, m_1)$. Consequently,

$$\begin{aligned} 13^2(2x_1^2-219y_1^2) = 2\cdot 25\cdot 13^{2\varphi(m_1)}-219\cdot 13^{2\varphi(m_1)} &\equiv 2\cdot 25-219 \\ &\equiv -13^2 (\mathrm{mod}\, m_1), \end{aligned}$$

whence, in virtue of the equality $(13, m_1) = 1$, we obtain $2x_1^2-219y_1^2$ $\equiv -1 (\mathrm{mod}\, m_1)$.

Now let $x_2 = 7\cdot 11^{\varphi(m_2)-1}$, $y = 11^{\varphi(m_2)-1}$. Since $(11, m_2) = 1$, we have $11^{\varphi(m_2)} \equiv 1 (\mathrm{mod}\, m_2)$, whence

$$\begin{aligned} 11^2(2x_2^2-219y_2^2) = 2\cdot 49\cdot 11^{2\varphi(m_2)}-219\cdot 11^{2\varphi(m_2)} &\equiv 2\cdot 49-219 \\ &\equiv -11^2 (\mathrm{mod}\, m_2) \end{aligned}$$

and so, by $(11, m_2) = 1$, we obtain $2x_2^2-219y_2^2 \equiv -1 \pmod{m_2}$. Now, since $(m_1, m_2) = 1$, in virtue of the Chinese remainder theorem (cf. Chapter I, § 12), there exist integers x, y such that

$$x \equiv x_1 \pmod{m_1}, \qquad x \equiv x_2 \pmod{m_2},$$

$$y \equiv y_1 \pmod{m_1}, \qquad y \equiv y_2 \pmod{m_2}.$$

Hence $2x^2-219y^2 \equiv 2x_1^2-219y_1^2 \equiv -1 \pmod{m_1}$ and $2x^2-219y^2 \equiv 2x_2^2-219y_2^2 \equiv -1 \pmod{m_2}$ and so, since $(m_1, m_2) = 1$ and $m = m_1 m_2$,

$$2x^2-219y^2 \equiv -1 \pmod{m},$$

which shows that the congruence is solvable for any natural number m.

We are going to solve another example of a congruence, this time a congruence whose left-hand side is not a polynomial. The congruence is

$$(*) \qquad 2^x \equiv x^2 \pmod{3}.$$

Since $2^2 \equiv 1 \pmod{3}$, we have $2^{x+2k} \equiv 2^x \pmod{3}$ for all non-negative integers x and $k = 0, 1, 2, \ldots$ Since $(x+3l)^2 \equiv x^2 \pmod{3}$ for any integers x, l, we see that if x is a solution of congruence $(*)$, then $x+6t$, $t = 0, 1, 2, \ldots$, is also a solution of $(*)$. Among the numbers $0, 1, 2, 3, 4, 5$ only 2 and 4 are solutions of congruence $(*)$. Thus all the solutions of the congruence are numbers $2+6t$ or $4+6t$, where $t = 0, 1, 2, \ldots$

Remark. A number which is congruent to a solution of congruence $(*)$ with respect to its modulus may not be a solution of $(*)$, e.g. number 5.

§ 4. Congruences of the first degree. Let

$$(10) \qquad ax \equiv b \pmod{m},$$

where m is a given modulus and a, b are given integers. As we have learned in § 2, congruence (10) is equivalent to the diophantine equation

$$(11) \qquad ax - my = b.$$

It follows from Theorem 15 of Chapter I that in order that equation (11) be solvable in integers x, y, it is necessary and sufficient that $(a, m) \mid b$. Consequently, this is also a necessary and sufficient condition for solvability of congruence (10).

Suppose now that this condition is satisfied. We are going to look for the method of finding both all the solutions of congruence (10) and their number. Let $d = (a, m)$. So the number b/d is an integer. Let x_0 be one of the solutions of congruence (10) and let x be an arbitrary solution of it. We have $ax_0 \equiv b \pmod{m}$ and, by (10), we see that $a(x-x_0) \equiv 0 \pmod{m}$. Consequently, $m \mid a(x-x_0)$, whence $\frac{m}{d} \Bigm| \frac{a}{d}(x-x_0)$. But

since, in virtue of $d = (a, m)$, the relation $\left(\frac{m}{d}, \frac{a}{d}\right) = 1$ holds, $\frac{m}{d}$ must divide $x-x_0$, whence $x = x_0 + \frac{m}{d}t$, where t is an integer.

Conversely, taking an arbitrary integer for t and an arbitrary root x_0 of congruence (10) and putting $x = x_0 + \frac{m}{d}t$, we obtain a root of congruence (10), since $ax = ax_0 + \frac{a}{d}tm \equiv ax_0 \equiv b \pmod{m}$.

Now, let t take the values $0, 1, 2, \ldots, d-1$, successively. We prove that no two among the numbers

$$(12) \qquad x_t = x_0 + \frac{m}{d}t$$

are congruent to one another with respect to the modulus m.

In fact, if $x_t \equiv x_u \pmod{m}$, then by (12) we would have $x_0 + \frac{m}{d} \equiv x_0 + \frac{m}{d}u \pmod{m}$ and consequently $\frac{m}{d}(t-u) = mz$, where z is an integer, whence $t-u = dz$, which is impossible whenever t, u are different numbers of the sequence $0, 1, 2, \ldots, d-1$.

Finally, we show that each root of congruence (10) is congruent with respect to the modulus m to one of the roots $x_0, x_1, \ldots, x_{d-1}$ (defined in (12)).

In fact, if x is a root of congruence (10), then for an integer t we have $x = x_0 + \frac{m}{d}t$. Let r be the remainder obtained by dividing t by d. (So r is one of the numbers $0, 1, 2, \ldots, d-1$.) We have $t = r + du$, where u is an integer. Hence $x = x_0 + \frac{m}{d}t = x_0 + \frac{m}{d}(r+du) = x_0 + \frac{m}{d}r + mu = x_r + mu$, whence $x \equiv x_r \pmod{m}$, as we have to prove.

Putting together the results just proved we obtain

THEOREM 2. *A congruence of the first degree $ax \equiv b \pmod{m}$ is solvable if and only if b is divisible by the greatest common divisor d of the coefficient of x and the modulus m. If this condition is satisfied, then the congruence has precisely d roots non-congruent with respect to the modulus m.*

In particular, if a and m are relatively prime numbers, then $d = 1$. Hence the following

COROLLARY. *If the coefficient of x is relatively prime to the modulus m, then the congruence of the first degree $ax \equiv b \pmod{m}$ has precisely one root.*

If a congruence $ax \equiv b(\mathrm{mod}\, m)$ is solvable and if $(a, m) = d > 1$, then another congruence is obtained from it, namely

$$\frac{a}{d}x \equiv \frac{b}{d}\left(\mathrm{mod}\,\frac{m}{d}\right), \quad \text{where} \quad \left(\frac{a}{d}, \frac{m}{d}\right) = 1.$$

Therefore, while solving a congruence of the first degree (in case the congruence is solvable), we may always assume that the coefficient at the unknown and the modulus are relatively prime.

C. Sardi [1] has given the following method for solving such congruences. Let $ax \equiv b(\mathrm{mod}\, m)$, where $a > 1$ and $(a, m) = 1$. Further, let $a_1 = m - a\left[\frac{m}{a}\right]$; clearly $0 < a_1 < a$, since m is divisible by a. Hence multiplying the congruence by $-\left[\frac{m}{a}\right]$ throughout we obtain $a_1 x \equiv -b\left[\frac{m}{a}\right](\mathrm{mod}\, m)$, i.e. a congruence in which $a_1 < a$. Proceeding in this way, we ultimately obtain $a_n = 1$, i.e. the congruence $x \equiv c(\mathrm{mod}\, m)$ whose unique solution is clearly $x = c$.

§ 5. Wilson's theorem and the simple theorem of Fermat. Let p be an odd prime and D an integer not divisible by p.

Any two numbers m, n of the sequence

(13) $$1,\ 2,\ 3,\ \ldots,\ p-1$$

are called *corresponding* if and only if the congruence

(14) $$mn \equiv D(\mathrm{mod}\, p)$$

holds. It follows immediately from the definition that, if m is a number corresponding to n, then n is a number corresponding to m.

We now prove that for each number of sequence (13) there is precisely one number corresponding to it. Let m be a number of sequence (13). In order that a number x of sequence (13) may be a corresponding number to m it is necessary and sufficient that the congruence $mx \equiv D$ $(\mathrm{mod}\, p)$ should hold. In virtue of the relation $mx \equiv D(\mathrm{mod}\, p)$ (where m is a number of sequence (13)) and in accordance with the corollary to theorem 2, the last congruence has precisely one root. Therefore we see that in the sequence $0, 1, 2, 3, \ldots, p-1$ there is one and only one number which satisfies the congruence. It cannot be the number 0, since D is not divisible by p. From this we infer that in sequence (13) there is precisely one number which satisfies the congruence, as we were to show.

It may happen that corresponding numbers are equal. Then congruence (14) assumes the form $m^2 \equiv D(\mathrm{mod}\, p)$. This is possible only if there exists a square which differs from D by a multiple of p; the number D is then called a *quadratic residue* for the modulus p. In the converse case, that is, if none of the squares is congruent to D with respect to the modulus p, we say that D is a *quadratic non-residue* for p. In other words, a number D not divisible by p is called a quadratic residue or a quadratic non-residue depending on whether the congruence $x^2 \equiv D(\mathrm{mod}\, p)$ is solvable or insolvable.

First we consider the case where D is a quadratic non-residue for a prime modulus p. Then each pair of corresponding numbers m, n consists of two different numbers of sequence (13). Therefore all the numbers of sequence (13) can be divided into pairs of corresponding numbers, the number of the pairs being equal to $(p-1)/2$. Writing down the congruence of the form (14) for each of the pairs we obtain the sequence of $(p-1)/2$ congruences

$$\begin{aligned} m_1 n_1 &\equiv D(\mathrm{mod}\, p), \\ m_2 n_2 &\equiv D(\mathrm{mod}\, p), \\ &\ldots\ldots\ldots\ldots\ldots \\ m_{\frac{p-1}{2}} n_{\frac{p-1}{2}} &\equiv D(\mathrm{mod}\, p). \end{aligned}$$

Then multiplying these congruences and noting that the product $m_1 n_1 m_2 n_2 \ldots m_{\frac{p-1}{2}} n_{\frac{p-1}{2}}$ differs from the product of the numbers of sequence (13) at most in the order of the factors, we obtain the congruence

(15) $$(p-1)! \equiv D^{\frac{1}{2}(p-1)}(\mathrm{mod}\, p).$$

Now we consider the case where D is a quadratic residue for the modulus p. Then the congruence

(16) $$x^2 \equiv D(\mathrm{mod}\, p)$$

is solvable. Let us calculate the number of the numbers of (13) which satisfy congruence (16). Since we have assumed that congruence (16) is solvable, in the sequence $0, 1, 2, \ldots, p-1$ there is at least one number k which is a solution of (16). It cannot be $k = 0$, since, according to our general assumption, D is not divisible by p. Consequently the number k is one of the numbers of sequence (13) and therefore $p-k$ is also a number of this sequence. It is different from k, since, as we have assumed, p is an odd number. For the number $l = p-k$ we have $l^2 \equiv k^2(\mathrm{mod}\, p)$, whence the congruence $k^2 \equiv D(\mathrm{mod}\, p)$ implies $l^2 \equiv D(\mathrm{mod}\, p)$.

Thus in the case where D is a quadratic residue for p we see that in sequence (13) there are at least two different numbers which satisfy congruence (16). We prove that there are precisely two such numbers.

Suppose that a number x of sequence (13) satisfies congruence (16). Since $k^2 \equiv D(\operatorname{mod} p)$, we have $x^2 \equiv k^2(\operatorname{mod} p)$, which proves that $p \mid x^2-k^2 = (x-k)(x+k)$. But, since p is a prime number, the last relation implies that either $p \mid x-k$ or $p \mid x+k$. If $p \mid x-k$, then, since x and k belong to sequence (13), we see that $x = k$. If $p \mid x+k$, then, since $0 < x < p$ and $0 < k < p$ and so $0 < x+k < 2p$, we see that $x+k = p$, whence $x = p-k = l$.

We have thus proved that k and l are the only numbers of sequence (13) which satisfy congruence (16). Hence, *if a number D which is not divisible by an odd prime p is a quadratic residue for the modulus p, then congruence* (16) *has precisely two roots.*

Now we remove the numbers k and l from sequence (13). None of the remaining $p-3$ numbers satisfies congruence (16), so they can be divided into $(p-3)/2$ pairs of corresponding numbers. We thus obtain $(p-3)/2$ congruences

$$m_1 n_1 \equiv D(\operatorname{mod} p),$$
$$m_2 n_2 \equiv D(\operatorname{mod} p),$$
$$\cdots\cdots\cdots\cdots\cdots$$
$$m_{\frac{p-3}{2}} n_{\frac{p-3}{2}} \equiv D(\operatorname{mod} p).$$

Since $kl = k(p-k) \equiv -k^2 \equiv -D(\operatorname{mod} p)$, we may add the congruence

$$kl \equiv -D(\operatorname{mod} p)$$

to the congruences above and multiply all the congruences. Then the product of the left sides of the congruences is equal to $(p-1)!$. Thus the congruence

$$(p-1)! \equiv -D^{\frac{1}{2}(p-1)}(\operatorname{mod} p) \tag{17}$$

is obtained.

We see that either (15) or (17) holds depending on whether D is a quadratic residue for the modulus p or not.

Putting together (15) and (17), we write

$$(p-1)! \equiv \pm D^{\frac{1}{2}(p-1)}(\operatorname{mod} p), \tag{18}$$

where on the right-hand side the sign $-$ or $+$ is taken, depending on whether D is a quadratic residue for p or not.

In particular, for $D = 1$ we see that, since number 1 is a quadratic residue for every p,

$$(p-1)! \equiv -1(\operatorname{mod} p). \tag{19}$$

The proof of (19) makes use of the assumption that p is an odd prime number and it fails for $p = 2$, but we can immediately verify that the result is still true since $(2-1)! = 1 \equiv -1(\operatorname{mod} 2)$. Thus we have proved the following

THEOREM 3 (Wilson). *If p is a prime number, then the number $(p-1)!+1$ is divisible by p.*

The converse is also true. In fact, if p is a natural number >1 and if $(p-1)!+1$ is divisible by p, then p is a prime. To see this we suppose to the contrary that p is not a prime. Then there is a divisor q of p such that $1 < q < p$. The number $(p-1)!+1$, being divisible by p, must also be divisible by q, but since $q < p$, $q \leqslant p-1$, so $q \mid (p-1)!$, whence $q \mid 1$, which is a contradiction. Hence

THEOREM 3^a. *A necessary and sufficient condition for a natural number $n > 1$ to be a prime is that the number $(n-1)!+1$ is divisible by n.*

This shows that, from a purely theoretical point of view, we are able to decide for a given natural number $n > 1$ whether it is a prime or not using only one division.

It follows from theorem 3 that for a prime p the number $w_p = \{(p-1)!+1\}/p$ is a natural number. C. E. Fröberg [2] has calculated the remainders obtained by dividing w_p by p for the prime numbers $p < 50000$. The primes for which $p^2 \mid (p-1)!+1$ are called *Wilson primes*. It follows from the tables given by Fröberg that among the primes $p < 50000$ there are only three Wilson primes, namely 5, 13 and 563.

From theorem 3^a and the remark that for $n > 2$ the relations $(n-1)! = (n-2)!(n-1) \equiv -(n-2)!(\operatorname{mod} n)$ hold we deduce

THEOREM 3^b (Leibniz). *In order that a natural number $n > 1$ be prime it is necessary and sufficient that* $(n-2)! \equiv 1(\operatorname{mod} n)$. (By 0! we understand of course number 1.)

It can be proved that *a natural number $p > 1$ is a prime if and only if there exists a natural number $n < p$ such that* $(n-1)!(p-n)! \equiv (-1)^n (\operatorname{mod} p)$ (cf. Dickson [8], vol. I, p. 64).

It is clear that if n is a natural number such that $n \mid (n-1)!$, then n is a composite number. It is easy to prove that if n is a composite number $\neq 4$, then $n \mid (n-1)!$

In fact, if n is a composite number, then there exist natural numbers a and b such that $n = ab$, $1 < a < n$, $1 < b < n$. If $a \neq b$, then a and b are different factors of the product $(n-1)!$ and, consequently, $n = ab$ divides $(n-1)!$. If $a = b$, then $n = a^2$ and, since n is a composite number $\neq 4$, $a > 2$. Hence it follows that $n = a^2 \neq 2a$ and therefore a and $2a$ are different factors of the product $(n-1)!$. Thus $(n-1)!$ is divisible by $2a^2$, whence, *a fortiori*, it is divisible by $a^2 = n$. For $n = 4$, however, we have $(n-1)! = 3! = 6 \equiv 2(\operatorname{mod} 4)$.

It follows immediately from theorem 3 that *there exist infinitely many natural numbers n for which $n!+1$ is a composite number*. Such are for instance the numbers $n = p-1$, where p is a prime >3. (For, $(p-1)! > 2(p-1) = p+(p-2) > p$.)

A. Schinzel [16] has proved that for every rational $c \neq 0$ there exist infinitely many composite integers of the form $cn!+1$.

We do not know, however, whether there exist infinitely many prime numbers of the form $n!+1$. For $n \leqslant 26$ the only prime numbers of this form are the numbers $1!+1 = 2$, $2!+1 = 3$, $11!+1 = 39916801$ (1). We do not know whether the number $27!+1$ is prime or not.

It is not known whether there exist infinitely many natural numbers k such that the number $P_k = p_1p_2\ldots p_k+1$ is a prime. Neither is it known whether there exist infinitely many k's for which P_k is composite. The following five numbers P_k are prime: $P_1 = 3$, $P_2 = 7$, $P_3 = 31$, $P_4 = 211$, $P_5 = 2311$, but $P_6 = 59\cdot 509$, $P_7 = 19\cdot 97\cdot 277$, $P_8 = 347\cdot 27953$, $P_9 = 317\cdot 703763$, $P_{10} = 331\cdot 571\cdot 34231$ are not prime.

It follows from theorem 3^b that *there exist infinitely many natural numbers n such that the number $n!-1$ is composite*. Such are, for instance, all the numbers $n = p-2$, where p is a prime >3. We do not know whether there exist infinitely many primes of this form. If $n < 23$, numbers $n!-1$ are prime only for $n = 3, 4, 6, 7, 12, 14, 20$. We do not know whether numbers $23!-1$ and $24!-1$ are prime or not. Number $25!-1$ is composite; it is divisible by 149.

Formulae (15) and (17) together with theorem 3 give

THEOREM 4. *If an integer D is not divisible by an odd prime p, then*

$$D^{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod{p}, \tag{20}$$

where the sign $+$ or $-$ is taken depending on whether D is a quadratic residue for the modulus p or not.

Hence, raising each side of (20) to the second power, we obtain

THEOREM 5. *If an integer D is not divisible by a prime p, then*

$$D^{p-1} \equiv 1 \pmod{p}. \tag{21}$$

This is the *simple theorem of Fermat*, given by him without a proof in 1640. The first proof was given by J. Ivory in 1806.

The proof of formula (20) fails if $p = 2$, but we can immediately verify that (21) still holds; for D, being non-divisible by $p = 2$, must be odd, and so $D \equiv 1 \pmod{2}$.

In particular, it follows from theorem 5 that, if p is an odd prime, then the number $2^{p-1}-1$ is divisible by p. Investigations have been made in order to find the numbers p for which $2^{p-1}-1$ is divisible by p^2. For $p < 10^6$ only two such numbers have been found, namely $p = 1093$, $p = 3511$. (Hausner and Sachs [1], cf. Riesel [2]).

A simple application of theorem 5 gives a solution of any congruence of the form $ax \equiv b \pmod{p}$ provided p is a prime and a is not divisible by p. In fact, $x = a^{p-2}b$ is a solution because, by theorem 5, $a^{p-1} \equiv 1 \pmod{p}$, whence $ax = a^{p-1}b \equiv b \pmod{p}$.

An immediate consequence of theorem 5 is

THEOREM 5^a. *If p is a prime number, then for every integer a we have $p \mid a^p - a$.*

Conversely, theorem 5 can easily be obtained from theorem 5^a. In fact, if a is an integer not divisible by a prime p, then the relation $p \mid a^p - a = a(a^{p-1}-1)$ implies $p \mid a^{p-1}-1$, that is $a^{p-1} \equiv 1 \pmod{p}$.

The theorems of Wilson and Fermat can be formulated together in a single theorem (cf. Moser [4]):

THEOREM 6. *If p is a prime and a an integer, then*

$$p \mid a^p + (p-1)!\,a. \tag{22}$$

In fact, if theorem 3 holds, then $(p-1)! \equiv -1 \pmod{p}$, consequently, $a^p + (p-1)!\,a \equiv a^p - a \pmod{p}$, which, in virtue of theorem 5^a, gives $a^p - a \equiv 0 \pmod{p}$, whence formula (22) follows.

On the other hand, if theorem 6 holds, then for $a = 1$ formula (22) gives theorem 3. Therefore for every integer a the congruence $a^p + (p-1)!\,a \equiv a^p - a \pmod{p}$ holds, whence it follows that (22) implies $a^p - a \equiv 0 \pmod{p}$. So theorem 5^a is valid, and this, as we know, is equivalent to the theorem of Fermat.

It is also easy to prove that the theorems of Fermat and of Wilson taken together are equivalent to the following

THEOREM 6^a. *If p is a prime and a is an integer, then*

$$p \mid (p-1)!\,a^p + a.$$

In this connection we wish to add that T. Szele [1] has proved the following generalization of theorem 5^a:

For every natural number m and every integer a the number $\sum_{d\mid m} \mu(d)\, a^{m/d}$ is divisible by m.

Hence, in particular, for each integer a and two different primes p and q we have $pq \mid a^{pq} - a^p - a^q + a$.

We derive another simple corollary from theorem 5:

THEOREM 7. *There exist infinitely many prime numbers of the form $4k+1$ (where k is a natural number).*

(1) An outline of the proof is to be found in a book of A. Ferrier, [1], p. 30.

Proof. Let n be an arbitrary natural number >1 and let

$$N = (n!)^2+1. \tag{23}$$

Number N is, of course, odd and >1. Let p denote the least prime divisor of the number N. By (23), $p>n$. Being odd, n is of the form $4k+1$ or $4k+3$. By (23) again, we have

$$(n!)^2 \equiv -1 (\mathrm{mod}\, p),$$

whence, raising each side of the congruence to the $(p-1)/2$-th power, we obtain $(n!)^{p-1} \equiv (-1)^{(p-1)/2} (\mathrm{mod}\, p)$. But $n!$ is not divisible by p, and so, in view of theorem 5, we have $(n!)^{p-1} \equiv 1 (\mathrm{mod}\, p)$, whence

$$(-1)^{\frac{1}{2}(p-1)} \equiv 1 (\mathrm{mod}\, p). \tag{24}$$

We cannot have $p = 4k+3$ because, if we could, formula (24) would give

$$(-1)^{\frac{1}{2}(p-1)} = (-1)^{2k+1} = -1 \equiv 1 (\mathrm{mod}\, p),$$

whence $p \mid 2$, which is impossible. Therefore p must be of the form $4k+1$.

We have thus proved that for every natural number $n>1$ there exists a prime $p>n$ of the form $4k+1$. (More precisely, we have proved that such is every prime divisor of number (23).) Theorem 7 is thus proved.

As far as the numbers $4k+3$ are concerned, it is very easy indeed to prove that there are infinitely many primes among them. In fact, let n denote an arbitrary natural number >3 and let

$$N_1 = n!-1. \tag{25}$$

N_1 is an odd number >1, and so each of its prime factors is odd. If each of them is of the form $4k+1$, then number N_1, as the product of (not necessarily different) numbers of the form $4k+1$, is itself of the form $4t+1$. But this, in view of (25) and the fact that $n>3$, is impossible.

Thus we have proved that for every natural number $n>3$ there exists a prime number $p>n$ of the form $4k+3$. Hence

THEOREM 7$^{\mathrm{a}}$. *There are infinitely many primes of the form $4k+3$ (where k is a natural number).*

For a given real number $x>1$ denote by $\pi_1(x)$ the number of primes $\leqslant x$ of the form $4k+1$; by $\pi_3(x)$ denote the number of primes $\leqslant x$ of the form $4k+3$. Let $\varDelta(x) = \pi_3(x)-\pi_1(x)$. In 1914 J. E. Littlewood proved that there exist infinitely many natural numbers n such that $\varDelta(n)>0$ and that there are infinitely many n for which $\varDelta(n)<0$. It seems curious that until recently none of the numbers n for which $\varDelta(n)<0$ were known. With the aid of the electronic computer EDSAC, J. Leech [1] has calculated the numbers $\varDelta(n)$ with $n \leqslant 3000000$. Thus he has shown that the least natural number n for which $\varDelta(n)<0$ is $n = 26861$. For this n we have $\pi_1(n) = 1473$, $\pi_3(n) = 1472$, and so $\varDelta(n) = -1$. It has been found that $\varDelta(623681) = -8$, $\varDelta(627859) = \varDelta(627860) = \ldots = \varDelta(627900) = 0$, $\varDelta(2951071) = 256$ (cf. Shanks [2]).

It follows from theorem 5 that if p is a prime number, then $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$, where $a = 1, 2, \ldots, p-1$. Adding up these $p-1$ congruences, we obtain

$$1^{p-1}+2^{p-1}+\ldots+(p-1)^{p-1} \equiv p-1 (\mathrm{mod}\, p).$$

Hence

$$p \mid 1^{p-1}+2^{p\;\;1}+\ldots+(p-1)^{p-1}+1$$

for any prime p. G. Giuga [1] has conjectured that this relation does not hold for composite numbers and proved this for $p \leqslant 10^{1000}$.

The theorem, which follows, is a corollary to theorem 3.

THEOREM 8. *If p is a prime of the form $4k+1$ (where k is a natural number), then*

$$p \left[\,\middle|\left(\frac{p-1}{2}\right)!\right]^2+1. \tag{26}$$

Proof. Since $\frac{1}{2}(p-1) = 2k$, we have the equality $1\cdot 2\cdot 3\ldots\frac{1}{2}(p-1) = (-1)(-2)\ldots\left(-\frac{p-1}{2}\right) \equiv (p-1)(p-2)\ldots\frac{p+1}{2} (\mathrm{mod}\, p)$; hence we obtain $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv 1\cdot 2\ldots\frac{p-1}{2}\cdot\frac{p+1}{2}\ldots(p-1) \equiv (p-1)! \equiv -1 (\mathrm{mod}\, p)$, and this gives formula (26).

On the basis of theorem 8 we prove the following

THEOREM 9 (Fermat). *Every prime number p of the form $4k+1$ is a sum of two squares.*

Proof. Let p be a prime number of the form $4k+1$ and $a = \left(\frac{p-1}{2}\right)!$. In virtue of theorem 8, we have $p \mid a^2+1$, a being of course relatively prime to p. In view of the theorem of Thue (cf. Chapter I, § 13) with p in place of m, there exist two natural numbers x, y, each $\leqslant \sqrt{p}$, such that for a suitable choice of the sign + or − the number $ax \pm y$ is divisible by p. Hence it follows that the number $a^2x^2-y^2 = (ax-y)(ax+y)$ is divisible by p.

$a^2x^2+x^2 = (a^2+1)x^2$ is divisible by p (since $p \mid a^2+1$). Consequently the number $x^2+y^2 = a^2x^2+x^2-(a^2x^2-y^2)$ is divisible by p. But, since x, y are natural numbers $\leqslant \sqrt{p}$, they are $<\sqrt{p}$, because p, being a prime, is not a square of a natural number. Thus x^2+y^2 is a natural number >1 and $<2p$ and, moreover, it is divisible by p, so it must be equal to p, i. e. $p=x^2+y^2$. This proves that p is the sum of two squares of natural numbers.

A number which is not of the form $4k+3$ (not necessarily prime) can not be the sum of two squares. The argument is that, since the square of an integer is congruent to 0 or $1 (\bmod 4)$, the sum of any two squares must be congruent to 0, 1 or 2 but never to 3. This shows that among prime numbers only the number $2=1^2+1^2$ and the primes of the form $4k+1$ are the sums of two squares.

According to H. Davenport [1] (pp. 120-122) four constructions for the decomposition of a prime of the form $4k+1$ are known. They are due to Legendre (1808), Gauss (1825), Serret (1848) and Jacobsthal (1906), respectively. The most elementary of them all (to formulate though not to prove) is the following construction, due to Gauss. If $p=4k+1$ is a prime number, we take integers x, y such that

$$x \equiv (2k)!/2(k!)^2 (\bmod p) \quad \text{and} \quad y \equiv (2k)!x (\bmod p),$$

with $|x|<\frac{1}{2}p$, $|y|<\frac{1}{2}p$. Then $p=x^2+y^2$. A proof has been given by Cauchy and another by Jacobsthal, but neither of them is simple. The calculation which leads to the numbers x, y is not easy. To illustrate this, take $p=29$. Then $x \equiv 14!/2\cdot(7!)^2 = 1716 \equiv 5 (\bmod 29)$, $y \equiv 14!x \equiv$ $\equiv 14!\cdot 5 \equiv 2 (\bmod 29)$, whence $x=5$, $y=2$.

We do not know whether there exist infinitely many primes p such that $p=x^2+(x+1)^2$, where x is a natural number. A positive answer follows from conjecture H (cf. Chapter III, § 8). For example, we have $5=1^2+2^2$, $13=2^2+3^2$, $41=4^2+5^2$, $61=5^2+6^2$, $113=7^2+8^2$, 181 $=9^2+10^2$, $313=12^2+13^2$, $421=14^2+15^2$, $613=17^2+18^2$, 761 $=19^2+20^2$.

As can easily be observed, the conjecture that there exist infinitely many primes, each of them being the sum of two consecutive squares, is equivalent to the conjecture that there exist infinitely many primes p for which $2p=a^2+1$, where a is a natural number. To see this we suppose $p=x^2+(x+1)^2$, where x is a natural number, then $2p=(2x+1)^2+1$. Conversely, if $2p=a^2+1$, where a is a natural number, then, for $p>2$, the number a must be odd >1, and so $a=2x+1$, where x is a natural number. Hence $2p=(2x+1)^2+1$, that is, $p=x^2+(x+1)^2$.

It follows from conjecture H that there exist infinitely many primes p such that $p=a^2+b^2$, where a and b are prime numbers. For example, $13=2^2+3^2$, $29=2^2+5^2$, $53=2^2+7^2$, $173=2^2+13^2$, 293 $=2^2+17^2$, $1373=2^2+37^2$.

It also follows from conjecture H that there exist infinitely many primes, each of them being the sum of three consecutive squares of natural numbers. For example, $29=2^2+3^2+4^2$, $149=6^2+7^2+8^2$, $509=12^2+$ $+13^2+14^2$, $677=14^2+15^2+16^2$, $1877=24^2+25^2+26^2$. In this connection, we note that conjecture H implies that there exist infinitely many prime numbers, each of them being the sum of three different squares of prime numbers. For example, $83=3^2+5^2+7^2$, $179=3^2+$ 7^2+11^2, $419=3^2+11^2+17^2$, $563=3^2+5^2+23^2$. (It is easy to prove that one of the squares must always be equal to 3^2.)

Another corollary which can be derived from conjecture H is that for every natural number n there exist infinitely many natural numbers x such that x^2+n^2 are primes.

It can be proved that for every natural number n there exists a prime p such that $p=a^2+b^2$ with $a>n$ and $b>n$ (cf. Chapter III, § 7, and the papers quoted there).

If a prime number is the sum of two or four squares of different prime numbers, then, as can easily be verified, one of the primes must be equal to 2. If a prime is the sum of three squares of different primes, then one of the primes must be equal to 3. However, it follows from conjecture H that for every natural number n there exists a prime $q>p_{n+3}$ such that the number $p=p_n^2+p_{n+1}^2+p_{n+2}^2+p_{n+3}^2+q^2$ is a prime. For example, we have $373=3^2+5^2+7^2+11^2+13^2$, $653=5^2+7^2+11^2+$ $+13^2+17^2$, $1997=7^2+11^2+13^2+17^2+37^2$.

We now prove that the decomposition of a prime into the sum of two squares of natural numbers, if it exists, is unique apart from the order of the summands. We prove a slightly more general

THEOREM 10. *If a and b are natural numbers, then the representation of a prime p in the form $p=ax^2+by^2$, where x, y are natural numbers, if it exists, is unique, apart from the obvious possibility of interchanging x and y in the case of $a=b=1$.*

Proof. Suppose that for a prime p

$$p=ax^2+by^2=ax_1^2+by_1^2, \tag{27}$$

where x, y, x_1, y_1 are natural numbers. Clearly, $(x, y)=(x_1, y_1)=1$. From (27) we have

$$p^2=(axx_1+byy_1)^2+ab(xy_1-yx_1)^2=(axx_1-byy_1)^2+ab(xy_1+yx_1)^2.$$

But

$$(axx_1+byy_1)(xy_1+yx_1)=(ax^2+by^2)x_1y_1+(ax_1^2+by_1^2)xy=p(x_1y_1+xy).$$

Consequently at least one of the factors on the left-hand side of this equality must be divisible by p. If $p \mid axx_1+byy_1$, then the first of the above formulae for p^2 gives $xy_1-yx_1=0$. Therefore $x/y=x_1/y_1$, which, in view of $(x, y)=(x_1, y_1)=1$, proves that $x=x_1$, $y=y_1$. If $p \mid xy_1+yx_1$, then the second of the formulae above for p^2 shows that $p^2 \geqslant abp^2$, which is possible only in the case of $a=b=1$. But then $xx_1-yy_1=0$, and so $x/y=y_1/x_1$, which, in virtue of $(x, y)=(x_1, y_1)=1$, shows that

$x = y_1, y = x_1$. Then the decompositions $p = x^2+y^2$ and $p = x_1^2+y_1^2$ differ only in the order of the summands. Theorem 10 is thus proved.

An immediate corollary to theorem 10 is that if a natural number admits two (or more) different representations in the form ax^2+by^2, where x, y are natural numbers, then it must be composite. The converse theorem is not true. Namely number 14 has a unique representation in the form $14 = 2x^2+3y^2$, where x, y are natural numbers ($x = 1$, $y = 2$) and the number 15, though composite, has no representation in the form $15 = 2x^2+3y^2$, where x, y are integers. Number 18 has a unique representation in the form $18 = x^2+y^2$, where x, y are natural numbers (namely $x = y = 3$). Each of the numbers 25 and 45 has a unique representation (apart from the order of the summands) in the form x^2+y^2, where x, y are natural numbers, namely $25 = 3^2+4^2$, $45 = 3^2+6^2$. However, the following theorem holds:

THEOREM 11. *A natural number of the form $4k+1 > 1$ is a prime if and only if it admits a unique representation (apart from the order of the summands) as the sum of two squares of integers $\geqslant 0$ and in this unique representation the squares are relatively prime.*

Proof. Suppose that the number $p = 4k+1$ is a prime. Then, by theorems 9 and 10, number p admits a unique representation (apart from the order of the summands) of the form $p = x^2+y^2$, where x, y are natural numbers. Obviously, there are no representations of number p other than the sum of two squares of integers because, if there were, one of the squares would be equal to zero, and so p would be the square of a natural number, which is impossible. It is obvious that in the representation $p = x^2+y^2$ the numbers x, y must be relatively prime; for otherwise, if $(x, y) = d > 1$, we would have $d^2 \mid p$, which is impossible. We have thus proved that the conditions of the theorem are necessary. In order to show that they are also sufficient, we prove the following

LEMMA. *If each of two given natural numbers of the form $4k+1$ with $k > 0$ is the sum of two squares of integers, then their product does not satisfy the conditions of theorem* 11.

Proof of the lemma. Suppose that $m = a^2+b^2$, $n = c^2+d^2$, where a, b, c, d are integers. We have

$$mn = (ac+bd)^2+(ad-bc)^2 = (ac-bd)^2+(ad+bc)^2. \tag{28}$$

Suppose that the two decompositions, just obtained, of number mn differ only in the order of factors. Then either $ac+bd = ad+bc$ or $ac+bd = |ac-bd|$. In the first case we have $a(c-d) = b(c-d)$. But $c \neq d$, since otherwise, i.e. when $c = d$, we have $n = 2c^2$, which contradicts the fact that n is an odd number. We then have $a = b$. But this is also impossible, since m is an odd number. In the other case, i.e. when $ac+bd = |ac-bd|$, we have either $ac+bd = ac-bd$ or $ac+bd = bd-ac$. Then in the first of these cases $bd = 0$, and so $b = 0$ or $d = 0$. If $b = 0$, then $m = a^2$, where $a > 1$ and $mn = (ac)^2+(ad)^2$, where ac and bd have a common divisor > 1, consequently number mn does not satisfy the conditions of the theorem. In the second case we have $ac = 0$, and so $a = 0$ or $c = 0$, whence, in analogy to the previous case, we infer that the number mn does not satisfy the conditions of theorem 11. Thus it only remains to consider the case where decompositions (28) differ not only in the order of the factors. In this case, however, number mn clearly does not satisfy the conditions of theorem 11. The lemma is thus proved.

We now return to the proof of the sufficiency of the conditions of theorem 11. Suppose, to the contrary, that a number $s = 4k+1 > 1$ satisfies the conditions of theorem 11 and is not a prime. Let p be an arbitrary prime factor of the number s. Clearly p is an odd number. If p were equal to $4t+3$, then, since by assumption $s = a^2+b^2$, where $(a, b) = 1$, we would have $a^2 \equiv -b^2 (\mathrm{mod}\, p)$, whence, raising each side of the last congruence to the $\frac{1}{2}(p-1) = (2k+1)$-th power, by theorem 5, we would obtain $1 \equiv -1 (\mathrm{mod}\, p)$, i.e. $2 \mid p$, which is impossible. Thus we see that p must be of the form $4t+1$ and therefore, by theorem 9, p is the sum of two squares of natural numbers. Hence each prime factor of the number s is the sum of two squares of integers, whence, by (28), each divisor of s has the same property. If the number s could be composite then it would be a product of natural numbers $n, m > 1$, each of them being the sum of two squares of integers and of the form $4t+1$ (since it is the product of prime factors of this form). Therefore, by the lemma, the number $s = mn$ does not satisfy the conditions of theorem 11, contrary to the assumption. Theorem 11 is thus proved.

Here is an application of theorem 11. If one has to decide whether a given natural number n of the form $4k+1$ is a prime or not one forms the sequence of numbers

$$n-0^2, \quad n-1^2, \quad \ldots, \quad n-([\sqrt{n}])^2$$

and checks which of these numbers are squares.

In this way, applying theorem 11, T. Kulikowski, with the aid of the electronic computer EMC of the Warsaw Polytechnic, has found that the number $2^{39}-7$ is a prime because it admits precisely one representation as the sum of two squares of integers,

$$2^{39}-7 = 64045^2+738684^2$$

and the integers are relatively prime.

It is known that the numbers 2^n-7, $n = 4, 5, \ldots, 38$, are composite. The problem whether there exist prime numbers of the form 2^n-7 was formulated by P. Erdös in 1956. We see that the answer is positive.

EXERCISES. **1.** Prove that natural numbers $n > 1$ and $n+2$ form a pair of twin primes if and only if the congruence

$$4\big((n-1)!+1\big)+n \equiv 0\,(\mathrm{mod}\, n(n+2)) \tag{29}$$

holds (Clement [1]).

Proof. Suppose that the numbers n and $n+2$ are both prime numbers. In view of theorem 3, we have $(n-1)!+1 \equiv 0(\mathrm{mod}\, n)$ and $(n+1)!+1 \equiv 0(\mathrm{mod}\, n+2)$. But, since $n \equiv -2(\mathrm{mod}\, n+2)$ and $n+1 \equiv -1(\mathrm{mod}\, n+2)$, we see that $(n+1)! \equiv (n-1)!2(\mathrm{mod}\, n+2)$. From this we infer that the left-hand side of (29) is divisible by n and that $4\big((n-1)!+1\big)+n \equiv (n+1)!2+2+n+2 = 2\big((n+1)!+1\big)+n+2 \equiv 0(\mathrm{mod}\, n+2)$. Therefore the left-hand side of (29) is also divisible by $n+2$. But since the numbers n, $n+2$ are different primes, then the left-hand side of (29) is divisible by the product $n(n+2)$; hence we see that formula (29) holds.

Now, suppose that for a natural number $n > 1$ congruence (29) is valid. If n were even, i.e. if $n = 2k$, where k is a natural number, then we would have $n-1 \geqslant k$, whence $k|(n-1)!$ and $2k|(n-1)!4$. Consequently $(n-1)!4 \equiv 0(\mathrm{mod}\, n)$, which, in view of (29), would imply $4 \equiv 0(\mathrm{mod}\, n)$ and this would give $2k|4$, whence $k|2$ and so $k = 1$ or $k = 2$ and consequently $n = 2$ or $n = 4$. But it is easy to verify that congruence (29) is valid neither for $n = 2$ nor for $n = 4$. Thus we see that congruence (29) implies the congruence $(n-1)!+1 \equiv 0(\mathrm{mod}\, n)$, and this, by theorem 3^a, shows that n is a prime number. Finally, since, as we have shown above, for natural numbers n the congruence $4\big((n-1)!+1\big)+n \equiv 2\big((n+1)!+1\big)(\mathrm{mod}\, n+2)$ holds, we deduce from (29), using the fact that $n+2$ is odd, that the congruence $(n+1)!+1 \equiv 0(\mathrm{mod}\, n+2)$ is valid. Hence, applying again theorem 3^a, we conclude that $n+2$ is a prime. We have thus shown that n, $n+2$ is a pair of twin primes.

2. Prove that if $n = a^2+b^2 = c^2+d^2$, where a, b, c, d are natural numbers such that $a \geqslant b$, $c \geqslant d$, $a > c$, $(a, b) = (c, d) = 1$, then the number

$$\delta = \frac{ac+bd}{(ac+bd,\, ab+cd)} \tag{30}$$

is a divisor of number n such that $1 < \delta < n$.

Proof. If $n = a^2+b^2 = c^2+d^2$, then

$$\begin{cases} n^2 = (ac+bd)^2+(ad-bc)^2 = (ad+bc)^2+(ac-bd)^2, \\ (ac+bd)(ad+bc) = n(ab+cd). \end{cases} \tag{31}$$

Hence $n|(ac+bd)(ad+bc)$. If $n|ac+bd$, then by (31) we have $ad-bc = 0$, whence $a/b = c/d$, which, since $(a, b) = (c, d) = 1$, gives $a = c$, contrary to the assumption that $a > c$. If $n|ad+bc$, then, by (31), $ac-bd = 0$, whence $a/b = d/c$, which, by $(a, b) = (c, d) = 1$, gives $a = d$, contrary to the assumption that $a > c \geqslant d$. Numbers $n_1 = ac+bd$ and $n_2 = ad+bc$ are not divisible by n, which, in view of the relation $n|n_1n_2$ of exercise 2, § 6, Chapter I and formula (31) implies that the number δ is a divisor of the number n and $1 < \delta < n$.

3. Prove the following theorem of Liouville [1]. If p is a prime > 5, then the number $(p-1)!+1$ is not the k-th power of p for any natural number k.

Proof. As we have proved above, if a natural number n is composite $\neq 4$, then $n|(n-1)!$. Therefore, if p is a prime > 5, then $p-1|(p-2)!$, whence $(p-1)^2|(p-1)!$. On the other hand, it follows from the binomial formula applied to $(1+(p-1))^k = p^k$, where k is a natural number, that $(p-1)^2|1+k(p-1)-p^k$. If $(p-1)!+1 = p^k$, then $(p-1)^2|k(p-1)-(p-1)!$ would hold, which, by the formula $(p-1)^2|(p-1)!$, would give $(p-1)^2|k(p-1)$, and so $p-1|k$, whence $k \geqslant p-1$ and consequently $(p-1)!+1 = p^k \geqslant p^{p-1}$, which is impossible since, of course, $(p-1)! \leqslant (p-1)^{p-2}$.

4. Prove that if p is a prime > 5, then the number $(p-1)!+1$ has at least two different prime divisors.

Proof. By theorem 3, the number $(p-1)!+1$ has at least one prime divisor p. But, since in view of exercise 3 it is not the k-th power of p for any natural number k, it must have another prime divisor.

5. Prove the theorem of Lerch [1] stating that if p is an odd prime number, then

$$1^{p-1}+2^{p-1}+\ldots+(p-1)^{p-1} \equiv p+(p-1)!\,(\mathrm{mod}\, p^2).$$

Proof. Let p be an odd prime number. By theorem 3 the number $\dfrac{(p-1)!+1}{p}$ is an integer. Let r be the remainder obtained by dividing it by p; thus we have $\dfrac{(p-1)!+1}{p} \equiv r(\mathrm{mod}\, p)$. Hence $(p-1)! \equiv pr-1(\mathrm{mod}\, p^2)$. In view of theorem 5, for $a = 1, 2, \ldots, p-1$ the number $\dfrac{a^{p-1}-1}{p}$ is integral, let r_a be the remainder obtained by dividing it by p, thus

$$\frac{a^{p-1}-1}{p} \equiv r_a(\mathrm{mod}\, p).$$

Hence

$$a^{p-1} \equiv pr_a+1\,(\mathrm{mod}\, p^2). \tag{32}$$

From this we obtain

$$\begin{aligned}((p-1)!)^{2p-1} = 1^{p-1}\cdot 2^{p-1}\ldots(p-1)^{p-1} &\equiv (pr_1+1)(pr_2+1)\ldots(pr_{p-1}+1)\\ &\equiv 1+p(r_1+r_2+\ldots+r_{p-1})\,(\mathrm{mod}\, p^2).\end{aligned}$$

But, since $(p-1)! \equiv pr-1(\mathrm{mod}\, p^2)$, we see that

$$((p-1)!)^{2p-1} \equiv (pr-1)^{p-1} \equiv 1-(p-1)pr \equiv 1+pr\,(\mathrm{mod}\, p^2).$$

Now, comparing the formulae for $((p-1)!)^{p-1}$, we obtain

$$p(r_1+r_2+\ldots+r_{p-1}) \equiv pr\,(\mathrm{mod}\, p^2),$$

whence, by (32),

$$\begin{aligned}1^{p-1}+2^{p-1}+\ldots+(p-1)^{p-1} &\equiv p(r_1+r_2+\ldots+r_{p-1})+p-1\\ &\equiv pr+p-1 \equiv (p-1)!+p\,(\mathrm{mod}\, p^2).\end{aligned}$$

6. Prove that every prime number $p > 5$ is a factor of the number $n_p = 111\ldots1$ written in the scale of ten with the use of $p-1$ digits, each of them equal to 1.

Proof. Let p be a prime number > 5. Then $(10, p) = 1$ and $9n_p = 10^{p-1}-1$. In view of theorem 5, $10^{p-1} \equiv 1(\mathrm{mod}\, p)$, whence $p|9n_p$. But, since $(p, 9) = 1$ (for, p is a prime > 5), we must have $p|n_p$.

7. Prove that if p is a prime and c an integer, then there exist infinitely many natural numbers x which satisfy each congruence of the following infinite sequence:

$$x \equiv c(\mathrm{mod}\, p), \quad x^x \equiv c(\mathrm{mod}\, p), \quad x^{x^x} \equiv c(\mathrm{mod}\, p), \quad \ldots \tag{*}$$

Proof. Let p be a prime and c a given integer. Since $(p, p-1) = 1$, then, as is known, there exist infinitely many natural numbers $x > 1$ such that $x \equiv c \pmod{p}$ and $x \equiv 1 \pmod{p-1}$. Hence $x^k \equiv 1 \pmod{p-1}$ for $k = 1, 2, \ldots$ Consequently $x^k = 1+(p-1)l_k$, where, in view of $x > 1$, l_k is a natural number. Hence $x^{x^k} \equiv x(x^{l_k})^{p-1} \pmod{p}$. If $p|c$, then $x \equiv 0 \pmod{p}$ and, clearly, x satisfies each of congruences (*). If c is not divisible by p, then $(c, p) = 1$ and, since $x \equiv c \pmod{p}$, $(x, p) = 1$ and $(x^{l_k}, p) = 1$. Hence, by theorem 5, we obtain $(x^{l_k})^{p-1} \equiv 1 \pmod{p}$ and so $x^{x^k} \equiv x \equiv c \pmod{p}$ for any $k = 1, 2, \ldots$ Substituting $1, x, x^x, x^{x^x}, \ldots$ for k successively, we obtain (*).

Congruences like (*) have been investigated also for arbitrary positive moduli (Schinzel and Sierpiński [4]).

8. Find all the natural numbers each of which admits precisely one representation as the sum of the squares of two relatively prime natural numbers. (Of course we do not consider two representations as being different if they differ only in the order of the summands.)

Solution. We are going to prove that the numbers in question are precisely the powers (the exponents being natural numbers) of the primes of the form $4k+1$.

LEMMA 1. *If p is a prime of the form $4t+1$, then, for $k = 1, 2, \ldots$, number p^k admits precisely one representation as the sum of the squares of two relatively prime natural numbers.*

Proof of lemma 1. In virtue of theorem 11 the lemma is true for $k = 1$. Let k denote an arbitrary natural number and suppose that the lemma is true for number k. Then there exist natural numbers c and d such that $(c, d) = 1$ and $p^k = c^2+d^2$. It follows from theorem 11 that there exist natural numbers a, b such that $(a, b) = 1$ and such that $p = a^2+b^2$. Hence

$$p^{k+1} = (a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2 = (ad+bc)^2+(ac-bd)^2. \tag{33}$$

If each of the numbers $ad-bc$ and $ac-bd$ is divisible by p, then $ad \equiv bc \pmod{p}$ and $ac \equiv bd \pmod{p}$, whence $a^2cd \equiv b^2cd \pmod{p}$, so $p|cd(a^2-b^2)$. But since $p_k = c^2+d^2$ and $(c, d) = 1$, neither of the numbers c and d can be divisible by p. Consequently $p|a^2-b^2$, which together with the relation $p|a^2+b^2$ gives $p|a$ and, since $p = a^2+b^2$, $p|b$, contrary to the assumption $(a, b) = 1$. Therefore at least one of the numbers $ad-bc$ and $ac-bd$ is not divisible by p. If this is the number $ad-bc$, then by (33) the number $ac+bd$ is not divisible by p either. Then the numbers $ac+bd$ and $ad-bc$ are relatively prime, since, as follows from (33), each of their common factor is a divisor of p^{k+1} and, as we have just seen, p does not divide any of them. Similarly, if $ac-bd$ is not divisible by p, then the numbers $ad+bc$ and $ac-bd$ are relatively prime. Thus in any case formula (33) gives a representation of p^{k+1} as the sum of the squares of two relatively prime natural numbers. This, by induction, proves that for every $k = 1, 2, \ldots$ the number p^k is the sum of the squares of two relatively prime natural numbers.

We now suppose that for a natural number k the number p^k admits two different representations as the sum of the squares of two relatively prime natural numbers. Let $p^k = a^2+b^2 = c^2+d^2$, where $(a, b) = (c, d) = 1$ and $a \geqslant b$, $c \geqslant d$, $a > c$. We have

$$p^{2k} = (ac+bd)^2+(ad-bc)^2 = (ad+bc)^2+(ac-bd)^2, \tag{34}$$

and

$$(ac+bd)(ad+bc) = (ab+cd)p^k.$$

Hence, at least one of the numbers $ac+bd$ and $ad+bc$ is divisible by p. If both were divisible by p, then, by (34), we would have $ad \equiv bc \pmod{p}$ and $ac \equiv bd \pmod{p}$, whence $p|cd(a^2-b^2)$, and, since $p^k = c^2+d^2$ and $(c, d) = 1$, we would also have $p|a^2-b^2$, which, in virtue of $p|a^2+b^2$, would give $p|2a^2$, whence, since p is odd, $p|a$. But hence, in view of $p|a^2+b^2$, we would also obtain $p|b$, which contradicts $(a, b) = 1$. Thus precisely one of the numbers $ac+bd$ and $ad+bc$ is divisible by p. But since their product is equal to a multiple of p^k, the one that is divisible by p must be divisible by p^k. If $p^k|ac+bd$, then, by (34), $ad-bc = 0$, whence $a/b = c/d$, which, by $(a, b) = (c, d) = 1$, implies $a = c$, contrary to the assumption. If $p^k|ad+bc$, then, by (34), $ac-bd = 0$, whence $a/b = d/c$, which, in virtue of $(a, b) = (c, d) = 1$, implies $a = d$, contrary to $a > c \geqslant d$. Lemma 1 is thus proved.

It follows that in order to prove the theorem it suffices to prove that if an odd natural number admits a unique representation (apart from the possibility of interchanging of the summands) as the sum of the squares of two relatively prime natural numbers, then n is a power with a natural number exponent of a prime of the form $4k+1$.

In order to do this we first prove the following

LEMMA 2. *If m and n are two odd natural numbers which are relatively prime and such that each of them is representable as the sum of the squares of two relatively prime natural numbers, then the product mn admits at least two representations as the sum of the squares of two relatively prime natural numbers which differ not only in the order of the summands.*

Proof of lemma 2. Suppose that m and n are relatively prime odd natural numbers and a, b, c, d are natural numbers such that $(a, b) = (c, d) = 1$, $m = a^2+b^2$, $n = c^2+d^2$. Suppose that $a \geqslant b$, $c \geqslant d$. We then have

$$mn = (ac+bd)^2+(ad-bc)^2 = (ad+bc)^2+(ac-bd)^2 \tag{35}$$

and

$$(ac+bd)(ad+bc) = cdm+abn. \tag{36}$$

The decompositions of number mn into the sum of squares given by (35) are different. The proof follows from the fact that if $ac+bd = ad+bc$, then we would have $(a-b)(c-d) = 0$, and so $a = b$ or $c = d$, which is impossible because the numbers m and n are odd; if $ac+bd = ac-bd$ (number $ac-bd$ is $\geqslant 0$, since $a \geqslant b$, $c \geqslant d$), then we would have $ac = 0$, which is impossible. Thus to complete the proof of lemma 2 it is sufficient to show that $(ac+bd, ad-bc) = 1$ and $(ad+bc, ac-bd) = 1$. If $(ac+bd, ad-bc) > 1$, then the numbers $ac+bd$ and $ad-bc$ would have a common prime divisor p. Hence, by (35), $p|mn$ and so $p|m$ or $p|n$. If $p|m$, then, by (36), we would have $p|abn$, which, in view of $p|m$ and $(m, n) = 1$, would give $p|ab$, so $p|a$ or $p|b$, which, in virtue of $p|m = a^2+b^2$, would give $p|a$ and $p|b$, contrary to the assumption that $(a, b) = 1$. If $p|n$, then, by (36), $p|cdm$, which, in view of $(m, n) = 1$, would give $p|cd$, which in virtue of $p|c^2+d^2$ and $(c, d) = 1$, leads to a contradiction again. The lemma is thus proved.

Suppose now that an odd number n has a unique representation as the sum of the squares of two relatively prime natural numbers. Let $n = a^2+b^2$ be this unique representation and let p denote a prime divisor of the number n. Then p is, plainly, an odd number. If $p = 4k+3$, then raising each side of the congruence $a^2 \equiv -b^2 \pmod{p}$ to the $\frac{1}{2}(p-1) = (2k+1)$-th power we obtain $a^{p-1} \equiv -b^{p-1} \pmod{p}$, but, in view of the relations $(a, b) = 1$ and $(a, p) = (b, p) = 1$ and theorem 5 we have $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p}$. Hence $1 \equiv -1 \pmod{p}$ that is $p|2$, which is impossible. Thus every prime divisor of number n is of the form $4k+1$. Therefore the factorization of n into primes is of the form $n = q_1^{a_1} q_2^{a_2} \dots q_k^{a_k}$, where $a_1, a_2, \dots, a_k$ and k are natural numbers and each of the primes q_i $(i = 1, 2, \dots, k)$ is of the form $4t+1$. If $k = 1$, then there is nothing to be proved. Suppose that $k > 1$. Then since any two of the numbers $q_1^{a_1}, q_2^{a_2}, \dots, q_k^{a_k}$ are relatively prime, lemma 1 implies that each of them is the sum of the squares of two relatively prime natural numbers. Then lemma 2 shows that the number $q_1^{a_1} q_2^{a_2} \dots q_{k-1}^{a_k-1}$ is the sum of the squares of two relatively prime numbers and, since $(q_1^{a_1} q_2^{a_2} \dots q_{k-1}^{a_k-1}, q_k^{a_k}) = 1$, number $q_1^{a_1} \cdot q_2^{a_2} \dots q_{k-1}^{a_k-1} \cdot q_k^{a_k} = n$ has at least two different representations as the sum of the squares of two relatively prime numbers, contrary to the assumption about number n. Therefore we must have $k = 1$, and this completes the proof (cf. Sierpiński [28]).

§ 6. Numeri idonei. Under this name we understand numbers d which have the following property: if an odd integer $n > 1$ admits a unique representation (apart from the obvious possibility of interchanging the summands) in the form $x^2 + y^2 d$, where x, y are non-negative integers and in this unique representation the summands are relatively prime, then n is a prime [1].

It follows from theorem 11 that 1 belongs to the class of these numbers. Euler gave the following 65 examples of these numbers. 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 15, 16, 18, 21, 22, 24, 25, 28, 30, 33, 37, 40, 42, 45, 48, 57, 58, 60, 70, 72, 78, 85, 88, 93, 102, 105, 112, 120, 130, 133, 165, 168, 177, 190, 210, 232, 240, 253, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760, 840, 1320, 1365, 1848.

Numbers d have been investigated up to 2500000 (J. D. Swift [1]) but no numerus idoneus greater than 1848 has been found.

S. Chowla [1] proved in 1934 that the number of numeri idonei is finite; later he and W. E. Briggs proved that there is at most one greater than 10^{65} (cf. Chowla and Briggs [1]). More information on numeri idonei is to be found in a paper of J. G. Melnikov [1].

§ 7. Pseudoprime and absolutely pseudoprime numbers. It follows from theorem 5^a that if n is a prime, then $n \mid 2^n - 2$. Chinese mathematicians claimed 25 centuries ago that the converse theorem is also true. In fact, this is true for the natural numbers $n \leqslant 300$ [2]. Number 341, however, is a composite number, it is equal to the product $11 \cdot 31$, and $341 \mid 2^{341} - 2$. In fact, since 11 and 31 are odd primes, by theorem 5 we have $2^{10} \equiv 1 \pmod{11}$ and, clearly, $2^{10} \equiv 1 \pmod{31}$. Hence $2^{341} \equiv 2 \cdot 2^{340} \equiv 2 \pmod{11}$ and $2^{341} \equiv 2 \pmod{31}$. Therefore number $2^{341} - 2$ is divisible by 11 and by 31, and so it is divisible by the product $11 \cdot 31 = 341$.

[1] The definitions of these numbers given by many authors are in general incorrect. A correct, though more complicated, definition of the numbers (which he has called *Euler numbers*) has been given by F. Grube [1].

[2] It is worth noticing that in the years 1680-81 Leibniz also claimed that the number $2^n - 2$ is not divisible by n unless it is a prime. His assertion, however, was based on a false argument. (Cf. Dickson [8], vol. I, p. 64.)

Composite numbers n for which $n \mid 2^n - 2$ are called *pseudoprimes*. The pseudoprimes $\leqslant 2000$ are the following: $341 = 11 \cdot 31$, $561 = 3 \cdot 11 \cdot 17$, $645 = 3 \cdot 5 \cdot 43$, $1105 = 5 \cdot 13 \cdot 17$, $1387 = 19 \cdot 73$, $1729 = 7 \cdot 13 \cdot 19$, $1905 = 3 \cdot 5 \cdot 127$. D. H. Lehmer [5] and P. Poulet [2] have found all the odd composite numbers $n \leqslant 10^8$ for which $n \mid 2^n - 2$.

THEOREM 12. *There are infinitely many pseudoprime numbers* [1].

LEMMA. *If n is an odd pseudoprime, then the number $m = 2^n - 1$ is also an odd pseudoprime. Clearly $m > n$.*

Proof of the lemma. Suppose that n is a pseudoprime. Then n is a composite number and consequently there exists a divisor q of n such that $1 < q < n$. We then have $1 < 2^q - 1 < 2^n - 1 = m$. From this we infer that m is a composite odd number. According to the assumption n is an odd number; therefore, since the fact that n is a pseudoprime implies that $(2^n - 2)/n$ is an integer, we see that number $(2^n - 2)/n$ is an even integer. From this we deduce that $2n \mid 2^n - 2$, whence $n \mid 2^{n-1} - 1$. Consequently, for an integer k, we have $2^{n-1} - 1 = kn$. Hence $2^{m-1} = 2^{2^n - 2} = 2^{2kn}$ and so $2^{m-1} - 1 = (2^n)^{2k} - 1$, which implies that $2^n - 1 \mid 2^{m-1} - 1$ and hence, immediately, $m \mid 2^m - 2$, i.e. m is a pseudoprime number. It is clear that $m > n$, since, by $n > 2$ (n is a composite number), we have $2^n > n+1$, and so $m > n$. The lemma is thus proved.

Theorem 12 is an immediate consequence of the lemma and the fact that there exist odd pseudoprime numbers, for example $n = 341$.

Until 1950 only odd pseudoprimes were known. D. H. Lehmer was the first to find an even pseudoprime number. This is $n = 161038$. It was by no means easy to find this number, however, the proof that in fact it is a pseudoprime is quite elementary and simple.

A straightforward verification shows that $n = 2 \cdot 73 \cdot 1103$, $n-1 = 3^2 \cdot 29 \cdot 617$, $2^9 - 1 = 7 \cdot 73$, $2^{29} - 1 = 233 \cdot 1103 \cdot 2089$. Since $9 \mid n-1$ and $29 \mid n-1$, we see that $2^9 - 1 \mid 2^{n-1} - 1$ and $2^{29} - 1 \mid 2^{n-1} - 1$. From this, keeping in mind the relations $73 \mid 2^9 - 1$ and $1103 \mid 2^{29} - 1$, we conclude that the number $2^{n-1} - 1$ is divisible by 73 and 1103. Hence, *a fortiori*, number $2^n - 2$ is divisible by 73 and 1103. But this is an even number, and so it must also be divisible by 2. Hence, looking at the factorization into primes of number n we see that $n \mid 2^n - 2$. This shows that n is a pseudoprime number.

N. G. W. H. Beeger [1] has proved that there exist infinitely many even pseudoprimes, and later A. Rotkiewicz [2] has proved that the following assertion is also true. *For arbitrary natural numbers a and b there exist infinitely many even numbers n such that $n \mid a^n b - ab^n$.* This in turn, implies that for every natural number a there exist infinitely many

[1] Cf. Cipolla [1], D. H. Lehmer [5], Sierpiński [6].

even numbers n such that $n \mid a^n - a$ [1]. A. Rotkiewicz [6] has proved that there exists infinitely many pseudoprime numbers of the form $ax+b$ $(x = 0, 1, 2, \ldots)$, where a, b are relatively prime integers; $a > 0$.

The pseudoprime numbers are sometimes called *Poulet numbers*, since, as we have already mentioned, Poulet has given the tables of these numbers. The numbers whose every divisor d satisfies the relation $d \mid 2^d - 2$ are called *super-Poulet* numbers (cf. Duparc [2]). An example of a super-Poulet number is the number $n = 2047$. In fact, we have $2047 = 2^{11} - 1 = 23\cdot 89$, whence, by theorem 5^{a}, $11 \mid 2^{11}-2$, so $2^{11}-1 \mid 2^{2^{11}-1}-2$, and this proves that 2047 is a pseudoprime number. The natural factors of 2047 are the numbers 1, 23, 89 and 2047. Hence, since by theorem 5^{a} $23 \mid 2^{23}-2$ and $89 \mid 2^{89}-2$, we see that 2047 is a super-Poulet number. There exist Poulet numbers which are not super-Poulet. For example, $561 = 3\cdot 11\cdot 17$. In fact, the number 560 is divisible by 2, 10 and 16; from this and from theorem 5 it follows that $3 \mid 2^2-1 \mid 2^{560}-1$, $11 \mid 2^{10}-1 \mid 2^{560}-1$, $17 \mid 2^{16}-1 \mid 2^{560}-1$. Hence $561 = 3\cdot 11\cdot 17 \mid 2^{560}-1 \mid 2^{561}-2$, which shows that 561 is a Poulet number. However, number 33, though it is a factor of number 561, is not a divisor of number $2^{33}-2$; for, $2^{33}-2$ is not divisible by 11. (In fact, $2^{10} \equiv 1 \pmod{11}$, whence $2^{30} \equiv 1 \pmod{11}$, and so $2^{33} \equiv 8 \pmod{11}$ and $2^{33}-2 \equiv 6 \pmod{11}$.) Thus 561 is not a super-Poulet number.

It follows from theorem 5^{a} that a Poulet number which is the product of two different prime factors is a super-Poulet number. Therefore it seems interesting to know whether there exist infinitely many pairs of different primes p, q such that $pq \mid 2^{pq}-2$. The answer to this question is positive. It follows from the more general theorem of A. Rotkiewicz [1]:

Given three arbitrary natural numbers a, b, s. There exist infinitely many natural numbers n which are the products of s different prime factors and such that $n \mid a^{n-1} - b^{n-1}$.

This theorem implies that for arbitrary natural numbers a and s there exist infinitely many natural numbers n, each of them being the product of s prime factors, such that $n \mid a^n - a$ (for $s = 2$, cf. Schinzel [11], for $a = 2$ see D. H. Lehmer [5], Erdös [11]). This implies, of course, that there exist infinitely many super-Poulet numbers.

On the other hand, it can be proved that there exist infinitely many Poulet numbers which are not super-Poulet (cf. exercise 1 below).

A composite number n is called an *absolutely pseudoprime number* if for every integer a number $a^n - a$ is divisible by n.

[1] Cf. Rotkiewicz [3]. The author proves that for every natural number $a \leqslant 13$ different from 4 and 8 and every natural number $s \geqslant 3$ there exists an even number n which is the product of s different primes and is such that $n \mid (a+2)^{n-1} - a^{n-1}$.

An absolutely pseudoprime number is, *a fortiori*, a pseudoprime, the converse implication, however, not being true.

For example, as we have already seen, number 341 is a pseudoprime, but it is not an absolutely pseudoprime number because number $11^{341}-11$ is not divisible by 31, whence *a fortiori*, it is not divisible by 341. (In fact, we have $11^2 \equiv -3 \pmod{31}$, whence $11^{10} \equiv (-3)^5 \equiv -243 \equiv 5 \pmod{31}$. Therefore $11^{11} \equiv 55 \equiv -7 \pmod{31}$. But, since $11^{30} \equiv 1 \pmod{31}$, $11^{341} \equiv 11^{11} \equiv -7 \pmod{31}$, whence $11^{341}-11 \equiv -18 \pmod{31}$.)

It is easy to prove that if n is the product of k different primes $q_1, q_2, \ldots, q_k$, where k is a natural number > 1, and if $q_i - 1 \mid n-1$, $i = 1, 2, \ldots, k$, then n is an absolutely pseudoprime number. In fact, theorem 5 proves that, if $i = 1, 2, \ldots, k$ and an integer a is not divisible by q_i, then $q_i \mid a^{q_i-1}-1$. Hence, since $q_i - 1 \mid n-1$, $q_i \mid a^{n-1}-1$ and we have $q_i \mid a^n - a$. The last relation is, of course, true also in the case where $q_i \mid a$.

Hence it follows that number $561 = 3\cdot 11\cdot 17$ is an absolutely pseudoprime number; for, number 560 is divisible by 2, 10 and 16. It can be proved that 561 is the least absolutely pseudoprime number.

It is easy to see that for every natural number m if $n = (6m+1)\times(12m+1)(18m+1)$, number $n-1$ is divisible by $36m$, whence, *a fortiori*, it is divisible by $6m$, $12m$ and $18m$. Thus, in consequence of what we have stated above, we see that, *if the numbers $6m+1$, $12m+1$ and $18m+1$ are prime, then $n = (6m+1)(12m+1)(18m+1)$ is an absolutely pseudoprime number* (Chernick [1]).

We do not know whether there exist infinitely many absolutely pseudoprime numbers. However, from conjecture H (Chapter III, § 8) we infer that there exist infinitely many natural numbers m such that each of the numbers $6m+1, 12m+1$ and $18m+1$ is a prime. Thus we see that conjecture H implies the existence of infinitely many absolutely pseudoprime numbers.

The numbers $6m+1$, $12m+1$ and $18m+1$ are primes simultaneously for $m = 1, 6, 35, 45, 51$. This yields the following absolutely pseudoprime numbers: $1729 = 7\cdot 13\cdot 19$, $294409 = 37\cdot 73\cdot 109$, $211\cdot 421\cdot 621$, $271\cdot 541\cdot 811$, $307\cdot 613\cdot 919$.

Here are other absolutely pseudoprime numbers:

$$5\cdot 29\cdot 73,\ 5\cdot 17\cdot 29\cdot 113,\ 5\cdot 17\cdot 29\cdot 113\cdot 337,\ 5\cdot 17\cdot 29\cdot 113\cdot 337\cdot 673,$$
$$5\cdot 17\cdot 29\cdot 113\cdot 337\cdot 673\cdot 2689,\ 7\cdot 23\cdot 41,\ 7\cdot 31\cdot 73,\ 7\cdot 73\cdot 101,$$
$$7\cdot 13\cdot 31,\ 7\cdot 13\cdot 31\cdot 61,\ 7\cdot 13\cdot 31\cdot 61\cdot 181,\ 7\cdot 13\cdot 31\cdot 61\cdot 181\cdot 541,$$
$$7\cdot 13\cdot 31\cdot 61\cdot 181\cdot 541\cdot 2161,\ 13\cdot 37\cdot 61,\ 13\cdot 37\cdot 91,\ 13\cdot 37\cdot 241,$$
$$13\cdot 61\cdot 397,\ 13\cdot 97\cdot 421,\ 43\cdot 3361\cdot 3907.$$

If n is an absolutely pseudoprime number, then, of course, $n \mid 2^n - 2$ and $n \mid 3^n - 3$. We cannot prove, however, that there exist infinitely many composite numbers for which $n \mid 2^n - 2$ and $n \mid 3^n - 3$.

If n is an absolutely pseudoprime number and a is an integer relatively prime to n, then, since $a^n-a = a(a^{n-1}-1)$ is divisible by n, number $a^{n-1}-1$ must be divisible by n. Composite numbers n such that $n \mid a^{n-1}-1$ holds if $(a,n)=1$ are called *Carmichael numbers*. Carmichael was the first to notice the existence of these numbers in 1909. We see that any absolutely pseudoprime number is a Carmichael number. It can be proved that the converse is also true. One can prove that a natural number n is a Carmichael number if and only if $n = q_1q_2\ldots q_k$, where $k \geqslant 3$ and $q_1, q_2, \ldots, q_k$ are different odd prime numbers such that $q_i-1 \mid n-1$, $i=1,2,\ldots,k$ (cf. Carmichael [2], [3], Sispanov [1], Duparc [1], Knödel [1], Erdös [17], Sierpiński [12], pp. 186-188).

There are natural numbers $n>2$ such that for every integer a $n \mid a^{n-2}-a$. For example $n=195$.

Since $195 = 3\cdot 5\cdot 13$, it is sufficient to prove that for every integer a number $a^{193}-a$ is divisible by 3, 5 and 13. Let p denote any of the numbers 3, 5 or 13. Then, as is easy to verify, $p-1 \mid 192$, because $192 = 4\cdot 48$. If $p \mid a$, then clearly $p \mid a^{193}-a$. If p does not divide a, then, by theorem 5, $p \mid a^{p-1}-1$, and consequently, since $p-1 \mid 192$, $p \mid a^{192}-1$, whence $p \mid a^{193}-a$. Therefore, in either case, the relation $p \mid a^{193}-a$ holds for any integer a and $p = 3, 5, 13$. Hence $195 \mid a^{193}-a$ for any integer a.

Similarly, since $399 = 3\cdot 7\cdot 19$, $18 \mid 396$, $1023 = 3\cdot 11\cdot 31$, $30 \mid 1020$, we can easily prove that for any integer a we have $399 \mid a^{397}-a$, $1023 \mid a^{1021}-a$.

If n is a natural number >3 such that $n \mid a^{n-2}-a$ for every integer a, then, of course, for $(a,n)=1$ we have $n \mid a^{n-3}-1$. Numbers $n>3$ for which $n \mid a^{n-3}-1$ holds for $(a,n)=1$, have been considered by D. C. Morrow [1], who has called them *D numbers*. We prove that *there are infinitely many D numbers*. As a matter of fact, we show that every number of the form $n=3p$, where p is a prime $\geqslant 3$, is a D number. If $p=3$, i. e. if $n=9$, we verify directly that $9 \mid a^6-1$ for any a with $(a,9)=1$. Suppose that p is a prime >3, and a is an integer such that $(a,3p)=1$. Then, *a fortiori*, $(a,p)=1$, and so, by theorem 5, $p \mid a^{p-1}-1$, whence $p \mid a^{3p-3}-1$. But, since $(a,3p)=1$, the number a is not divisible by 3 and the number $p-1$ is even (since the number p is an odd prime), therefore $3 \mid a^{3(p-1)}-1$. This shows that the number $a^{3p-3}-1$ is divisible by p and by 3; consequently, since $(p,3)=1$, it is also divisible by $3p$. Thus we arrive at the conclusion that $3p \mid a^{3p-3}-1$ holds for any a with $(a,3p)=1$, and this means that $3p$ is a D number.

A. Mąkowski [8] has proved a more general theorem, namely that for any natural number $k \geqslant 2$ there exist infinitely many composite numbers n such that for every integer a with $(a,n)=1$ the relation $n \mid a^{n-k}-1$ holds. (The proof of this theorem will be given in Chapter VI, § 5.)

EXERCISES. **1.** Prove that there are no even super-Poulet numbers.

Proof. Suppose, to the contrary, that $2n$ is a super-Poulet number. Then $2n \mid 2^{2n}-2$, whence $n \mid 2^{2n-1}-1$, and this shows that n must be an odd number. Since $2n$ is a super-Poulet number, $n \mid 2^n-2$, whence, since n is odd, $n \mid 2^{n-1}-1$. Consequently, since $n \mid 2^{2n-1}-1$, $n \mid 2^{2n-1}-2^{n-1} = 2^{n-1}(2^n-1)$. Hence, using again the fact that n is odd, we obtain $n \mid 2^n-1$, which, compared with $n \mid 2^n-2$, proves that $n=1$, which is impossible, since $2n$ is a composite number.

We have already mentioned Beeger's theorem that there exist infinitely many even Poulet numbers. In view of exercise 1 these numbers cannot be super-Poulet. Thus we see that there exist infinitely many Poulet numbers which are not super-Poulet.

2. Prove the fact, observed by S. Maciąg, that $n = 2\cdot 73\cdot 1103\cdot 2089$ is a pseudoprime number.

Proof. We have $n = 2089m$, where, in accordance with what we have proved above, m is a pseudoprime number and $9 \mid m-1$, $29 \mid m-1$. Hence $n-1 = (m-1)\times$ $\times 2089+2088$. Since $2088 = 2^3\cdot 3^2\cdot 29$, by $9 \mid m-1$ and $29 \mid m-1$, we infer that $9 \mid n-1$ and $29 \mid n-1$. Hence, since $2^9-1 = 7\cdot 73$ and $2^{29}-1 = 233\cdot 1103\cdot 2089$, it follows that $73 \mid 2^{n-1}-1$, $1103 \mid 2^{n-1}-1$ and since $2089 \mid 2^{29}-1$, $2089 \mid 2^{n-1}-1$. Now, looking at the factorization of number n into prime factors, we see that $n \mid 2^n-2$.

3. Prove that there exist infinitely many Mersenne numbers which are Poulet numbers.

The proof follows immediately from the lemma in the proof of theorem 12 (and the fact that there exist odd Poulet numbers, for example 341).

However, we do not know whether there exist infinitely many Mersenne numbers which are super-Poulet numbers.

4. Prove that the relation $n \mid 2^n-1$ cannot hold for a natural number $n>1$.

Proof (due to A. Schinzel). Suppose to the contrary that n is a natural number greater than 1 such that $n \mid 2^n-1$ holds. Let p be the least prime divisor of the number n and δ the least natural number for which $p \mid 2^\delta-1$. Since $p>1$, we must have $\delta>1$. Moreover, the relation $p \mid 2^n-1$ implies $\delta \mid n$. For, if n divided by δ leaves the remainder r with $0<r<\delta$, then $n = k\delta+r$, whence $2^n-1 = 2^{k\delta}2^r-1$. But, since $p \mid 2^\delta-1$ we have $2^\delta \equiv 1 \pmod{p}$, whence $2^n-1 \equiv 2^r-1 \pmod{p}$ and so, since $p \mid 2^n-1$, we have $p \mid 2^r-1$, contrary to the definition of δ. In virtue of the theorem of Fermat, $p \mid 2^{p-1}-1$ (this is because n and, consequently, p are odd). Hence the definition of δ implies that $\delta \leqslant p-1$ which gives $1<\delta<p$, contrary to the definition of the prime p.

Remark. It is easy to prove that there exist infinitely many natural numbers n such that $n \mid 2^n+1$, for example, such are the numbers $n = 3^k$, where $k = 0, 1, 2, \ldots$ It is also not difficult to prove that there exist infinitely many natural numbers n such that $n \mid 2^n+2$. In fact, we see that it is trivially true for $n=2$, and, if n is an even natural number such that $n \mid 2^n+2$ and $n-1 \mid 2^n+1$, then the number $m = 2^n+2$ safisfies the relations $m \mid 2^m+2$ and $m-1 \mid 2^m+1$. Thus we obtain the numbers $n = 2, 6, 66, \ldots$ A. Schinzel has proved that there are no natural numbers $n>1$ such that $n \mid 2^{n-1}+1$.

5. Prove that there exist infinitely many composite numbers n which satisfy the relation $n \mid a^{n-1}-a$ for any integer a.

Hint. It is easy to prove that it suffices to put $n=2p$, where p is an odd prime.

§ 8. Lagrange's theorem.

THEOREM 13 (Lagrange). *If n is a natural number and $f(x)$ is a polynomial of degree n with respect to x with integral coefficients; if, moreover, the coefficient of x^n is not divisible by p, then the congruence $f(x) \equiv 0 \pmod{p}$ has at most n roots.*

Proof. It follows from the corollary to theorem 2 that theorem 13 is true for $n = 1$. Let n denote an arbitrary natural number >1 and suppose that theorem 13 holds for polynomials of degree $n-1$. Let $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$ be a polynomial with integral coefficients such that a_0 is not divisible by a prime number p and suppose that the congruence

$$f(x) \equiv 0 \pmod{p} \tag{37}$$

has more than n roots. Then there exist $n+1$ numbers $x_1, x_2, \ldots, x_{n+1}$ which are different roots of congruence (37). Thus, in particular, $f(x_1) \equiv 0 \pmod{p}$. We have

$$f(x)-f(x_1) = a_0(x^n - x_1^n) + a_1(x^{n-1} - x_1^{n-1}) + \ldots + a_{n-1}(x-x_1).$$

But, since

$$x^k - x_1^k = (x-x_1)(x^{k-1} + x^{k-2}x_1 + \ldots + x_1^{k-1}),$$

this gives

$$f(x)-f(x_1) = (x-x_1)g(x), \tag{38}$$

where $g(x)$ is a polynomial of degree $n-1$ with respect to x and integral coefficients. Moreover, the coefficient of x^{n-1} is a_0, which, by assumption, is not divisible by p. Thus, by (38) and the fact that $f(x_1) \equiv 0 \pmod{p}$, congruence (37) is equivalent to the congruence

$$(x-x_1)g(x) \equiv 0 \pmod{p}. \tag{39}$$

Consequently, each of the numbers $x_1, x_2, \ldots, x_{n+1}$ is a root of congruence (39). For $i = 2, 3, \ldots, n+1$ we then have $p \mid (x_i - x_1)g(x_i)$, which, since $x_1, x_2, \ldots, x_{n+1}$ are different roots of congruence (37), implies that $p \mid g(x_i)$ for $i = 2, 3, \ldots, n+1$. This proves that the congruence $g(x) \equiv 0 \pmod{p}$ has at least n different roots, which contradicts the assumption that theorem 13 holds for polynomials of degree $n-1$.

From this we conclude that congruence (37) cannot have more than n roots, and this, by induction, completes the proof of theorem 13.

It is essential for theorem 13 that the modulus p is prime. For example, the congruence $x^2 - 1 \equiv 0 \pmod{8}$ has four roots: 1, 3, 5, 7; similarly, the congruence $x^2 + 3x + 2 \equiv 0 \pmod{6}$ has four roots 1, 2, 4, 5, though the leading coefficient in either of the congruences is relatively prime to the modulus.

It can be proved that if m is a composite number, then only in the case $m = 4$ the following theorem holds: *if $f(x)$ is a polynomial of degree n with integral coefficients such that the leading coefficient is relatively prime to m, then the congruence $f(x) \equiv 0 \pmod{m}$ has at most n different roots* (cf. Sierpiński [12], pp. 180-181).

COROLLARY. *If a congruence of degree n, with integral coefficients and a prime modulus p has more than n roots, then all the coefficients are divisible by p.*

Proof. Let (37) be a congruence satisfying the conditions and let

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n.$$

Suppose that among $a_0, a_1, \ldots, a_n$ there are coefficients which are not divisible by p, and let a_m be the first term of the sequence $a_0, a_1, \ldots, a_n$ which is not divisible by p. Then for every integer x we have

$$f(x) \equiv a_mx^{n-m} + a_{m+1}x^{n-m-1} + \ldots + a_{n-1}x + a_n \pmod{p}.$$

If $n = m$, then $f(x) \equiv a_n \pmod{p}$, and, since congruence (37) has more than n roots, there exists an integer x such that $f(x) \equiv 0 \pmod{p}$, whence $a_n \equiv 0 \pmod{p}$. This shows that m must be $< n$. Consequently the polynomial $a_mx^{n-m} + \ldots + a_{n-1}x + a_n$ satisfies the conditions of theorem 13, and so it has at most $n-m \leqslant n$ different roots, contrary to the assumption. The corollary is thus proved.

If all the coefficients of a congruence are divisible by the modulus, then, of course, the congruence holds identically. The converse, however, is not true. For example, the congruence $x^2 + x \equiv 0 \pmod{2}$ holds identically. Similarly, by theorem 5^a^, the congruence $x^{17} - x \equiv 0 \pmod{17}$ holds identically.

A simple application of theorem 5^a^ leads us to the conclusion that every congruence, where the modulus is a prime p, is equivalent to a congruence of a degree not greater than p. In fact, by theorem 5^a^, for every integer x we have

$$x^p \equiv x \pmod{p}, \qquad x^{p+1} \equiv x^2 \pmod{p}, \qquad \text{and so on.}$$

This shows that any power $\geqslant p$ of the unknown x can be replaced by a power $\leqslant p-1$ of x.

THEOREM 14. *If $m = ab$, where a, b are relatively prime natural numbers, then the number of the roots of the congruence*

$$f(x) \equiv 0 \pmod{m}, \tag{40}$$

where $f(x)$ is a polynomial in x with integral coefficients, is equal to the product of the number of the roots of the congruence

$$f(x) \equiv 0 \pmod{a} \tag{41}$$

and the number of the roots of the congruence

$$f(x) \equiv 0 \pmod{b}. \tag{42}$$

Proof. If x is a root of congruence (40), then it is a root of each of the congruences (41) and (42). The reason is that, if $m \mid f(x)$, then, *a fortiori*, $a \mid f(x)$ and $b \mid f(x)$. Thus we see that to each root of congruence (40) there corresponds a pair u, v, u being a root of congruence (41) and v being a root of congruence (42). (To be more precise: u is the remainder obtained by dividing x by a, v is the remainder obtained by dividing x by b.) It is easy to verify that different pairs u, v correspond to different roots of congruence (40). In fact, if to two different roots x, y corresponds the same pair u, v, then $x \equiv y \pmod{a}$ and $x \equiv y \pmod{b}$, which, in virtue of $(a, b) = 1$, implies $m = ab \mid x-y$ and consequently $x \equiv y \pmod{m}$, contrary to the assumption that the roots x, y are different.

Now suppose that u is a root of congruence (41) and v a root of congruence (42). Then, since $(a, b) = 1$, in virtue of the Chinese remainder theorem (cf. Chapter I, § 12), there exists an integer x such that

$$x \equiv u \pmod{a} \quad \text{and} \quad x \equiv v \pmod{b},$$

whence, by theorem 1, $f(x) \equiv f(u) \pmod{a}$ and $f(x) \equiv f(v) \pmod{b}$. But, since $f(u) \equiv 0 \pmod{a}$ and $f(v) \equiv 0 \pmod{b}$, we have $f(x) \equiv 0 \pmod{a}$ and $f(x) \equiv 0 \pmod{b}$; consequently, since $(a, b) = 1$ and $ab = m$, $f(x) \equiv 0 \pmod{m}$.

Thus we have shown that to each pair (u, v), where u is a root of congruence (41) and v is a root of congruence (42), there corresponds a root of congruence (40). This proves the existence of a one-to-one correspondence between all the roots (non-congruent with respect to the modulus m) of congruence (40) and all the pairs u, v consisting of the roots of congruences (41) and (42), respectively. Thus we see that the number of the roots of congruence (40) is equal to the number of the pairs u, v, where u is a root of congruence (41) and v is a root of congruence (42). Hence theorem 14 follows.

COROLLARY. *If $m = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k}$ is the factorization of an integer m into primes, then the number of the roots of congruence (40) is equal to the product of the numbers of the roots of the following k congruences:*

$$f(x) \equiv 0 \pmod{q_1^{\alpha_1}}, \quad f(x) \equiv 0 \pmod{q_2^{\alpha_2}}, \quad \dots, \quad f(x) \equiv 0 \pmod{q_k^{\alpha_k}}.$$

This gives a method of reducing the solution of a congruence with respect to an arbitrary modulus m to the solution of congruences with respect to moduli each of which is a power of a prime number.

EXERCISE. Prove that for every natural number n there exists a modulus m such that the congruence $x^2 \equiv 1 \pmod{m}$ has more than n roots.

Proof. If p is an odd prime, then the congruence $x^2 \equiv 1 \pmod{p}$ has precisely two roots, 1 and $p-1$ (cf. § 5). It follows from the corollary to theorem 14 that the congruence $x^2 \equiv 1 \pmod{p_2 p_3 \dots p_{s+1}}$ has precisely 2^s roots. Thus it remains to find a natural number s such that $2^s > n$. For example, the congruence $x^2 \equiv 1 \pmod{105}$ has 8 roots, since $105 = p_2 p_3 p_4$. (The roots are 1, 29, 34, 41, 64, 71, 76, 104.)

§ 9. Congruences of the second degree. Let us consider a congruence of the second degree

$$ax^2 + bx + c \equiv 0 \pmod{m}, \tag{43}$$

where m is a given natural number, and a, b, c are given integers. We assume that $a \not\equiv 0 \pmod{m}$, since otherwise if $a \equiv 0 \pmod{m}$, (43) becomes a congruence of degree less than two.

Since the relation $m \mid ax^2+bx+c$ is equivalent to the relation $4am \mid 4a(ax^2+bx+c)$, congruence (43) is equivalent to the congruence

$$4a(ax^2 + bx + c) \equiv 0 \pmod{4am}. \tag{44}$$

Let $D = b^2 - 4ac$. Then, in virtue of the identity

$$4a(ax^2+bx+c) = (2ax+b)^2 - (b^2 - 4ac),$$

congruence (44) can be rewritten in the form

$$(2ax+b)^2 \equiv D \pmod{4am}. \tag{45}$$

Let x be a root of congruence (43) and let $z = 2ax+b$. Then, by (45), z is a root of the binomial congruence

$$z^2 \equiv D \pmod{4am}. \tag{46}$$

Thus, we see that to each root x of congruences (43) corresponds a root of congruence (46).

In order to establish the converse correspondence, that is, to find for a given root z of congruence (46) all the roots x of (43) to which the root z corresponds, we have to solve the congruence $2ax+b \equiv z \pmod{4am}$. (This, as we know, is solvable whenever $(2a, 4am) \mid z-b$, i.e. whenever $2a \mid z-b$.) Thus we arrive at the conclusion that the solution of a congruence of the second degree can be reduced to the solution of a congruence of the first degree and a binomial congruence (46). In view of the remark in the corollary to theorem 14, the solution of congruence (46) reduces to the solution of the congruences

$$z^2 \equiv D \pmod{p^\alpha}, \tag{47}$$

where p is a prime and α is a natural number.

We are going to solve congruence (47) now. At first we suppose that $p \mid D$. Then $D = p^{\mu}D_1$, where μ is a natural number and D_1 is not divisible by p.

If $\mu \geqslant \alpha$, then $D \equiv 0 (\bmod p^{\alpha})$ and so (47) becomes the congruence $z^2 \equiv 0 (\bmod p^{\alpha})$, which is easy to solve.

If $\mu < \alpha$, the congruence (47) is equivalent to the equation

$$z^2 = p^{\mu}(D_1 + tp^{\alpha-\mu}), \tag{48}$$

where t is a suitably chosen integer and the number $D_1 + tp^{\alpha-\mu}$ is not divisible by p (because D_1 is not divisible by p). Hence we infer that μ is the highest exponent of p for which p^{μ} divides z^2. Consequently, μ must be an even number. We then write $\mu = 2\lambda$, where λ is a natural number. Hence $z = p^{\lambda}z_1$ and so, by (48), $z_1^2 = D_1 + tp^{\alpha-\mu}$. This yields the congruence

$$z_1^2 \equiv D_1 (\bmod p^{\alpha-\mu}).$$

Thus we see that the solution of congruence (47) reduces to the solution of a congruence of the same type, the right-hand side of which is not divisible by p. We then suppose in congruence (47) that $D \not\equiv 0 (\bmod p)$. If z satisfies this congruence, then, *a fortiori*, it satisfies the congruence

$$z^2 \equiv D (\bmod p),$$

which proves that D is a quadratic residue for the modulus p. From this we conclude that a necessary condition for the solvability of congruence (47) (with D not divisible by p) is that D should be a quadratic residue for the modulus p. We prove that this condition is also sufficient. For this purpose, it is of course sufficient to prove that, if the congruence

$$z^2 \equiv D (\bmod p^{\alpha-1}), \tag{49}$$

where α is a natural number > 1, is solvable, then congruence (47) is solvable as well.

The cases where p is odd and $p = 2$ are treated separately.

At first we suppose that p is odd. Let y be an integer satisfying congruence (49). Then

$$y^2 \equiv D (\bmod p^{\alpha-1}). \tag{50}$$

Hence it follows that the number

$$M = \frac{y^2 - D}{p^{\alpha-1}} \tag{51}$$

is an integer. Denote by x the root of the congruence

$$2xy + M \equiv 0 (\bmod p). \tag{52}$$

The solvability of (52) follows from the fact that since D is not divisible by p, y is not divisible by p, whence, since p is odd, $2y$ is not divisible by p. Let $z = y + p^{\alpha-1}x$. Hence $z^2 = y^2 + 2p^{\alpha-1}xy + p^{2\alpha-2}x^2$. Since, by (51), $y^2 = D + Mp^{\alpha-1}$, we see that

$$z^2 = D + (2xy + M)p^{\alpha-1} + x^2p^{2\alpha-2} \tag{53}$$

holds. In view of (52), number $2xy + M$ is divisible by p. In virtue of $2\alpha - 2 = \alpha + (\alpha - 2) \geqslant \alpha$ (since $\alpha > 1$), $p^{\alpha} \mid p^{2\alpha-2}$. Therefore, by (53), z satisfies congruence (47). Thus we have shown that the condition is sufficient. We formulate the result as follows:

THEOREM 15. *Congruence* (47), *where p is an odd prime, α a natural number and D an integer not divisible by p, is solvable if and only if D is a quadratic residue for the modulus p.*

We now prove that under the conditions of theorem 15 congruence (47) has precisely two roots.

If z is a root of congruence (47), then, clearly, the number $z_1 = -z$ is also a root of that congruence. Moreover, z and z_1 are not congruent with respect to the modulus p^{α}, since, if they were, we would have $p^{\alpha} \mid 2z$, which, since p is odd, would give $p^{\alpha} \mid z$ and hence $p \mid D$, contrary to the assumption. Thus we see that there exist at least two different roots of congruence (47): z and z_1. We are going to prove that they are the only roots of (47). Suppose that t is a root of congruence (47). Then $t^2 \equiv D (\bmod p^{\alpha})$, which by $z^2 \equiv D (\bmod p^{\alpha})$ implies $t^2 \equiv z^2 (\bmod p^{\alpha})$. Hence $p^{\alpha} \mid (t-z)(t+z)$. If the numbers $t-z$ and $t+z$ were both divisible by p, then $p \mid 2z$, which: since p is odd, would give $p \mid z$ and hence $p \mid D$, contrary to the assumption. Consequently, one of the numbers $t-z$ and $t+z$ is not divisible by p. If $t+z$ is not divisible by p, then $p^{\alpha} \mid t-z$, that is, $t \equiv z (\bmod p^{\alpha})$, if $t-z$ is not divisible by p, then $p \mid t+z$, whence $t \equiv -z (\bmod p^{\alpha})$. Thus we see that each root of congruence (47) is congruent with respect to the modulus p^{α} either to z or to $-z$. This proves that congruence (47) has precisely two roots.

Now, let $p = 2$. Then for $\alpha = 1$ formula (47) gives $z^2 \equiv D (\bmod 2)$, where D, which is not divisible by 2, is odd. An immediate consequence of this is that in this case the congruence has precisely one solution, namely $z = 1$.

For $\alpha = 2$ the congruence has the form $z^2 \equiv D (\bmod 4)$. But the square of an integer is congruent with respect to the modulus 4 either to zero or to 1. Hence, since D is odd, the congruence is solvable only in the case where D is of the form $4k+1$. Then, as can be verified directly, the congruence has two solutions, $z = 1$ and $z = 3$.

For $\alpha = 3$ the congruence is of the form $z^2 \equiv D (\bmod 8)$. Since D is odd, number z must also be odd, whence, since the square of an odd integer is $\equiv 1 \pmod 8$, we see that for the congruence to be solvable it is necessary that D should be of the form $8k+1$. As is easy to verify, the condition is also sufficient and the congruence has four solutions: $1, 3, 5, 7$.

Now let $a > 3$. We have to consider the congruence

$$z^2 \equiv D \pmod{2^a} \quad \text{where} \quad a > 3. \tag{54}$$

We see that congruence (54) implies the congruence $z^2 \equiv D \pmod 8$. For the latter to be solvable it is necessary that $D = 8k+1$. We prove that this, in turn, is a sufficient condition for the solvability of (54). To do this suppose that $D = 8k+1$ and that the congruence

$$z^2 \equiv D \pmod{2^{a-1}} \tag{55}$$

is solvable. (This, as proved above, is true for $a = 4$.) Then there exists an integer y such that $y^2 \equiv D \pmod{2^{a-1}}$ and, since D is odd, y, of course, must also be odd. Let

$$M = \frac{y^2 - D}{2^{a-1}}. \tag{56}$$

Then M is an integer. Further, let x be the root of the congruence

$$xy + M \equiv 0 \pmod 2, \tag{57}$$

of the first degree with respect to x. This is solvable since the coefficient y of the unknown and modulus 2 are relatively prime. Let $z = y + x2^{a-2}$. In virtue of (56) we have

$$z^2 = y^2 + xy2^{a-1} + x^2 2^{2a-4} = D + (xy+M)2^{a-1} + x^2 2^{2a-4}. \tag{58}$$

But, in view of (57), the number $xy+M$ is even, whence $(xy+M)2^{a-1} \equiv 0 \pmod{2^a}$ and, in virtue of $2a-4 = a+(a-4) \geqslant a$ (which is valid because $a \geqslant 4$), $x^2 2^{2a-4}$ is divisible by 2^a. Consequently, $x^2 2^{2a-4} \equiv 0 \pmod{2^a}$. Thus we see that (58) implies (54), which proves that for any $a > 3$ the solvability of congruence (55) implies the solvability of congruence (54). But since, as we have assumed, $D = 8k+1$, the congruence $z^2 \equiv D \pmod{2^3}$ is solvable; hence, by induction we see that (for $D = 8k+1$) congruence (54) is solvable for the natural numbers $a > 3$. We have thus proved the following

THEOREM 16. *In order that the congruence* $z^2 \equiv D \pmod{2^a}$, *where* D *is odd and* a *is a natural number, be solvable, it is necessary and sufficient that* D *should be of the form* $2k+1$, $4k+1$ *or* $8k+1$ *depending on whether* $a = 1$, $a = 2$ *or* $a > 2$.

We now prove that for $a > 3$ congruence (54) (with $D = 8k+1$) has precisely four roots.

We have proved that (under the assumptions made) the congruence has at least one root. Denote it by z_0. Let z be an arbitrary root of congruence (54). We have $z_0^2 \equiv D \pmod{2^a}$, whence, by (54), $2^{a-1} \mid (z-z_0)(z+z_0)$. Since D is odd, the numbers z and z_0 are also odd, whence it follows that the numbers $z-z_0$ and $z+z_0$ are even. They cannot both be divisible by 4, since if they were, number $2z$ would be divisible by 4, and so $2 \mid z$, which is impossible. Thus one of the numbers $z-z_0$, $z+z_0$ is not divisible by 4. If $z-z_0$ is not divisible by 4, then number $\frac{1}{2}(z-z_0)$ is odd. But, since $2^{a-1} \mid \frac{1}{2}(z-z_0)(z+z_0)$, we have $2^{a-1} \mid z+z_0$, and consequently $z = -z_0 + 2^{a-1}t$, where t is an integer. If t is even, then $z = -z_0 \pmod{2^a}$; if t is odd, then $z = -z_0 + 2^{a-1} \pmod{2^a}$. Now we consider the other case, i.e., that $z+z_0$ is not divisible by 4. Then the number $\frac{1}{2}(z+z_0)$ is odd, whence, in virtue of $2^{a-1} \mid (z-z_0)\frac{1}{2}(z+z_0)$, we infer that $2^{a-1} \mid z-z_0$, and so $z = z_0 + 2^{a-1}u$, where u is an integer. If u is even, this gives $z \equiv z_0 \pmod{2^a}$; if u is odd, then $z = z_0 + 2^{a-1} \pmod{2^a}$.

We have thus proved that any root z of congruence (54) must satisfy one of the following four congruences:

$$\begin{aligned} z &\equiv -z_0 \pmod{2^a}, \qquad & z &\equiv -z_0 + 2^{a-1} \pmod{2^a}, \\ z &\equiv z_0 \pmod{2^a}, \qquad & z &\equiv z_0 + 2^{a-1} \pmod{2^a}. \end{aligned} \tag{59}$$

This shows that the number of the roots cannot be greater than four. On the other hand, it is easy to verify that each number given by any of the congruences (59) satisfies congruence (54) (whenever it is true for z_0) and, since for $a \geqslant 3$ any two of these numbers are not congruent with respect to the modulus 2^a, we see that they are different roots of congruence (54).

The results we have obtained can be formulated in the following

THEOREM 17. *In order that the congruence* $z^2 \equiv D \pmod m$, *where* D *is an integer and* $(D, m) = 1$, *be solvable it is necessary and sufficient that* 1° D *should be a quadratic residue for every modulus that is an odd prime factor of number* m *and* 2° D *should be of the form* $4k+1$ *for* m *divisible by* 4 *but not divisible by* 8 *and of the form* $8k+1$ *for* m *divisible by* 8. *The number of the roots of the congruence is equal to* $2^{\lambda+\mu}$, *where* λ *is the number of odd prime factors of the number* m *and* $\mu = 0$ *for* m *not divisible by* 4, $\mu = 1$ *for* m *divisible by* 4 *but not divisible by* 8, *and, finally,* $\mu = 2$ *for* m *divisible by* 8.