number F_{1945} has more than 10^{582} digits, it is quite impossible even to write it down, let alone to divide it by m. But our aim is not to divide F_{1945} by m but to establish whether F_{1945} is divisible by m or not. The method by means of which we can do it is as follows.

We denote by $\bar{t}$ the remainder left by an integer t divided by m. It follows from the definition of $\bar{t}$ that for any integer t we have $m \mid t-\bar{t}$. We define the sequence r_k $(k=1,2,\ldots)$ by the conditions

$$r_1 = 2^2, \quad r_{k+1} = \overline{r_k^2}, \quad k = 1, 2, \ldots \tag{19}$$

We are going to prove by induction that

$$m \mid 2^{2^k} - r_k \quad \text{for any} \quad k = 1, 2, \ldots \tag{20}$$

Formula (20) is clearly true for $k=1$ because $2^{2^1}-r_1 = 0$. Suppose that it is true for a natural number k. By (20), we have $m \mid 2^{2^{k+1}} - \overline{r_k^2}$, whence, in view of $m \mid t-\bar{t}$ for $t = r_k^2$, we obtain $m \mid r_k^2 - \overline{r_k^2}$. This gives $m \mid 2^{2^{k+1}} - \overline{r_k^2}$ and so, by (19), $m \mid 2^{2^{k+1}} - r_{k+1}$. Thus formula (20) is proved by induction. For $k = 1945$ it gives

$$m \mid F_{1945} - r_{1945} - 1,$$

whence it follows that number F_{1945} is congruent to $r_{1945}+1 \pmod m$. Consequently, in order to establish whether F_{1945} is divisible by m, it is sufficient to find whether $r_{1945}+1$ is divisible by m.

Let us see what calculations are involved in calculating number r_{1945}. It follows from (19) that the numbers $r_1, r_2, \ldots$ are the remainders obtained by dividing by m, so any of them is less than m, whence it has not more than 587 digits. Thus, it follows from (19) that in order to obtain number r_{1945} one has to calculate the squares of 1944 natural numbers, each having not more than 587 digits, and to divide these squares (i.e. numbers that have no more than 1175 digits) by number m, which has 587 digits.

Present day electronic computers have proved capable of carrying out these calculations. In this way number F_{1945} has been shown to be divisible by number $m = 2^{1947}\cdot 5+1 < F_{1945}$ and so it is a composite number. The investigations of numbers $2^{1947}k+1$ for $k = 1, 2, 3, 4$, presented above together with theorem 5, show that m is the least natural divisor >1 of the number F_{1945}, and so m is a prime.

In a similar way the least prime divisors of all the other known composite Fermat numbers except the numbers F_7, F_8, F_{13}, and F_{14} have been found.

CHAPTER XI

REPRESENTATIONS OF NATURAL NUMBERS AS SUMS OF NON-NEGATIVE kth POWERS

§ 1. Sums of two squares.

THEOREM 1. *A natural number n is the sum of two squares of integers if and only if the factorization of n into prime factors does not contain any prime of the form $4k+3$ that has an odd exponent.*

LEMMA. *If an odd prime p divides the sum of the squares of two relatively prime integers, then it must be of the form $4k+1$.*

Proof of the lemma. Let a, b be two relatively prime integers and p an odd prime such that $p \mid a^2+b^2$. Then $a^2 \equiv -b^2 \pmod p$; this, raised to the $(p-1)/2$-th power gives $a^{p-1} \equiv (-1)^{(p-1)/2} b^{p-1} \pmod p$. But, since $(a, b) = 1$, the numbers a, b are not divisible by p, whence, by the theorem of Fermat, $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod p$; consequently, $(-1)^{(p-1)/2} \equiv 1 \pmod p$, which by $p > 2$, gives $(-1)^{(p-1)/2} = 1$ and proves that $(p-1)/2$ is even. Therefore p must be of the form $4k+1$.

Proof of the theorem. Suppose that a number n can be represented as the sum of the squares of two integers,

$$n = a^2+b^2. \tag{1}$$

Let

$$n = q_1^{\alpha_1} q_2^{\alpha_2} \ldots q_s^{\alpha_s} \tag{2}$$

be the factorization of n into prime factors. Finally, let p be a prime divisor of the form $4k+3$ of the number n. Write $d = (a, b)$, $a = da_1$, $b = db_1$, where $(a_1, b_1) = 1$. In virtue of (1), $d^2 \mid n$, and so $n = d^2 n_1$, where n_1 is a natural number. Suppose that the exponent on p in factorization (2) is odd. Then, since $n = d^2 n_1$, we must have $p \mid n_1 = a_1^2 + b_1^2$, which contradicts the lemma. Thus we have proved that the condition of the theorem is necessary.

In order to prove that it is sufficient we note that without any loss of generality we may assume that n is greater than 1, since for the number 1 we have $1 = 1^2+0^2$. Suppose that (2) is the factorization of n into prime factors. Let m be the greatest natural number whose square

divides n. Then $n = m^2k$, where k either is equal to 1 or is a product of different prime numbers among which no prime of the form $4k+3$ occurs. Since $2 = 1^2+1^2$, in virtue of theorem 9 of Chapter V, each of these primes is the sum of the squares of two natural numbers. The identity

$$(a^2+b^2)(c^2+d^2) = (ab+cd)^2+(ad-bc)^2$$

represents the product of two (and, by induction, of any finite number) natural numbers, each of them being the sum of the squares of two integers, as the sum of the squares of two integers. Consequently, k is the sum of the squares of two integers. So $k = u^2+v^2$, whence $n = m^2k = (mu)^2+(mv)^2$. This completes the proof of sufficiency of the condition. Theorem 1 is thus proved.

In connection with theorem 1 the question arises how many different representations as sums of two squares a natural number n admits. The answer to this question is to be found in Chapter XIII, § 9.

COROLLARY. *If a natural number is not the sum of the squares of two integers, then it is not the sum of the squares of two rational numbers either.*

Proof. If a natural number n is not the sum of the squares of two integers, then, by theorem 1, there is a prime p of the form $4k+3$ that divides n to an odd power exactly. Suppose that $n = \left(\frac{l}{m}\right)^2+\left(\frac{l_1}{m_1}\right)^2$ where m, m_1 are natural numbers and l, l_1 are integers. Then $(mm_1)^2n = (lm_1)^2+(l_1m)^2$. But p must appear with an odd exponent in the factorization of the left-hand side of the equality and, by theorem 1, this cannot be true regarding the right-hand side of the equality; thus a contradiction is reached and so the corollary is proved.

As proved by E. Landau [1], if $f(x)$ denotes the number of natural numbers $\leqslant x$ that are sums of two squares, then $f(x):\frac{x}{\sqrt{\log x}}$ tends to a finite positive limit as x increases to infinity.

The representations $n = x^2+y^2$, where x, y are integers, $0 \leqslant x \leqslant y$, and $n \leqslant 10000$, are given by A. Wijngarden [1]. The number of decomposition of n into two squares for $n \leqslant 20000$ is given by H. Gupta [2].

EXERCISES. **1.** Find a necessary and sufficient condition for a rational number l/m to be the sum of the squares of two rational numbers.

Solution. Such a condition is that the number lm be the sum of the squares of two integers. We easily verify it on the basis of the remark that, if $\frac{l}{m} = \left(\frac{l_1}{m_1}\right)^2+\left(\frac{l_2}{m_2}\right)^2$, then $lm(m_1m_2)^2 = (mm_2l_1)^2+(mm_1l_2)^2$. On the other hand, if $lm = a^2+b^2$, then $\frac{l}{m} = \left(\frac{a}{m}\right)^2+\left(\frac{b}{m}\right)^2$.

Remark. Exercise 1 and theorem 1 imply that an irreducible fraction l/m, where l, m are natural numbers, is the sum of the squares of two rational numbers if and only if each of the numbers l, m is the sum of the squares of two integers.

2. Prove that if a rational $r \neq 0$ is the sum of the squares of two rationals, then it has infinitely many representations as the sum of the squares of two positive rationals.

Proof. First, we suppose that $r = a^2+b^2$, where a, b are rationals both different from zero. Therefore, without loss of generality, we may assume that a, b are positive and that $a \geqslant b$. For any natural k we have

$$r = \left(\frac{(k^2-1)a-2kb}{k^2+1}\right)^2+\left(\frac{(k^2-1)b+2ka}{k^2+1}\right)^2,$$

which gives a representation of r as the sum of the squares of two rationals. If $k \geqslant 3$, we have $3k^2-8k = 3k(k-3)+k \geqslant 3$, whence

$$\frac{k^2-1}{2k} \geqslant \frac{4}{3} > \frac{b}{a} \quad \text{and so} \quad a_k = \frac{(k^2-1)a-2kb}{k^2+1} > 0.$$

Moreover it is easy to prove that a_k increases with k. Therefore numbers a_k are all different and, for $k \geqslant 3$, positive. This, for $k \geqslant 3$, gives different representations of r as sums of the squares of positive rationals. Thus we see that r admits infinitely many such representations.

Now we suppose that $r = a^2$, where a is a rational. Since $r \neq 0$, we may assume that $a > 0$. For natural k we have

$$r = \left(\frac{(k^2-1)a}{k^2+1}\right)^2+\left(\frac{2ka}{k^2+1}\right)^2.$$

As it is easy to prove, numbers $a_k = (k^2-1)a/(k^2+1)$ increase with k. Consequently, there are infinitely many representations of the numbers r into sums of the squares of positive rational numbers.

3. Given a natural number m, find a natural number n that has at least m different representations as the sum of the squares of two natural numbers.

Solution. Let $n = a^2$, where $a = (3^2+1)(4^2+1)\ldots((m+2)^2+1)$. The numbers $a/(k^2+1)$ are natural for any $k = 3, 4, \ldots, m+2$. Consequently also the numbers

$$a_k = \frac{k^2-1}{k^2+1}a, \quad b_k = \frac{2ka}{k^2+1} \quad (k = 3, 4, \ldots, m+2)$$

are natural. But, in virtue of the identity

$$a^2 = \left(\frac{k^2-1}{k^2+1}a\right)^2+\left(\frac{2ka}{k^2+1}\right)^2,$$

if $a_k = \frac{k^2-1}{k^2+1}a$, $b_k = \frac{2ka}{k^2+1}$, we have $n = a^2 = a_k^2+b_k^2$, $k = 3, 4, \ldots, m+2$. But

$$a_k-b_k = \frac{k^2-2k-1}{k^2+1}a = \frac{(k-1)^2-2}{k^2+1}a > 0 \quad \text{for} \quad k = 3, 4, \ldots, m+2$$

and

$$a_k = a-\frac{2a}{k^2+1}, \quad \text{whence} \quad a_3 < a_4 < \ldots < a_{m+2}.$$

Thus we see that the representations $n = a_k^2+b_k^2$, $k = 3, 4, \ldots, m+2$, are all different, their number being m. Therefore the number m has the required properties.

At the same time we have proved that for a given natural number m there exist at least m non-congruent Pythagorean triangles that have the same hypothenuse.

4. Given: a representation as the sum of two squares of a natural number n. Find a similar representation of the number $2n$.

Solution. If $n = a^2+b^2$, then $2n = (a+b)^2+(a-b)^2$.

§ 2. The average number of representations as sums of two squares. Now our aim is to consider the problem how to find all the representations of a given natural number as sums of two squares.

If n is representable as the sum of two squares, i.e. if

$$n = x^2+y^2, \tag{3}$$

then $n \geqslant x^2$ and $n \geqslant y^2$, whence $|x| \leqslant \sqrt{n}$, $|y| \leqslant \sqrt{n}$. Thus, to solve the problem, it is sufficient to substitute for x in (3) integers whose absolute values are not greater than $\sqrt{n}$ each, and see whether the number $n-x^2$ is a square or not. If $n-x^2$ is a square, then, putting $y = \pm\sqrt{n-x^2}$, we obtain a representation of n as the sum of two squares. If $n-x^2$ is not a square, such a representation is not obtained. It is plain that we may confine our consideration to non-negative x's only because the change of the sign of x does not cause any change of the value of $n-x^2$. It is worth-while to notice that the sequence n, $n-1^2$, $n-2^2$, $n-3^2$, ... has the following property: the differences of the consecutive numbers of the sequence are $1, 3, 5, \ldots$, i.e. they form the sequence of odd natural numbers.

Examples. Let $n = 10$. We form the sequence 10, 9, 6, 1. In this sequence the second term and the fourth term are squares so we put $x = \pm 1$, $y = \pm 3$ or $x = \pm 3$, $y = \pm 1$. Thus eight decompositions are obtained. They are

$$10 = 1^2+3^2 = 1^2+(-3)^2 = (-1)^2+3^2 = (-1)^2+(-3)^2 = 3^2+1^2$$
$$= 3^2+(-1)^2 = (-3)^2+1^2 = (-3)^2+(-1)^2.$$

Now let $n = 25$. We form the sequence 25, 24, 21, 16, 9, 0. Here 25, 16, 9, 0 are squares. Therefore for x, y the following values are obtained:

$$x = 0,\ y = \pm 5;\quad x = \pm 3,\ y = \pm 4;\quad x = \pm 4,\ y = \pm 3;\quad x = \pm 5,\ y = 0$$

(where all combinations of the signs $\pm$ are allowed). Thus 25 has 12 representations as sums of two squares.

Let $\tau(n)$ denote the number of all the representations of a natural number n as sums of two squares, two representations being regarded as different also when they differ in the order of summands only. As above, we find

$$\tau(1) = 4,\quad \tau(2) = 4,\quad \tau(3) = 0,\quad \tau(4) = 4,\quad \tau(5) = 8,$$
$$\tau(6) = 0,\quad \tau(7) = 0,\quad \tau(8) = 4,\quad \tau(9) = 4,\quad \tau(10) = 8.$$

As we have proved in § 5, Chapter V, each prime of the form $4k+1$ has a unique representation (apart from the order of the summands) as the sum of two squares. This shows that for any prime p of the form $4k+1$ we have $\tau(p) = 8$. The reasoning presented above shows that for any natural number n the inequality $\tau(n) \leqslant 4\sqrt{n}$ holds. Exercise 3 of § 1 implies that there is no upper bound for $\tau(n)$.

Now we are going to calculate the sum

$$T(n) = \tau(1)+\tau(2)+\ldots+\tau(n). \tag{4}$$

The number $\tau(k)$ is the number of solutions of the equation $x^2+y^2 = k$ in integers x, y. Hence the number $T(n)$ is the number of solutions of the inequalities

$$0 < x^2+y^2 \leqslant n. \tag{5}$$

We divide the solutions of (5) into classes by saying that two solutions belong to the same class if and only if the values of x are equal. We are going to find the number of solutions in each of these classes.

If $x = 0$, then, by (5), y may assume integral values such that $y^2 \leqslant n$, i.e. $|y| \leqslant \sqrt{n}$. As it is easy to verify, the number of such y's is $2[\sqrt{n}]$. If $x = k \neq 0$, then, by (5), we must have $k^2 \leqslant n$; so $|k| \leqslant \sqrt{n}$ and $y^2 \leqslant n-k^2$, whence $|y| \leqslant \sqrt{n-k^2}$. The number of those y's is $1+2[\sqrt{n-k^2}]$ (number 1 must be added since $y = 0$ is included). Since k may assume any of the values $\pm 1, \pm 2, \ldots, \pm[\sqrt{n}]$ and the sign $\pm$ has no influence on the value of k^2, we obtain

$$2[\sqrt{n}]+2\sum_{k=1}^{[\sqrt{n}]}\left(1+2[\sqrt{n-k^2}]\right) = 4[\sqrt{n}]+4\sum_{k=1}^{[\sqrt{n}]}[\sqrt{n-k^2}]$$

and so

$$T(n) = 4\sum_{k=0}^{[\sqrt{n}]}[\sqrt{n-k^2}]. \tag{6}$$

Thus, for example, for $n = 100$ we have

$$T(100) = 4\left([\sqrt{100}]+[\sqrt{99}]+[\sqrt{96}]+[\sqrt{91}]+[\sqrt{84}]+[\sqrt{75}]+[\sqrt{64}]+\right.$$
$$\left.+[\sqrt{51}]+[\sqrt{36}]+[\sqrt{19}]\right) = 4(10+9+9+9+8+8+7+6+4) = 316.$$

Sum (4) has a simple geometric interpretation. Since, as we have learned, number $1+T(n)$ is the number of pairs of integers that satisfy the inequality $x^2+y^2 \leqslant n$, it is equal to the number of points of the plane whose coordinates are integers (these being called *lattice* points) inside or on the circumference of a circle C whose centre is placed at the point $(0,0)$ and radius is equal to $\sqrt{n}$. To cut it short, number $1+T(n)$ is equal to the number of lattice points that are inside or on the circumference of circle C.

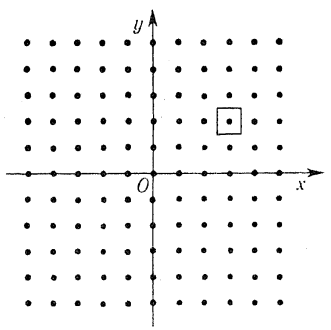

Fig. 1.

Now, to each lattice point we assign a square in which the middle point is a lattice point, the sides are parallel to the axes of coordinates and the area is equal to 1 (see Fig. 1). The area P covered by the squares assigned to the lattice point that are not outside the circle C is equal to the number of these points, and so it is equal to $1+T(n)$. The circle C_1 the centre of which is $(0,0)$ and radius $\sqrt{n}+\frac{1}{\sqrt{2}}$ contains (inside and on the circumference) all the points covered by the squares assigned to the points of the circle C. This is evident, since $1/\sqrt{2}$ is the greatest possible distance from a point of a square of area 1 to its middle points. Therefore the area P is less than the area of the circle C_1. Hence $P \leqslant \pi\left(\sqrt{n}+\frac{1}{\sqrt{2}}\right)^2$. On the other hand, the area of the circle C_2, whose centre is also $(0,0)$ and radius is $\sqrt{n}-\frac{1}{\sqrt{2}}$, is less than P, so $P > \pi\left(\sqrt{n}-\frac{1}{\sqrt{2}}\right)^2$. This, by the equality $P = 1+T(n)$, gives

$$\pi\left(\sqrt{n}-\frac{1}{\sqrt{2}}\right)^2 - 1 < T(n) < \pi\left(\sqrt{n}+\frac{1}{\sqrt{2}}\right)^2 - 1. \tag{7}$$

We note that $\pi\sqrt{2} < 5$ and that, for any natural number n, $0 < \frac{1}{2}\pi - 1 < 1 \leqslant \sqrt{n}$. Hence

$$\pi\left(\sqrt{n}+\frac{1}{\sqrt{2}}\right)^2 - 1 = \pi n + \pi\sqrt{2}\sqrt{n} + \tfrac{1}{2}\pi - 1 < \pi n + 6\sqrt{n},$$

$$\pi\left(\sqrt{n}-\frac{1}{\sqrt{2}}\right)^2 - 1 = \pi n - \pi\sqrt{2}\sqrt{n} + \tfrac{1}{2}\pi n - 1 > \pi n - 6\sqrt{n}.$$

From this, by (7), we obtain $\pi n - 6\sqrt{n} < T(n) < \pi n + 6\sqrt{n}$, whence $|T(n) - \pi n| < 6\sqrt{n}$ for any natural number n, whence

$$\left|\frac{T(n)}{n} - \pi\right| < \frac{6}{\sqrt{n}}. \tag{8}$$

From (8) and (4) it follows that

$$\lim_{n\to\infty} \frac{\tau(1)+\tau(2)+\ldots+\tau(n)}{n} = \pi,$$

which means that the mean value of the function $\tau(n)$ is π. This can also be expressed by saying that on the average there are π representations of a natural number as the sum of two squares. As we have found above, $T(100) = 316$ (i.e. natural numbers not greater than 100 have, on the average, 3.16 decompositions into the sum of two squares); similarly, by (6), we can easily find that $T(400) = 1256$, whence $T(400)/400 = 3.14$, and $T(1000) = 3148$, whence $T(1000)/1000 = 3.148$.

By formula (6), $T(n)$ can be calculated for any n (though the calculation may be very long), this, by (8), indicates a method of calculating the number π with a given accuracy.

In virtue of (8), we have $|T(n) - \pi n| < 6\sqrt{n}$ for any natural number n. In the year 1906, I used the method of Voronoï to find that there exist a constant A such that $|T(n) - \pi n| < A\sqrt[3]{n}$ (Sierpiński [1]). After that, stronger results were obtained by van der Corput and others; for the best result at present, see Chen Jing-Run [1].

As so far we have calculated the number of lattice points that are contained in a circle whose centre is $(0,0)$, which, of course, is a lattice point. In 1957, H. Steinhaus [1] proposed the following exercise: *prove that for any natural number n there exists such a circle on the plane as contains precisely n lattice points.*

We are going to show that if $p = (\sqrt{2}, \frac{1}{3})$, then for any natural number n there is a circle C_n with centre p containing precisely n lattice points inside.

Suppose that two different lattice points (x_1, y_1) and (x_2, y_2) are at equal distances from point p. Then

$$(x_1-\sqrt{2})^2 + (y_1-\tfrac{1}{3})^2 = (x_2-\sqrt{2})^2 + (y^2-\tfrac{1}{3})^2.$$

Hence

$$2(x_2-x_1)\sqrt{2} = x_2^2+y_2^2-x_1^2-y_1^2+\tfrac{2}{3}(y_1-y_2).$$

Since $\sqrt{2}$ is irrational, $x_1-x_2 = 0$, whence $y_2^2-y_1^2+\frac{2}{3}(y_1-y_2) = 0$, and so $(y_2-y_1)(y_2+y_1-\frac{2}{3}) = 0$. But $y_2+y_1-\frac{2}{3} \neq 0$ because y_1 and y_2

are integers, consequently $y_2-y_1=0$. This gives $x_1=x_2$ and $y_1=y_2$, contrary to the assumption that the points are different.

Now let n denote an arbitrary natural number. It is clear that any circle C with centre p and a radius large enough contains more than n lattice points. It is also clear that the number of lattice points contained in C is finite. Since, in virtue of what we proved above, the distances from p to the lattice points are all different, we may arrange the lattice points that are inside circle C in the sequence $p_1, p_2, \ldots, p_n, p_{n+1}, \ldots$ according to their distances from the point p. Let C_n denote the circle whose centre is p and radius is equal to the distance of point p_{n+1} from point p. It is plain that the only lattice points inside circle C_n are the points $p_1, p_2, \ldots, p_n$. Consequently, circle C_n possesses the required properties; the theorem of Steinhaus is thus proved.

It is not difficult to prove that there is no point p in the plane whose coordinates are rationals such that for any natural number n there exists a circle with centre p which contains precisely n lattice points (cf. Sierpiński [18], p. 26).

On the other hand, it can be proved that for any natural n there exists a circle whose centre has rational coordinates and which contains precisely n lattice points inside.

Let us mention here that H. Steinhaus has proved that for any natural number n there exists a circle with area n containing precisely n lattice points inside. However, the proof of this statement is difficult.

It can be proved that for any natural number n there exists a square that contains precisely n lattice points inside (cf. Sierpiński [18], pp. 28-30).

It is also true that for any natural number n in the three-dimensional space there exists a sphere that contains precisely n points whose coordinates are integers.

In order to prove this it is sufficient to note firstly that if u, v, w are rational numbers such that $u\sqrt{2}+v\sqrt{3}+w\sqrt{5}$ is a rational, then $u=v=w=0$, and secondly that any sphere whose centre is at the point $(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and radius is equal to 3 contains at least one point whose coordinates are all integers. From these two facts the proof is deduced as in the case of the circle in the plane.

J. Browkin has proved, that for any natural number n there exists a cube (in the three-dimensional space) that contains inside precisely n points whose coordinates are integers.

A. Schinzel [8] has proved that *for any natural number n there exists a circle on the circumference of which there are precisely n lattice points.* As a matter of fact, what he has proved is that if n is odd, i.e. $n=2k+1$, where k is a non-negative integer, then the circle with centre $(\frac{1}{3}, 0)$ and radius $5^k/3$ has the required property. If n is even, i.e. if $n=2k$, where

k is a natural number, then the circle with centre $(\frac{1}{2}, 0)$ and radius $5^{(k-1)/2}/2$ has the required property.

T. Kulikowski [1] has proved that for any natural number n there exists a sphere (in the three-dimensional space), on the boundary of which there are precisely n points whose coordinates are integers. He generalized this theorem for spheres in spaces of an arbitrary $\geqslant 3$ dimension.

Rational points (i.e. points whose coordinates are rational numbers) on the circumference of a circle have also been investigated. There exist circles in the plane in which there are no rational points; for example, such is the circle $x^2+y^2=3$. There are circles on which there lies precisely one rational point, for example, on the circle $(x-\sqrt{2})^2+(y-\sqrt{2})^2=4$ there is precisely one rational point, namely the point $(0, 0)$. There are also circles on which there are precisely two rational points, for example, such is the circle $x^2+(y-\sqrt{2})^2=3$, the only rational points on it being $(1, 0)$ and $(-1, 0)$.

In general, we prove that *if there are there rational points on a circle, then there are infinitely many rational points on it.* It is easy to prove that if there are three rational points on a circle, then the centre of the circle is a rational point and the square of the radius of the circle is also rational. Since by subtracting a rational number from two rational numbers successively we again obtain rational numbers, then, without any loss of generality, we may assume that the centre of the circle is the point $(0, 0)$. Denote this circle by C. It is not difficult to prove that if C contains at least one rational point, then it must contain infinitely many rational points. In fact, if a, b are rationals such that $a^2+b^2=r^2$, then for any rational number t the point (x, y) where $x=\dfrac{2at+b(1-t^2)}{1+t^2}$, $y=\dfrac{a(1-t^2)-2bt}{1+t^2}$ is rational and $x^2+y^2=r^2$.

We sum up the facts thus obtained in saying that for a given circle only the following cases are possible: it contains no rational points, it contains precisely one rational point, it contains precisely two rational points, or finally, it contains infinitely many rational points. It can be proved that, in the last case, rational points form a dense subset of the circle, which means that on any arc of the circle there is a rational point.

It has been proved (cf. Sierpiński [20]) that if r^2 is a rational number, then the circle C with radius r contains infinitely many points such that the distance of any two of them is a rational number. As an immediate consequence of this we infer that for any natural number n there exists a circle which contains n points such that the distance of any two of them is a natural number. This again has an important consequence,

namely that for any natural n there exists a set consisting of n points no three of which lie on one line such that the distance of any two of them is a natural number. This theorem was first proved by W. H. Anning and P. Erdös (their proof was different)(1). The authors proved also that if in an infinite set of points in the plane the distance of any two points of the set is integral, then all the points lie on a straight line (cf. Erdös [7] and Trost [2]).

EXERCISE. Prove that the set of rational points of the plane can be divided into two subsets, one having finitely many points in common with any vertical line, the other having finitely many points in common with any horizontal line.

Proof. As is easy to see, the condition will be satisfied if the first subset consists of the point $\left(\frac{l}{m}, \frac{r}{s}\right)$, the fractions being irreducible and such that the numerators are integral and the denominators natural, and that they satisfy the relation $|l|+m < |r|+s$. The second subset comprises all the rest of the rational points of the plane.

It can be proved that the set of points in the three-dimensional space whose coordinates are rational can be divided into three parts such that each part has finite intersection with any line parallel to a coordinate line (fixed for the part). The same statement for the set of all points of the three-dimensional space is equivalent to the continuum hypothesis (cf. Sierpiński [13] and [21], p. 397).

§ 3. Sums of two squares of natural numbers.

THEOREM 2. *A natural number n is the sum of the squares of two natural numbers if and only if all prime factors of the form $4k+3$ of the number n have even exponents in the standard factorization of n into primes and either the prime 2 has an odd exponent (in the factorization of n) or n has at least one prime divisor of the form $4k+1$.*

Proof. Suppose that there exists a natural number which is the sum of the squares of two natural numbers, and has the following properties: it does not possess a prime divisor of the form $4k+1$, and in its factorization into primes the prime 2 has even exponent $\geqslant 0$. Let n be the least natural number with this properties. Since it is the sum of the squares of two natural numbers, by theorem 1 all prime factors of n of the form $4k+3$ have even exponents in the standard form of n. Consequently, $n = 2^{2k}m^2$, where m is an odd natural number and k is an integer $\geqslant 0$. Thus we may write $2^{2k}m^2 = a^2+b^2$, where a, b are natural numbers. If $k > 0$, then the left-hand side of the last equality is divisible by 4; consequently the numbers a, b, are both even, i.e. $a = 2a_1$, $b = 2b_1$, whence $2^{2(k-1)}m^2 = a_1^2+b_1^2 < n$, contrary to the definition of n. Hence $k = 0$ and so $n = m^2 = a^2+b^2 > 1$. The numbers a, b must be relatively prime because in the case $(a, b) = d > 1$ we would have

(1) Anning and Erdös [1]; see also Hadwiger [1], p. 85, where a list of references is given.

$a = da_2$, $b = db_2$, where a_2, b_2 are natural numbers, whence $m = dm_1$ and $m_1^2 = a_2^2+b_2^2 < m^2 = n$, contrary to the definition of n. So $(a, b) = 1$. But, since m is odd and > 1 (having no prime divisor of the form $4k+1$), it has a prime divisor $p = 4k+3$. This implies that $p \mid a^2+b^2$, whence $a^2 \equiv -b^2 \pmod p$. If we raise each side of the last congruence to the $(2k+1)$th power, then, by the fact that $2(2k+1) = p-1$ and by the theorem of Fermat, we obtain $1 \equiv (-1)^{2k+1} \pmod p$, which is impossible.

We have thus proved that a natural number that is the sum of the squares of two natural numbers has the following property: either in its factorization into prime factors the prime 2 has an odd exponent, or it has a prime divisor of the form $4k+1$. Moreover, by theorem 1, it follows that all prime divisors of the form $4k+3$ have even exponents in the factorization of the number into primes. This shows that the condition of theorem 2 is necessary.

Now, suppose that a natural number n satisfies the conditions of the theorem. Thus we have either $n = 2m^2$ or $n = 2^\alpha m^2 l$, where $\alpha = 0$ or 1 and l is the product of prime factors of the form $4k+1$. If $n = 2m^2$, then $n = m^2+m^2$, and so it is the sum of the squares of two natural numbers. Suppose that $n = 2^\alpha m^2 l$, where l is the product of primes of the form $4k+1$. By theorem 9, Chapter V, each of the factors is the sum of two positive squares. But the product of two odd numbers, each of them the sum of two positive squares, is again the sum of two positive squares. The argument to this is that, if $n_1 = a^2+b^2$, $n_2 = c^2+d^2$, where n_1, n_2 are odd, then one of the numbers a and b, say a, must be odd, the other being even; the same is true for the numbers c, d; so let c be odd, d even. Then $n_1 n_2 = (a^2+b^2)(c^2+d^2) = (ad+bc)^2+(ac-bd)^2$, where $ac-bd$ is odd, and so $\neq 0$. Thus we see that the number $n_1 n_2$ is the sum of the squares of two natural numbers. By induction, we infer that the same remains true for an arbitrary number of factors of the form $4k+1$. Hence we conclude that the number l is the sum of the squares of two natural numbers, i.e. $l = a^2+b^2$, whence $m^2 l = (ma)^2+$ $+(mb)^2$ and $2m^2 l = (ma+mb)^2+(ma-mb)^2$ and $ma-mb \neq 0$ (because a must be different from b since the number $l = a^2+b^2$ is odd). Thus we see that in any event the number n is the sum of the squares of two natural numbers. Therefore the condition of theorem 2 is sufficient.

Theorem 2 is thus proved.

From theorem 2 it follows that in order that a square n^2 be the sum of two squares of two natural numbers it is necessary and sufficient that the number n should have at least one prime divisor of the form $4k+1$. This can be expressed by saying that

A natural number n is a hypotenuse of a Pythagorean triangle if and only if n has at least one prime divisor of the form $4k+1$.

Cf. also the corollary to exercise 3, § 1.

EXERCISES. **1.** Prove that a natural number n is the sum of the squares of two different natural numbers if and only if 1° the primes of the form $4k+3$ which appear in the factorization of n into prime factors have even exponents, 2° the number n has at least one prime divisor of the form $4k+1$.

Proof. The necessity of condition 1° follows from theorem 1. Suppose that a natural number n does not satisfy condition 2°, i.e. that it has no prime divisor of the form $4k+1$. Conesquently, if $n = a^2+b^2$ for two different natural numbers a, b, then, for $d = (a, b)$, we have $n = d^2(a_1^2+b_1^2)$, where $a = da_1$, $b = db_1$ and a_1, b_1 are different relatively prime natural numbers. Number $a_1^2+b_1^2$ has no prime divisor of the form $4k+1$, and so, since $(a_1, b_1) = 1$, the reasoning used in the proof of theorem 2 shows that number $a_1^2+b_1^2$ has no prime divisor of the form $4k+3$, either. Therefore $a_1^2+b_1^2 = 2^s$, where s is a natural number > 1, since a_1, b_1 are different natural numbers. Consequently, number $a_1^2+b_1^2$ is divisible by 4, whence it follows that the numbers a_1, b_1 are even, but this contradicts the fact that $(a_1, b_1) = 1$.

Now suppose that a natural number n satisfies conditions 1° and 2°. Then, by theorem 2, we have $n = a^2+b^2$, where a, b are natural numbers. If $a = b$, then $n = 2a^2$ and, since n satisfies condition 2°, it has a prime divisor of the form $4k+1$, so, in virtue of what we have shown above, a is the hypotenuse of a Pythagorean triangle. This means that $a^2 = c^2+d^2$, where c, d are natural numbers. Clearly $c \neq d$ since, if $c = d$, then $a^2 = 2c^2$, which, in view of the fact that $\sqrt{2}$ is irrational, is impossible. Hence $n = 2a^2 = (c+d)^2+(c-d)^2$, where $c-d \neq 0$ and $c+d \neq c-d$ (since d is a natural number). Consequently, n is the sum of the squares of two different natural numbers. Thus we see that conditions 1° and 2° are sufficient. This completes the proof.

2. Prove that a natural number n is the sum of the squares of two relatively prime natural numbers if and only if n is divisible neither by 4 nor by a natural number of the form $4k+3$.

Proof. Suppose that a natural number n is the sum of the squares of two relatively prime natural numbers: $n = a^2+b^2$. If $n = 4k$, then the numbers a, b are both even, contrary to $(a, b) = 1$. If n has a divisor of the form $4k+3$, then, as we know, it has a prime divisor of this form, which, as was shown in the proof of theorem 2, cannot divide the sum of the squares of two relatively prime natural numbers. Thus we see that the condition is necessary. Suppose that a natural number n satisfies the condition. If $n = 2$, then $n = 1^2+1^2$, and so it is the sum of the squares of two relatively prime natural numbers. If $n > 2$, then the condition implies that n is the product of prime numbers of the form $4k+1$ or the product of number 2 and primes of the form $4k+1$. In the former case n is odd and each of the prime factors of n is the sum of the squares of two relatively prime natural numbers. Hence, by lemma 2 and by exercise 8 of § 5, Chapter V, simple induction shows that n is the sum of the squares of two relatively prime natural numbers. In the latter case, i.e. if n is the product of number 2 and the primes of the form $4k+1$, we have $n = 2(a^2+b^2)$, where a, b are two relatively prime natural numbers. Since a^2+b^2 is odd, one of the numbers a, b is odd and the other is even. We have $n = (a+b)^2+(a-b)^2$, where $a+b$ and $a-b$ are odd natural numbers; moreover, they are relatively prime because if $d \mid a+b$ and $d \mid a-b$, where d is a natural number, then $d \mid 2a$ and $d \mid 2b$; since d, as a divisor of an odd number $a+b$, is odd, we have $d \mid a$ and $d \mid b$, which, in virtue of $(a, b) = 1$, implies $d = 1$. Therefore $(a+b, a-b) = 1$. We have thus proved that the condition is sufficient and the proof is completed.

§ 4. Sums of three squares.

THEOREM 3. *A natural number n can be the sum of three squares only if it is not of the form $4^l(8k+7)$, where k, l are integers $\geqslant 0$.*

Proof. Suppose that there exist natural numbers of the form $4^l(8k+7)$, where k, l are integers $\geqslant 0$, that are the sums of the squares of three integers. Let n be the least of them. We then have $n = 4^l(8k+1) = a^2+b^2+c^2$, where a, b, c are integers. If among the numbers a, b, c there is precisely one odd number, then the sum of their squares is of the form $4t+1$, and so it is different from n. If two of the numbers a, b, c are odd, then the sum of their squares is of the form $4t+2$, and so it is $\neq n$. If all the numbers a, b, c are odd, then the sum of their squares is of the form $8t+3$, and so it is $\neq n$. Consequently, each of the numbers a, b, c must be even. We put $a = 2a_1$, $b = 2b_1$, $c = 2c_1$, where a_1, b_1, c_1 are integers. Hence $4^{l-1}(8k+7) = a_1^2+b_1^2+c_1^2$, contrary to the definition of n. Thus we have proved that no natural number of the form $4^l(8k+7)$, where k, l are non-negative integers, can be the sum of the squares of three integers, and this is precisely what theorem 3 asserts.

It can be shown that the condition of theorem 3 is also sufficient in order that a number n be the sum of the squares of three integers. Gauss was the first to prove that *every natural number which is not of the form $4^l(8k+7)$, k and l being non-negative integers, is the sum of the squares of three integers.*

The original proof of Gauss was simplified later by Lejeune Dirichlet and Landau (cf. Landau [2], vol. I, pp. 114-125). Recently N. C. Ankeny [1] gave an "elementary" proof of the theorem of Gauss. His proof is based on the theorem of Minkowski concerning lattice points contained in a convex body and on the theorem on arithmetical progression (cf. Mordell [7]).

As an immediate consequence of the theorem of Gauss we infer that every natural number of the form $8k+3$ is the sum of the squares of three integers, which, of course, must all be odd. Thus

$$8k+3 = (2a+1)^2+(2b+1)^2+(2c+1)^2,$$

where a, b, c are non-negative integers. Hence

$$k = \frac{a(a+1)}{2} + \frac{b(b+1)}{2} + \frac{c(c+1)}{2} = t_a+t_b+t_c.$$

Thus the theorem of Gauss implies a theorem (first formulated by Fermat) stating that *any natural number is the sum of three or fewer triangular numbers.*

As regards numbers of the form $8k+1$, there is a conjecture that except 1 and 25 all of them are sums of the squares of three natural numbers. It follows from the results of A. Schinzel [12] and J. D. Swift [1] that this is true up to 2500000. Among the numbers of the form $8k+5$ that are less than 2500000 only the numbers 5, 13, 37 and 85 are not sums of the squares of three natural numbers. No number of the form $8k+7$ is the sum of the squares of three integers, and so, *a fortiori*, it cannot be the sum of the squares of three natural numbers. A number of the form $4k$ is the sum of the squares of three natural numbers if and only if k itself is the sum of three such squares. In fact, if $4k = a^2+b^2+c^2$, where a, b, c are natural numbers, then, as is easy to see, the numbers a, b, c must be even, and so $a = 2a_1$, $b = 2b_1$, $c = 2c_1$, where a_1, b_1, c_1 are natural numbers. Hence $k = a_1^2+b_1^2+c_1^2$. Conversely, the last equality implies that $4k = (2a_1)^2+(2b_1)^2+(2c_1)^2$. From this we easily deduce that no number of the form 2^n, $n = 1, 2, \ldots$ is the sum of three positive squares. But $8\cdot 3n^2 = (2n)^2+(2n)^2+(4n)^2$, and so we see that among the numbers of the form $8k$ there exist infinitely many natural numbers which are sums of the squares of three natural numbers and infinitely many numbers which are not sums of three squares. As regards the numbers $8k+2$, G. Pall [1] says: "It is conjectured that every $2(8n+1)$ except 2 is a sum of three positive squares". As noticed by A. Schinzel [1] this conjecture is false: the number $2(8\cdot 8+1) = 130$ is not the sum of the squares of three natural numbers (cf. exercise 1, below).

A number of the form $8k+4$ is the sum of the squares of three natural numbers if and only if number $2k+1$ has this property. Consequently, numbers $8(4k+3)+4 = 4(8k+7)$, $k = 0, 1, 2, \ldots$ are not sums of the squares of three natural numbers. On the other hand, numbers $8(4k+1)+4 = 4(8k+3)$, $k = 0, 1, 2, \ldots$ are sums of the squares of three natural numbers. Any number of the form $8k+6$ is the sum of the squares of three natural numbers because, as follows from the theorem of Gauss, it is the sum of the squares of three integers; it cannot, however, be the sum of two squares because $8k+6 = 2(4k+3)$.

By means of the theory of quadratic forms one proves that any sufficiently large number of the form $8k+1$, $8k+2$, $8k+5$ is the sum of the squares of three natural numbers. (cf. Schinzel [12] and Grosswald, Calloway and Calloway [1]).

Denote by $r_3(n)$ the number of different representations of a number n as the sum of the squares of three integers. For $n \leqslant 10$ we have $r_3(1) = 6$, $r_3(2) = 12$, $r_3(3) = 8$, $r_3(4) = 6$, $r_3(5) = 24$, $r_3(6) = 24$, $r_3(7) = 0$, $r_3(8) = 12$, $r_3(9) = 30$, $r_3(10) = 24$.

Theorem 3 implies that for infinitely many n's we have $r_3(n) = 0$.

As regards the number $T_3(n) = r_3(1)+r_3(2)+\ldots+r_3(n)$, a geometric argument, similar to that used in § 2 for the sum of two squares (we

replace rational points of the plane by points of the three-dimensional space, whose coordinates are integers and we consider spheres and cubes instead of circles and squares, respectively), gives the inequality

$$\frac{4}{3}\pi\left(\sqrt{n}-\frac{\sqrt{3}}{2}\right)^3 - 1 < T_3(n) < \frac{4}{3}\pi\left(\sqrt{n}+\frac{\sqrt{3}}{2}\right)^3 - 1.$$

From this we obtain for all natural numbers n the evaluation

$$|T_3(n) - \tfrac{4}{3}\pi n\sqrt{n}\,| < 10n,$$

whence it follows

$$\lim_{n\to\infty}\frac{T_3(n)}{\frac{4}{3}\pi n\sqrt{n}} = 1.$$

Denote by $f(x)$ the number of natural numbers x which are representable as sums of three squares. From Gauss's theorem it follows that the number $x-f(x)$ is precisely the number of numbers x which are of the form $4^l(8k+7)$, where k, l are integers $\geqslant 0$. Therefore, for a given non-negative integer l we have $8(k+1)-1 \leqslant 4^{-l}x$, and so $k+1 \leqslant \frac{1}{8}(4^{-l}x+1)$, the number of k's $\geqslant 0$ being clearly $[\frac{1}{8}(4^{-l}x+1)]$. Hence, as an immediate consequence, we obtain

$$x-f(x) = \sum_{l=0}^{[x]}\left[\frac{4^{-l}x+1}{8}\right].$$

If $l > \log x/\log 4$, then $4^l > x > x/7$, whence $(4^{-l}x+1)/8 < 1$. Consequently

$$x-f(x) = \sum_{l=0}^{[\log x/\log 4]}\left[\frac{4^{-l}x+1}{8}\right],$$

and so

$$x-f(x) = \sum_{l=0}^{[\log x/\log 4]}\frac{4^{-l}x+1}{8} - \alpha\left(\frac{\log x}{\log 4}+1\right), \qquad \text{where} \qquad 0 \leqslant \alpha < 1.$$

But

$$\sum_{l=[\log x/\log 4]+1}^{\infty} 4^{-l} = \frac{4}{3}\cdot 4^{-[\log x\log 4]-1} < \frac{4}{3}\cdot 4^{-\log x/\log 4} = \frac{4}{3x}.$$

Since $\sum_{l=0}^{\infty}\frac{4^{-l}x}{8} = \frac{x}{6}$, we obtain $\lim_{x\to+\infty}\frac{x-f(x)}{x} = \frac{1}{6}$, whence

$$\lim_{x\to+\infty}\frac{f(x)}{x} = \frac{5}{6}.$$

This formula was discovered by Landau in 1908. Let us mention here that M. C. Chakrabarti [1] has investigated the function

$$g(x) = \frac{f(x) - \frac{5}{6}x}{\log x}$$

and has proved that $\liminf_{x\to+\infty} g(x) = 0$, $\limsup_{x\to+\infty} g(x) = \frac{1}{\log 8}$ and that the values of the function $g(x)$ are dense in the interval $\left(0, \frac{1}{\log 8}\right)$.

EXERCISES. **1.** Prove that 130 is not representable as the sum of three positive squares.

Proof. Suppose that $130 = a^2+b^2+c^2$, where a, b, c are natural numbers. Without loss of generality we may assume that $a \geqslant b \geqslant c$. Consequently, $a^2+1+1 \leqslant 130 \leqslant 3a^2$, whence $43 < a^2 < 128$, and so $7 \leqslant a < 11$. But $130-7^2 = 81 = 3^4$, $130-8^2 = 66 = 2\cdot 3\cdot 11$, $130-9^2 = 49 = 7^2$, $130-10^2 = 30 = 2\cdot 3\cdot 5$, $130-11^2 = 9 = 3^2$; thus, looking at the factorizations of numbers 81, 66, 49, 30, 9 into primes, we see that none of them satisfies the condition of theorem 2, and so none of them is the sum of the squares of two natural numbers. Thus the assumption that 130 is the sum of the squares of three natural numbers leads to a contradiction.

Remark. It is easy to prove that 130 is the least natural number of the form $2(8k+1)$ which is not the sum of the squares of three natural numbers.

2. Using the theorem of Gauss prove that a natural number is the sum of the squares of three rational numbers if and only if it is the sum of the squares of three integers.

Proof. Suppose that a natural number n is the sum of the squares of three rational numbers. Reducing all the three rational numbers to the same denominator, we may write $m^2n = a^2+b^2+c^2$, where a, b, c are integers. If $n = 4^l(8k+7)$, where k, l are integers $\geqslant 0$, then, putting $m = 2^r(2s+1)$, s and r being non-negative integers, we obtain $m^2n = 4^{k+r}(8t+7)$, where $k+r$ and t are non-negative integers. But, in virtue of theorem 3, this is impossible because $m^2n = a^2+b^2+c^2$. Consequently, number n cannot be of the form $4^l(8k+7)$, where k, l are integers. Thus, by the theorem of Gauss, it is the sum of the squares of three integers. Thus we see that the condition is necessary; plainly it is sufficient as well.

3. Prove that there are no rational numbers x, y, z that satisfy the equation $x^2+y^2+z^2+x+y+z = 1$.

Proof. The equation is equivalent to the equation

$$(2x+1)^2+(2y+1)^2+(2z+1)^2 = 7. \tag{9}$$

In the proof of exercise 2 we proved (without using Gauss's theorem) that no number of the form $4^l(8k+7)$, where k and l are non-negative integers, can be the sum of the squares of three rationals. Thus, in particular, number 7 cannot be such a sum, which, in turn, implies that numbers x, y, z cannot satisfy equation (9).

4. Making use of the theorem of Gauss prove that any odd natural number is of the form $a^2+b^2+2c^2$, where a, b, c are integers.

Proof. Let t be an arbitrary non-negative integer. Number $4t+2$ is not of the form $4^l(8k+7)$, where k, l are non-negative integers. Therefore, by Gauss's theorem, $4t+2 = x^2+y^2+z^2$, where x, y, z are integers. Not all of them are even, since the left-hand side of the equality is not divisible by 4. However, the number of odd numbers among them must be even (since the left-hand side is even); therefore let x, y be odd, z being even, i.e. $z = 2c$. The numbers $x+y$ and $x-y$ are even, and so $x+y = 2a$, $x-y = 2b$, whence $x = a+b$, $y = a-b$. Hence $4t+2 = (a+b)^2+(a-b)^2+4c^2$, whence $2t+1 = a^2+b^2+2c^2$, where a, b, c are integers. This completes the proof.

5. Deduce from the theorem of Gauss that any natural number is either of the form $a^2+b^2+c^2$ or of the form $a^2+b^2+2c^2$, where a, b, c are integers.

Proof. If a natural number is not a sum of three squares, then, by Gauss's theorem, it is of the form $4^l(8k+7)$, where k, l are non-negative integers. But, by exercise 4, $8k+7 = x^2+y^2+2z^2$, where x, y, z are integers. Hence $4^l(8k+7) = (2^lx)^2+(2^ly)^2+2(2^lz)^2$, and so our number is of the form $a^2+b^2+2c^2$, where a, b, c are integers.

6. Prove that if a number $\neq 0$ is representable as the sum of the squares of three rationals, then it has infinitely many representations in this form.

Proof. This theorem is an immediate consequence of the theorem proved in exercise 2 of § 1 which says that a number $\neq 0$ which is representable as the sum of the squares of two rationals has infinitely many representations in this form.

7. Prove that the theorem of E. Lionnet stating that each odd natural number is the sum of the squares of four integers two of which are consecutive numbers is a consequence of the theorem of Gauss.

Proof. Let $n = 2k+1$, where $k = 0, 1, 2, \ldots$ From the theorem of Gauss it follows that the number $4k+1$ is the sum of three squares; consequently $4k+1 = x^2+y^2+z^2$. As it is easy to notice, one of the numbers x, y, z must be odd, the other being even. Let $x = 2a$, $y = 2b$, $z = 2c+1$, where a, b, c are integers. Hence $n = 2k+1 = (a+b)^2+(a-b)^2+c^2+(c+1)^2$, which was to be proved.

8. Show that there exist infinitely many primes of the form $a^2+b^2+c^2+1$, where a, b, c are natural numbers. For the proof use Gauss's theorem.

Proof. By theorem 1, Chapter IX, there exist infinitely many primes of the form $8k+7$. If p is a prime of this form, then $p-1 = 8k+6$. But, as we have already learned, Gauss's theorem implies that any number of the form $8k+6$ is the sum of the squares of three natural numbers. Thus $p-1 = a^2+b^2+c^2$, where a, b, c are natural numbers, and so $p = a^2+b^2+c^2+1$.

9. Find an example showing that the product of two numbers, each of them the sum of three squares, need not be a sum of three squares.

Solution. $63 = 3\cdot 21 = (1^2+1^2+1^2)(1^2+2^2+4^2)$. The number 63, however, being of the form $8k+7$, cannot be the sum of three squares.

10. Deduce from the theorem of Gauss that every natural number is representable as the sum of ten (or fewer) squares of odd numbers [1].

Proof. As we know, Gauss's theorem implies that every natural number of the form $8k+3$, where k is an integer $\geqslant 0$, is the sum of the squares of three odd numbers. On the other hand, any natural number $n > 3$ is of the form $8k+3+r$, where $r = 0, 1, 2, 3, 4, 5, 6, 7$. We see that r is the sum of at most seven squares of the number 1, consequently, n is the sum of the squares of at most 10 squares of odd natural numbers. There exist infinitely many natural numbers that are not representable as sums of fewer than 10 squares of natural numbers (cf. exercise 12, below).

---

[1] This theorem has been stated without proof by F. Pollock [1], and has been proved by S. Turski [1].

Remark. The theorem, which we have just proved, and which we shall call for the time being theorem T, implies that every natural number of the form $8k+3$, where k is a non-negative integer, is the sum of the squares of three odd numbers.

In fact, by theorem T, if $k \geqslant 0$, then

$$(*) \qquad 8k+3 = n_1^2+n_2^2+\ldots+n_s^2,$$

where s is a natural number $\leqslant 10$, $n_1, n_2, \ldots, n_s$ being odd. Thus we have $n_i^2 \equiv 1 \pmod 8$ for $i = 1, 2, \ldots, s$ and so, by (*), $3 \equiv s \pmod 8$, which, in virtue of the inequality $1 \leqslant s \leqslant 10$, proves that $s = 3$. Therefore, by (*), the number $8k+3$ is the sum of the squares of three odd numbers (cf. Sierpiński [8]).

11. Prove that the sth power, s being a natural number, of the sum of the squares of three integers, is also the sum of three squares.

Proof. If s is 1 or 2, the proof is immediate. Therefore it is sufficient to consider the case where s is of the form $2k+3$, k being a non-negative integer. We have $n^{2k+3} = (n^k)^2 n^3$, therefore it is sufficient to prove our theorem for $s = 3$. But this follows immediately from the identity of Catalan:

$$(x^2+y^2+z^2)^3 = x^2(3z^2-x^2-y^2)^2+y^2(3z^2-x^2-y^2)^2+z^2(z^2-3x^2-3y^2)^2.$$

12. Prove that there exist infinitely many natural numbers that are not representable as sums of fewer than ten squares of odd natural numbers.

Proof. Such are numbers of the form $72k+42$, where $k = 0, 1, 2, \ldots$ In fact, suppose that a natural number $n = 72k+42$ is the sum of the squares of $s < 10$ odd natural numbers. Since the square of an odd natural number is $\equiv 1 \pmod 8$, we have $n \equiv s \pmod 8$, whence, since $n = 72t+42 \equiv 2 \pmod 8$, we have $s \equiv 2 \pmod 8$. But this, by the fact that $0 < s < 10$, gives $s = 2$. Consequently, n is the sum of two squares. But this is impossible because $n = 3(24t+14) = 9(8t+4)+6$ is divisible by 3 but not divisible by 9. Similarly, we can prove that none of the numbers $72k+66$, $k = 0, 1, 2, \ldots$, is the sum of fewer than ten squares.

§ 5. Representation by four squares.

We are going to prove the following theorem known as Lagrange's theorem.

THEOREM 4 (Lagrange). *Every non-negative integer is representable as a sum of four squares.*

LEMMA 1. *Suppose that an odd prime p is a divisor of the sum of the squares of four integers, at least one of which is not divisible by p. Then p is the sum of four squares.*

Proof of lemma 1. Suppose that a prime p satisfies the assumption of the lemma. Then there is a multiple of p which is the sum of the squares of four integers not all of which are divisible by p. Let n be the least such multiple of p. We then have

$$(10) \qquad n = mp,$$

where m is a natural number, and

$$(11) \qquad n = a^2+b^2+c^2+d^2,$$

where a, b, c, d are integers, of which at least one, say a, is not divisible by p. Let a_0, b_0, c_0, d_0 be integers such that

$$(12) \qquad a_0 \equiv a \pmod p, \quad b_0 \equiv b \pmod p, \quad c_0 \equiv c \pmod p, \quad d_0 \equiv d \pmod p$$

and

$$(13) \qquad |a_0| < p/2, \quad |b_0| < p/2, \quad |c_0| < p/2, \quad |d_0| < p/2$$

(in order to find the number a, for instance, it suffices to find the remainder r left by a divided by p and to put $a_0 = r$ if $r < p/2$, or $a_0 = r-p$ if $r > p/2$).

Since a is not divisible by p, so is a_0 and, by a successive application of (12), (10) and (11), we have

$$a_0^2+b_0^2+c_0^2+d_0^2 \equiv a^2+b^2+c^2+d^2 \equiv 0 \pmod p.$$

Hence, by the definition of n, in view of (13), we infer

$$n \leqslant a_0^2+b_0^2+c_0^2+d_0^2 \leqslant 4(p/2)^2.$$

Consequently, $n < p^2$, which, by (10), implies $mp < p^2$, whence

$$(14) \qquad m < p.$$

In virtue of (10) and (11), it remains to prove that $m = 1$. Suppose that $m \neq 1$. Since m is a natural number, by (14) we have

$$(15) \qquad 1 < m < p.$$

We find natural numbers a_1, b_1, c_1, d_1 that satisfy the conditions

$$(16) \qquad a_1 \equiv a \pmod m, \quad b_1 \equiv b \pmod m, \quad c_1 \equiv c \pmod m, \quad d_1 \equiv d \pmod m$$

and

$$(17) \qquad |a_1| \leqslant m/2, \quad |b_1| \leqslant m/2, \quad |c_1| \leqslant m/2, \quad |d_1| \leqslant m/2.$$

By (16) we see that $a_1^2+b_1^2+c_1^2+d_1^2 \equiv a^2+b^2+c^2+d^2 \pmod m$, whence, by (11) and (10), we obtain $m \mid a_1^2+b_1^2+c_1^2+d_1^2$, so

$$(18) \qquad a_1^2+b_1^2+c_1^2+d_1^2 = ml,$$

where l is an integer $\geqslant 0$.

If $l = 0$, then by (18), $a_1 = b_1 = c_1 = d_1 = 0$, whence, by (16) all the numbers a, b, c, d are divisible by m, whence, by (11), n is divisible by m^2 and so, by (10), $m \mid p$, contrary to (15), since p is a prime. Consequently, l is a natural number.

Suppose that

$$(19) \qquad |a_1| = |b_1| = |c_1| = |d_1| = m/2,$$

this being possible only in the case of even m, i.e. when

$$(20) \qquad m = 2k,$$

where k is a natural number. The congruence $a_1 \equiv a \pmod m$ gives $a = a_1 + mt$, where t is an integer. Therefore, by (20) and (19) we have $a = \pm k + 2kt = (2t \pm 1)k = k_1 k$, where k_1 is odd. Similarly we find

$$a = k_1 k, \quad b = k_2 k, \quad c = k_3 k, \quad d = k_4 k,$$

where k_1, k_2, k_3, k_4 are all odd numbers. Hence, by (20), (10) and (11) we obtain $n = 2kp = k^2(k_1^2+k_2^2+k_3^2+k_4^2)$. Consequently, $2p = k(k_1^2+k_2^2+k_3^2+k_4^2)$. The square of an odd number is congruent to $1 \pmod 4$, whence we infer that the second factor of the right-hand side of the last equality is divisible by 4, and so $2 \mid p$, contrary to the assumption. This shows that equalities (19) cannot hold. Consequently, for at least one of the inequalities of (17) the equality is impossible. This implies that $a_1^2+b_1^2+c_1^2+d_1^2 < 4 \cdot \frac{m^2}{4}$, whence, by (18), we obtain $ml < m^2$, so

$$l < m. \tag{21}$$

Consider the identity of Euler

$$(a^2+b^2+c^2+d^2)(a_1^2+b_1^2+c_1^2+d_1^2) = (aa_1+bb_1+cc_1+dd_1)^2 + \tag{22}$$
$$+ (ab_1-ba_1+cd_1-dc_1)^2 + (ac_1-ca_1+td_1-db_1)^2 + (ad_1-da_1+bc_1-cd_1)^2$$

Its left-hand side is, by (11), (10) and (18), equal to m^2lp.

By (16) we have

$$a_1 = a+ma_2, \quad b_1 = b+mb_2, \quad c_1 = c+mc_2, \quad d_1 = d+md_2, \tag{23}$$

where a_2, b_2, c_2, d_2 are integers. By (11) and (10), formulae (23) give

$$\begin{aligned} aa_1+bb_1+cc_1+dd_1 &= a^2+b^2+c^2+d^2+m(aa_2+bb_2+cc_2+dd_2) \\ &= m(p+aa_1+bb_1+cc_1+dd_1) = mt_1, \\ ab_1-ba_1+cd_1-dc_1 &= m(ab_2-ba_2+cd_2-dc_2) = mt_2, \\ ac_1-ca_1+bd_1-db_1 &= m(ac_2-ca_2+bd_2-db_2) = mt_3, \\ ad_1-da_1+bc_1-cb_1 &= m(ad_2-da_2+bd_2-cb_2) = mt_4, \end{aligned}$$

where t_1, t_2, t_3, t_4 are integers. Substituting them in the right-hand side of (22), the left-hand side of which is m^2lp, we obtain $m^2lp = m^2(t_1^2+t_2^2+t_3^2+t_4^2)$, whence

$$lp = t_1^2+t_2^2+t_3^2+t_4^2. \tag{24}$$

If the numbers t_1, t_2, t_3, t_4 were all divisible by p, then $p^2 \mid lp$, and so $p \mid l$, which is impossible, since l is a natural number and, by (21) and 1(4), $l < p$. Formula (24) gives a representation of the number lp as the sum of the squares of four integers, not all of which are divisible by p. It follows from the definition of n that $n \leqslant lp$, and so, by (10), $mp \leqslant lp$, whence $m \leqslant l$, contrary to (21). Thus we see that the assumption that $m \neq 1$ leads to a contradiction; consequently m must be equal to 1, and this is precisely what was to be proved.

LEMMA 2. *Every prime number is the sum of four squares.*

Proof of lemma 2. We have $2 = 1^2+1^2+0^2+0^2$, therefore there is no loss of generality in assuming that p is an odd prime. By lemma 1 it is sufficient to show that p is a divisor of the sum of the squares of four integers which are not all divisible by p. The remainders obtained by dividing the numbers

$$1+0^2, \ 1+1^2, \ \ldots, \ 1+\left(\frac{p-1}{2}\right)^2 \tag{25}$$

by p are different because, as we have already learned (cf. Chapter V, § 5), the numbers $0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2$ divided by p leave different remainders. Similarly, the numbers

$$-0^2, \ -1^2, \ \ldots, \ -\left(\frac{p-1}{2}\right)^2 \tag{26}$$

divided by p leave different remainders. Suppose that the remainders obtained by dividing the numbers of (25) by p are all different from the remainders obtained by dividing the numbers of (26) by p. Then the total number of different remainders obtained by dividing both the numbers of (25) and those of (26) would be equal to $2\left(1+\frac{p-1}{2}\right) = p+1$, which is impossible. Consequently, there exists at least one term of sequence (25), say $1+x^2$, that leaves the same remainder as a term, say $-y^2$, of sequence (26). We have $p \mid 1^2+x^2+y^2+0^2$, which shows that p is a divisor of the sum of the squares of four integers one of which (here the number 1) is not divisible by p. Hence, by lemma 1, p is the sum of the squares of four integers. The proof of lemma 2 is thus completed.

Proof of theorem 4. In virtue of identity (22), the product of two numbers, each of them the sum of four squares, is also the sum of four squares. This, by induction, extends to any finite number of factors. Hence, since any number > 1 is a product of primes, we infer by lemma 2 that the number itself is the sum of four squares. Since, moreover, $0 = 0^2+0^2+0^2+0^2$ and $1 = 1^2+0^2+0^2+0^2$, the theorem is proved. Let us mention here a result of D. H. Lehmer [6] saying that among natural numbers only the numbers 1, 2, 5, 7, 11, 15, 23 and the num-

bers of the form $4^h m$, where $h = 0, 1, 2, \ldots$, $m = 2, 6$, or 14, are such that the representation of any of them as the sum of four squares is unique apart from the order of the summands.

S. Ramanujan [2] has investigated the systems of natural numbers a, b, c, d such that any natural number n is representable in the form $ax^2+by^2+cz^2+dt^2$, where x, y, z, t are integers. He has proved that for a fixed order of a, b, c, d, say for $a \leqslant b \leqslant c \leqslant d$, there are only 54 such systems, namely $1,1,1,d$, where $d = 1, 2, \ldots, 7$; $1,1,2,d$, where $d = 2, 3, \ldots, 14$; $1,1,3,d$ where $d = 3, 4, 5, 6$; $1,2,2,d$, where $d = 2, 3, \ldots, 7$; $1,2,3,d$, where $d = 3, 4, \ldots, 10$; $1,2,4,d$, where $d = 4, 5, \ldots, 14$; $1,2,5,d$, where $d = 6, 7, \ldots, 10$ (cf. Dickson [7], p. 104, theorem 95).

We now prove the following theorem of Jacobi:

Any natural number is of the form $x^2+2y^2+3z^2+6t^2$, where x, y, z, t are integers.

Proof. Let n be a natural number. By theorem 4 there exist integers a, b, c, d such that

$$n = a^2+b^2+c^2+d^2. \tag{27}$$

We are going to prove that after a suitable change of notation and the signs at a, b, c, d we have $3 \mid a+b+c$. This is plain if at least three of the numbers a, b, c, d are divisible by 3. Suppose that only two of them, say c and d, are divisible by 3. Then $a \equiv \pm 1 \pmod 3$ and $b \equiv \pm 1 \pmod 3$, whence for a suitable choice of the sign we have $3 \mid a \pm b$, so $3 \mid a \pm b + c$. Finally, if at least three of the numbers a, b, c, d, say a, b, c, are not divisible by 3, then for a suitable choice of the sign $\pm$ we have $3 \mid a \pm \pm b \pm c$. Thus without any loss of generality we may assume that

$$a+b+c = 3z, \tag{28}$$

where z is an integer. But among three integers at least two are congruent mod 2; therefore, in addition we may assume that $a \equiv b \pmod 2$, whence it follows that $a+b = 2k$, where k is an integer, and so $a-b = 2(k-b) = 2y$, where y is an integer. But, it is easy to verify that the following identity holds:

$$3(a^2+b^2+c^2) = (a+b+c)^2+2\left(\frac{a+b}{2}-c\right)^2+6\left(\frac{a-b}{2}\right)^2,$$

whence

$$3(a^2+b^2+c^2) = (a+b+c)^2+2(k-c)^2+6y^2,$$

which, by (28), proves that $3 \mid k-c$; so $k-c = 3t$, where t is an integer. Hence, by (28), $a^2+b^2+c^2 = 3z^2+6t^2+2y^2$, and so, by (27), $n = d^2+2y^2+3z^2+6t^2$, and this completes the proof of the theorem of Jacobi

EXERCISES. **1.** On the basis of theorem 4 prove that every natural number which is divisible by 8 is the sum of the squares of eight odd integers.

Proof. If n is a natural number, then, by theorem 4, there exist four integers a, b, c, d such that

$$n-1 = a^2+b^2+c^2+d^2,$$

whence

$$8n = (2a-1)^2+(2a+1)^2+(2b-1)^2+(2b+1)^2+(2c-1)^2+(2c+1)^2+ \\ +(2d-1)^2+(2d+1)^2.$$

2. Prove that no natural number divisible by 8 is the sum of the squares of fewer than eight odd integers.

Proof. As it is easy to prove, the sum of the squares of s odd numbers is of the form $8k+s$, where k is a non-negative integer. So, if the sum is divisible by 8, then $8 \mid s$, and thus $s > 8$.

§ 6. The sums of the squares of four natural numbers. As an immediate consequence of theorem 4, we conclude that any natural number is the sum of the squares of four, or fewer, natural numbers. Using Gauss's theorem we now prove

THEOREM 5. *A natural number n is the sum of the squares of four natural numbers if and only if it does not belong to the sequence of the numbers* 1, 3, 5, 9, 11, 17, 29, 41, $4^h \cdot 2, 4^h \cdot 6, 4^h \cdot 14$, *where* $h = 0, 1, 2, \ldots$ [1].

Proof. We say that a natural number is S_m if it is the sum of the squares of m natural numbers. It is easy to prove that none of the numbers 1, 3, 5, 9, 11, 29, 41 is S_4. We prove this for 41, for instance. Suppose, to the contrary, that 41 is S_4, i.e. that $41 = a^2+b^2+c^2+d^2$, where a, b, c, d are natural numbers, and $a \geqslant b \geqslant c \geqslant d$. Hence $a^2 < 41 \leqslant 4a^2$, and so $4 \leqslant a \leqslant 6$. If $a = 6$, then $5 = b^2+c^2+d^2$, which is impossible. If $a = 5$, then $16 = b^2+c^2+d^2$, which again is impossible, since, as is easy to see, 16 is not S_3. If $a = 4$, then $25 = b^2+c^2+d^2$, which is impossible, since 25 is not S_3. Consequently, 41 cannot be S_4.

Now, let m denote any of the numbers 2, 6, 14. Then m is of the form $4k+2$. Suppose that there exists a non-negative integer h such that $4^h m$ is S_4. Let h denote the least of such integers. Since 2, 6 and 14 are not S_4, $h \geqslant 1$. We then have $4^h m = a^2+b^2+c^2+d^2$, where a, b, c, d are natural numbers and the left-hand side of the equality is divisible by 8 because $h \geqslant 1$ and $m = 2(2k+1)$. From this we easily infer that each of the numbers a, b, c, d must be even. Thus $a = 2a_1$, $b = 2b_1$, $c = 2c_1$, $d = 2d_1$, where a_1, b_1, c_1, d_1 are natural numbers. Hence $4^{h-1} m = a_1^2+b_1^2+c_1^2+d_1^2$, which means that $4^{h-1} m$ is S_4 contrary to the definition of the number h. Thus we have proved that the number $4^h m$,

[1] G. Pall [1], p. 11. The truth of this theorem was conjectured by Descartes.

where $m = 2, 6, 14$, is not S_4 for any non-negative integer h. This shows that the condition of theorem 5 is necessary.

Now let n denote an odd natural number that satisfies the conditions of theorem 5. Consequently, $n \neq 1, 3, 5, 9, 11, 17, 29, 41$. Since n is odd, it must be of one of the forms $8k+1$, $8k+3$, $8k+5$, $8k+7$.

Suppose that $n = 8k+1$. We are going to consider four cases $k = 4t$, $k = 4t+1$, $k = 4t+2$, $k = 4t+3$. If $k = 4t$, then $n = 32t+1$ and, since $n \neq 1$, we must have $t \geqslant 1$, and so $t = u+1$, where u is a non-negative integer. Hence $n = 32(u+1)+1 = 4(8u+6)+9$. By Gauss's theorem, the number $8u+6$ is the sum of the squares of three integers. Since $8u+6 = 2(4u+3)$ cannot be the sum of the squares of two integers, we see that $8u+6$ is S_3, whence it follows that the number $n = 2^2(8u+6)+3^2$ is S_4. If $k = 4t+1$, then $n = 32t+9$. Therefore, since $n \neq 9$ and $n \neq 41$, we have $t \geqslant 2$, so $t = u+2$ where t is an integer $\geqslant 0$. Hence $n = 32(u+2)+9 = 2^2(8u+6)+7^2$, whence, as above, we infer that n is S_4. If $k = 4t+2$, then $n = 32t+17$ and, by $n \neq 17$, we have $t \geqslant 1$, and so $t = u+1$, where t is an integer $\geqslant 0$. Hence $n = 32(u+1)+17 = 2^2(8u+6)+5^2$, where n is S_4. If $k = 4t+3$, then $n = 32t+25 = 2^2(8t+6)+1^2$, whence n is S_4. Thus we see that the condition of theorem 5 is sufficient provided $n = 8k+1$.

Now suppose that $n = 8k+3$. Since $n \neq 3$ and $n \neq 11$, we have $k \geqslant 2$, and so $k = t+2$, where t is a non-negative integer. We then have $n = 8(t+2)+3 = 8t+3+4^2$; therefore, in virtue of Gauss's theorem, which implies that the number $8t+3$ is the sum of the squares of three odd numbers, we conclude that n is S_4. The condition of theorem 5 is thus sufficient also for the numbers $n = 8k+3$.

Further, suppose that $n = 8k+5$. We are going to consider four cases: $k = 4t$, $k = 4t+1$, $k = 4t+2$, $k = 4t+3$. If $k = 4t$, then $n = 32t+5$ and, since $n \neq 5$, we have $t > 0$, so $t = u+1$, where u is a non-negative integer. Hence $n = 32(u+1)+5 = 2^2(8u+3)+5^2$, whence we infer that n is S_4. If $k = 4t+1$, then $n = 32t+13 = 2^2(8t+3)+1^2$, which shows that n is S_4. If $k = 4t+2$, then $n = 32t+21 = 2^2(8t+3)+3^2$, whence n is S_4. If $k = 4t+3$, then $n = 32t+29$ and, since $n \neq 29$, we have $t > 0$, so $t = u+1$, where $u \geqslant 0$, whence $n = 32(u+1)+29 = 2^2(8u+3)+7^2$, which shows that n is S_4. The condition of theorem 5 is thus sufficient for the numbers $n = 8k+5$.

Finally, we consider $n = 8k+7$. Then, by theorem 4, there exist integers a, b, c, d such that $n = a^2+b^2+c^2+d^2$. On the other hand, by theorem 3, since $n = 8k+7$, none of the numbers a, b, c, d can be equal to zero. Thus n is S_4.

We have thus proved that *in order that an odd natural number be the sum of the squares of four natural numbers it is necessary and sufficient that it should not be any of the numbers* 1, 3, 5, 9, 11, 17, 29, 41. *This*

implies that any odd natural number > 41 *is the sum of the squares of four natural numbers.*

Now let n denote an even natural number different from $4^h \cdot 2$, $4^h \cdot 6$, $4^h \cdot 14$, where $h = 0, 1, 2, \ldots$ Let 4^h denote the highest power of the number 4 which divides the number n. We have $n = 4^h m$, where m is not divisible by 4. Consequently, $m = 4k+1$, $m = 4k+2$, or $m = 4k+3$.

If $m = 4k+1$ with even k, i.e. with $k = 2t$, then $m = 8t+1$, which, as proved above, is S_4. If, in addition, $m \neq 1$, 9, 17, 41, then also $n = 4^h m$ is S_4. But, since n is even, in virtue of the fact that m is not divisible by 4, we must have $h > 0$. Clearly, 4 is S_4, $4 \cdot 17 = 68 = 1^2+3^2+3^2+7^2$, $4 \cdot 41 = 164 = 1^2+1^2+9^2+9^2$, whence $4^h \cdot 1 = 4(2^{h-1})^2$, $4^h \cdot 9 = 4(2^{h-1} \cdot 3)^2$, $4^h \cdot 17 = 4 \cdot 17(2^{h-1})^2$, $4^h \cdot 41 = 4 \cdot 41(2^{h-1})^2$ are all S_4. Thus we see that, if $m = 4k+1$ and k is even, then $n = 4^h m$ is S_4. If $m = 4k+1$ and k is odd, i.e. $k = 2t+1$, then $m = 8t+5$, as proved above, is S_4 provided $m \neq 5$ and $m \neq 29$. But $4 \cdot 5 = 20 = 1^2+1^2+3^2+3^2$, $4 \cdot 29 = 116 = 1^2+3^2+5^2+9^2$, whence, by the fact that m is odd, n is even and h is a natural number, we infer that both numbers are S_4. Thus we have proved that if $m = 4k+1$, then $n = 4^h m$ is S_4.

Suppose that $m = 4k+2$, then, if $k = 2t$, we have $m = 8t+2$. Since $n \neq 4^h \cdot 2$, and since $n = 4^h m$, we have $m \neq 2$, and so $t > 0$, i.e. $t = u+1$, where u is a non-negative integer. We then have $m = 8(u+1)+2 = 8u+6+2^2$. Since, as we have already learned, $8u+6$ is S_3, we infer that m is S_4, and consequently $n = 4^h m$ is also S_4. In the case of $k = 2t+1$ we have $m = 8t+6$, and since $n \neq 4^h \cdot 6$ and $n \neq 4^h \cdot 14$, we must have $t \geqslant 2$; so $t = u+2$, where u is a non-negative integer. Hence $m = 8(u+2)+6 = 8u+6+4^2$, which, in virtue of the fact that $8u+6$ is S_3, implies that m is S_4, whence it follows that $n = 4^h m$ is also S_4. Thus we have proved that if $m = 4k+2$, then $n = 4^h m$ is S_4.

Finally, if $m = 4k+3$, then, in the case of $k = 2t$, we have $m = 8t+3$. But, as is shown above, for $m \neq 3$ and $m \neq 11$ the number $m = 8t+3$ is S_4. Thus, if $m = 4k+3$, then the number $n = 4^h m$ is S_4 provided $n \neq 4^h \cdot 3$, $n \neq 4^h \cdot 11$. But $4 \cdot 3 = 12 = 1^2+1^2+1^2+3^2$ and $4 \cdot 11 = 44 = 1^2+3^2+3^2+5^2$. Thus $n = 4^h m$, where $h > 0$, is S_4 because n is even and m odd. In the case of $k = 2t+1$ we have $m = 8t+7$, and so, as we know, m is S_4. This implies that $n = 4^h m$ is also S_4. Thus we have proved that, if $m = 4k+3$, then $n = 4^h m$ is S_4.

We sum up the results we have just proved in the statement that, if n is an even number different from $4^h \cdot 2$, $4^h \cdot 6$, $4^h \cdot 14$, where $h = 0, 1, 2, \ldots$, then n is S_4. We have also proved that *an even natural number* n *is the sum of the squares of four natural numbers if and only if it is none of the numbers* $4^h \cdot 2$, $4^h \cdot 6$, $4^h \cdot 14$, *where* $h = 0, 1, 2, \ldots$

This, combined with the results obtained for odd numbers, completes the proof of theorem 5.

Theorem 5 implies the following

COROLLARY. *The square of any natural number >1, with the exception of 3^2, is the sum of the squares of four natural numbers.*

EXERCISE. Without using the theorem of Gauss, prove that any positive rational number is the sum of the squares of four positive rationals.

Proof. Let r be a positive rational, $r = l/m$, where l and m are natural numbers. By theorem 4 it follows that every natural number is the sum of the squares of four or fewer natural numbers. If $lm = a^2+b^2+c^2+d^2$, where a, b, c, d are natural numbers, then $r = l/m = (a/m)^2+(b/m)^2+(c/m)^2+(d/m)^2$, whence we see that r is the sum of the squares of four natural numbers. If $lm = a^2+b^2+c^2$, where a, b, c are natural numbers, then $r = l/m = (a/m)^2+(b/m)^2+(3c/5m)^2+(4c/5m)^2$. If $lm = a^2+b^2$, where a, b are natural numbers, then $r = l/m = (a/m)^2+(b/3m)^2+(2b/3m)^2+(2b/3m)^2$. Finally, if $lm = a^2$, where a is a natural number, then $r = l/m = 4(a/2m)^2$. Thus, in any case, r is the sum of the squares of four positive rational numbers.

Remark. It can be proved that each positive rational number is the sum of the squares of four different positive rationals, and that for any positive rational there are infinitely many such representations.

As it is proved in § 4, the numbers 2^n, where $n = 1, 2, \ldots$, and, *a fortiori*, the numbers $4^h\cdot 2$, $h = 0, 1, 2, \ldots$, are not S_3. On the other hand, $3 = 1^2+1^2+1^2$, $9 = 1^2+2^2+2^2$, $11 = 1^2+1^2+3^2$, $17 = 2^2+2^2+3^2$, $29 = 2^2+3^2+4^2$, $41 = 1^2+2^2+6^2$, $4^h\cdot 6 = (2^h)^2+(2^h)^2+(2^{h+1})^2$, $4^h\cdot 14 = (2^h)^2+(2^{h+1})^2+(2^h\cdot 3)^2$ for $h = 0, 1, 2, \ldots$ Thus, by theorem 5, we deduce

THEOREM 6. *A natural number n is the sum of the squares of three or four natural numbers if and only if n is none of the numbers 1, 5, and $4^h\cdot 2$, where $h = 0, 1, 2, \ldots$*

This, in consequence, gives the following

COROLLARY. *An odd natural number n is the sum of the squares of three or four natural numbers if and only if n is different from 1 and 5.*

This corollary is the basis of the proof (due to A. Schinzel) of the following

THEOREM 7 (Hurwitz [1]). *The only natural numbers n for which n^2 is not the sum of the squares of three natural numbers are the numbers $n = 2^h$ and $n = 2^h\cdot 5$, where $h = 0, 1, 2, \ldots$*

Proof. In § 4 we proved that, if k is not S_3, then the number $4k$ is not S_3. But, since the numbers 1 and 5^2 are not S_3, the numbers 4^h and $4^h\cdot 5^2$, $h = 0, 1, 2, \ldots$, are not S_3. Thus it remains to prove that, if n is a natural number $\neq 2^h$ and $\neq 2^h\cdot 5$, where $h = 0, 1, 2, \ldots$, then n^2 is S_3.

Suppose therefore that n is a natural number such that $n \neq 2^h$ and $n \neq 2^h\cdot 5$, where $h = 0, 1, 2, \ldots$ Let s be the greatest exponent for which 2^s divides n. We have $n = 2^s m$, where m is odd. Moreover, in virtue of the condition on n, m must be different from 1 and 5. From the

corollary to theorem 6 it follows that m is the sum of the squares of three or four natural numbers; so $m = a^2+b^2+c^2+d^2$, where a, b, c are natural numbers and d is a non-negative integer. Hence

$$m^2 = (a^2+b^2+c^2+d^2)^2 = (a^2+b^2-c^2-d)^2+(2(ac+bd))^2+(2(ad-bc))^2$$
$$= (a^2+b^2-c^2-d^2)^2+(2(ad+bc))^2+(2(ac-bd))^2.$$

Since m is odd, the equality $m = a^2+b^2+c^2+d^2$ implies that among the numbers a, b, c, d either one or three numbers are odd, the remaining ones being even. Therefore the number $a^2+b^2-c^2-d^2$ is odd, and so it is different from zero. Since a, b, c are natural numbers, $ac+bd$ and $ad+bc$ are also natural numbers. We are going to prove that at least one of the numbers $ad-bc$, $ac-bd$ is different from zero. In fact, suppose that $ad = bc$ and $ac = bd$. Then $adc = bc^2$ and $acd = bd^2$, whence $bc^2 = bd^2$, and so, since $b > 0$, $c^2 = d^2$. Hence, in view of $c > 0$ and $d \geqslant 0$, it follows that $c = d$, and, since $ad = bc$ and $c > 0$, $a = b$, whence $m = 2(a^2+c^2)$, which is impossible, since m is odd. Therefore either $ad-bc \neq 0$ or $ac-bd \neq 0$ (or both). Thus at least one of the sums written above gives a representation of the number m^2 as the sum of the squares of three natural numbers. We thus have $m^2 = x^2+y^2+z^2$, where x, y, z are natural numbers.

Hence, $n^2 = (2^s x)^2+(2^s y)^2+(2^s z)^2$, which proves that n^2 is S_3.

Theorem 7 is thus proved.

By theorem 7 it follows that *a natural number n is a principal diagonal of a rectangular parallelepiped whose edges are natural numbers if it is not of the form 2^h or $2^h\cdot 5$, where $h = 0, 1, 2, \ldots$*

From Theorem 7 it follows that for any odd natural number t different from 1 and 5 there exist natural numbers x, y, z such that $t^2 = x^2+y^2+z^2$. The question arises whether for any odd natural number t different from 1 and 5 there exist natural numbers x, y, z such that $(x, y, z) = 1$ and $x^2+y^2+z^2 = t^2$. As proved by A. Schinzel ([12], Corollary 1), the answer to this question is in the positive. (It is easy to prove that for even t there are no such x, y, z.) F. Steiger [1] has found 347 such systems x, y, z for $t \leqslant 100$. For example, $3^2 = 1^2+2^2+2^2$, $7^2 = 2^2+3^2+6^2$, $9^2 = 1^2+4^2+8^2 = 4^2+4^2+7^2$, $11^2 = 2^2+6^2+9^2$, $13^2 = 3^2+4^2+12^2$, $15^2 = 2^2+5^2+14^2 = 2^2+10^2+11^2$, $17^2 = 1^2+12^2+12^2 = 8^2+9^2+12^2$, $19^2 = 1^2+6^2+18^2 = 6^2+6^2+17^2 = 6^2+10^2+15^2$.

A. Schinzel ([12], Theorem 1) gives necessary and sufficient conditions for a natural number n to be representable in the form $x^2+y^2+z^2$, where x, y, z are natural numbers such that $(x, y, z) = 1$. The conditions however are somewhat complicated.

The problem of representing a natural number as the sum of the squares of four different integers has also been considered. We have namely the following theorem of G. Pall [1].

The only natural numbers that cannot be represented as the sums of four different squares $\geqslant 0$ are the numbers $4^h a$, where $h = 0, 1, 2, \ldots$, $a = 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 23, 25, 27, 31, 33, 37, 43, 47, 55, 67, 73, 97, 103, 2, 6, 10, 18, 22, 34, 58, 82$.

§ 7. Sums of $m \geqslant 5$ positive squares. By theorem 5 any odd natural number > 41 is S_4. Therefore, if to any such number we add 1^2 or 2^2, we see that any even number > 42 and any odd number > 45 are S_5. Thus it remains to consider numbers $\leqslant 45$. By theorem 5 numbers 4, 7, 10, 12, 15, 16, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 30, 31, 33, 34, 35, 36, 37, 38, 39, 40, 42, 43, 44 are S_4. So, adding 1 or 4 to any of them we obtain numbers of S_5. There are still the numbers 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18 and 33 to be considered. It is easy to prove that none of them is S_5. We exemplify this by proving that 33 is not S_5. Suppose that 33 is S_5, i.e. that $33 = a^2+b^2+c^2+d^2+e^2$, where a, b, c, d, e are natural numbers such that $a \geqslant b \geqslant c \geqslant d \geqslant e$. Hence $a^2+4 \leqslant 33 \leqslant 5a^2$; so $6 < a^2 \leqslant 29$, which shows that $3 \leqslant a \leqslant 5$, whence $a = 3$ or 4 or 5. In the case of $a = 3$ the number $33-a^2 = 24 = 4\cdot 6$ is S_4, contrary to theorem 5. If $a = 4$, the number $33-a^2 = 17$ is S_4, which, as in the previous case, contradicts theorem 5; the case of $a = 5$ gives $33-a^2 = 8 = 4\cdot 2$ and this is also impossible, since, by theorem 5, $4\cdot 2$ is not S_4.

We have thus proved

THEOREM 8. *The only natural numbers that are not the sums of the squares of five natural numbers are the numbers* 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33.

Now let m be a natural number $\geqslant 6$. We are going to find the natural numbers $\leqslant m+13$ that are S_m. Suppose that n is such a number. Then there exist natural numbers $a_1, a_2, \ldots, a_m$ such that $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_m$ and $n = a_1^2+a_2^2+\ldots+a_m^2$. Hence $a_1^2+(m-1) \leqslant n \leqslant m+13$, which implies $a_1^2 \leqslant 14$, and so $a_1 \leqslant 3$. Therefore $a_1 = 1$ or $a_1 = 2$ or $a_1 = 3$. In the case of $a_1 = 1$ (since $a_1 \geqslant a_2 \geqslant \ldots \geqslant a_m$) we have $a_1 = a_2 = \ldots = a_m = 1$, and so $m = n$. Suppose that $a_1 = 2$. If at least four of the numbers $a_2, a_3, \ldots, a_m$ are equal to 2, then $n \geqslant 5\cdot 4+(m-5) = m+15$, contrary to the assumption that $n \leqslant m+13$. Consequently, at most three of the numbers $a_2, a_3, \ldots, a_m$ can be equal to 2. Therefore there are four possibilities: 1. none of them is equal to 2, and then $n = 4+(m-1) = m+3$; 2. one is equal to 2, then $n = 2\cdot 4 = (m-2) = m+6$; 3. two are equal to 2, then $n = 3\cdot 4+(m-3) = m+9$; 4. three of the numbers $a_1, a_3, \ldots, a_m$ are equal to 2, then $n = 4\cdot 4+(m-4) = m+12$. Thus all that remains to be considered is the case $a_1 = 3$. Then $n-9 = a_2^2+a_3^2+\ldots+a_m^2$. If $a_2 = 3$, then $n \geqslant 18+(m-2)$, contrary to the assumption that $n \leqslant m+13$. Consequently $a_2 \leqslant 2$. If $a_2 = 1$, then $a_3 = a_4 = \ldots = a_m = 1$; so $n = 3^2+m-1 = m+8$. If $a_2 = 2$ and,

if among the numbers $a_2, a_3, \ldots, a_m$ there are two or more numbers equal to 2, then $n \geqslant 3^2+2^2+2^2+(m-3) = m+14$, contrary to the assumption that $n \leqslant m+13$. Hence $a_3 = a_4 = \ldots = a_m = 1$, whence $m = 3^2+2^2+(m-2) = m+11$.

We have thus proved that among the natural numbers $\leqslant m+13$ only the numbers $m, m+3, m+6, m+8, m+9, m+11$ $m+12$ are S_m.

Now we suppose that n is a natural number $> m+13$. If $n = m+28$, then, since $m \geqslant 6$, we have $n = m+28 = 2\cdot 3^2+4\cdot 2^2+(m-6)\cdot 1^2$, which shows that n is S_m. Suppose that $n \neq m+28$. Then $n-(m-5) > 18$ (since $n > m+13$) and $n-(m-5) \neq 23$. By theorem 8 it follows that the number $n-(m-5)$ is S_5; so the number $n = n-(m-5)+(m-5)\cdot 1^2$ is S_m.

We sum up the results we have just obtained in

THEOREM 9 (Pall [1]). *If m is a natural number $\geqslant 6$, then the only positive integers that are not the sums of the squares of m natural numbers are the numbers* $1, 2, 3, \ldots, m-1, m+1, m+2, m+4, m+5, m+7, m+10, m+13$.

By theorems 8 and 9 we deduce that, if m is a natural number $\geqslant 5$, then any sufficiently large natural number is the sum of the squares of m natural numbers. This is not true for $m = 1, 2, 3, 4$, because there exist infinitely many natural numbers

1) which are not the squares of natural numbers (e.g. the numbers n^2+1, where $n = 1, 2, \ldots$),

2) which are not S_2 (e.g. the numbers of the form $4k+3$, where $k = 0, 1, 2, \ldots$),

3) which are not S_3 (e.g. the numbers of the form $8k+7$, where $k = 0, 1, 2, \ldots$),

4) which are not S_4 (e.g. the numbers of the form $4^h\cdot 2$, where $h = 0, 1, 2, \ldots$).

Equally, there exist infinitely many natural numbers which are not the sums of the squares of three or fewer natural numbers, e.g. numbers of the form $8k+7$, where $k = 0, 1, 2, \ldots$ However, by the theorem of Lagrange, any natural number is the sum of the squares of four or fewer natural numbers.

EXERCISES. **1.** Prove that for any natural number m there exist infinitely many natural numbers which are S_i, $i = 1, 2, \ldots, m$, simultaneously.

Proof. We show that any number of the form $(13k)^2$ greater than $m+13$ has this property. In fact, we have $n = (13k)^2 = (5k)^2+(12k)^2 = (3k)^2+(4k)^2+(12k)^2 = (2k)^2+(4k)^2+(7k)^2+(10k)^2$. Thus we see that the number n is S_1, S_2, S_3 and S_4. If $i > 4$ and $i < m$, then we have $n = (13k)^2 > 33$ and $n > m+13$; so $n > i+13$, which in virtue of theorems 8 and 9 shows that n is S_i.

Remark. It can be proved that the least natural number which is S_1, S_2 and S_3 is 169. This number is S_i for all $i \leqslant 155$ and among the i's between 155 and 169 it is S_i only for $i = 157, 158, 160, 161, 163, 166$ and 169. The proof that 169 is S_{100} follows for instance from the formula $169 = 23\cdot 2^2+77\cdot 1^2$ or from the formula $169 = 8^2+2\cdot 2^2+97\cdot 1^2$.

2. Find the least natural number n which is S_i for any $i \leqslant 1000$.

Solution. $n = 34^2$. In fact, since n is S_1, and so $n = k^2$, where k is a natural number, we have since n is S_{1000}, $k^2 \geqslant 1000$, and so $k \geqslant 32$. But, by theorem 2, the numbers $32^2 = 2^{10}$ and $33^2 = (3\cdot 11)^2$ cannot be S_2. However, $34^2 = 16^2+30^2 = 2^2+24^2+24^2$, whence we infer that 34^2 is S_1, S_2, S_3. By theorem 5 we see that 34^2 is S_4 and by theorem 8 it is S_5. Now a simple application of theorem 9 shows that 34^2 is S_i provided $34^2 > i+13$ and $i \geqslant 6$. Therefore 34^2 is S_i for any $i \leqslant 1142$. An example of a representation of 34^2 as the sum of 1000 squares is $34^2 = 2\cdot 8^2+2\cdot 4^2+ +999\cdot 1^2$.

3. Prove that the only natural numbers n such that n^2 is not S_5 are the numbers 1, 2, 3 and that the only natural numbers n for which n^2 is not S_6 are the numbers 1, 2, 4.

The proof follows immediately from theorems 8 and 9.

§ 8. The difference of two squares.

THEOREM 10. *An integer k is representable as the difference of two squares if and only if k is not of the form $4t+2$, where t is an integer.*

Proof. If a and b are two even numbers, then a^2-b^2 is divisible by 4; if both a and b are odd, then a^2-b^2 is divisible by 8; if, finally, one of the numbers a, b is even and the other is odd, then a^2-b^2 is odd. We have thus proved that the condition of theorem 10 is necessary.

Now suppose that an integer k is not of the form $4t+2$. Consequentlys either k is odd or it is divisible by 4. If k is odd, then both k and $k+1$ are even; so $(k-1)/2$ and $(k+1)/2$ are integers. We have

$$k = \left(\frac{k+1}{2}\right)^2 - \left(\frac{k-1}{2}\right)^2.$$

If k is divisible by 4, then

$$k = \left(\frac{k}{4}+1\right)^2 - \left(\frac{k}{4}-1\right)^2.$$

Thus we see that the condition is sufficient as well. This completes the proof of theorem 10.

The argument used to prove theorem 10 will also prove the following

THEOREM 10^a. *Any natural number different from 1 and 4, which is not of the form $4t+2$, is the difference of the squares of two natural numbers.*

As is easy to prove, none of the numbers 1 and 4 can be represented as the difference of the squares of two natural numbers.

Our present aim is to determine all the representations of a given natural number n as the difference of the squares of two natural numbers.

Let n be a natural number different from 1 and 4 which is not of the form $4z+2$. Suppose that $n = x^2-y^2$, where x, y are natural numbers. We then have $n = (x+y)(x-y)$ and, if $d = x-y$, then d is a natural divisor of the number n less than the divisor $d' = x+y$, complementary to it. Moreover, the divisors d and d' are either both even or both odd because $d'-d = 2y$. Now let d denote an arbitrary natural divisor of the number n which is less than the complementary divisor $d' = n/d$ and such that d and d' are either both even or both odd. Then $x = \frac{d'+d}{2}$, $y = \frac{d'-d}{2}$ are natural numbers and $x^2-y^2 = \left(\frac{d'+d}{2}\right)^2 - \left(\frac{d'-d}{2}\right)^2 = dd' = n$. So $n = x^2-y^2$. We see that in this way all the representations of the number n as the difference of the squares of two natural numbers are obtained. Thus the number of the representations is equal to the number of natural divisors of the number n that are less than the complementary divisors, respectively, and such that the divisor and the divisor complementary to it are either both even of both odd. This, in particular, shows that any odd prime number has precisely one representation as the difference of the squares of two natural numbers, namely $p = \left(\frac{p+1}{2}\right)^2 - \left(\frac{p-1}{2}\right)^2$. Another consequence is that, if an odd natural number is not the square of a natural number, then it has $d(n)/2$ different representations as the difference of the squares of two natural numbers. If the number n is a square, then it has $(d(n)-1)/2$ such representations. (By $d(n)$ we mean the number of the divisors of n.) This shows that odd primes are not the only numbers that have precisely one representation as the difference of squares of two natural numbers. The squares of odd primes have the same property; we have $p^2 = \left(\frac{p^2+1}{2}\right)^2 - \left(\frac{p^2-1}{2}\right)^2$. But any odd composite number that is not the square of a prime number has at least two representations as the difference of the squares of two natural numbers.

It is easy to prove that among the natural numbers divisible by 4 only the numbers of the form $4p$ or $4p^2$, where p is a prime $\geqslant 2$, have precisely one representation as the difference of the squares of natural numbers.

EXERCISE. Prove that for any natural number m there exists a natural number n which has precisely m representations as the difference of the squares of two natural numbers.

Proof. For n we may set $n = 2^{2m+1}$. In fact, it has precisely m representations as the difference of the squares of two natural numbers because, as it is easy to see, the only such representations are $2^{2m+1} = (2^{2m-k}+2^{k-1})^2-(2^{2m-k}-2^{k-1})^2$, $k = 1, 2, \ldots, m$.

§ 9. Sums of two cubes. It is easy to prove that any integer $\neq 0$ has a finite number $l \geqslant 0$ of representations as the sum of two cubes. Clearly, it suffices to prove this for natural numbers. The number of representations of a number as the sum of two non-negative cubes is, obviously, finite. Suppose that $n = x^3+y^3$, where x, y are integers, $x > 0$, $y < 0$. We then have $n = (x+y)(x^2-xy+y^2)$, where $-xy > 0$. But, since $x+y > 0$, whence $x+y \geqslant 1$, we have $x^2-xy+y^2 \leqslant n$, which, in virtue of the fact that $-xy > 0$, proves that $x < \sqrt{n}$ and $0 < -y < \sqrt{n}$. From this we infer that the number of pairs x, y is finite.

Using the fact that the cube of an integer is congruent to 0, 1 or 8 (mod 9), one can easily prove that no integer of the form $9k \pm 4$, where k is an integer, can be the sum of three or fewer cubes. Consequently, there exist infinitely many natural numbers that are not representable as sums of two cubes. It is also easy to answer the question which are the prime numbers that are representable as sums of the cubes of two natural numbers. In fact, if $p = x^3+y^3$, where x, y are natural numbers, then $p = (x+y)((x-y)^2+xy)$, whence, since $x+y \geqslant 2$, we must have $p = x+y$ and $(x-y)^2+xy = 1$, which shows that $x = y$ and $xy = 1$, and so $x = y = 1$ and $p = 2$. Thus we see that the number 2 is the only prime which can be represented as the sum of the cubes of two natural numbers.

Now we suppose that a prime p is the sum of the cubes of two integers one of which is not a natural number. Then prime p is the difference of the cubes of two natural numbers. Let $p = a^3-b^3$. We then have $p = (a-b)(a^2+ab+b^2)$, which implies $a-b = 1$ and $p = a^2+ab+b^2 = 3b(b+1)+1$. From this we see that, if a prime p is representable as the difference of the cubes of two natural numbers, then p must be of the form $p = 3b(b+1)+1$, where b is a natural number. On the other hand, if p is of this form, then $p = (b+1)^3-b^3$. Thus the primes of the form $3b(b+1)+1$ are precisely the ones which are representable as the differences of the cubes of natural numbers. We do not know whether there exist infinitely many primes of this form. (The answer in the positive follows from the conjecture H.) However, many primes of this form are known. For example, $7 = 2^3-1^3$, $19 = 3^3-2^3$, $37 = 4^3-3^3$, $61 = 5^3-4^3$, $127 = 7^3-6^3$.

THEOREM 11. *For any natural number m there exists a natural number n that is representable as the sum of the cubes of two integers in at least m different ways.*

Proof. In § 15, Chapter II, we have proved that there exists an infinite sequence of systems x_k, y_k, z_k $(k = 1, 2, \ldots)$ of integers such that $(x_k, y_k) = 1$, $x_k^3+y_k^3 = 7z_k^3$ and $0 < |z_1| < |z_2| < \ldots$ Changing, if necessary, the signs of x_k and y_k we may assume that $z_k > 0$ for any $k = 1, 2, \ldots$

Let $n = 7z_1^3z_2^3\ldots z_m^3$, $a_k = \dfrac{z_1z_2\ldots z_m}{z_k}x_k$, $b_k = \dfrac{z_1z_2\ldots z_m}{z_k}y_k$ for $k = 1, 2, \ldots, m$. All a_k and b_k are integers and, moreover, $a_k^3+b_k^3 = n$.

If for some different indices i, j of the sequence $1, 2, \ldots, m$ we have $a_i = a_j$, then, since $z_k \neq 0$ for any $k = 1, 2, \ldots, m$, $x_i/z_i = x_j/z_j$, whence, in virtue of $(x_i, z_i) = (x_j, z_j) = 1$ we obtain $x_i = x_j$ and $z_i = z_j$, which is impossible. Similarly, if $a_i = b_j$, then $x_i/z_i = y_j/z_j$, which, in virtue of $(x_i, z_i) = (y_j, z_j) = 1$, is impossible. Thus we have obtained m different representations of the number n as a sum of the cubes of two integers. This completes the proof of theorem 11.

THEOREM 12. *Let n be a natural number that is neither the cube of a natural number nor the cube of a natural number multiplied by 2. If n is representable as the sum of the cubes of two rational numbers, then n has infinitely many such representations.*

Proof. Let r be the greatest integer for which r^3 divides n. Then $n = r^3a$, where a is a natural number which is not divisible by the cube of any natural number > 1. By assumption, a cannot be equal to 1 or 2. Suppose that n is the sum of the cubes of two rational numbers. If we reduce them to the same denominator, we may write $n = (u/t)^3+(v/t)^3$, where u, v are integers and t is a natural number. Hence $u^3+v^3 = a(rt)^3$. The numbers u, v are different from zero, since, by assumption, n is not the cube of a natural number, and so it cannot be the cube of a rational number. Thus $d = (u, v)$ is a natural number. Let $u = dx$, $v = dy$, where x, y are integers such that $(x, y) = 1$. We also have $d^3 \mid a(rt)^3$, whence, since a is not divisible by the cube of any natural number, we easily infer that $d \mid rt$, and so $rt = dz$, where z is a natural number. We see that the numbers x, y, z satisfy the equation $x^3+y^3 = az^3$. Thus, by theorem 10, § 15, Chapter II, we deduce that this equation has infinitely many solutions in integers x, y, z with $(x, y) = (x, z) = (y, z) = 1$ and $z \neq 0$. For any such solution we have $nz^3 = a(rz)^3 = (rx)^3+(ry)^3$, whence $n = (rx/z)^3+(ry/z)^3$. Moreover, we see that different solutions give different representations of n as the sum of two cubes, because the fractions x/z and y/z are irreducible. Theorem 12 is thus proved.

COROLLARY. *If r is a rational number which is neither the cube of a rational number nor the cube of a rational number multiplied by 2, and if r is representable as the sum of the cubes of two rational numbers, then r has infinitely many such representations.*

Proof. Clearly, we may suppose that r is a positive rational number, i.e. that $r = l/m$, where l and m are natural numbers and $(l, m) = 1$. According to the hypothesis, there exist integers u, v and a natural number t such that

$$\frac{l}{m} = \left(\frac{u}{t}\right)^3 + \left(\frac{v}{t}\right)^3, \quad \text{whence} \quad lm^2 = \left(\frac{um}{t}\right)^3 + \left(\frac{vm}{t}\right)^3.$$

Thus the natural number lm^2 is the sum of the cubes of two rational numbers and it is neither the cube of a rational number nor the cube of a rational number multiplied by two, because, if it were, $r = l/m$ would be either the cube of a rational number or the cube of a rational number multiplied by two, contrary to the assumption. Thus, by theorem 12, we see that the number lm^2 has infinitely many representations as the sum of the cubes of two rational numbers, which, in turn, implies that the number $r = lm^2/m^3$ has this property. This completes the proof of the corollary.

§ 10. The equation $x^3+y^3 = z^3$. Now we are going to present an elementary proof of Fermat Last Theorem for the exponent 3. The proof which we present here has been worked out by J. Browkin on the basis of ideas due to R. D. Carmichael [4], pp. 67-70.

THEOREM 13. *The equation $x^3+y^3 = z^3$ is insolvable in integers $x, y, z \neq 0$.*

LEMMA. *All the solutions of the equation*

$$s^3 = a^2+3b^2 \tag{29}$$

in integers a, b, s such that $(a, b) = 1$, s is odd are given by the following formulae

$$s = \alpha^2+3\beta^2, \quad a = \alpha^3-9\alpha\beta^2, \quad b = 3\alpha^2\beta-3\beta^3, \tag{30}$$

where the numbers α, β satisfy the conditions

$$\alpha \not\equiv \beta \pmod 2, \quad (\alpha, 3\beta) = 1. \tag{31}$$

Proof of the lemma. First we suppose that the integers α, β satisfy conditions (31). Let the numbers a, b, s be given by formulae (30). Then, using the identity

$$(A^2+3B^2)^3 = (A^3-9AB^2)^2+3(3A^2B-3B^3)^2, \tag{32}$$

we easily verify that the numbers a, b, s satisfy equation (29). By (31) we infer that $(a, b) = (\alpha(\alpha^2-9\beta^2), 3\beta(\alpha^2-\beta^2)) = (\alpha^2-9\beta^2, \alpha^2-\beta^2) = (8\beta^2, \alpha^2-\beta^2) = 1$ and that s is odd.

Suppose that integers a, b, s satisfy equation (29) and that $(a, b) = 1$ and s is odd. In order to prove the lemma we have to find integers α, β that satisfy conditions (30) and (31).

In order to do this we note that any prime divisor of the number s is of the form $6k+1$. In fact, if $p \mid s$, then, since s is odd, $p \geqslant 3$. If $p = 3$, then by (29), $3 \mid a^2$; so $3 \mid a$, and, again by (29), $9 \mid 3b^2$, whence $3 \mid b$, contrary to the assumption that $(a, b) = 1$. Thus we see that $p > 3$. Since $p \mid s$ and $(a, b) = 1$, by (29) we infer that $(b, p) = 1$, so $0 \equiv a^2+3b^2 \equiv b^2(a^2b^{p-3}+3) \pmod p$. Hence $(ab^{(p-3)/2})^2 \equiv -3 \pmod p$. This shows that -3 is a quadratic residue to the modulus p. As is known, this implies that p is of the form $6k+1$.

The construction of α, β can now be carried out by induction with respect to the number n of the prime factors of the integer s.

If $n = 0$, then, since $s^3 = a^2+3b^2 \geqslant 0$, we obtain $s = 1$. So $a = \pm 1$, $b = 0$. Thus the numbers α, β are defined by setting $\alpha = \pm 1$, $\beta = 0$. It is plain that conditions (30) and (31) are satisfied.

Now we suppose that the lemma is proved for a natural number $n \geqslant 0$. Let an integer s that has $n+1$ prime factors and two relatively prime integers a, b satisfy equation (29). Let p be a prime divisor of s; so $s = tp$, where t has n prime factors.

Since p is of the form $6k+1$, there exist integers α_1, β_1 such that $p = \alpha_1^2+3\beta_1^2$, where α_1, β_1 satisfy conditions (31). If $c = \alpha_1^3-9\alpha_1\beta_1^2$, $d = 3\alpha_1^2\beta_1-3\beta_1^3$, in virtue of identity (32), we obtain $p^3 = c^2+3d^2$ and, by (31), $(c, d) = 1$.

We have

$$t^3p^6 = s^3p^3 = (a^2+3b^2)(c^2+3d^2) = (ac \pm 3bd)^2+3(ad \mp bc)^2. \tag{33}$$

Consider the product

$$(ad-bc)(ad+bc) = (ad)^2-(bc)^2 = (a^2+3b^2)d^2-b^2(c^2+3d^2) \tag{34}$$

$$= t^3p^3d^2-b^2p^3 = p^3(t^3d^2-b^2).$$

If $p \mid ad-bc$ and $p \mid ad+bc$, then $p \mid 2ad$ and $p \mid 2bc$, whence, in virtue of the fact that p is odd, we obtain $p \mid ad$ and $p \mid bc$. But $p^3 = c^2+3d^2$ and $(c, d) = 1$. Hence $(p, c) = (p, d) = 1$ and so $p \mid a$ and $p \mid b$, contrary to $(a, b) = 1$.

Consequently, only one of the numbers $ad-bc$ and $ad+bc$ can be divisible by p. But, by (34), this number is divisible by p^3. Consequently, for the appropriate choice of the sign in the brackets at the end of (33) the number in the brackets is divisible by p^3. Since, in addition, the left-hand side of (33) is divisible by p^6, we see that the other number in

the brackets on the right-hand side of (33) must be divisible by p^3. Therefore if the signs are suitably chosen,

$$u = \frac{ac \pm 3bd}{p^3} \quad \text{and} \quad v = \frac{ad \mp bc}{p^3} \tag{35}$$

are integers. Thus formula (33) turns into the form

$$t^3 = u^2 + 3v^2. \tag{36}$$

We solve (35) for a and b to find

$$a = uc + 3vd \quad \text{and} \quad \pm b = ud - vc.$$

Hence, in view of $(a, b) = 1$, we infer that $(u, v) = 1$. In virtue of the inductive hypothesis and formulae (36), there exist integers α_2, β_2 which satisfy (31) and are such that

$$t = \alpha_2^2 + 3\beta_2^2, \quad u = \alpha_2^3 + 9\alpha_2\beta_2^2, \quad v = 3\alpha_2^2\beta_2 - 3\beta_2^3. \tag{37}$$

We write

$$\alpha = \alpha_1\alpha_2 + 3\beta_1\beta_2, \quad \beta = \alpha_2\beta_1 - \beta_2\alpha_1.$$

Then

$$\begin{aligned} s &= tp = (\alpha_1^2 + 3\beta_1^2)(\alpha_2^2 + 3\beta_2^2) = \alpha^2 + 3\beta^2, \\ a &= cu + 3dv = (\alpha_1^3 - 9\alpha_1\beta_1^2)(\alpha_2^3 - 9\alpha_2\beta_2^2) + 3(3\alpha_1^2\beta_1 - 3\beta_1^3)(3\alpha_2^2\beta_2 - 3\beta_2^3) \\ &= \alpha^3 - 9\alpha\beta^2, \\ \pm b &= du - cv = (3\alpha_1^2\beta_1 - 3\beta_1^3)(\alpha_2^3 - 9\alpha_2\beta_2^2) - (\alpha_1^3 - 9\alpha_1\beta_1^2)(3\alpha_2^2\beta_2 - 3\beta_2^3) \\ &= 3\alpha^2\beta - 3\beta^3. \end{aligned}$$

Changing, if necessary, the sign of β, we see that the numbers α, β satisfy equations (30). From this, since $(a, b) = 1$, we infer that the integers α, β satisfy (31).

Proof of theorem 13. Suppose that numbers x, y, z satisfy equation (29) and, moreover, that they are chosen in such a way that the number $|xyz| \neq 0$ assumes the least possible value. Clearly any two of the numbers x, y, z are relatively prime, since otherwise a common divisor $d > 1$ of two of them would divide all the three and thus we could divide equation (29) throughout by d^3, which would produce a smaller solution.

It is very easy to verify that x, y, z are not all odd, and, by what we have proved above, only one of them is even. Consequently, we may

assume that the number z is even and the numbers x, y are odd. So the numbers $x+y$ and $x-y$ are even, whence

$$x + y = 2u, \quad x - y = 2w. \tag{38}$$

Hence

$$x = u + w, \quad y = u - w. \tag{39}$$

By (39), in virtue of $(x, y) = 1$, since the numbers x, y are odd, we infer that $(u, w) = 1$ and $u \not\equiv w \pmod 2$. Substituting the values for x, y obtained from (39) in equation (29) we obtain

$$2u(u^2 + 3w^2) = z^3. \tag{40}$$

If $(u, 3) = 1$, then, since $u \not\equiv w \pmod 2$, we have $(2u, u^2+3w^2) = 1$, so

$$2u = t^3, \quad u^2 + 3w^2 = s^3, \tag{41}$$

where s is an odd number and $(u, w) = 1$. In virtue of the lemma there exist integers α, β that satisfy conditions (31) and are such that $u = \alpha^3 - 9\alpha\beta^2$. Hence, by (41), $t^3 = 2u = 2\alpha(\alpha - 3\beta)(\alpha + 3\beta)$.

Now we verify without difficulty that any two of the numbers 2α, $\alpha - 3\beta$, $\alpha + 3\beta$ are relatively prime; so $2\alpha = \sigma^3$, $\alpha - 3\beta = \tau^3$, $\alpha + 3\beta = \varrho^3$, which gives the equality $\sigma^3 = \varrho^3 + \tau^3$. But $|\varrho\sigma\tau| = |t^3| = |2u| = |x+y| \neq 0$ and $|x+y| \leqslant xyz \mid < |xyz|^3$, contrary to the assumption that $|xyz|$ is minimal.

If $3 \mid u$, i.e. if $u = 3v$, then (40) can be rewritten is the form

$$18v(3v^2 + w^2) = z^3, \tag{42}$$

whence, in view of $3v \not\equiv w \pmod 2$ and $(3v, w) = 1$, we obtain $(18v, 3v^2 + w^2) = 1$; so

$$18v = t^3, \quad 3v^2 + w^2 = s^3, \tag{43}$$

where s is odd and $(v, w) = 1$. In virtue of the lemma there exist integers α, β which satisfy conditions (31) and are such that $v = 3\beta\alpha^2 - 3\beta^3$. Hence, by (43), $t^3 = 18v = 27 \cdot 2\beta(\alpha + \beta)(\alpha - \beta)$. It is easy to verify that any two of the numbers 2β, $\alpha + \beta$, $\alpha - \beta$ are relatively prime; so $2\beta = \sigma^3$, $\alpha + \beta = \tau^3$, $\alpha - \beta = \varrho^3$ which gives $\tau^3 = \sigma^3 + \varrho^3$. But

$$|\varrho\sigma\tau|^3 = |\tfrac{1}{27}t^3|^3 = |\tfrac{2}{3}v| = \tfrac{2}{9}|u| = \tfrac{1}{9}|x+y| \neq 0 \quad \text{and} \quad \tfrac{1}{9}|x+y| \leqslant |xyz| \leqslant |xyz|^3,$$

contrary to the assumption that $|xyz|$ is minimal. Theorem 13 is thus proved.

As an immediate consequence of theorem 13 we obtain the following

COROLLARY. *The equation* $x^3+y^3=z^3$ *has no solution in rational numbers* $\neq 0$.

EXERCISES. **1.** Prove that theorem 13 is equivalent to the theorem stating that the equation $3x^2+1=4y^3$ has no solution in rational numbers except $x=\pm 1$, $y=1$ (J. Browkin).

Proof. If two rational numbers $x\neq\pm 1$ and y satisfy the equation $3x^2+1=4y^3$, then $u=(3x-1)/2$ is a rational number, $u\neq 1$ and $u\neq -2$. Moreover, $u^2+u+1=3y^3$, whence $y\neq 0$ (because the equation $u^2+u+1=0$ has no solution in rational numbers); consequently $(2+u)^3+(1-u)^3=(3y)^3$, contrary to the corollary to theorem 13. On the other hand, suppose that theorem 13 is false. Then there exist rational numbers u, v different from zero and such that $u^3+v^3=1$ and $x=(u-v)/(u+v)$, $y=1/(u+v)$ are rational numbers such that $3x^2+1=4y^3$. If $x=\pm 1$ and $y=1$, then $u+v=1$, $u-v=\pm 1$, whence $u=0$ or $v=0$, contrary to the definition of the numbers u, v.

2. Prove that the equation $x^3+y^3=z^3+1$ has infinitely many solutions in natural numbers x, y, z.

The proof follows immediately from the identity of Gérardin:

$$(9n^4)^3+(9n^3+1)^3=(9n^3+3n)^3+1, \quad n=1,2,\ldots$$

For example, if $n=1$, $9^3+10^3=12^3+1$; if $n=2$, $144^3+73^3=150^3+1$. We also have $64^3+94^3=103^3+1$.

3. Find three different natural numbers a, b, c such that the numbers $\sqrt[3]{a}$, $\sqrt[3]{b}$, $\sqrt[3]{c}$ are irrational and $\sqrt[3]{a}+\sqrt[3]{b}=\sqrt[3]{c}$.

Answer $a=2$, $b=16$, $c=54$.

§ 11. Sums of three cubes. According to what we noticed at the beginning of § 9 no integer of the form $9k\pm 4$ is the sum of three of fewer cubes. On the other hand, we do not know whether every integer which is not of the form $9k\pm 4$ (where k is an integer) is the sum of three cubes. This, being easy to prove for any integer n, $-30<n<30$, turns to be rather difficult for the number 30; we do not know any representation of 30 as the sum of three cubes and we do not know whether such a representation exists.

J. C. P. Miller and M. F. C. Woollett [1] have found the solutions of the equation $x^3+y^3+z^3=k$ with $|k|\leqslant 100$ in integers x, y, z with $|x|\leqslant|y|\leqslant|z|\leqslant 3164$. They have shown that there are no such solutions for $k=30$, 33, 39, 42, 52, 74, 75, 84, 87 and that for $k=12$ there is precisely one solution $z=-11$, $y=10$, $x=7$; for $k=9$ there are two solutions $z=2$, $y=1$, $x=0$ and $z=217$, $y=-216$, $z=-32$.

This result, however, does not indicate whether there are other solutions of the equation in integers x, y, z among which at least one in its absolute value is greater than 3164.

There are some integers k for which we are able to prove that there are infinitely many representations of k as sums of three cubes. For example (cf. Mordell [4]):

$$0=n^3+(-n)^3+0^3, \quad 1=(9n^4)^3+(1-9n^3)^3+(3n-9n^4)^3,$$

$$2=(1+6n^3)^3+(1-6n^3)^3+(-6n^2)^3 \quad \text{for any } n=0,\pm 1,\pm 2,\ldots$$

For $k=1$ there are representations of k as the sum of three cubes others than these given by the above formula. For example, $1=94^3+64^3+(-103)^3$. D. H. Lehmer [9] has proved that there exist infinitely many such representations (cf. Godwin [1]). In fact, let $x=3^3t^4(2^43^2t^6-5)$, $y=-3t(6^4t^9+2^43^3t^6+3^3t^3-1)$, $z=2^43^5t^9+2^33^4t^6-3^2t^3+1$. It is easy to verify that for any t, $x^3+y^3+z^3=1$. If t is a natural number which is not divisible by 3, then the solution thus obtained is different from any of the solutions $9n^4$, $1-9n^3$, $3n-9n^4$, because, as one verifies directly, none of the numbers x, y, z is equal to $9n^4$, since y, z are not divisible by 3 and, if $x=9n^4$, then in virtue of $3^3t^4\mid x$, we obtain $3t\mid n$, so $n=3ut$ (u an integer), whence $2^43^2t^6-5=3^3u^4$, which is impossible.

Substituting $t=1$ we obtain $n=3753$, $y=-5262$, $z=4528$. For $t=-1$ we have $x=3753$, $y=-2676$, $z=-3230$.

For $k=2$ we do not know any representation of k as the sum of three cubes different from the one given above. We do not know any integer k not of the form $9t\pm 4$ for which it could be proved that it has only finitely many representations as the sum of three cubes. On the other hand, it is easy to prove that there exist infinitely many k's not of the form $9t\pm 4$ which are not representable as sums of the cubes of three natural numbers.

For $k=3$ we know only four representations of k as the sum of three cubes; these are $(x,y,z)=(1,1,1)$, $(-5,4,4)$, $(4,-5,4)$, $(4,4,-5)$ and we do not know whether there are any other such representations. As we shall see later, the number 3, like every other positive rational number, has infinitely many representations as the sum of the cubes of three positive rational numbers (cf. theorem 14).

Representations of an integer in the form $x^3+y^3+2z^3$, where x, y, z are integers, have also been considered. To this end, Chao Ko [1] has proved that any natural number $\leqslant 100$, except perhaps 76 and 99, admits at least one such representation. (For example, $13=(-35)^3+(-62)^3+2(52)^3$, $20=63^3+(-3)^3+2(-50)^3$, $31=53^3+31^3+2(-44)^3$.) 76 is the least natural number about which we do not know whether it is of the form $x^3+y^3+2z^3$, where x, y, z are integers. The number 2, except the trivial decompositions $2=t^3+(-t)^3+2\cdot 1^3$, has infinitely many such decompositions. This follows immediately from the identity $2=(1-t-t^2)^3+(1+t-t^2)^3+2(t^2)^3$, valid for any integer t, this being the consequence of an identity due to B. Segre [1].

A. Mąkowski has proved that any natural number n, $100 < n \leqslant 220$, except perhaps the numbers 113, 148, 183, 190, 195, is representable in the form $x^3+y^3+2z^3$, where x, y, z are integers. The decomposition $113 = (-133)^3+(-46)^3+2\cdot 107^3$ has been found by K. Moszyński and J. Swiniewicz [1].

THEOREM 14. *Every positive rational number has infinitely many representations as the sum of the three rational positive cubes.* (Cf. Hardy and Wright [1], pp. 197-199, Theorem 34.)

Proof. Let r be a given positive rational number. We define v as a rational number such that $\sqrt[3]{3r/2} < v < \sqrt[3]{3r}$. Let $u = (3r-v^3)/(3r+v^3)$, $s = v(1+u)$, $z = su$, $t = s/3(1-u^2)$, $x = s-t$, $y = t-z$.

Since $v < \sqrt[3]{3r}$, the number u is positive and less than 1; the numbers u, s, z, t are positive rationals, and x, y are rational numbers. In virtue of $v > \sqrt[3]{3r/2}$, we have $v^3 > \frac{3}{2}r$, whence $u = 6r/(3r+v^3)-1 < \frac{1}{3}$. Consequently, $3(1-u^2) > 1$, $s > t$ and $3u(1-u^2) < 1$, whence $z < t$. Therefore $x > 0$ and $y > 0$. But

$$x^3+y^3+z^3 = (s-t)^3+(t-z)^3+z^3 = s^3-3(s^2-z^2)t+3(s-z)t^2$$

and

$$3(s^2-z^2) = 3s^2(1-u^2),$$

whence

$$3(s^2-z^2)t = s^3,$$

so

$$x^3+y^3+z^3 = 3(s-z)t^2 = 3s(1-u)t^2$$

$$= \frac{s^3(1-u)}{3(1-u^2)^2} = \frac{s^3}{3(1+u)(1-u^2)} = \frac{v^3(1+u)^2}{3(1-u^3)} = \frac{v^3(1+u)}{3(1-u)} = r.$$

In virtue of the fact that any rational number less than $\sqrt[3]{3r}$ and sufficiently close to $\sqrt[3]{3r}$ can be chosen as v, the number u and consequently the number $su = z$ can be arbitrarily small. This implies that the equation has infinitely many solutions in positive rational numbers. This completes the proof of theorem 14.

For $r = 3$, $v = 1$, the formulae above give the decomposition $3 = \left(\frac{2}{15}\right)^3+\left(\frac{17}{75}\right)^3+\left(\frac{36}{25}\right)^3$.

Theorem 14 has the following two corollaries:

COROLLARY 1. *For any natural number n the equation $x^3+y^3+z^3 = nt^3$ has infinitely many solutions in natural numbers x, y, z, t such that $(x, y, z, t) = 1$.*

COROLLARY 2. *For any natural number $s \geqslant 3$ any positive rational number has infinitely many representations as the sum of the cubes of s positive rational numbers.*

If the proof of theorem 14 is modified in the way that the number v we choose a little greater than $\sqrt[3]{3r}$, then $u < 0$, $1+u > 0$, $1-u^2 > 0$, $u^2 < \frac{2}{3}$, so $s > 0$, $z < 0$, $t > 0$, $y > 0$, $x > 0$. This gives the proof of the following theorem:

Any positive rational number has infinitely many representations in the form $x^3+y^3-z^3$, where x, y, z are rationals > 0.

Applying this to the number $r+t^3$, where r, t are positive rationals, we obtain

THEOREM 15. *Any rational number has infinitely many representations in the form $x^3+y^3-z^3-t^3$, where x, y, z, t are positive rationals.*

§ 12. Sums of four cubes. Several years ago I formulated the following conjecture:

C. *Any integer has infinitely many representations in the form $x^3+y^3-z^3-t^3$, where x, y, z, t are natural numbers.*

The conjecture has been proved for the integers g with $-1000 \leqslant g \leqslant 1000$ and for an infinite set of other numbers, e.g. for the integers divisible by 3 (1). The proof is based on the following theorem due to L. J. Mordell [3]:

If $g = a^3+b^3-c^3-d^3$, where a, b, c, d are integers, $(a+b)(c+d) > 0$ and $a \neq b$ or $c \neq d$ and, moreover, if the number $(a+b)(c+d)$ is not the square of a natural number, then conjecture C *is true for the number g.*

For $g = 0$ the truth of conjecture C is an immediate consequence of the identity $0 = n^3+1^3-n^3-1^3$, for any $n = 1, 2, \ldots$

We are going to present here a straightforward verification of conjecture C for $g = 1$. For this purpose it is sufficient to show that the equation

$$(t+13)^3+(u+14)^3-(t+3)^3-(u+17)^3 = 1$$

has infinitely many solutions in integers t, u. But this follows from the fact that the equation is satisfied for $t = u = 0$, and that, if is satisfied by the numbers t and u, then the numbers $t_1 = 11t+6u+173$, $u_1 = 20t+11u+315$ also satisfy it. For example, since $t = 0$ and $u = 0$ satisfy the equation, then also $t_1 = 173$, $u_1 = 315$ satisfy it and, moreover, $186^3+329^3-176^3-332^3 = 1$.

The fact that the equation $x^3+y^3-z^3-t^3 = 1$ has infinitely many solutions in natural numbers x, y, z, t implies that there exist infinitely many natural numbers n such that both n and $n+1$ are sums of two positive cubes.

(1) Cf. Schinzel and Sierpiński [2], Mąkowski [1], and unpublished manuscript of J. Całczyńska deposited in the archives of the University of Warsaw.

If $g = 2$, an immediate proof of conjecture C follows from the identity

$$2 = (9n^4)^3 + 1^3 - (9n^3 - 1)^3 - (9n^4 - 3n)^3 \quad \text{for any} \quad n = 1, 2, \ldots$$

In particular, for $n = 1$ we have $2 = 9^3 + 1^3 - 8^3 - 6^3$.

If $g = 3$, the truth of conjecture C is a consequence of the identity

$$3 = (6n^3 + 1)^3 + 1^3 - (6n^3 - 1)^3 - (6n^2)^3 \quad \text{for} \quad n = 1, 2, \ldots$$

We also know positive integral solutions of the equation $x^3 + y^3 + z^3 - t^3 = 1$, for example, $4^3 + 4^3 + 6^3 - 7^3 = 1$, $4^3 + 38^3 + 58^3 - 63^3 = 1$, $4^3 + 37^3 + 63^3 - 67^3 = 1$, and recently J. A. Gabovič [1] has proved that the equation has infinitely many solutions in natural numbers.

On the other hand, it is easy to prove that there exist infinitely many solutions of the equation $x^3 - y^3 - z^3 - t^3 = 1$ in natural numbers x, y, z, t. This is an immediate consequence of the identity

$$(6n^3 + 1)^3 - 1^3 - (6n^2)^3 - (6n^3 - 1)^3 = 1 \quad \text{for} \quad n = 1, 2, \ldots$$

As is shown by A. Mąkowski ([1], p. 121), the equation $x^3 - y^3 - z^3 - t^3 = 2$ has infinitely many solutions in natural numbers. This fact follows immediately from the identity

$$(3n^3 + 1)^3 - (3n^3 - 1)^3 - (3n^2)^3 - (3n^2)^3 = 2 \quad \text{for} \quad n = 1, 2, \ldots$$

The equation has also solutions that are not given by the above identity, for example $235^3 - 3^3 - 69^3 - 233^3 = 2$, $683^3 - 650^3 - 353^3 - 2^3 = 2$.

EXERCISE. Prove that there exist infinitely many natural numbers g for which each of the equations

$$g = x^3 + y^3 - z^3 - t^3, \quad g = x^3 + y^3 + z^3 - t^3, \quad g = x^3 - y^3 - z^3 - t^3$$

has infinitely many solutions in natural numbers x, y, z, t.

Proof. All $g = a^3 - b^3$, where a and $b < a$ are arbitrary natural numbers, are such numbers. The proof follows immediately from the identities:

$$a^3 - b^3 = a^3 + n^3 - b^3 - n^3,$$

$$a^3 - b^3 = a^3 + ((9n^3 - 1)b)^3 + ((9n^4 - 3n)b)^3 - (9n^4 b)^3,$$

$$a^3 - b^3 = (9n^4 a)^3 - ((9n^3 - 1)a)^3 - ((9n^4 - 3n)a)^3 - b^3.$$

(cf. Schinzel and Sierpiński [2], pp. 26-27).

It is easy to prove that *any integer has infinitely many representations as the sum of five cubes.*

The identity

$$6t = (t+1)^3 + (t-1)^3 + (-t)^3 + (-t)^3$$

shows that any integer divisible by 6 is the sum of four cubes. In order to prove that any integer has infinitely many representations as the sum of five cubes it is sufficient to show that for any integer there exists an arbitrarily large natural number such that the difference between the integer and the cube of the natural number is divisible by 6.

Let g denote an arbitrary integer, r the remainder left by g divided by 6. Then $g = 6k + r$. For any natural number n we have $6k + r - (6n + r)^3 \equiv r - r^3 \equiv 0 \pmod 6$ so $6 \mid g - (6n + r)^3$.

§ 13. Equal sums of different cubes. In connection with theorem 13 it seems interesting to know which natural numbers m and $n \geqslant m$ are such that the equation

$$x_1^3 + x_2^3 + \ldots + x_m^3 = y_1^3 + y_2^3 + \ldots + y_n^3 \tag{44}$$

has solution in different natural numbers $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n$. It is clear that there are no solutions for $n = m = 1$. Theorem 13 implies that in the case of $m = 1$, $n = 2$ there are no solutions either. We prove

THEOREM 16. *In order that equation* (44), *where* n, m *are natural numbers,* $n \geqslant m$, *be solvable in different natural numbers* $x_1, x_2, \ldots, x_m, y_1, y_2, \ldots, y_n$ *it is necessary and sufficient that neither* $m = n = 1$ *nor* $m = 1$, $n = 2$ (cf. Sierpiński [23]).

All that we have to prove is the sufficiency of the condition.

LEMMA. *For any natural number* $n > 2$ *there exists a natural number whose cube is the sum of* n *different positive cubes.*

Proof of the lemma. The formulae $6^3 = 3^3 + 4^3 + 5^3$ and $13^3 = 5^3 + 7^3 + 9^3 + 11^3$ prove the lemma for $n = 3$ and $n = 4$. Suppose that the lemma is true for a natural number $n > 2$. Then there exist natural numbers $a_1 < a_2 < \ldots < a_n < a_0$ such that $a_0^3 = a_1^3 + a_2^3 + \ldots + a_n^3$. Hence

$$(6a_0)^3 = (3a_1)^3 + (4a_1)^3 + (5a_1)^3 + (6a_2)^3 + (6a_3)^3 + \ldots + (6a_n)^3$$

and, moreover, $3a_1 < 4a_1 < 5a_1 < 6a_2 < \ldots < 6a_n$, which proves the truth of the lemma for $n+2$. Thus we see that the assumption that the lemma is true for a natural number n implies that the lemma is true for $n+2$. This, combined with the fact that the lemma is proved to be true for $n = 3$ and $n = 4$, gives the proof of the lemma for any natural number $n > 2$.

The lemma implies the following

COROLLARY. *Theorem* 16 *is true for any natural numbers* m, n *with* $m > 3$, $n > 3$.

Proof of the corollary. If $m > 3$ and $n > 3$, then, by the lemma, there exist natural numbers $b_1 < b_2 < \ldots < b_{n-1} < a_1$ such that $a_1 = b_1^3 + b_2^3 + \ldots + b_{n-1}^3$ and numbers $a_2 < a_3 < \ldots < a_m < b_n$ such that $a_2^3 + a_3^3 + \ldots + a_m^3 = b_n^3$. Moreover, we may assume that $a_2 > a_1$, since, if it is not already true, we replace each of the numbers $a_2, a_3, \ldots, a_m, b_n$ by the product of its multiplication by the number $a_1 + 1$. Therefore the numbers $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n$ are different. Adding together

the equalities obtained above we see that $a_1^3+a_2^3+\ldots+a_m^3 = b_1^3+b_2^3+\ldots+b_n^3$, and this is what was to be proved in order to verify theorem 16 for the numbers m and n. The corollary is thus proved. In order to obtain theorem 16 in its whole generality it remains to prove that it is valid for $m = 2$ and $m = 3$ and any $n \geqslant m$.

If $m = 2$, $n = 2, 3, 4, 5$, the truth of theorem 16 follows from the formulae

$$9^3+10^3 = 1^3+11^3, \quad 7^3+8^3 = 1^3+5^3+9^3,$$

$$6^3+36^3 = 4^3+5^3+27^3+30^3, \quad 26^3+28^3 = 2^3+3^3+4^3+5^3+34^3.$$

If $m = 2$ and $n > 5$, then, by the lemma, there exist natural numbers $b_1 < b_2 < \ldots < b_{n-3} < a_1$ such that $a_1^3 = b_1^3+b_2^3+\ldots+b_{n-3}^3$, whence $a_1^3+(6a_1)^3 = (3a_1)^3+(4a_1)^3+(5a_1)^3+b_1^3+b_2^3+\ldots+b_{n-3}^3$, which, by $a_1 < 3a_1 < 4a_1 < 5a_1 < 6a_1$ proves the theorem for n and m.

If $m = 3$, $n = 3$, 4 the truth of theorem 16 follows from the formulae

$$1^3+12^3+15^3 = 2^3+10^3+16^3, \quad 12^3+13^3+14^3 = 3^3+9^3+10^3+17^3.$$

If $m = 3$, $n > 4$, then, by the lemma, there exist natural numbers $b_1 < b_2 < \ldots < b_{n-2} < a_1$ such that $a_1^3 = b_1^3+b_2^3+\ldots+b_{n-2}^3$, whence $a_1^3+(2a_1)^3+(16a_1)^3 = (9a_1)^3+(15a_1)^3+b_1^3+b_2^3+\ldots+b_{n-2}^3$, and so, by $a_1 < 2a_1 < 9a_1 < 15a_1 < 16a_1$, the truth of theorem 16 for the numbers m, n follows.

Theorem 16 is thus proved.

§ 14. Sums of biquadrates. In virtue of Fermat Last Theorem for the exponent 4 (cf. Chapter II, § 6) there is no biquadrate that is the sum of two positive biquadrates. According to the conjecture of Euler, there is no biquadrate which is the sum od three positive biquadrates either. However, there are biquadrates which are sums of four, five or six biquadrates. For example, $353^4 = 30^4+120^4+272^4+315^4$, $15^4 = 4^4+6^4+8^4+9^4+14^4$, $91^4 = 14^4+24^4+34^4+49^4+58^4+84^4$.

THEOREM 17. *For any natural number $n > 3$ there exists a biquadrate which is the sum of n different positive biquadrates.*

Proof. Let S denote the set of the natural numbers $n > 1$ for which there exists a biquadrate that is the sum of n different positive biquadrates. As we have just shown numbers 4, 5, 6 belong to the set S. We now prove that if numbers n, m belong to S, then the number $m+n-1$ also belongs to S. In fact, if m and n belong to S, then there exist natural numbers $a_1 < a_2 < \ldots < a_m < a_0$ and $b_1 < b_2 < \ldots < b_n < b_0$ such that

$$a_0^4 = a_1^4+a_2^4+\ldots+a_m^4, \quad b_0^4 = b_1^4+b_2^4+\ldots+b_n^4.$$

Hence

$$(a_0b_0)^4 = (a_1b_1)^4+(a_1b_2)^4+\ldots+(a_1b_n)^4+(a_2b_0)^4+(a_3b_0)^4+\ldots+(a_mb_0)^4$$

and, moreover, $a_1b_1 < a_1b_2 < \ldots < a_1b_n < a_2b_0 < a_3b_0 < \ldots < a_mb_0$. This shows that the number $m+n-1$ belongs to the set S. Now the proof is almost over, we simply notice that if a set S of natural numbers is such that the numbers 4, 5 belong to S and that together with any natural numbers m and n of S the number $m+n-1$ is in S, then S contains any natural number $\geqslant 7$. In fact, since 4 and 5 belong to S, then $4+4-1 = 7$, $5+4-1 = 8$, $5+5-1 = 9$ belong to S. By simple induction we verify that, if m belongs to S, then $m+3k$, where $k = 1, 2, \ldots$, is in S (this is because $m+3k = m+3(k-1)+4-1$). Consequently, the set S contains every number of the form $7+3k$, $8+3k$, $9+3k$, when $k = 0, 1, 2, \ldots$, that is S contains any natural numbers $\geqslant 7$. Since the numbers 5, 4, 6 belong to S, we see that S contains every natural number > 3. Theorem 17 is thus proved.

We know some natural numbers which have two different representations as sums of two positive biquadrates. For example, $133^4+134^4 = 59^4+158^4$. However, we do not know any natural number which has more than two different representations as the sum of two positive biquadrates, provided representations that differ only in the order of the summands are regarded as identical.

The following equality holds $8^4+9^4+17^4 = 3^4+13^4+16^4$.

We hereby note that the identity

$$4^4 255^4 x = (8(255+2x))^4-(8(255-2x))^4+(32x-255)^4-(32x+255)^4$$

implies that any rational number is an algebraic sum of four rational biquadrates.

It can be proved that for any natural number $n > 4$ that is different from 8 there exists a natural number that is the sum of the fifth powers of n different natural numbers. For example, $12^5 = 4^5+5^5+6^5+7^5+9^5+11^5$, $92^5 = 2^5+9^5+11^5+22^5+51^5+58^5+89^5$, $32^5 = 3^5+6^5+7^5+8^5+10^5+11^5+13^5+14^5+15^5+16^5+18^5+31^5$ (cf. A. S. Bang [1]). According to P. Erdös, it can be proved that for any natural number m there exists a natural number k_m such that for any natural number $n > k_m$ there exists a natural number $l_{n,m}$ such that any natural number greater than $l_{n,m}$ is the sum of n different numbers each of which is a positive mth power.

§ 15. Waring's theorem. In 1782 Waring stated without proof the following theorem:

For any exponent s there exist a natural number k such that any natural number n is the sum of k non-negative s-th powers.

This theorem was proved by D. Hilbert in 1909. An elementary proof of Waring's theorem, due to Yu. V. Linnik [2] and based on the idea of L. Schnirelman, is presented in a book of A. Ya. Khinchin [1].

For $s = 1$ Waring's theorem is true but irrelevant. If $s = 2$, theorem 4 (of Lagrange) provides an evaluation for k as $k = 4$. For $s = 3$ Waring claimed that k can be assumed to be equal to 9, i.e. that any natural number is the sum of nine or fewer positive cubes. It was not until 1909 that A. Wieferich proved it true. For $s = 4$ Waring stated that $k = 19$ is good. This, however, has not been proved or disproved. F. C. Auluck [1] proved by the method of Hardy and Littlewood that it is true for the natural numbers $> 10^{10^{89}}$. L. E. Dickson [4] has proved (not in an elementary way) that $k = 35$ is good for any natural number. This is still the best evaluation for k (cf. Palamà [1]).

We are going to give an elementary proof that k can be assumed to be equal to 50 (cf. theorem 18).

For a natural number s we denote by $g(s)$ the least natural number k such that any natural number is the sum of k or less sth powers. Waring's theorem asserts that for any s the natural number $g(s)$ exists. We prove that

$$g(s) \geqslant 2^s + \left[\left(\tfrac{3}{2}\right)^s\right] - 2, \quad s = 1, 2, \ldots \tag{45}$$

Let

$$n = 2^s\left[\left(\tfrac{3}{2}\right)^s\right] - 1. \tag{46}$$

Clearly, n is a natural number, and, since $[x] \leqslant x$, we have

$$n < 3^s. \tag{47}$$

It follows from the definition of $g(s)$ that there exist non-negative integers x_i $(i = 1, 2, \ldots, g(s))$ such that

$$n = x_1^s + x_2^s + \ldots + x_{g(s)}^s. \tag{48}$$

By (47), any number x_i $(i = 1, 2, \ldots, g(s))$ must be less than 3. Consequently, the numbers x_i can take only the three values, 0, 1 and 2. Suppose that among the x_i's there are k different numbers equal to 2, l equal to 1, and r equal to 0. Plainly, k, l, r are non-negative integers and

$$g(s) = k + l + r \geqslant k + l \tag{49}$$

with

$$n = 2^s k + l. \tag{50}$$

Hence $n \geqslant 2^s k$, and, since, by formula (46), $n < 2^s\left[\left(\tfrac{3}{2}\right)^s\right]$, we obtain $k < \left[\left(\tfrac{3}{2}\right)^s\right]$, i.e.

$$k \leqslant \left[\left(\tfrac{3}{2}\right)^s\right] - 1. \tag{51}$$

In virtue of (50), we have $l = n - 2^s k$, and so

$$k + l = k + n - 2^s k = n - (2^s - 1)k. \tag{52}$$

Since s is a natural number, $2^s - 1$ is also a natural number; we multiply (51) by it to obtain

$$(2^s - 1)k \leqslant (2^s - 1)\left(\left[\left(\tfrac{3}{2}\right)^s\right] - 1\right).$$

Hence, by (49), (52) and (46),

$$g(s) \geqslant k + l \geqslant n - (2^s - 1)\left(\left[\left(\tfrac{3}{2}\right)^s\right] - 1\right) = 2^s + \left[\left(\tfrac{3}{2}\right)^s\right] - 2,$$

which proves (45).

If $s = 2$, inequality (45) gives $g(2) \geqslant 2^2 + \left[\tfrac{9}{4}\right] - 2 = 4 + 2 - 2$, and so $g(2) \geqslant 4$. But, as we know, $g(2) = 4$. If $s = 3$, (45) shows that $g(s) \geqslant 2^3 + \left[\tfrac{27}{8}\right] - 2 = 9$. There exist natural numbers, for example 23, which are not representable as sums of eight non-negative cubes. As we have already mentioned, Wieferich proved that $g(3) = 9$.

If $s = 4$, (45) gives the inequality $g(4) \geqslant 2^4 + \left[\tfrac{81}{16}\right] - 2 = 19$. By (46), there exist natural numbers (e.g. 79) which are not representable as sums of 18 non-negative biquadrates. The conjecture of Waring states that $g(4) = 19$.

If $s = 5$, inequality (45), by a simple calculation, gives $g(5) \geqslant 37$. We do not know whether $g(5) = 37$ or, perhaps $g(5) > 37$. All that is known is that $37 \leqslant g(5) \leqslant 40$ (cf. Cheng Jing-jun [1]).

L. E. Dickson [5], [6] (cf. Pillai [3]) has proved that the formula

$$g(s) = 2^s + \left[\left(\tfrac{3}{2}\right)^s\right] - 2$$

is valid for $6 \leqslant s \leqslant 400$, (actually, this is true also for $s = 2$ and $s = 3$). K. Mahler [1] has proved that the above formula is valid for any sufficiently large number s and R. M. Stemmler [1] has verified its validity for $400 < s \leqslant 200000$.

For a natural number s denote by $G(s)$ the least natural number k such that all sufficiently large natural numbers (i.e. all numbers with at most a finite number of exceptions) are representable by k non-negative sth powers. It has been proved that

$$G(2) = 4, \quad G(3) \leqslant 7\ (^1), \quad G(4) = 16, \quad G(5) \leqslant 23, \quad G(6) \leqslant 36$$

(cf. Hardy and Wright, [1], p. 336).

Now we are going to present an elementary proof that $g(4) \leqslant 50$.

(1) This was proved by Yu. V. Linnik [1] in 1942; a simpler proof is given by G. L. Watson [1].

Accordingly we recall the identity of E. Lucas (found in 1876)

$$(53)\quad 6(x_1^2+x_2^2+x_3^2+x_4^2)^2 = (x_1+x_2)^4+(x_1-x_2)^4+(x_1+x_3)^4+(x_1-x_3)^4+ \\ +(x_1+x_4)^4+(x_1-x_4)^4+(x_2+x_3)^4+(x_2-x_3)^4+ \\ +(x_2+x_4)^4+(x_2-x_4)^4+(x_3+x_4)^4+(x_3-x_4)^4.$$

Let n be a natural number divisible by 6, i.e. $n = 6m$, where m is a natural number. In virtue of theorem 4, we have $m = a^2+b^2+c^2+d^2$, where a, b, c, d are non-negative integers. Hence $n = 6a^2+6b^2+6c^2+6d^2$. But, in virtue of theorem 4, there exist non-negative integers x_1, x_2, x_3, x_4 such that $a = x_1^2+x_2^2+x_3^2+x_4^2$. Hence, by (53), $6a^2 = a_1^4+a_2^4+\ldots$ $\ldots+a_{12}^4$, where a_i $(i = 1, 2, \ldots, 12)$ are non-negative integers. We represent each of the numbers $6b^2, 6c^2, 6d^2$ in a similar way as the sum of twelve biquadrates. From this we infer that the number $n = 6m$ is the sum of 48 biquadrates.

Thus we have proved that any natural number divisible by 6 is the sum of 48 biquadrates.

Any natural number $\leqslant 95$ is representable in the form 2^4k+r, where $0 \leqslant k \leqslant 5$, $0 \leqslant r \leqslant 15$, and so it is the sum of 20 biquadrates. Consequently, to complete the proof we may suppose that the number n is greater than 95. Then $n = 6m+r$, where $m > 15$ and $0 \leqslant r \leqslant 5$. The numbers $m, m-2, m-13$ are positive and so, for $r = 0, 1, 2, \ldots, 5$ we have $n = 6m$, $n = 6m+1^4$, $n = 6m+1^4+1^4$, $n = 6(m-13)+3^4$, $n = 6(m-2)+2^4$, $n = 6(m-2)+1^4+2^4$, respectively. Hence, in virtue of what we have proved above, we see that, since any natural number divisible by 6 is the sum of 48 biquadrates, every natural number is the sum of 50 biquadrates. Thus in an elementary way we have proved

THEOREM 18. *Every natural number is the sum of* 50 *biquadrates.*

Using the theorem of Gauss one can elementarily prove that $g(4) \leqslant 37$ (cf. Wieferich [1]).

For any natural number s we denote by $v(s)$ the least natural number k such that any natural number is the algebraic sum of k numbers each of which is the sth power of an integer.

It is easy to prove that $v(2) = 3$ and that $4 \leqslant v(3) \leqslant 5$, however we do not know whether $v(3)$ is equal to 4 or to 5. It is proved that $9 \leqslant v(4) \leqslant 10$, $5 \leqslant v(5) \leqslant 10$.

Now we are going to prove that for any natural number s the number $v(s)$ exists. To this aim we start with the identity of P. Tardy [1] (cf. Dickson [8], vol. II, pp. 723, 728)

$$\sum_{a_1,a_2,\ldots,a_s} (-1)^{a_1+a_2+\ldots+a_s}\left((-1)^{a_1}x_1+(-1)^{a_2}x_2+\ldots+(-1)^{a_s}x_s\right)^s \\ = s!\,2^s x_1 x_2 \ldots x_s,$$

where s is a natural number, and the summation on the left-hand side extends all over the 2^s sequences $a_1, a_2, \ldots, a_s$ the terms of which are 0 and 1.

Hence, for $x_1 = x_2 = \ldots = x_s = 1$, we deduce that every integer divisible by $s!2^s$ is an algebraic sum of 2^s sth powers. Therefore, since any integer is of the form $s!2^s k \pm r$, where k, r are integers and $0 \leqslant r \leqslant s!2^{s-1}$, we see that any integer is an algebraic sum of $2^s+s!2^{s-1}$ sth powers. This proves that

$$v(s) \leqslant 2^s+s!2^{s-1}, \quad \text{for any } s = 1, 2, \ldots$$