WA CLAW SIERPINSKI

A Selection of Problems
-in the-
Theory of Numbers
A SELECTION OF PROBLEMS

in the

THEORY OF NUMBERS

by

WACLAW SIERPINSKI

TRANSLATED FROM THE POLISH BY

A. SHARMA

A Pergamon Press Book

THE MACMILLAN COMPANY
NEW YORK
1964
CONTENTS

ON THE BORDERS OF GEOMETRY AND ARITHMETIC 7

WHAT WE KNOW AND WHAT WE DO NOT KNOW ABOUT PRIME NUMBERS 25

1. What are prime numbers? 25
2. Prime divisors of a natural number 26
3. How many prime numbers are there? 27
4. How to find all the primes less than a given number 28
5. Twin primes 30
6. Conjecture of Goldbach 32
7. Hypothesis of Gilbreath 34
8. Decomposition of a natural number into prime factors 35
9. Which digits can there be at the beginning and at the end of a prime number? 40
10. Number of primes not greater than a given number 42
11. Some properties of the n-th prime number 43
12. Polynomials and prime numbers 45
13. Arithmetic progressions consisting of prime numbers 47
14. Simple Theorem of Fermat 48
15. Proof that there is an infinity of primes in the sequences 4k + 1, 4k + 3 and 6k + 5 52
16. Some hypotheses about prime numbers 56
17. Lagrange's theorem 58
18. Wilson's theorem 60
19. Decomposition of a prime number into the sum of two squares 63
20. Decomposition of a prime number into the difference of two squares and other decompositions 69
21. Quadratic residues 74
22. Fermat numbers 77
23. Prime numbers of the form $n^p + 1$, $m^q + 1$, etc. 84
24. Three false propositions of Fermat 88
ACKNOWLEDGEMENT

The references and some of the comments prepared by A. Mąkowski for the Polish edition of this book have been included, with some modifications, in the English text.
ON THE BORDERS OF GEOMETRY
AND ARITHMETIC

We draw on the entire plane squares like those in square graph paper. The plane is thus divided into squares of the same size. The vertices of our squares are called lattice points (see fig. 1).

\[ \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \]
\[ \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \]
\[ \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \]
\[ \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \]
\[ \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \]
\[ \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \]
\[ \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \]
\[ \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \]
\[ \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \]
\[ \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \bullet \]

Fig. 1

It may seem that there is little to be said about these lattice points, so evenly spaced on the plane, and that they are unlikely to involve any interesting or difficult problems.

However, for one hundred and fifty years, from the time of Gauss until now, lattice points have been the subject of various interesting mathematical inquiries. Different problems were posed on this theme. We have known the answer to many of them for a long time, but there are some that are still unanswered. There are also problems which have been proposed during the last few years. We begin with a problem of this kind proposed recently by H. Steinhaus.
For every natural number (i.e. positive integer) \( n \), does there exist in the plane a circle having in its interior exactly \( n \) lattice points?

It is easy to show that there exist natural numbers \( n \) for which no circle with a lattice point as centre has exactly \( n \) lattice points in its interior. It is clear that, if we have a circle with a lattice point as centre and radius \( \leq 1 \), then there is only one lattice point in its interior (viz. the centre of our circle), but if the radius of our circle is \( > 1 \) and \( \leq 2 \), then inside our circle there lie exactly five lattice points. There is no circle with a lattice point as centre in which there would lie exactly two, three or four lattice points.

If there were a circle with radius \( \leq \frac{1}{2} \) and centre at the midpoint of a side of any one of our squares, then in our circle there would be no lattice point, but for a radius \( r \) such that \( \frac{1}{2} < r \leq \sqrt{5}/2 \) there would be exactly two lattice points inside such a circle.

If there were a circle with centre at the centre of any one of our squares and radius \( \leq \sqrt{2}/2 \), then there would be no lattice points in its interior, but for a radius \( r \) such that \( \sqrt{2}/2 < r \leq \sqrt{10}/2 \), there would be exactly four lattice points in its interior.

Now if the centre of our circle were slightly removed from the centre of our square along a diagonal, then taking the radius of our circle to be the distance of our new centre from the farthest vertex of our square, we would get a circle which could contain in its interior exactly three lattice points.

We now show that the plane can be turned about the centre of the circle so that with a suitable radius there lies inside our circle an arbitrary finite number of lattice points. We take one of our lattice points as the origin of the Cartesian coordinates and as axes of coordinates we take the straight lines passing through this point and perpendicular to the sides of a square.

We show that if we take as the centre of the circle the point \( p \) with coordinates \((\sqrt{2}, \frac{1}{2})\), then, for every natural number \( n \), there exists a radius \( r_n \) such that inside the circle with centre \( p \) and radius \( r_n \) there lie exactly \( n \) lattice points.
But to show this, we first prove that any two distinct lattice points are at different distances from the point $p$.

We then suppose that two distinct lattice points $P_1$ and $P_2$ are at the same distance from $p$. In our system of coordinates the lattice points are, as is easy to see, those points of the plane whose coordinates are integers. Let $(a, b)$ be the coordinates of $P_1$ and $(c, d)$ those of $P_2$. Since $P_1$ and $P_2$ are equidistant from $p$, the squares of their distances from $p$ are equal. Hence by the theorem of Pythagoras we have the identity

$$(a - \sqrt{2})^2 + (b - \frac{1}{2})^2 = (c - \sqrt{2})^2 + (d - \frac{1}{2})^2,$$

whence

$$2(c - a)\sqrt{2} = c^2 + d^2 - a^2 - b^2 + \frac{2}{3}(b - d).$$

The right side of this equation is obviously a rational number and so the left side must also be rational, which is possible only for $c = a$; but then we have

$$d^2 - b^2 + \frac{2}{3}(b - d) = 0,$$

i.e.

$$(d - b)(d + b - \frac{2}{3}) = 0.$$

The second factor on the left side of this equation is not zero because $d$ and $b$ are integers. Therefore the first factor must be zero, so that $d - b = 0$, whence $d = b$. Thus $a = c$ and $b = d$, contrary to the assumption that the points $(a, b)$ and $(c, d)$ are distinct.

We have thus shown that every two distinct lattice points are at different distances from the point $p (\sqrt{2}, \frac{1}{2})$.

Now let $n$ denote a given natural number. It is clear that each circle with centre $p$ and sufficiently large radius will contain more than $n$ lattice points. Let $k$ be one such circle. Inside $k$ there obviously lies a finite number of lattice points. As they are at different distances from $p$, we can arrange them in a finite sequence according to increasing distances from the point $p$. Let $P_1, P_2, \ldots, P_n, P_{n+1}, \ldots$ be this sequence. Let $k_{n+1}$ denote a circle with centre $p$ passing through the point $P_{n+1}$. It is clear that
the only points lying inside the circle $k_{n+1}$ are the points $p_1, p_2, \ldots, p_n$; thus there are exactly $n$ of them.

We have thus proved that:

**For every natural number $n$ there exists a circle with centre $p$ containing exactly $n$ lattice points.**

The problem now suggests itself whether there exist points $p$ of the plane with both coordinates rational (we call such points *rational points*) such that for every natural number $n$ there exists a circle with centre $p$ in which there lie $n$ lattice points. However, A. Schinzel has proved that this is not possible. Indeed, if there is a point in the plane whose coordinates are both rational, i.e. such that, when reduced to a common denominator, they can be put in the form $k/m$ and $l/m$ where $k$ and $l$ are integers and $m$ is a natural number, then if one at least of the numbers $k$ and $l$ is different from zero, the lattice points $(l, -k)$ and $(-l, k)$ are different and are at the same distance from the point $(k/m, l/m)$, since, as is easy to verify,

$$
(l - \frac{k}{m})^2 + (-k - \frac{l}{m})^2 = (-l - \frac{k}{m})^2 + (k - \frac{l}{m})^2.
$$

If $k = l = 0$, then the lattice points $(1, 0)$ and $(-1, 0)$ are different and are equidistant from the point $(0, 0)$.

Therefore, if in the circle with centre $(k/m, l/m)$ passing through the point $(l, -k)$ there lie $s$ lattice points, then, as is easy to see, no circle with the same centre will contain $s+1$ lattice points.

However, it can be proved that for every natural number $n$, there exists a circle with a rational point as centre containing in its interior exactly $n$ lattice points. As we know, there exists a circle $K$ with centre at the point $(\sqrt{2}, \frac{1}{2})$ containing inside exactly $n$ lattice points. Since none of these $n$ points lies on the circumference of the circle $K$, there exists a positive number $d$ less than the distance of each of them from the circumference of the circle $K$. The circle $K'$ with centre $p$ and radius $r-d$ will therefore contain in its interior $n$ lattice points. Circles $K$ and $K'$ are concentric. But it is easy to show that if we have in the plane two different
concentric circles, then there always exists a circle with a rational point as centre, containing the smaller of our circles and contained in the bigger one. Such a circle (obtained for the circles \( K \) and \( K' \)) will therefore contain in its interior exactly \( n \) lattice points.

We also observe that H. Steinhaus proved that for every natural number \( n \) there exists a circle with area \( n \), which contains in it exactly \( n \) lattice points. The proof of this theorem is difficult.

The question has been asked whether, for every natural number \( n \), there exists a circle on whose circumference lie exactly \( n \) lattice points. A. Schinzel proved in [2] that the answer to the question is in the affirmative. Using some elementary theorems of number theory he proved that if \( n \) is odd, \( n = 2k + 1 \), where \( k \) is an integer \( \geq 0 \), then the circle on whose circumference lie exactly \( n \) lattice points is the circle with centre \( (\frac{1}{2}, 0) \) and radius \( \frac{1}{2} 5^k \), but if \( n \) is even, \( n = 2k \), where \( k \) is a natural number, such a circle is the circle with centre \( (\frac{1}{2}, 0) \) and radius \( \frac{1}{2} \cdot 5^{(k-1)/2} \).

The following question has also been investigated: does there exist in the plane, for every natural number \( n \), a square containing exactly \( n \) lattice points? J. Browkin proved that the answer to this question is in the affirmative. The proof is even more difficult than that for the circle (cf. Sierpiński [3]).

It would be easier to prove that for every natural number \( n \) there exists in three-dimensional space a sphere containing exactly \( n \) points having integral coordinates (points which are vertices of cubes with side 1, into which three-dimensional space is divided). One can show that there exists such a sphere with centre at the point \( (\sqrt{2}, \sqrt{3}, \frac{1}{2}) \). T. Kulikowski [1] has also shown that for every natural number \( n \) there exists in three-dimensional space a sphere on whose surface lie exactly \( n \) points with integral coordinates.

We also remark that J. Browkin has proved that for every natural number \( n \) there exists a cube in the three-dimensional space containing exactly \( n \) points with integral coordinates.

Returning again to lattice points lying in a circle, we remark that it would be difficult to give a formula which, for every natural number \( n \), would allow us to calculate the radius of a circle contain-
ing exactly \( n \) lattice points. However, it is not difficult to give an approximate formula for that radius with an error which is comparatively small for large \( n \).

For this purpose we take any point \( Q \) in the plane and a circle \( K \) with centre \( Q \) and given radius \( r \). About each lattice point \( P \) we draw a square with centre \( P \) and sides equal to 1 and parallel to the coordinate axes. Let \( S \) be that part covered by the squares drawn about all the lattice points lying in the circle \( K \). If there are \( n \) lattice points, then obviously the area of \( S \) will be \( n \).

Let \( K_1 \) be the circle with centre \( Q \) and radius \( r + \sqrt{\frac{1}{2}} \). Since \( \sqrt{\frac{1}{2}} \) is the greatest distance of the points of a square with side 1 from its centre, it follows easily that the interior of the circle \( K_1 \) together with its circumference covers \( S \). Since the area of the circle \( K_1 \) is \( \pi (r + 1/\sqrt{2})^2 \) and the area of \( S \) is \( n \), we have, the inequality

\[
n \leq \pi \left( r + \frac{1}{\sqrt{2}} \right)^2.
\]

Similarly we deduce that for \( r > 1/\sqrt{2} \) \( S \) covers the interior and boundary of the circle with centre \( Q \) and radius \( r - 1/\sqrt{2} \) whence we have the inequality

\[
\pi \left( r - \frac{1}{\sqrt{2}} \right)^2 \leq n.
\]

These inequalities give

\[
\sqrt{n} - \frac{1}{\sqrt{2}} \leq r \leq \sqrt{n} + \frac{1}{\sqrt{2}},
\]

which gives an approximate value \( \sqrt{n/\pi} \) of the radius of the circle, containing in its interior exactly \( n \) lattice points.

From our inequality it also follows that (for \( r > 1/\sqrt{2} \))

\[
\frac{n}{\left( r + \frac{1}{\sqrt{2}} \right)^2} \leq \pi \leq \frac{n}{\left( r - \frac{1}{\sqrt{2}} \right)^2}.
\]
Thus by drawing a circle of sufficiently large radius and counting the number of lattice points lying in it, it is possible to approximate the number $\pi$ with arbitrary accuracy. This is interesting but in Analysis we know more convenient practical methods of calculating $\pi$ up to one hundred thousand decimal places.

There are many other questions about circles and lattice points. For example, what must be the radius of a circle with a lattice point as centre if at least one lattice point is to lie on its circumference? It can shown, although it is not easy, that it is necessary and sufficient that the radius of such a circle be equal to the square root of a natural number which, when divided by its greatest square factor, gives a quotient which is a number having no divisor which on dividing by 4 leaves the remainder 3. As we see, the answer to apparently so simple a question is complicated.

Thus from the given conditions it follows that of all circles with a lattice point as centre and with radius $\leq 5$, those with a lattice point on its circumference are the circles with radii $1, \sqrt{2}, 2, \sqrt{5}, 2\sqrt{2}, 3, \sqrt{10}, \sqrt{13}, 4, \sqrt{17}, 3\sqrt{2}, 2\sqrt{5}, 5$.

It would be more difficult to answer the question how many lattice points lie on the circumference of a circle with a lattice point as centre and a given radius $r$. The answer to this problem is known.

It appears simpler to answer the question how many lattice points may lie on the circumference of a circle with a lattice point as centre. It can be shown that the number of those points can be any natural number provided it is divisible by 4. In general, it can be shown that for a natural number $k$, a circle with centre at a lattice point and with radius $\sqrt{5k-1}$ will have on its circumference exactly $4k$ lattice points. The proof is elementary but not simple.

It is easy to show that if for a given natural number $n$ we describe from the point $(0,0)$ as centre a circle with radius $\sqrt{n}$, then denoting by $x$ and $y$ respectively the abscissa and ordinate of any point lying on the circumference of the circle, we shall have $n = x^2 + y^2$. From this we easily deduce that all the lattice points lying on the circumference of our circle determine all possible decompositions
of the integer $n$ into the sum of the squares of two integers. It is an interesting interpretation of the decomposition of a natural number $n$ into the sum of two squares, not suitable, however, for practical determination of such decompositions.

We can show that the square is the only regular polygon which can be so placed that all its vertices are lattice points. Besides trivial arrangements, we also have others, for example

![Fig. 2](image)

One can show that every parallelogram which has lattice points as vertices and which has no other lattice points either inside or on its boundary has area 1. Here are examples of such a parallelogram:

![Fig. 3](image)

It has also been proved that every parallelogram with area $> 4$ whose centre is a lattice point will contain in its interior at least one more lattice point. For a more general result, see, e.g. Hardy and Wright [1], p. 394.

Regarding lattice points, we might ask how many of them
lie on a straight line. In the plane there are straight lines on which there are no lattice points: such are, for example, straight lines passing through the mid-points of two adjacent or opposite sides of squares of area 1.

There are straight lines on which there lies only one lattice point. We can prove that if on a straight line there is more than one lattice point, then there are an infinity of lattice points on it and they are evenly spaced. It can also be proved that if there is only one lattice point on a straight line, then lattice points can be found arbitrarily close to the straight line.

On the plane there are infinitely many lattice points which can be divided into infinitely many sets without common points, for example, by assigning to the same set all those lattice points which lie on the same line parallel on the axis of abscissae. However, it is easy to arrange all the lattice points in an ordinary infinite sequence, i.e. assign natural numbers to them in such a way that different lattice points correspond to different numbers. This can be done, for example, as follows:

![Diagram showing the arrangement of lattice points](image)

The set of all lattice points in the plane can be divided into two sets of which the first is finite on every line parallel to the axis of the abscissae and the second is finite on every line parallel to the axis of the ordinates.
To obtain such a decomposition of lattice points it is enough to trace in the plane two straight lines: \( y = x \), \( y = -x \) and to assign to the first set all those lattice points \((x, y)\) for which \(|x| \leq |y|\), and to the second set the remaining lattice points, i.e. those for which \(|y| < |x|\). The proof that these components possess the desired property presents no difficulty.

Here is a hitherto unsolved problem regarding lattice points proposed by H. Steinhaus:

\textit{Does there exist a set \( Z \) of points in the plane such that every set of points congruent to the set \( Z \) contains exactly one lattice point?}

Another problem concerning lattice points was proposed in 1951 by K. Zarankiewicz:

\textit{For a natural number \( n \geq 3 \), let us take \( n^2 \) lattice points \((x, y)\) where \( x \) and \( y \) are natural numbers \( \leq n \); let \( R_n \) denote the set of those \( n^2 \) points. The problem is to find the smallest natural number \( k(n) \) for which each subset of \( R_n \) having \( k(n) \) points contains nine points in three different rows and three different columns.}

It can easily be shown that \( k(4) = 14 \) and \( k(5) = 21 \). It is more difficult to show that \( k(6) = 27 \) (see Sierpiński [1]). J. Brzeziński proved that \( k(7) = 34 \). No value of \( k(n) \) is known for \( n > 7 \).

This problem was also discussed by C. Hyltén-Cavallius [1].

Certain simple constructions lead to various complicated sets which can be applied to solutions of a number of difficult arithmetical problems. Let us draw \( n \) successive lines through the point \((0, 0)\) and the points with abscissa 1 and ordinates natural numbers \( \leq n \), i.e. through the points \((1, 1)\), \((1, 2)\), \((1, 3)\), ..., \((1, n)\). Let \( S \) denote the set of these straight lines, and let \( Z \) be the set of all lattice points lying in the set \( S \). It is easy to show that for every natural number \( k \leq n \) the abscissae of all points of the set \( Z \) with ordinate \( k \) give all natural divisors of the number \( k \).

Here is another simple mathematical construction due to D. Blanuša in 1949, giving all composite numbers. We place in the \( y \)-axis the set \( A \) all points with ordinates \( \frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \ldots \)
(reciprocals of all natural numbers) and in the $x$-axis the set $B$ all points whose abscissae are 2, 3, 4, ... (natural numbers > 1). Now if we join each of the points of the set $A$ to each of the points of the set $B$ by straight lines, then the abscissae of all the points of intersection of those straight lines with the straight line $y = -1$ form the set of composite numbers.

In fact, the set $A$ is the set of points with coordinates $(0, 1/m)$ where $m = 1, 2, ...$ and the set $B$ is the set of all points with coordinates $(n+1, 0)$ where $n = 1, 2, ...$ The straight line passing through the points $(0, 1/m)$ and $(n+1, 0)$ is

$$\frac{x}{n+1} + my = 1.$$  

The point of intersection of this straight line with the line $y = -1$ is therefore a point with abscissa $x = (m+1)(n+1)$, i.e. an abscissa which is a composite number. On the other hand, every composite number is, as we know, the product of two natural numbers greater than 1, and so is of the form $x = (m+1)(n+1)$ where $m$ and $n$ are natural numbers; hence it is the abscissa of the point of intersection of the straight line passing through the point $(0, 1/m)$ of the set $A$ and the point $(n+1, 0)$ of the set $B$ with the straight line $y = -1$.

The construction of Blanuša may be considered as a geometrical interpretation of the well-known sieve of Eratosthenes.

A generalization of lattice points is the set of rational points in the plane. We first consider the question how many rational points can lie on the circumference of a circle.

There exist in the plane circles with centres at lattice points on whose circumferences there are no rational points. Such is, for example, the circle $x^2 + y^2 = 3$. Let us suppose that such a point $(x, y)$ is rational. The numbers $x$ and $y$ are thus rational and, when reduced to their least common denominator, they can be put in the form $x = k/m, y = l/m$, where $k$ and $l$ are integers. Then $k^2 + l^2 = 3m^2$. This means that if the numbers $k$ and $l$ were both divisible by 3, then the right side of our equation would be divisible by 9, whence the number $m$ would be divisible by 3, and our fractions could be reduced by 3, contrary to the supposition
that \( m \) is the least common denominator. Thus at least one of the numbers \( k \) and \( l \) is not divisible by 3. But, as we know, the square of an integer not divisible by 3 gives, when divided by 3, the remainder 1. If neither of the numbers \( k \) and \( l \) is divisible by 3, the sum \( k^2 + l^2 \) divided by 3 gives the remainder 2, which is impossible since this sum, being equal to \( 3m^2 \), is divisible by 3. But if one of the numbers \( k \) and \( l \) is divisible by 3, the sum \( k^2 + l^2 \) leaves the remainder 1 when divided by 3, which is also impossible. Thus we have proved that on the circumference of the circle \( x^2 + y^2 = 3 \) there is no rational point.

There exist on the plane circles which have only one rational point on their circumference, for example, the circle \((x-\sqrt{2})^2 + (y-\sqrt{2})^2 = 4\). For if \((x, y)\) is a rational point lying on the circumference of this circle, then we have \( x^2 + y^2 = 2(x+y)\sqrt{2} \) which, because of the rationality of \( x \) and \( y \), is possible only if \( x+y = 0 \), whence also \( x^2 + y^2 = 0 \), and these two equations give immediately \( x = 0 \) and \( y = 0 \); on the other hand, it is easy to verify that the rational point \((0, 0)\) lies on the circumference of our circle.

There exist on the plane circles having two and only two rational points on their circumference. Such is, for example, the circle \( x^2 + (y-\sqrt{2})^2 = 3 \). For if \((x, y)\) is a rational point lying on the circumference of this circle, then \( x^2 + y^2 - 1 = 2\sqrt{2}y \), which, since \( x \) and \( y \) are rational, gives \( y = 0 \) and \( x^2 + y^2 = 1 \), so that \( x = \pm 1 \). On the other hand, as is easy to verify, each of the points \((1, 0)\) and \((-1, 0)\) lies on the circumference of our circle.

We now suppose that on the circumference of a circle \( K \) there lie at least three different rational points. It is easy to show that the centre of the circle \( K \) is a rational point and the square of the radius of the circle is a rational number. Since the difference of two rational numbers is a rational number, we may suppose without loss of generality that the centre of the circle \( K \) is the point \((0, 0)\).

Now it is easy to prove that if the centre of the circle \( K \) is the point \((0, 0)\) and on the circumference of this circle there lies at
least one rational point, then there are infinitely many rational points on our circle. From this it follows that if \( a \) and \( b \) are rational numbers such that \( a^2 + b^2 = r^2 \), then, as is easy to verify, for every rational number \( w \) the point \((x, y)\), where

\[
x = \frac{2aw + b(1 - w^2)}{1 + w^2}, \quad y = \frac{a(1 - w^2) - 2bw}{1 + w^2}
\]

will be rational and \( x^2 + y^2 = r^2 \).

Thus on the circumference of a circle there may be no rational point, or only one or two rational points, or even an infinity of rational points. It can also be proved that in the last case the rational points lie everywhere dense on the circumference, i.e. lie in every arc of the circumference.

The set of all rational points in the plane can be divided into two sets of which the first is finite on every line parallel to the y-axis and the other finite on every line parallel to the x-axis. To obtain such a decomposition it is enough to assign to the first set all the points \((l/m, r/s)\) where the fractions are irreducible with integers as numerators and natural numbers as denominators such that

\[
|l| + m < |r| + s,
\]

and to the second set all the remaining points of the plane with both coordinates rational. It can also be shown that the set of all points of three-dimensional space with rational coordinates is the sum of three sets each of which is finite on each straight line parallel to one of the coordinate axes.

The question arises whether the set of all points in the three-dimensional space can be decomposed into the sum of three sets each of which is finite on every straight line parallel to one of the coordinate axes. In 1951, I proved that this question is equivalent to the question whether or not the continuum hypothesis is true (see Sierpiński [2]).

From the results of F. Bagemihl and R. O. Davies it follows that the question whether there exist in the plane three straight lines \( P_i \), \((i = 1, 2, 3)\) such that the plane is the sum of three sets \( S_i \), \((i = 1, 2, 3)\) such that for \( i = 1, 2, 3 \), the set \( S_i \) is finite
on each of the straight lines parallel to the straight line $P_i$ is equivalent to the continuum hypothesis.

We now concern ourselves with the following question: How many points must there be in a set $Z$ lying on the circumference of a circle with given radius $r$ such that the distance between any two points of the set $Z$ is rational?

Let $K$ be the circumference of a circle with radius $r$ and $P$ any point lying on $K$. If $w$ is a rational number $\leq 2r$, then the circle with centre $P$ and radius $w$ obviously meets the circle $K$ in at least one point. If $Q$ is such a point, then the distance of $P$ from $Q$ is equal to $w$ and so is rational. Therefore, for every point $P$ lying on the circumference of any circle, there exist on the same circle infinitely many points $Q$ such that the distance of $P$ from $Q$ is rational.

Now let $K$ be the circumference of the circle with radius $r$ and let us suppose that on $K$ there lie three different points such that the distance between any two is rational. The circle $K$ therefore circumscribes a triangle with rational sides whose lengths we denote by $a, b$ and $c$. As is known from elementary geometry, $r = \frac{abc}{4S}$ where $S$ is the area of the triangle with sides $a, b$ and $c$, or equivalently

$$r = \frac{abc}{\sqrt{4a^2b^2-(a^2+b^2-c^2)^2}}.$$

It follows that if on the circumference $K$ of the circle of radius $r$ there lie three different points whose distances from one another are rational then $r^2$ is a rational number. Thus we conclude, for example, that on a circle of radius $\sqrt{2}$ no three points are such that their distances from one another are rational.

Now we shall prove that:

If $K$ is the circumference of a circle with radius $r$, where $r^2$ is a rational number, then on $K$ there exists a set with infinitely many points any two of which are at a rational distance from each other (cf. Sierpiński [5]).

Let $K$ be the circumference of a circle with radius $r$, where $r^2 = \frac{l}{m}$ with $l$ and $m$ are natural numbers. Therefore $mr = \sqrt{lm} \geq 1$, whence
so that
\[ 0 < \frac{4mr}{4lm+1} < 1. \]

There exists therefore an angle \( \alpha \) such that \( 0 < \alpha < \pi/2 \) and

\[
\sin \alpha = \frac{4mr}{4lm+1}, \quad \cos \alpha = \frac{4lm-1}{4lm+1}.
\]

We show that

\[ \sin k\alpha \neq 0 \quad \text{for} \quad k = 1, 2, \ldots \]

Using well-known formulae in trigonometry it is easy to prove the identity

\[ \sin(k+2)\alpha = 2 \sin(k+1)\alpha \cos \alpha - \sin k\alpha \quad \text{for} \quad k = 1, 2, \ldots \]

Let

\[ t_k = (4lm+1)^k \sin k\alpha \quad \text{for} \quad k = 1, 2, \ldots \]

Because of (4), (1) and \( mr^2 = l \), we put

\[
t_1 = (4lm+1)r \sin \alpha = 4mr^2 = 4l,
\]

\[
t_2 = (4lm+1)^2 r \sin 2\alpha \\
= 2(4lm+1)^2 r \sin \alpha \cos \alpha \\
= 8mr^2(4lm-1) = 8l(4lm-1),
\]

so that \( t_1 \) and \( t_2 \) are natural numbers. Hence from (3) and (4) we deduce by induction that the numbers \( t_k \) are integers for \( k = 1, 2, 3, \ldots \).

From (1), (3) and (4) we easily get the formula

\[
t_{k+2} = 2(4lm-1)t_{k+1} - (4lm+1)^2 t_k \quad \text{for} \quad k = 1, 2, \ldots
\]

The number \( h = 4lm+1 \) is odd and prime to each of the numbers \( 2, l \) and \( 4lm-1 \); from (5) we have \( t_1 < h \), so that \( (t_1, h) = 1 \). We have also \( (t_2, h) = 1 \). Hence we easily deduce from (6) by induction that the numbers \( t_k \) \( (k = 1, 2, \ldots) \) are not divisible by \( h \), and thus are \( \neq 0 \). From (4) we have inequality (2), which was to be proved.
We now take on the circumference $K$ of the circle any point $P_0$ and form an infinite sequence $P_1, P_2, \ldots$ of points on $K$, so that the angles $P_{k-1} O P_k$, where $O$ is the centre of the circle with circumference $K$, are equal to $2\alpha$.

If $u$ and $v$ are integers such that $0 < u < v$, then the angles $P_u O P_v$ will obviously be equal to $2(u-v)\alpha$, and, since $r$ is the radius of the circle with circumference $K$, the distance of the point $P_u$ from $P_v$ will be $2r|\sin(v-u)\alpha|$. Since we know that the numbers (4) are rational, it follows that $2r|\sin(v-u)\alpha|$ is also rational and $\neq 0$ because of (2) and because $v-u$ is a natural number. Thus the points $P_0, P_1, P_2, \ldots$ are all different and the distance between any two of them is rational.

We now consider, for an arbitrary natural number $n$, the points $P_0, P_1, P_2, \ldots, P_{n-1}$ on the circle $K$. Each of the distances $P_u P_v$ where $0 \leq u < v < n$ is, as we know, a rational number and their number is $\frac{1}{2}n(n-1)$; let $s$ denote their common denominator. It is clear that if we enlarge the radius of our circle $s$ times, then on the enlarged circle instead of the points $P_0, P_1, P_2, \ldots, P_{n-1}$ we obtain points $Q_0, Q_1, Q_2, \ldots, Q_{n-1}$ such that the distance between every two of them is a natural number. Since the points $Q_0, Q_1, Q_2, \ldots, Q_{n-1}$ all lie on the circumference of a certain circle, no three of them lie in a straight line. We have thus proved that:

*It is possible to find an arbitrary finite number of points in the plane such that no three of them lie on the same straight line and that the distance between any two of them is a natural number.*

This theorem was proved for the first time by W. H. Anning and P. Erdös [1], see also H. Hadwiger [1]. These authors also proved that:

*If in the plane we have an infinite set of points any two of which have integral distances, then all the points must lie on one straight line.*

Obviously on a straight line there exist infinitely many points such that the distance between any two of them is an integer, because it suffices to lay off successively segments of length 1 infinitely many times on the straight line and take the ends of those segments.
S. Ulam posed the question whether there exists in the plane an everywhere dense set of points every two of which are at a rational distance from each other. A set of points in the plane is everywhere dense if inside every circle there is a point of the set.

We do not know the answer to Ulam's question. We return again to our circle, on whose circumference $K$ we have an infinite sequence of points $P_0, P_1, P_2, \ldots$, but let us now suppose that the radius of our circle is rational, for example $r = 1$, and as the point $P_0$ let us take a point on the circumference of the circle $K$ lying on the positive part of the $x$-axis. The polar coordinates of the point $P_k$ will now be 1 and $2k\alpha$. Let $x_k, y_k$ be the Cartesian coordinates of the point $P_k$. Since $r = 1$, we have $l = m = 1$, formula (1) gives $\sin \alpha = \frac{4}{5}$, $\cos \alpha = \frac{3}{5}$ and shows that $\sin \alpha$ and $\cos \alpha$ are rational, whence, as we know from trigonometry, it follows that $\sin ka$ and $\cos ka$ are rational for every integer $k$. But, the polar coordinates of the point $P_k(x_k, y_k)$ being 1 and $2k\alpha$, we find $x_k = \cos 2k\alpha$, $y_k = \sin 2k\alpha$, so $P_k$ is a rational point for $k = 0, 1, 2, \ldots$

We have thus proved that on the circumference of the circle $x^2 + y^2 = 1$ there lies an everywhere dense set of rational points any two of which are at a rational distance from each other. We consider $n$ such points $P_0, P_1, P_2, \ldots, P_{n-1}$. Let $s$ denote the least common multiple of the denominators of the $2n$ numbers $x_k$ and $y_k$ ($k = 0, 1, 2, \ldots, n-1$). It is clear that taking $s$ as the radius of a circle with centre $(0, 0)$, we obtain on its circumference, instead of the points $P_0, P_1, P_2, \ldots, P_{n-1}$ the points $Q_0, Q_1, \ldots, Q_{n-1}$ which are lattice points and such that the distance between any two of them is a rational number and hence an integer. Indeed, it is easy to prove that, if the distance between two lattice points is rational, then it is integer (because it is always the square root of an integral, and, as we know, a rational number which is the $k$th root of an integer, $k$ being a natural number, is itself an integer). We have thus proved that:

For an arbitrary natural number $n$ there exist $n$ lattice points lying on the circumference of some circle and such that the distance between any two of them is given by an integer.
One more question on the borders of arithmetic and geometry is the question whether there exists a rectangular parallelepiped whose edges, diagonals of the faces and inner diagonals are natural numbers. As follows from well-known theorems of elementary geometry, this problem is equivalent to the question whether there exist natural numbers $x, y$ and $z$ such that each of the numbers $x^2 + y^2, x^2 + z^2, y^2 + z^2$ and $x^2 + y^2 + z^2$ are squares of natural numbers.

We may put it otherwise as the question whether the system of four equations in seven unknowns $x, y, z, t, u, v, w$

$$
x^2 + y^2 = t^2, \quad x^2 + z^2 = u^2, \quad y^2 + z^2 = v^2, \quad x^2 + y^2 + z^2 = w^2$$

has a solution in natural numbers. This question, concerning a system of four equations of the second degree in seven unknowns, we are unfortunately not able to answer.

It can be proved that there exist infinitely many non-congruent rectangular parallelepipeds in which the edges and the diagonals of all its lateral faces are natural numbers.

To the borderland of arithmetic and geometry belongs the question whether a square can be divided into smaller squares no two of which are congruent.

A long time ago it was believed that this decomposition was not possible. A few years ago such a decomposition was found. One can, for example, divide the square with side 175 into 24 non-congruent squares with integral sides, of which the smallest is 1 and the biggest 81. We do not know if 24 is the smallest number of non-congruent squares into which a square can be divided. For this and similar problems see Meschkowski [1].

Finally, we recollect that in 1914, Mazurkiewicz occupied himself with the question of whether or not there exists in the plane a set of points with which every straight line in the plane has exactly two points in common. With the help of the so-called axiom of choice he proved that such a set exists, but no concrete example of such a set is known so far.
WHAT WE KNOW AND WHAT WE DO NOT KNOW ABOUT PRIME NUMBERS

1. What are prime numbers?

We are led to an understanding of prime numbers by some simple problems which are suggested by such an elementary process of arithmetic as multiplication of natural numbers, i.e. positive integers.

As we know, the product of two natural numbers is always a natural number. Therefore there are natural numbers which are the products of two natural numbers greater than 1. But there are also natural numbers greater than 1 which are not the products of two natural numbers greater than 1, for example the numbers 2, 3, 5 and 13. We call such numbers prime numbers. And thus:

A prime number is a natural number greater than 1 which is not the product of two natural numbers greater than 1.

The question arises if for every natural number \( n > 1 \) we can determine whether or not it is a prime number.

Now the definition of a prime number suggests a method of determining this.

For if a natural number \( n > 1 \) is not a prime, then it is the product of two natural numbers \( a \) and \( b \), greater than 1. We have then \( n = a \cdot b \) where \( a > 1 \) and \( b > 1 \), from which it follows immediately that \( n > a \) and \( n > b \). A natural number \( n > 1 \) which is not a prime is therefore the product of two natural numbers less than itself; we call such numbers composite. If the number \( n \) is composite, then we have \( n = a \cdot b \) where \( a \) and \( b \) are natural numbers \( > 1 \) and \( < n \). The quotient \( n:a = b \) is a natural number, so that \( a \) is a natural divisor of the number \( n \) greater than 1 and less than \( n \). Thus, in order to determine whether a natural number
\( n > 1 \) is prime, it is sufficient to find out if it has natural divisors
\( \geq 2 \) but \( < n \) and to do this it is enough to perform \( n - 2 \) times
the division of \( n \) successively by the numbers \( 2, 3, \ldots, n-1 \). If
and only if the number \( n \) is not divisible without remainder by
any of these, then the number \( n \) is prime.

Therefore, it is always possible, at least theoretically, to say
(after a finite number of divisions) whether a given natural number
\( n \) is or is not a prime number. In practice, however, this method
can present great difficulties when the number \( n \) is large. It is not
possible, to this day, because of the lengthy calculations involved, to
apply this method to the number \( 2^{101} - 1 \) having thirty-one digits (in
the decimal scale) although it has been proved in another way that
this number is composite. We do not know so far any of its de­
compositions as a product of two natural numbers greater than 1
(but we know that such a decomposition exists).

We still do not know whether the number \( 2^{217} + 1 \) is prime
or not.

2. Prime divisors of a natural number

We shall now prove some simple theorems on prime numbers.

**Theorem 1.** Every natural number \( n > 1 \) has at least one prime
divisor.

*Proof.* Let \( n \) be a natural number greater than 1; it has a
divisor greater than 1, for example \( n \) itself. Among the divisors
of the number \( n \) greater than 1 there exists one which is the small­
est, \( p \). If \( p \) were not a prime number, then, by the definition of
a prime number, \( p \) would be the product of two natural numbers
\( a, b \) both greater than 1, \( p = ab > a \) and \( a \) would be a divisor
of \( p \) greater than 1 and therefore it would be a divisor of the
number \( n \) less than \( p \), contrary to the definition of \( p \).

**Theorem 2.** Every composite number \( n \) has at least one prime
divisor \( \leq \sqrt{n} \).

*Proof.* If \( n \) is a composite number, then \( n = ab \), where \( a \) and \( b \)
are natural numbers \( < n \). Without loss of generality, we may
assume that \( a \leq b \). Hence \( n = ab \geq a^2 \) so that \( a \leq \sqrt{n} \). But
the number $a$ is $> 1$, because if $a = 1$, then we should have $n = b$ while at the same time $b < n$. By Theorem 1, the number $a$ has a prime divisor $p$ which is obviously $\leq a$ and so $\leq \sqrt{n}$. But $p$, being a divisor of a divisor $a$ of the number $n$, is also a divisor of $n$. The number $n$ has therefore a prime divisor $p \leq \sqrt{n}$. We have thus proved Theorem 2.

3. How many prime numbers are there?

In order to answer this question we shall prove the following

**Theorem 3.** If $n$ is a natural number $> 2$, then between $n$ and $n!$ there is at least one prime number ($n!$ denotes the product $1 \cdot 2 \cdot 3 \ldots n$).

**Proof.** As $n > 2$, the integer $N = n! - 1$ is $> 1$ and, by Theorem 1, it has a prime divisor $p$, which is obviously $\leq N$ and so $< n!$. Now we cannot have $p \leq n$, because then $p$ would be one of the factors in the product $n! = 1 \cdot 2 \cdot 3 \ldots n$, and hence $p$ would be a divisor of the number $n!$, and being also a divisor of the number $N$, it would be a divisor of the difference of these numbers, i.e. the numbers $n! - N = 1$, which is impossible. Therefore $p > n$, and as we know, $p < n!$ we have $n < p < n!$ and Theorem 3 is proved.

Therefore, for every natural number there exists a prime number greater than that number, whence it follows that the number of primes is infinite, which was known to Euclid. In particular, it follows that there exist prime numbers having (in the decimal scale) at least three thousand digits, but no such number is known. The greatest known prime number today has 1332 digits: it is the number $2^{4423} - 1$ which was verified (cf. Hurwitz and Selfridge [1]) to be prime in the year 1961 (with the help of the electronic computer IBM 7090). It is worth while to observe the process of discovering prime numbers during the last fifteen years. At the beginning of the year 1951 the greatest known prime number was $2^{127} - 1$, having thirty-nine digits, which had already been proved to be a prime number in 1876.

In connection with Theorem 3 we observe that in 1850 Chebyshev proved a stronger theorem (the Bertrand postulate), stating
that for a natural number \( n > 3 \), there is at least one prime number between \( n \) and \( 2n - 2 \). It follows from this that in Theorem 3 the number \( n! \) can be replaced by the number \( 2n \). We now know how to give an elementary proof of this theorem, but it is rather long. It can even be proved that for a natural number \( n > 5 \) there are at least two prime numbers between \( n \) and \( 2n \) (see W. Sierpiński [7], pp. 395-400).

From the theorem of Chebyshev it easily follows that for every natural number \( s \) there exist at least three prime numbers each having \( s \) digits. Since each of the numbers

\[
10^{s-1}, \quad 2 \cdot 10^{s-1}, \quad 4 \cdot 10^{s-1} \quad \text{and} \quad 8 \cdot 10^{s-1}
\]

have \( s \) digits, by Chebyshev’s theorem for \( s > 1 \) there exist prime numbers \( p, q \) and \( r \) such that

\[
10^{s-1} < p < 2 \cdot 10^{s-1} < q < 4 \cdot 10^{s-1} < r < 8 \cdot 10^{s-1};
\]

it is clear that each of the numbers \( p, q, r \) has \( s \) digits.

For \( s = 1 \), we have four primes of one digit: 2, 3, 5 and 7. The number of two-digit primes is twenty-one, of three-digit primes is 143. Thus there exist at least three prime numbers of a hundred digits each. Until quite recently we did not know any such prime number. R. M. Robinson [4] has found three prime numbers of a hundred digits:

\[
81 \cdot 2^{324} + 1, \quad 63 \cdot 2^{326} + 1, \quad 35 \cdot 2^{327} + 1.
\]

We do not know so far any prime number having a thousand digits, although we know that there exist at least three such numbers.

4. How to find all the primes less than a given number

The method which we shall give was known a long time ago; it bears the name of the Sieve of Eratosthenes.

Suppose we want to find all the prime numbers not greater than some natural number \( a \). For this purpose we write down all the successive natural numbers greater than 1 up to \( a \) and from this sequence we cancel all those numbers which are not prime, i.e. all those numbers greater than 1 which, for every natural
number $n > 1$, are greater than $n$ and are divisible by $n$. As is easy to see, in this way every composite number $\leq a$ is cancelled and only prime numbers remain.

Thus in the sequence $1, 2, 3, 4, \ldots, a$ we cancel 1, then all numbers greater than two and divisible by 2, and further numbers greater than 3 and divisible by 3. It is not necessary now to cancel numbers divisible by 4, because every number $> 2$ and divisible by 2 has already been cancelled. We further cancel numbers greater than 5 and divisible by 5 and so on. We need not now cancel any number $> \sqrt{a}$, because, if $n$ is a composite number $\leq a$, then, by Theorem 2, the number $n$ has a prime divisor $p \leq \sqrt{n}$ and so $\leq \sqrt{a}$; thus, since $p \leq \sqrt{a}$, the number $n$ has already been cancelled, as we have cancelled numbers greater than $p$ and divisible by $p$.

Thus, for example, to obtain all prime numbers $\leq 100$, we cancel from the sequence $1, 2, 3, \ldots, 100$ the number 1 and then the numbers $> 2$ and divisible by 2, then numbers $> 3$ and divisible by 3, then numbers $> 5$ and divisible by 5, and lastly those $> 7$ and divisible by 7. All the numbers remaining in our sequence will be prime. We obtain in this manner the following sequence (in which the cancelled numbers are underlined and all those not underlined are prime)

\[1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100.\]
We denote the $n$th successive prime by $p_n$. Thus $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_{10} = 29$, $p_{25} = 97$. It is easy to calculate that $p_{100} = 541$.

In 1909 a table of primes less than 10 million was published. In this table, for each natural number $\leq 10,170,600$, not divisible by 2, 3, 5, or 7 the smallest of its prime factors is given: D.N. Lehmer, *Factor Table for the First Ten Millions*, Washington, Carnegie Institute 1909. In the year 1951 a table for prime numbers up to 11 million was published: J. P. Kulik, L. Poletti, R. J. Porter, *Liste des nombres premiers du onzième million (plus précisément de 10,006,741 à 10,999,997)*, Amsterdam 1951. A Pole, Jacob Philip Kulik (born in Lwow in 1793, died in Prague in 1863) prepared a manuscript (kept in the Austrian Academy of Sciences in Vienna) in which all prime numbers up to one hundred million are given.

These tables (after being checked) were useful when the tables of primes of the 11-th million, published in 1951, were in preparation.

Recently C. L. Backer and F. J. Gruenberger have prepared microcards containing all primes $< p_{6,000,000} = 104,395,301$. The microcards bear the name: *The first six million prime numbers*. The RAND Corporation, Santa Monica, published by the Microcard Foundation, Madison, Wisconsin 1959. The American scholars have announced that they will soon have an electronic computer containing in its memory 500 million consecutive primes (all numbers $p_n$ for $n \leq 500,000,000$).

5. Twin primes

There arise a series of questions about the infinite sequence of consecutive prime numbers, i.e. the sequence $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, \ldots$ Only some of these questions can be answered easily.

Thus, for example, the smallest two prime numbers are 2 and 3. These are successive natural numbers. The question then arises if there are other successive natural numbers which are both prime. It is easy to show that there are no such numbers because
of two successive natural numbers one is even, and, if it is > 2, then it is composite.

However, there are many pairs of successive odd numbers which are both prime, for example 3 and 5, 5 and 7, 11 and 13, 17 and 19, 29 and 31, 41 and 43. We call such pairs *twin numbers*. There are 152,892 such pairs of numbers less than 30 million.

Long ago the question was asked whether the number of twin primes is infinite. We do not know the answer to this question. In other words, we thus do not know whether the number 2 can be written as the difference of two primes in an infinity of ways.

It was conjectured that every even number can be written as the difference of two successive prime numbers in an infinity of ways, but we are not even able to prove that every even number can be written in at least one way as the difference of two successive prime numbers. This is verified for many successive even numbers, for example, \( 2 = 5 - 3 \), \( 4 = 11 - 7 \), \( 6 = 29 - 23 \), \( 8 = 97 - 89 \), \( 10 = 149 - 139 \), \( 12 = 211 - 199 \), \( 14 = 127 - 113 \), \( 16 = 1847 - 1831 \), \( 18 = 541 - 523 \), \( 20 = 907 - 887 \). Also, we cannot prove that every even number is the difference of two prime numbers (not necessarily successive).

We can, however, determine all odd numbers which are the differences of two prime numbers. For if an odd natural number \( n \) is the difference of two primes \( n = p - q \) then one of the primes must be even, i.e. one of the numbers \( p \) and \( q \) (the number \( q \), as is easy to see) must be equal to 2. Therefore \( n = p - 2 \) where \( p \) is an odd prime number. Thus all the odd natural numbers which can be expressed as the differences of two prime numbers are numbers less by 2 than an odd prime number, i.e. the numbers

\[
1, 3, 5, 9, 11, 15, ...
\]

Their number is, therefore, infinite.

But there are infinitely many odd numbers which are not the differences of two primes, for example all numbers of the form \( 6k + 1 \) where \( k \) is a natural number. In fact, we cannot have \( 6k + 1 = p - 2 \) where \( p \) is a prime number because then we would have \( p = 6k + 3 = 3(2k + 1) \) and thus \( p \) would be composite.
6. Conjecture of Goldbach

In 1742, Ch. Goldbach stated the conjecture that each even number > 2 is the sum of two primes. This conjecture still remains neither proved nor disproved. A stronger conjecture has been made, namely that every even number > 6 is the sum of two distinct prime numbers, and this is verified for numbers < 100,000 (see Pipping [1], [2]).

It can be proved that the last conjecture is equivalent to the statement that every natural number > 17 is the sum of three different primes. On the other hand, A. Schinzel has proved that the conjecture of Goldbach implies that every odd number > 17 is the sum of three different primes.

From the conjecture of Goldbach it easily follows that every odd number > 7 is the sum of three odd primes. For if \( n \) is a natural number and \( 2n+1 > 7 \) then \( 2n+1-3 = 2(n-1) > 4 \). The even number \( 2(n-1) > 4 \) is, by the conjecture of Goldbach, the sum of two primes \( p \) and \( q \), which cannot be even, because our number is > 4. The prime numbers \( p \) and \( q \) are therefore odd and the number \( 2n+1 = 3+p+q \) is the sum of three odd primes.

We do not know whether every odd number > 7 is the sum of three odd primes, but in 1937, I. Vinogradov proved that every sufficiently large odd number is the sum of three odd primes. We know a number \( a \) such that every odd number > \( a \) is the sum of three odd primes: \( a = 3^{15} \).

We can say that the decision about the question whether every odd number > 7 is the sum of three odd primes, is hindered only by the length of the necessary calculations, because it would be enough to explore only odd numbers > 7 and \( \leq a \), and for each given odd number one can decide after a finite number of simple arithmetical operations whether it is or is not the sum of three odd primes.

The position is different as regards the conjecture of Goldbach: here we cannot say that the decision whether the conjecture is true or not is hindered only by the length of the necessary calculations.
It has been proved by a method much more elementary than that of Vinogradov that every sufficiently large natural number is the sum of eighteen or fewer primes (see Yin Wen-Lin [1]).

It has been proved that every natural number \( > 11 \) is the sum of two or more different primes. For example, \( 12 = 5 + 7, 13 = 2 + 11, 17 = 2 + 3 + 5 + 7, 29 = 3 + 7 + 19 \). A. Mąkowski has proved that every natural number \( > 55 \) is the sum of different primes of the form \( 4k + 3 \), and has proved three analogous theorems about the sum of prime numbers each of the forms \( 4k + 1 \), \( 6k + 1 \) and \( 6k + 5 \).

From the conjecture of Goldbach it easily follows that every odd (positive or negative) integer can be written in an infinity of ways in the form \( p + q - r \) where \( p, q \) and \( r \) are odd primes.

Indeed, for every integer \( k \) there exists an odd prime number \( r \) such that \( 2k - 1 + r > 4 \) (it is enough to take for \( r \) a sufficiently large prime number). But then \( 2k - 1 + r \) is an even number > 4, and therefore, by the conjecture of Goldbach, \( 2k - 1 + r = p + q \), where \( p \) and \( q \) are odd prime numbers. Hence \( 2k - 1 = p + q - r \), in which the prime number \( r \) may be arbitrarily large. From this follows the interesting result of which we have spoken.

This result was proved in 1937 by J. G. van der Corput. However, the proof is extremely difficult (see J. G. van der Corput [1]).

As regards the conjecture of Goldbach, we observe that it is easy to prove that every natural number \( > 11 \) is the sum of two composite numbers. For, if \( n > 11 \) is an even number, then \( n - 4 \) is an even number > 2, i.e. a composite number, and \( n \) is the sum of two composite numbers \( 4 \) and \( n - 4 \). But if \( n > 11 \) is odd, then \( n - 9 \) is an even number > 2, i.e. it is composite, and \( n \) is the sum of two composite numbers \( 9 \) and \( n - 9 \). We should not conclude from this that the inquiry into composite numbers is easier than investigations about prime numbers. Thus we are not able to answer the question whether or not among the numbers \( F_n = 2^{2^n} + 1 \), where \( n = 1, 2, 3, \ldots \), we have infinitely many composite numbers (so far we only known thirty-eight such composite numbers, of which the greatest is \( F_{1945} \)).
G. H. Hardy and J. E. Littlewood made in [1] the conjecture (so far unproved) that every sufficiently large natural number which is not a perfect square is the sum of a square of an integer and a prime number.

As regards the conjecture of Hardy and Littlewood, we observe that it is easy to prove that there exist infinitely many squares of natural numbers which are, as also those which are not the sum of a prime number and the square of an integer.

For, on the one hand, if \( p \) is an odd prime, then \( \frac{p+1}{2} \) is a natural number and we have

\[
\left( \frac{p+1}{2} \right)^2 = \left( \frac{p-1}{2} \right)^2 + p;
\]

on the other hand, if \( n = 3k+2 \), where \( k \) is a natural number, then for some integer \( x \) and a prime number \( p \) we cannot have

\[ n^2 = x^2 + p, \]

for then \( n \) would be \( > x \) and

\[ p = n^2 - x^2 = (n+x)(n-x), \]

whence, considering that \( p \) is prime, \( n-x = 1 \) and \( n+x = p \), so that

\[ p = 2n-1 = 3(2k+1), \]

which is not possible for a natural number \( k \).

7. Hypothesis of Gilbreath

N. L. Gilbreath (in 1958) made the following conjecture.

If we write the sequence of successive prime numbers, and under it in the first row the sequence of successive differences of the prime numbers, in the second row the sequence of the absolute values of the differences of the successive terms in the first row, in the third row the sequence of the absolute values of the differences of the successive terms in the second row and so on, then in each row the first term will be 1.
Thus for example the first seventeen rows (without the sequence of primes) will be like this:

\[
\begin{array}{cccccccccccccc}
2, & 3, & 5, & 7, & 11, & 13, & 17, & 19, & 23, & 29, & 31, & 37, & 41, & 43, & 47, & 53, & 59, & 61 \\
1, & 2, & 4, & 2, & 4, & 2, & 4, & 6, & 4, & 2, & 4, & 6, & 2, & 6, & 2, & 4, & 2 \\
1, & 2, & 2, & 2, & 2, & 2, & 2, & 4, & 4, & 2, & 2, & 2, & 2, & 2, & 0, & 4 \\
1, & 2, & 0, & 0, & 0, & 0, & 0, & 2, & 0, & 0, & 0, & 2, & 4 \\
1, & 2, & 0, & 0, & 0, & 2, & 2, & 2, & 2, & 0, & 0, & 2, & 2 \\
1, & 2, & 0, & 0, & 0, & 2, & 0, & 0, & 2, & 0, & 2, & 0 \\
1, & 2, & 0, & 0, & 0, & 2, & 0, & 0, & 2, & 0, & 0 \\
1, & 2, & 2, & 2, & 2, & 2, & 2, & 0, & 0 \\
1, & 0, & 0, & 0, & 0, & 0, & 0, & 2, & 0 \\
1, & 0, & 0, & 0, & 0, & 0, & 2, & 2 \\
1, & 0, & 0, & 2, & 2 \\
1, & 0, & 2, & 2 \\
1, & 2, & 0 \\
1 & \\
\end{array}
\]

Thus we have \(a_1 = 3, a_2 = 8, a_3 = 14\) (see the table given above). It has been calculated that \(a_4 = 14, a_5 = 25, a_6 = 24, a_7 = 23, a_8 = 22, a_9 = 25, a_{10} = 59, a_{14} = 97, a_{15} = 174, a_{22} = 289, a_{23} = 740, a_{24} = 874, a_{34} = 866, a_{35} = 2180, a_{64} = 5940, a_{65} = 23,266, a_{94} = 31,533.\)

If one can prove that \(a_n > 2\) for any natural number \(n\) then the truth of the conjecture of Gilbreath would easily follow.

8. Decomposition of a natural number into prime factors

With the help of Theorem 1 we now prove

**Theorem 4.** Every natural number > 1 is the product of factors each of which is a prime number. We do not exclude products having only one factor.
Proof. Let \( n \) be a given natural number \( > 1 \). By Theorem 1, the number \( n \) has (at least one) prime divisor \( p' \) and we may assume that \( p' \) is the smallest prime factor of \( n \). We then have \( n = p'n' \) where \( n' \) is a natural number.

If \( n' = 1 \), then \( n = p' \) and \( n \) is the product formed from only one factor. If \( n' > 1 \) then \( n' \) has a prime divisor \( p'' \) of which one may suppose that it is the smallest prime divisor of \( n' \). This is at the same time a prime divisor of \( n \) and by the definition of the number \( p' \) it follows that we must have \( p' \leq p'' \). We thus have \( n' = p''n'' \) and either \( n'' = 1 \), in which case \( n \) is the product of two primes \( p' \) and \( p'' \) (not necessarily different), or \( n'' > 1 \) and we can proceed with \( n'' \) as has been done earlier with the \( n \) and \( n' \) and so on. As \( n = p'n' \) and \( p' > 1 \) we have \( n' < n \). Similarly we have \( n'' < n' \) and so on. The natural numbers \( n, n', n'', ... \) then form a decreasing sequence, which cannot therefore have more than \( n \) terms. So, for a certain natural number \( k \), \( n^{(k)} \) will be the last term of this sequence; then certainly \( n^{(k)} = 1 \), because in case \( n^{(k)} > 1 \) we could subdivide

\[ n^{(k)} = p^{(k+1)}n^{(k+1)} \]

and we would obtain \( n^{(k+1)} \) as a term of our sequence. We have, therefore,

\[ n = p'n', \quad n' = p''n'', \ldots, \quad n^{(k-1)} = p^{(k)}n^{(k)} \quad \text{and} \quad n^{(k)} = 1, \]

whence we find

(1) \[ n = p'p''p''' \ldots p^{(k)}, \]

where \( p', p'', p''', \ldots, p^{(k)} \) are primes and we may suppose that \( p' \leq p'' \leq p''' \leq \ldots \leq p^{(k)} \) (as for each of the numbers \( n, n', \ldots \) we denote thereby its smallest prime divisor).

Among the prime factors (1) some may be equal. If we write out equal factors as the powers of one of them with the corresponding natural number as exponent, then from formula (1) we have the formula

(2) \[ n = q_1^{a_1}q_2^{a_2} \ldots q_s^{a_s} \]

where \( s \) is a natural number, \( q_1, q_2, \ldots, q_s \) are prime numbers
in increasing order and \(a_1, a_2, \ldots, a_s\) are natural exponents. We call formula (2) the canonical decomposition of \(n\) into prime factors.

We have not only proved Theorem 4 but also given a method of obtaining for each natural number \(n > 1\) its canonical decomposition. Theoretically it is always possible to obtain this decomposition for a given natural \(n > 1\), but in practice one may be involved in very difficult and lengthy calculations. For some numbers these calculations become so long that at present even with the use of the biggest calculating machines we are not able to obtain them. We do not know, for example, the decomposition into prime factors of the number \(2^{101} - 1\) (having 31 digits); it has only been proved that it is the product of two different prime factors of which the lesser (not known so far) has at least 11 digits (cf. Brillhart and Johnson [1]). Also we do not know the decomposition into prime factors of the number \(F_{13} = 2^{2^{13}} + 1\). However, for the number \(F_{1945} = 2^{2^{1945}} + 1\), which has more than \(10^{582}\) digits (because \(2^{1945} = 32 \cdot 2^{1940} = 32(2^{10})^{194} > 30(10^3)^{194} = 3 \cdot 10^{583}\), whence \(F_{1945} > 2^{3 \cdot 10^{583}} = (2^{10})^{3 \cdot 10^{582}} > 10^9 \cdot 10^{582}\) and whose digits we are unable to give, the smallest prime divisor was obtained a few years ago: it is \(5 \cdot 2^{1947} + 1\) having 587 digits (Robinson [4]). However, we do not know any other prime divisors of the number \(F_{1945}\) or its decomposition into prime factors (see § 22).

Regarding the decomposition (2) of the number \(n > 1\) into prime factors, the question arises whether such a decomposition is unique (if the numbers \(q_1, q_2, \ldots, q_s\) form an increasing sequence). The proof of unicity depends on some simple theorems on prime numbers.

Theorem 5. The prime number \(p\) has only two natural divisors: 1 and \(p\).

Proof. If the number \(p\) has another divisor \(a\) other than 1 and \(p\), then obviously we have \(1 < a < p\) and \(p = a \cdot b\), where \(b\) is a natural number > 1, because in case \(b = 1\), \(p\) would be equal to \(a\), contrary to the supposition about the number \(a\). The number \(p\) would then be the product of two natural numbers
greater than 1, contrary to the supposition that \( p \) is a prime number. We have thus proved Theorem 5.

As is easy to see, the following theorem holds:

*If the natural number \( p \) has exactly two natural divisors, then it is a prime number.*

Namely \( p \) must then be > 1, and, if \( p \) were not prime, then \( p \) would be the product of two natural divisors greater than 1, \( a \) and \( b \), so that \( p = a \cdot b \) and \( b > 1 \), \( 1 < a < p \) and \( a \) would be a divisor of \( p \) different from 1 and \( p \); therefore the number \( p \) would have at least three different natural divisors.

We thus have

**Theorem 6.** In order that a natural number be prime, it is necessary and sufficient that it have exactly two different natural divisors (obviously 1 and itself).

We also prove

**Theorem 7.** If \( a \) and \( b \) are natural numbers and the product \( ab \) is divisible by the prime number \( p \), then one at least of the numbers \( a \) and \( b \) is divisible by \( p \).

*Proof.* If Theorem 7 were not true, there would exist a least prime number \( p \) for which it is not true and for such a prime number there would exist a least product \( ab \) of two natural numbers \( a \) and \( b \) divisible by \( p \), although none of the factors \( a \) and \( b \) is divisible by \( p \). We show that the numbers \( a \) and \( b \) are then less than \( p \). Indeed if, for example, \( a > p \), we would have \( a = kp + a_1 \), where \( a_1 < p \) and \( a_1 > 0 \), because \( a \) is not divisible by \( p \). Hence \( ab = (kp + a_1)b = kpb + a_1b \), and since \( ab \) and \( kpb \) are divisible by \( p \), \( a_1b \) is divisible by \( p \). But \( a_1 < p < a \) and \( a_1 \) is not divisible by \( p \), so that \( a_1b < ab \) — which contradicts the supposition about the product \( ab \). Therefore \( a < p \), and similarly we prove that \( b < p \), whence \( ab < p^2 \).

Since \( ab \) is divisible by \( p \), we have \( ab = lp \), where \( l \) is a natural number, greater than 1, because otherwise \( p \) would be equal to \( ab \), where \( a > 1 \), \( b > 1 \) (for the numbers \( a \) and \( b \) are not divisible by \( p \)). On the other hand, since \( ab < p^2 \), we have \( l < p \). The number \( l \), being a natural number > 1, has a prime divisor \( q \leq l < p \). Because \( q < p \) and by the definition of the number
WHAT WE KNOW AND WHAT WE DO NOT KNOW

$p$, the product $ab$, being divisible by $l$, is divisible by the prime number $q < p$; hence one at least of the factors $a$ and $b$ must be divisible by $q$. For example, if $a$ is divisible by $q$, then $a = a'q$. But $l$ is divisible by $q$, so $l = tq$, where $t$ is a natural number. Because $ab = lp$, we have $a'qb = tqp$, whence $a'b = tp$, whereby because $a = a'q$, we have $a' < a$, whence $a'b < ab$—contrary to the supposition about the product $ab$. The supposition that Theorem 7 is not true thus leads to a contradiction.

From the theorem proved above we easily infer by induction the following

**Corollary.** If $a_1, a_2, ..., a_m$ is a finite sequence of natural numbers whose product is divisible by the prime number $p$, then one at least of the numbers $a_1, a_2, ..., a_m$ must be divisible by $p$.

**Proof.** The corollary is true for $m = 2$. We suppose that it is true for a number $m$ and let $a_1, a_2, ..., a_m, a_{m+1}$ be $m+1$ natural numbers. If the product $a_1a_2...a_m a_{m+1}$ is divisible by the prime number $p$, then, by Theorem 7, one at least of the numbers $a_1a_2...a_m$ and $a_{m+1}$ is divisible by $p$. If the number $a_1a_2...a_m$ is divisible by $p$, then, by the supposition that the corollary is true for the number $m$, at least one of the numbers $a_1, a_2, ..., a_m$ is divisible by $p$. From the truth of the corollary for $m$ follows its truth for $m+1$.

We now suppose that there exist natural numbers which have two different canonical decompositions into prime factors. Among such natural numbers there exists one which is the smallest. Let this be the number $n$, having besides the canonical decomposition

$$n = q_1^{a_1}q_2^{a_2}...q_s^{a_s}$$

also the decomposition

(3) $$n = r_1^{b_1}r_2^{b_2}...r_t^{b_t}$$

where $r_1, r_2, ..., r_t$ is an increasing sequence of prime numbers and $b_1, b_2, ..., b_t$ are natural numbers. By (2) the number $n$ is divisible by $q_1$, and thus by (3) and by means of the corollary to Theorem 7, at least one of the numbers $r_1, r_2, ..., r_t$ must be divisible by $q_1$—obviously $r_1$ because $q_1$ is the smallest prime divisor
of number (3). But by Theorem 5, the prime number \( r_1 \) has only two natural divisors: 1 and \( r_1 \), so that since the prime number \( q_1 \) is also a divisor of \( r_1 \), we must have \( r_1 = q_1 \). Putting in formula (3) \( q_1 \) instead of \( r_1 \), we obtain from (2) for a natural number \( n' \), where \( n = q_1n' \), the equation

\[
n' = q_1^{a_1-1}q_2^{a_2} \ldots q_s^{a_s} \cdot r_2^{b_2} \ldots r_1^{b_1};
\]

because the number \( n' \) is less than \( n \) by the supposition about the number \( n \) the number \( n' \) has only one canonical decomposition into prime factors, whence it easily follows that \( s = r_1 = q_2, r_3 = q_3, \ldots, r_s = q_s, a_1 = b_1, a_2 = b_2, \ldots, a_s = b_s \). Decompositions (2) and (3) are thus identical, contrary to the supposition. The supposition that there exist natural numbers having two different canonical decomposition into prime factors leads to a contradiction.

We have thus proved

**Theorem 8.** Every natural number \( n > 1 \) has only one decomposition into prime factors if we do not consider the order of the factors.

9. Which digits can there be at the beginning and at the end of a prime number?

The last digit of a prime number having more than one digit cannot be even because then the number would be \( > 2 \), and thus even and composite; also, the last digit cannot be 5 because then the number would be greater than 5 and divisible by 5, and so it would be composite. Thus the last digit of a prime number \( > 10 \) can only be 1, 3, 7 or 9. The question then arises whether we can say something more about the digits of a prime number, for example about the set of the last few or the first few digits of a prime number. It appears that more than this cannot be said because of the following theorem:

*If we have two arbitrary sequences of digits (of the decimal system) \( a_1, a_2, \ldots, a_m \) and \( b_1, b_2, \ldots, b_n \) where \( b_n = 1, 3, 7 \) or 9, then there exist arbitrarily many prime numbers \( p \) such that their first \( m \) digits are successively \( a_1, a_2, \ldots, a_m \) and their last \( n \) digits are successively \( b_1, b_2, \ldots, b_n \).*
The proof of this theorem is difficult, although it can be carried out in an elementary way (see Sierpiński [4]).

It follows from this theorem that there exist prime numbers having at the beginning and at the end an arbitrarily large number of digits equal to 1 (but the middle digits may be other than 1).

In this connection the problem arises whether there exist infinitely many prime numbers whose digits are all 1. We do not know the answer to this question. We know only a few prime numbers whose digits are all 1, for example 11 and

\[ 11,111,111,111,111,111,111,111 = \frac{10^{23} - 1}{9}. \]

The proof (given by M. Kraitchik [1], vol. II) that the last number is prime, is not easy. However, it is easy to prove that, if a number whose digits are all 1 is prime, then the number of its digits must be prime. This property, however, is not sufficient because, for example,

\[ 111 = 3 \times 37, \quad 11,111 = 41 \times 271, \quad 1,111,111 = 239 \times 4649. \]

Also the number \((10^{37} - 1)/9\) having thirty-seven digits is composite, and the number \((10^{641} - 1)/9\) having 641 digits is composite (divisible by 1283).

Prime numbers other than those formed of the same digits have been found which remain prime after every permutation of their digits, e.g. 13, 113. We do not know if their number is finite.

Also, we do not know if there exist infinitely many prime numbers whose first and last digits are 1, and the remaining ones are 0, as for example the number 101. It is easy to prove that such a prime number must be of the form \(10^{2n} + 1\), where \(n\) is natural number, but this property is not sufficient because of the example \(10^{22} + 1 = 73.137\). We cannot answer the question whether the sequence of sums of the digits of consecutive prime numbers tends to infinity.
10. Number of primes not greater than a given number

For a given number \( x \), we denote by \( \pi(x) \) the number of prime numbers not greater than \( x \). We then have, for example, \( \pi(1) = 0 \), \( \pi(2) = 1 \), \( \pi(3) = 2 \), \( \pi(4) = 2 \), \( \pi(5) = 3 \), \( \pi(10) = 4 \), \( \pi(100) = 25 \), \( \pi(1000) = 168 \), \( \pi(10,000) = 1229 \), \( \pi(10^8) = 5,761,455 \), \( \pi(10^9) = 50,847,534 \), \( \pi(10^{10}) = 455,052,512 \).

L. Locher-Ernst observed that for \( n > 50 \) the expression

\[
f(n) = \frac{n}{1 + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \ldots + \frac{1}{n}}
\]

gives a fairly good approximate value of the number \( \pi(n) \). For example, \( \pi(10^3) = 168 \), while \( f(10^3) = 167.1 \). For \( n = 10^9 \) the quotient \( \frac{\pi(n)}{f(n)} \) is 1.007 and for \( n = 10^{10} \) it is 1.005.

We can also prove in an elementary way, although the proof is lengthy and complicated, that the ratio \( \frac{\pi(n)}{f(n)} \) tends to 1 as \( n \) tends to infinity.

For large \( n \) the expression \( f(n) \) is difficult to compute. However, other approximate expressions for the number \( \pi(n) \) are known, for example the expression \( n / \log n \), where \( \log n \) denotes the natural logarithm of \( n \) (logarithm to the base \( e \)). J. Hadamard and Ch. de la Vallée Poussin proved in 1896 that the ratio of \( \pi(n) \) to \( n / \log n \) tends to 1 when \( n \) tends to infinity. This implies that the ratio of \( p_n \) to \( n \log n \) tends to 1 when \( n \) tends to infinity. We can prove that the milliardth prime (i.e. the number \( p \)) has eleven digits.

It is easy to prove that for integral \( n > 1 \)

\[
\frac{\pi(n-1)}{n-1} < \frac{\pi(n)}{n},
\]

where \( n \) is a prime number, and

\[
\frac{\pi(n-1)}{n-1} > \frac{\pi(n)}{n},
\]

where \( n \) is a composite number. We can prove in an elementary way that the ratio of \( \pi(n) \) to \( n \) tends to zero when \( n \) tends to infinity.
It is clear that \( \pi(p_n) = n \) for any natural \( n \).

It is easy to prove that there exist arbitrarily long sequences of natural numbers which contain no prime numbers. A sequence of \( m \) such successive numbers is, for example, the sequence \((m+1)! + 2, (m+1)! + 3, (m+1)! + 4, \ldots, (m+1)! + (m+1)\), because the first number of this sequence is divisible by 2, the second by 3, etc., and the last by \( m+1 \); thus they are all composite.

For \( m = 100 \) the numbers would be gigantic, but between the prime numbers 370,261 and 370,373 there lie 111 successive composite numbers. Among the hundred successive numbers from 1,671,800 to 1,671,900 there is no prime number.

It is difficult to prove that there exist prime numbers on both sides of which there are arbitrarily many composite numbers, i.e. that for every natural \( m \) there exist prime numbers \( p \) such that each of the numbers \( p-k \), and \( p+k \), where \( k = 1, 2, \ldots, m \), is composite.

It is also difficult to prove a theorem of E. Landau stating that for a sufficiently large natural numbers \( n \) we have \( \pi(2n) < 2\pi(n) \), i.e. that for such \( n \) the number of primes \( \leq n \) is greater than the number of primes lying between \( n \) and \( 2n \).

We do not know if \( \pi(x+y) \leq \pi(x) + \pi(y) \) for all natural numbers \( x > 1 \) and \( y > 1 \).

11. Some properties of the \( n \)th prime number

The proof of the theorem of H. J. Scherk (announced by him in 1830)—that for a natural \( n \) we have, for suitably chosen signs + or −, the formulae

\[
\begin{align*}
p_{2n} &= 1 \pm p_1 \pm p_2 \pm \ldots \pm p_{2n-2} + p_{2n-1}, \\
p_{2n+1} &= 1 \pm p_1 \pm p_2 \pm \ldots \pm p_{2n-1} + 2p_{2n}
\end{align*}
\]

hold, is difficult.

Thus for example,

\[
\begin{align*}
p_6 &= 1 + p_1 - p_2 - p_3 + p_4 + p_5, \\
p_7 &= 1 + p_1 - p_2 - p_3 + p_4 - p_5 + 2p_6,
\end{align*}
\]

i.e.

\[
13 = 1 + 2 - 3 - 5 + 7 + 11, \quad 17 = 1 + 2 - 3 - 5 + 7 - 11 + 2.13.
\]
We can also prove that for a natural $n$ and a suitable choice of signs $+$ or $-$ we have

$$p_{2n+1} = \pm p_1 \pm p_2 \pm \cdots \pm p_{2n-1} \pm p_{2n}.$$  

For example,

$$p_7 = p_1 + p_2 - p_3 - p_4 + p_5 + p_6,$$

that is

$$17 = 2 + 3 - 5 - 7 + 11 + 13.$$  

It can be proved that, if $a$ and $b > a$ are two positive numbers, then there exist prime numbers $p$ and $q$ such that $a < p/q < b$ (see Sierpiński [7], pp. 410–411). It can be proved that, for every positive real number $x$, the sequence $p_{n(x^y)/n}$ tends to $x$ as $n$ tends to infinity.

It has been proved that there exist infinitely many prime numbers $p$ such that the prime number following $p$ is nearer to $p$ than the prime preceding $p$, and also that there exist infinitely many prime numbers $p$ such that the prime preceding $p$ is nearer to $p$ than the following prime. In other words—it has been proved that there are infinitely many natural numbers $n$ such that

$$p_{n+1} - p_n < p_n - p_{n-1}, \quad \text{i.e.,} \quad p_n > \frac{p_{n-1} + p_{n+1}}{2},$$

and also that there are infinitely many natural numbers $n$ such that $p_n < (p_{n-1} + p_{n+1})/2$.

However, we do not know if there exist infinitely many $n$ for which $p_n = (p_{n-1} + p_{n+1})/2$. It is conjectured that the answer is affirmative. We have

$$p_n = \frac{p_{n-1} + p_{n+1}}{2} \text{ for } n = 16, 37, 40, 47, 55, 56, 240, 273.$$

P. Erdős and P. Turán have even proved that there exist infinitely many natural numbers $n$ such that $p_n^2 > p_{n-1}p_{n+1}$ and infinitely many $n$ for which $p_n^2 < p_{n-1}p_{n+1}$.

Also it has been shown that $p_{n+1} < p_{n-1} + p_n$ for $n = 3, 4, 5, \ldots$

We have the following theorem (whose proof is not difficult but is certainly lengthy):
For every natural number $m$, there exists a natural number $n$ such that

$$\frac{1}{p_1} + \frac{1}{p_2} + \ldots + \frac{1}{p_n} > m.$$  

There exist sequences of four successive prime numbers containing two twin primes, for example 11, 13, 17, 19 or 179, 181, 191, 193. If such a set of four is formed of prime numbers $p$, $p+2$, $p+6$, and $p+8$, then we say that we have a quadruplet. The first of the given sets of fours is a quadruplet, the second is not. We get other examples of quadruplets for $p = 5$, 101, 191, 821, 1481, 3251. The conjecture has been advanced that there are infinitely many such quadruplets.

W. A. Golubew calculated in 1959 that in the first 10 million numbers we have 899 quadruplets and in the first fifteen million numbers we have 1209. The greatest quadruplet known so far, as stated by A. Ferrier, is obtained for $p = 2,863,308,731$.

12. Polynomials and prime numbers

The question arises if there exists a polynomial $f(x)$ in the variable $x$, having integral coefficients, which for each natural number $x$ gives a prime number $f(x)$. We shall show that there is no such polynomial. Let

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

be a polynomial of degree $m$ with integral coefficients $a_0$, $a_1$, ..., $a_m$, where $a_0 \neq 0$. If $a_0 < 0$ then, for sufficiently large $x$, $f(x) < 0$; we then suppose that $a_0 > 0$. Then, as we know, there exists such an integer $x_0$ that

$$n = f(x_0) > 1$$

and that

$$f(x) > f(x_0) \quad \text{for} \quad x > x_0.$$  

We shall show that, for an arbitrary natural number $k$, $f(x_0 + kn)$ is composite. For, if $x$ and $h$ are natural numbers, then for every natural $i$ the number $(x+h)^i - x^i$ is divisible by $(x+h)^i -
$-x = h$; consequently we deduce that the numbers $a_{m-i} (x+h)^i - a_{m-i} x^i$ for $i = 0, 1, 2, \ldots, m$ are divisible by $h$, whence the number $f(x+h) - f(x)$ is divisible by $h$. It follows that the number $f(x_0 + kn) - f(x_0)$ is divisible by $kn$, i.e. $f(x_0 + kn) - n = tn$, which gives $f(x_0 + kn) = (t+1)n$ and it is proved that the number $f(x_0 + kn)$, which we know to be $> f(x_0) = n$, is divisible by the natural number $n > 1$, and so it is composite.

We have thus proved that if $f(x)$ is a polynomial with integral coefficients, the coefficient of the highest power of $x$ being positive, then for infinitely many natural numbers $x$ the number $f(x)$ is composite.

However, we know polynomials which for many successive natural numbers assume prime numbers as their value. Such is, for example, the polynomial of Euler $x^2 + x + 41$, which for $x = 0, 1, 2, \ldots, 39$ gives different prime numbers. It has been conjectured that there exist infinitely many natural numbers $x$ for which $x^2 + x + 41$ is a prime number. The polynomial $y^2 - 79y + 1601$ gives prime numbers for $y = 0, 1, 2, \ldots, 79$ but not all different. (This polynomial is obtained from $x^2 + x + 41$ by the substitution $x = y - 40$.)

The question now arises if there exist polynomials which for natural values of the variable give infinitely many prime numbers.

Obviously there exists such a polynomial of the first degree, for example the polynomial $2x + 1$. But we do not know any polynomial of degree $> 1$ which gives infinitely many prime numbers (for a natural value of $x$). We do not know if the binomial $x^2 + 1$ is such a one.

This binomial gives prime numbers for $x = 1, 2, 4, 6, 10$. It has been calculated that for $x \leq 10,000$ there are 842 prime numbers of the form $x^2 + 1$ (where $x$ is a natural number); for $x \leq 100,000$ there are 6656 such numbers and for $x \leq 180,000$ there are 11,223 such prime numbers (see Shanks [1]). The conjecture has been made that for every natural number $k$ there exist infinitely many prime numbers of the form $x^2 + k$ where $x$ is a natural number.

Obviously there exists only one prime number of the form
$x^3 + 1$, where $x$ is a natural number, but the conjecture has been put forth that there is an infinity of primes of the form $x^3 + 2$, where $x$ is a natural number (we obtain prime numbers for $x = 1, 3, 5, 29$) and also of the form $x^3 - 2$ (we have prime numbers for $x = 9, 15, 19, 27$).

B. M. Bredihin [1] has proved that there exist infinitely many prime numbers of the form $x^2 + y^2 + 1$ where $x$ and $y$ are natural numbers. The proof is very laborious and difficult. Later (in § 19) we prove that there exists an infinity of prime numbers of the form $x^2 + y^2$ where $x, y$ are natural numbers. Nevertheless we do not know if there are an infinity of primes which are the sums of the cubes of three integers.

13. Arithmetic progressions consisting of prime numbers

It has been proved that there are infinitely many arithmetic progressions formed of three different prime numbers, but the proof is difficult (see van der Corput [1]). However, we do not know if there are infinitely many arithmetic progressions of three different primes of which the first term is 3. We know many such progressions, for example 3, 7, 11; 3, 11, 19; 3, 13, 23; 3, 17, 31; 3, 23, 43; 3, 31, 59; 3, 37, 71; 3, 41, 79; 3, 43, 83.

It is easy to prove that there are no arithmetic progressions of three different primes of which the first term is the number 2 (because then the third term of the progression would be even and $> 2$). However, the conjecture has been made that there exist infinitely many arithmetic progressions of three prime numbers of which the first term is any arbitrarily given odd prime number.

There is only one arithmetic progression of prime numbers with common difference 2, namely 3, 5, 7 (since of three successive odd numbers one is always divisible by 3). It is also easy to prove that there exists only one arithmetic progression of three primes with difference 4, viz. 3, 7, 11. Obviously there is no arithmetic progression of three primes with an odd number as common difference. It has been conjectured that there exist infinitely many arithmetic progressions of three prime numbers with difference 6. Such are, for example, the progressions: 5, 11, 17; 11, 17, 23; 17, 23, 29. We thus have also a progression of five terms with difference 6.
formed from five primes: 5, 11, 17, 23, 29, but there is only one such progression because in every progression of five natural numbers with difference 6 one at least is divisible by 5.

The question arises whether there exist arithmetic progressions formed from an arbitrary number of different prime numbers. The longest known arithmetic progression of different primes has 13 terms: this progression with first term 4943 and difference 60,060 was found by Seredinski. We do not know if there exists an arithmetic progression of a hundred different primes.

M. Cantor [1] has proved that, in an arithmetic progression formed from \( n > 1 \) prime numbers greater than \( n \), the common difference must be divisible by each prime number \( \leq n \). This implies that if there is an arithmetic progression of a hundred different prime numbers, then the common difference of that progression must be a gigantic number having at least some scores of digits.

The conjecture has been made that if \( r \) is a natural number divisible by each prime number \( \leq n \) (where \( n \) is a given natural number \( > 1 \)) then there are infinitely many arithmetic progressions with difference \( r \), formed from \( n \) successive prime numbers. For example 47, 53, 59 is an arithmetic progression with difference 6, formed from three successive prime numbers. Other such progressions are 151, 157, 163; 167, 173, 179. We also know arithmetic progressions of four successive prime numbers with difference 6, for example, 251, 257, 263, 269 and 1741, 1747, 1753, 1759.

14. Simple Theorem of Fermat

**Theorem 9.** If \( p \) is a prime number, then for every integer \( a \) the number \( a^p - a \) is divisible by \( p \).

**Proof.** Let \( p \) be a given prime number. The theorem is obviously true for \( a = 1 \). Now let \( a \) be a given natural number and we suppose that the theorem is true for the number \( a \). By Newton's binomial theorem, we have.

\[
(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a + 1,
\]
where for \( k = 1, 2, \ldots, p-1 \) we have

\[
\binom{p}{k} = \frac{p(p-1) \cdots (p-k+1)}{1 \cdot 2 \cdot \ldots \cdot k},
\]

and, which is well known, the numbers \( \binom{p}{k} \) are integers. We deduce that the number \( 1 \cdot 2 \cdots k \binom{p}{k} \) is divisible by \( p \), so that, by corollary to Theorem 7, one at least of the numbers \( 1, 2, \ldots, k, \binom{p}{k} \) must be divisible by \( p \). But since \( k < p \), none of the numbers \( 1, 2, \ldots, k \) is divisible by \( p \), whence we deduce that the number \( \binom{p}{k} \) must be divisible by \( p \). Hence, because of (4), we deduce that the number \( (a+1)^p - a^p - 1 \) is divisible by \( p \). Adding to this the number \( a^p - a \), divisible by \( p \) (because we have assumed that the theorem is true for the number \( a \)), we deduce that the number \( (a+1)^p - (a+1) \) is divisible by \( p \), i.e. the theorem is true for the number \( a+1 \).

Thus we have proved by induction that the theorem is true for every natural number \( a \). For the number \( 0 \) it is obviously true. If \( p \) is an odd prime number, then we have \( (-a)^p = -a^p \) and so \( (-a)^p - (-a) = -(a^p - a) \), whence we deduce that the theorem is also true for negative integer \( a \). Now, if \( p = 2 \) we have \( a^2 - a = (a-1)a \) and of two successive integers \( a-1 \) and \( a \) one is always even and so we always have \( 2 \mid a^2 - a \). \(^{(1)}\)

Theorem 9 is therefore proved.

As a particular case of Theorem 9 for \( a = 2 \) we find that for every prime number \( p \) the number \( 2^p - 2 \) is divisible by \( p \). The question arises whether, conversely, if \( n \) is a natural number \( > 1 \) such that \( n \mid 2^n - 2 \), \( n \) must be prime.

To many theorems and conjectures we are led by an examination of large number of particular cases. If, for example, we consider all the successive natural numbers \( > 1 \) and \( \leq 300 \), it will be found that every natural number \( n \) such that \( 1 < n \leq 300 \) and for which the number \( 2^n - 2 \) is divisible by \( n \) is a prime number. This is probably what led the Chinese 25

\(^{(1)}\) The symbol \( r \mid s \) denotes that the number \( s \) is divisible by \( r \).
centuries ago to declare the theorem that, if for a natural \( n > 1 \) the number \( 2^n - 2 \) is divisible by \( n \), then the number \( n \) is prime. It turned out, however, that the theorem is false because the number \( 2^{341} - 2 \), as we shall see presently, is divisible by 341 and the number \( 341 = 11 \cdot 31 \) is composite.

That the number \( 2^{341} - 2 \) is divisible by 341 we may see in the following manner. We obviously have \( 2^{341} - 2 = (2^{31})^{11} - 2^{11} + 2^{11} - 2 \). The number \( 2^{10} - 1 = 1023 = 3 \cdot 341 \) is divisible by 341 and so the number \( (2^{10})^3 - 1 \) is divisible by 341. The numbers \( 2^{11} - 2 = 2(2^{10} - 1) \) and \( 2^{31} - 2 = 2((2^{10})^3 - 1) \) are therefore divisible by 341, whence it follows that the number \( (2^{31})^{11} - 2^{11} \) is divisible by 341 (because for natural numbers \( a, b \) and \( k \) the number \( a^k - b^k \) is, as we know, divisible by \( (a - b) \)). Hence, because of our equation for the number \( 2^{341} - 2 \), it follows at once that it is divisible by 341. This completes the proof.

We come to the next question, namely whether there are infinitely many numbers \( n \) for which the Chinese theorem is false. In order to show that the answer to this question is in the affirmative it is sufficient (since we know that the odd composite number 341 does not satisfy the Chinese theorem) to show that for every composite odd number \( n \), not satisfying the Chinese theorem, there exists an odd composite number greater than \( n \) which also does not satisfy the Chinese theorem. We therefore assume that the odd composite number \( n = ab \), where \( a \) and \( b \) are natural numbers > 1, does not satisfy the Chinese theorem, so that \( n | 2^n - 2 \). The number \( m = 2^n - 1 = (2^a)^b - 1 \) is odd, composite, because it is divisible by the number \( 2^a - 1 > 1 \) (as \( a > 1 \)) and less than \( m \) (as \( b > 1 \)) and also \( m > n \) (as \( n > 1 \)). It is then enough to show that \( m | 2^n - 2 \). Now, since \( n | 2^n - 2 \) and considering that \( n \) is an odd number, we have \( n | 2^{n-1} - 1 \), so \( 2^{n-1} - 1 = kn \) where \( k \) is a natural number. Hence \( 2^{n-1} = 2^{2(2^{n-1} - 1)} = 2^{2kn} = (2^n)^{2k} \).

The number \( 2^{n-1} - 1 = (2^n)^{2k} - 1 \) is therefore divisible by the number \( 2^n - 1 = m \) and thus \( 2^{n-1} - 2 \) is divisible by \( m \), whence the composite number \( m \) does not satisfy the Chinese theorem.

The problem now arises whether there exist even composite numbers not satisfying the Chinese theorem. Only in 1950, D. H. Lehmer discovered such a number, 161,038. Finding this
WHAT WE KNOW AND WHAT WE DO NOT KNOW

number was somewhat difficult but to verify that it is a divisor of the number $2^{161,038} - 2$ is not difficult. It is easy to see that $161,038 = 2 \cdot 73 \cdot 1103$, $161,037 = 3^{2} \cdot 29 \cdot 617$, $2^{9} - 1 = 7,73$, $2^{29} - 1 = 1103 \cdot 486,737$. The number $2^{161,037} - 1$ is therefore divisible by $2^{9} - 1$ and by $2^{29} - 1$ so also by 73 and by 1103, and therefore the number $2^{161,038} - 2$ is divisible by 2, 73 and 1103, since these are different prime numbers, therefore the number $2^{161,038} - 2$ is divisible by their product, i.e. by the number 161,038.

In 1951, N.G.W.H. Beeger [1] proved that there exist infinitely many even numbers $n$ for which $2^{a} - 2$ is divisible by $n$.

It has also been proved that there exist infinitely many pairs of distinct prime numbers $p$ and $q$ such that the number $2^{pq} - 2$ is divisible by $pq$, and A. Schinzel [1] has proved that for each integer $a$ and each natural number $m$, there exist distinct primes $p > m$ and $q > m$ such that $pq \mid a^{pq} - a$.

In connection with the falsity of the Chinese theorem the question arises whether there exists a composite number $n$ such that for each integer $a$ the number $a^{n} - a$ is divisible by $n$. Such a composite number $n$ we call an absolute pseudoprime (1). The conjecture has been put forth (still unproved) that there are infinitely many such numbers. The smallest absolute pseudoprime is the number $561 = 3 \cdot 11 \cdot 17$.

In order to prove that the number 561 is an absolute pseudoprime it is sufficient to show that for each integer $a$ the number $a^{561} - a$ is divisible by each of the prime numbers 3, 11 and 17.

The number $a^{561} - a$ is obviously divisible by 3, if $a$ is divisible by 3. But if $a$ is not divisible by 3, then $a$ is of the form $3k \pm 1$, whence $a^{2} - 1 = (3k \pm 1)^{2} - 1 = 3(3k \pm 2)k$, so that $3 \mid a^{2} - 1$, whence $3 \mid a^{2 \cdot 280} - 1$ and so a fortiori $3 \mid a^{561} - a$.

The number $a^{561} - a$ is obviously divisible by 11, if the number $a$ is divisible by 11. By Fermat's theorem we have, for every integer $a$, $11 \mid a^{11} - a = a(a^{10} - 1)$ and, if $a$ is not divisible by 11, it follows that $11 \mid a^{10} - 1$, whence $11 \mid a^{10 \cdot 56} - 1$ and so obviously $11 \mid a^{561} - a$.

(1) The name pseudoprime remains for composite numbers $n$ for which the number $2^{a} - 2$ is divisible by $n$. 
The number \( a^{561} - a \) is divisible by 17, if \( a \) is divisible by 17. By Fermat's theorem we have for every integer \( a \), \( 17|a^{17} - a \) and, if \( a \) is not divisible by 17, it follows that \( 17|a^{16} - 1 \), whence \( 17|a^{16 \cdot 35} - 1 \), and so obviously \( 17|a^{561} - a \) (because \( 16 \cdot 35 + 1 = 561 \)). We have thus proved that the number 561 is an absolute pseudoprime.

The numbers

\[
5.29.73, \quad 7.13.31, \quad 7.23.31, \quad 7.31.73,
\]

\[
13.37.61, \quad 5.17.29.113.337.673.2689
\]

are also absolute pseudoprimes.

From the Simple Theorem of Fermat it follows that if \( p \) is a prime number > 2, then the number \( 2^{p-1} - 1 \) is divisible by \( p \). The question then arises whether there exist prime numbers \( p \) for which \( 2^{p-1} - 1 \) would be divisible by \( p^2 \). We know only two such primes \( p \), namely 1093 and 3511, and we know that there are no other such primes \( p < 100,000 \); we do not know, however, if there are any greater than this number or if their number is finite. We do not know whether the number of primes such that \( 2^{p-1} - 1 \) is not divisible by \( p^2 \) is finite.

From Fermat's theorem it follows easily that, if \( p \) is a prime number, then the number

\[
1^{p-1} + 2^{p-1} + 3^{p-1} + \ldots + (p-1)^{p-1} + 1
\]

is divisible by \( p \). G. Giuga in 1950 put up the hypothesis that this divisibility holds only for prime numbers, and it was verified for all numbers \( \leq 10^{1000} \).

15. Proof that there is an infinity of primes in the sequences \( 4k+1 \), \( 4k+3 \) and \( 6k+5 \)

Now let \( n \) denote an arbitrary integer > 1. The number \( n! \) is then even, and the odd number \( (n!)^2 + 1 \), being greater than 1, obviously has, by Theorem 1, a prime factor \( p \), of the form \( 4k+1 \) or \( 4k+3 \) (where \( k \) is an integer) which is greater than \( n \). We suppose that \( p = 4k+3 \). We obviously have \( (n!)^2 + 1 | (n!)^{2(2k+1)} + 1 \)
because, as we know, for a natural number \(a\) and an odd \(m\) \(a^m+1\) is divisible by \(a+1\) (because \(a^m+1 = (a+1)(a^{m-1}-a^{m-2}+\ldots-a+1)\). We have \(2(2k+1) = 4k+2 = p-1\), and so, since \(p|(n!)^2+1\), we shall have \(p|(n!)^{p-1}+1\), and hence \(p|(n!)^p+n!\). But by Fermat's theorem we have \(p|(n!)^{p-n!}\). Hence \(p|2.n!\), which is not possible because \(p\) is an odd number > \(n\). Hence \(p\) must be a number of the form \(4k+1\). We have thus proved that for every natural number \(n > 1\) there exists a prime number > \(n\), of the form \(4k+1\). We have thus proved

**Theorem 10.** Prime numbers of the form \(4k+1\) are infinitely many.

In connection with our proof the question arises whether for each prime number \(p\) of the form \(4k+1\) there exists a natural number \(n\) such that \(p|(n!)^2+1\). (We have for example \(5|(2!)^2+1\), \(13|(6!)^2+1\).) Now it can be shown (which we do in § 19) that, if \(p\) is a prime number of the form \(4k+1\), then \(p \left\lfloor \left( \frac{p-1}{2} \right)! \right\rfloor ^2 + 1\).

Thus \(17|(8!)^2+1\), \(29|(14!)^2+1\), \(37|(18!)^2+1\).

Regarding Theorem 10, the problem arises as to how many primes there are of the form \(4k+3\). The proof that they are infinite is particularly easy. One uses the following

**Lemma.** Every natural number of the form \(4k+3\) has at least one prime divisor of the same form.

**Proof.** Let \(n = 4k+3\). This number has obviously natural divisors of the form \(4t+3\) (where \(t\) is an integer) because it is itself of this form. We denote by \(p\) the smallest of such divisors. Then \(p > 1\). If \(p\) were composite then \(p = ab\), where \(a\) and \(b\) are natural numbers greater than 1 and less than \(p\), and also odd, because \(p\), as a number of the form \(4k+3\), is odd. The numbers \(a\) and \(b\) cannot both be of the form \(4t+1\), because then their product \(p = ab = (4t_1+1)(4t_2+1) = 4(4t_1t_2+t_1+t_2)+1\) would be of the form \(4t+1\), which is impossible. So at least one of the numbers \(a\) and \(b\) is of the form \(4t+3\). Since divisors of the number \(p\) are at the same time divisors of the number \(n\), the number \(n\) would have natural divisors of the form \(4t+3\) less than \(p\), contrary
to the definition of the number \( p \). The number \( p \) is therefore prime. Our lemma is thus proved.

Now let \( n \) denote an arbitrary natural number. The number \( 4 \cdot n! - 1 \) is obviously natural of the form \( 4k+3 \). By the lemma, it has at least one prime divisor of the form \( 4k+3 \). Then \( p \) must be \( > n \), because \( 4 \cdot n! - 1 \) is divisible by \( p \), and is obviously not divisible by any natural number \( > 1 \) and \( \leq n \). We have thus proved that for every natural number \( n \) there exist prime numbers \( > n \) and of the form \( 4k+3 \).

We have thus proved

**Theorem 11.** There are infinitely many primes of the form \( 4k+3 \).

For a real number \( x \), we denote by \( \pi_1(x) \) the number of primes of the form \( 4k+1 \) not greater than \( x \), and by \( \pi_3(x) \) the number of primes of the form \( 4k+3 \) not greater than \( x \). Thus, for example, \( \pi_1(10) = 1 \), \( \pi_3(10) = 2 \); \( \pi_1(17) = \pi_3(17) = 3 \); \( \pi_1(100) = 11 \), \( \pi_3(100) = 13 \).

It has been computed that \( \pi_1(x) \leq \pi_3(x) \) for \( x < 26,861 \). It would be erroneous to conclude on the basis of so many cases that we always have \( \pi_1(x) \leq \pi_3(x) \), because, as J. Leech [1] calculated in 1957, for \( x = 26,861 \) we have \( \pi_1(x) = 1473 \) and \( \pi_3(x) = 1472 \).

In 1914 Littlewood proved that there are infinitely many natural numbers \( x \) for which \( \pi_1(x) > \pi_3(x) \) and also infinitely many numbers for which \( \pi_1(x) < \pi_3(x) \). We thus know how erroneous a conjecture about prime numbers can be even if it is based on an investigation of very many particular cases.

Theorems 10 and 11 can be stated in the following way:

*Each of the arithmetic progressions*

\[
1, 5, 9, 13, 17, 21, \ldots, \\
3, 7, 11, 15, 19, 23, \ldots
\]

contains an infinity of primes.

In this connection the problem arises which infinite arithmetic progressions of natural numbers contain an infinity of prime numbers.
Let an infinite arithmetic progression

$$a, a+r, a+2r, \ldots$$

be given with first term $a$ and common difference $r$.

If the numbers $a$ and $r$ have a common divisor $d > 1$, then obviously each of the numbers of our progression will be divisible by $d$ and, as is easy to see, none of the terms of the progression with the possible exception of the first term can be a prime. It follows that a necessary condition for an arithmetic progression with first term $a$ and common difference $r$ to have an infinity of primes is that the numbers $a$ and $r$ have no common factor other than 1. Now in 1837 P. G. Dirichlet proved that this condition is also sufficient. The proof of this theorem, although simplified later by various authors, is still complicated and lengthy. It would not be easier to prove the theorem stating that in every arithmetic progression whose first term and common difference are natural numbers having no common factor other than 1 there is at least one prime number. It is easy to prove that this theorem, although apparently weaker than the theorem of Dirichlet, is equivalent to it.

Some particular cases of the theorem of Lejeune Dirichlet (also called the theorem on arithmetic progression) are easy to prove. We give here the proof for $a = 5$, $r = 6$. We begin by proving the following

**Lemma.** Every natural number of the form $6k+5$ has at least one prime divisor of this form.

The proof of this lemma is quite similar to the proof of the lemma for numbers of the form $4k+3$ with the difference that instead of the form $4k+3$, we write the form $6k+5$ and later we use the remark that numbers of the form $6k+5$, being not divisible by 2 and by 3 must have divisors only of the form $6t+1$ or $6t+5$, and that the product of two numbers of the form $6t+1$ is also of this form.

For the proof of the theorem itself we write for a given natural number $n$ the number $6.n!−1$, which is obviously of the form $6k+5$ and, by the lemma, has prime divisors $p$ of the same form,
for which it is easy to prove that \( p > n \). For each natural number \( n \) there exists a prime number \( p > n \) of the form \( 6k + 5 \). Hence

**Theorem 12.** Prime numbers of the form \( 6k + 5 \) are infinitely many.

So the arithmetic progression \( 5, 11, 17, 23, 29, 35, \ldots \) contains infinitely many prime numbers. Hence the arithmetic progression

\[
2, 5, 8, 11, 14, 17, 20, \ldots
\]

will obviously contain infinitely many prime numbers because it contains all the terms of the progression \( 5, 11, 17, 23, \ldots \).

Thus there exist infinitely many prime numbers of the form \( 3k + 2 \).

There are, however, some other arithmetic progressions of which it is quite easy to prove that they contain infinitely many prime numbers. Such is for example the progression \( 8k + 1 \) (where \( k = 1, 2, 3, \ldots \)).

**16. Some hypotheses about prime numbers**

Now let \( n \) be a given natural number \( > 1 \). We arrange the natural numbers \( 1, 2, 3, \ldots, n^2 \) in \( n \) rows with \( n \) numbers in each row, i.e. we form the table

\[
\begin{array}{cccccccc}
1, & 2, & \ldots, & & k, & \ldots, & n, & \\
n+1, & n+2, & \ldots, & & n+k, & \ldots, & 2n, & \\
2n+1, & 2n+2, & \ldots, & & 2n+k, & \ldots, & 3n, & \\
\end{array}
\]

\[(n-1)n+1, (n-1)n+2, \ldots, (n-1)n+k, \ldots, n^2\]

The columns of this table form an arithmetic progression (with \( n \) terms). A. Schinzel advanced the conjecture that if \( k \) is a natural number \( < n \) not having any common factor \( > 1 \) with \( n \), then the \( k \)th column of our table will contain at least one prime number. A. Gorzelewski verified this conjecture for all natural numbers \( n \leq 100 \).
I have put forth the conjecture that every row written in the table (where \( n > 1 \)) will contain at least one prime number. This hypothesis has been verified by A. Schinzel with the help of the tables of A. Western and D. H. Lehmer for all \( n \leq 4500 \). The first row of our table (for \( n > 1 \)) will always contain the prime number 2. The theorem stating that the second row of our table contains at least one prime number is easily seen to be equivalent to the theorem of Chebyshev, and is therefore true. It has also been proved that for \( n \geq 3 \), the third row of our table contains at least one prime number, in other words, that for \( n \geq 3 \) there is at least one prime number between \( 2n \) and \( 3n \) (which is also true for \( n = 2 \)). More generally, it has been proved that for \( n \geq 9 \) each of the first nine rows of our table has at least one prime number.

As the last two rows of our table are

\[
(n-1)^2, \quad (n-1)^2 + 1, \ldots, \quad n^2 - n,
\]

\[
n^2 - n + 1, \quad n^2 - n + 2, \ldots, \quad n^2,
\]

so from our hypothesis it follows that between squares of two consecutive natural numbers there are at least two prime numbers. Since it is easy to prove that if \( m \) is a natural number there exists a natural number \( n \) such that

\[
m^3 \leq (n-1)^2 \quad \text{and} \quad n^2 \leq (m+1)^3,
\]

it follows from our theorem that between every two cubes of consecutive natural numbers there are at least two prime numbers. We do not know whether it is true; however, it has been proved that for a sufficiently large natural number \( m \) between \( m^3 \) and \( (m+1)^3 \) there are arbitrarily many primes (it follows from the result of Ingham [1]).

In this connection we recollect, as L. Skula observed, that from the hypothesis about our table (for \( n = 2, 3, \ldots \)) it follows that the \((n+1)\)-th row and also the \((n+2)\)-th row contain at least one prime number (that is for natural \( n > 1 \) each of the sequences \( n^2 + 1, \quad n^2 + 2, \quad \ldots, \quad n^2 + n \) and \( n^2 + n + 1, \quad n^2 + n + 2, \quad \ldots, \quad n^2 + 2n \) contains at least one prime number). This is not in general true.
for the \((n+3)\)-th row, for example for \(n = 2\) or for \(n = 4\) (where the sequences 9, 10 and 25, 26, 27, 28 do not contain any prime numbers).

From the hypothesis about our table it would be easy to obtain the corollary that if all natural numbers are written successively in rows, \(n\) numbers in the \(n\)th row, and if we form an infinite triangular table

\[
\begin{array}{cccc}
1 \\
2, & 3 \\
4, & 5, & 6 \\
7, & 8, & 9, & 10 \\
11, & 12, & 13, & 14, & 15 \\
\ldots & \ldots & \ldots & \ldots & \ldots
\end{array}
\]

then in each row of this table beginning from the second there is at least one prime number. We do not know if this is true.

17. Lagrange's theorem

**Theorem 13.** If \(p\) is a prime number and

\[(i)\quad f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n\]

a polynomial of degree \(n \geq 1\) with integral coefficients, and the coefficient of the highest power of \(x\), \(a_0\), is not divisible by \(p\), then among the numbers

\[(ii)\quad x = 0, 1, 2, 3, \ldots, p-1\]

there exist no more than \(n\) numbers for which \(f(x)\) is divisible by \(p\).

**Proof.** The theorem is true for polynomials of degree 1. In fact, if among the numbers (ii) there were at least two different numbers \(x_1\) and \(x_2 > x_1\) such that \(p|f(x_1)\) and \(p|f(x_2)\), then we would have \(p|f(x_2) - f(x_1)\), and as \(f(x) = a_0x + a_1\), we would have \(p|a_0(x_2 - x_1)\) where \(x_2 - x_1\), being the difference of two distinct numbers of the sequence (ii) and therefore less than \(p\), is not divisible by \(p\); so \(p\) would be a divisor of the product of two natural numbers not divisible by \(p\), contrary to Theorem 7.
Now let \( n \) denote a natural number \( > 1 \). We suppose that the theorem is true for polynomials of degree \( n-1 \). We suppose that Lagrange's theorem is still not true for some polynomial \((i)\) of degree \( n \), and therefore there exist \( n+1 \) integers \( \geq 0, x_1 < x_2 < \ldots < x_{n+1} < p \) such that \( p | f(x_i) \) for \( i = 1, 2, \ldots, n+1 \).

We have

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

Hence as

\[
x^k - x_1^k = (x-x_1)(x^{k-1} + x_1 x^{k-2} + \ldots + x_1^{k-2} x + x_1^{k-1})
\]

for \( k = 2, 3, \ldots, n \),

we easily get

(iii) \( f(x) - f(x_1) = (x-x_1)f_1(x) \),

where \( f_1(x) \) is a polynomial of degree \( n-1 \) and with integral coefficients (depending on \( a_0, a_1, \ldots, a_n \) and \( x_1 \)), in which the coefficient of \( x^{n-1} \) will be \( a_0 \) and so a number not divisible by \( p \).

Because of the identity (iii) we get

(iv) \( f(x_i) - f(x_1) = (x_i-x_1)f_1(x_i) \) for \( i = 2, 3, \ldots, n+1 \).

But from \( p | f(x_i) \) for \( i = 1, 2, \ldots, n+1 \) it follows that

\( p | f(x_i) - f(x_1) \) for \( i = 2, 3, \ldots, n+1 \),

whence because of (iv)

\( p | (x_i-x_1)f_1(x_i) \) for \( i = 2, 3, \ldots, n+1 \),

and, as the numbers \( x_i-x_1 \), for \( i = 2, 3, \ldots, n+1 \), are not divisible by \( p \), we must have by Theorem 7

\( p | f_1(x_i) \) for \( i = 2, 3, \ldots, n+1 \),

contrary to the supposition that the theorem is true for polynomials of degree \( n-1 \).

**Corollary.** If \( p \) is a prime number and \( f \) is a polynomial of degree \( n \) with integral coefficients and if there exist more than \( n \) natural numbers \( x < p \) for which \( f(x) \) is divisible by \( p \), then all the coefficients of the polynomial \( f \) must be divisible by \( p \).
Proof. We suppose that the polynomial \( f \) has the property of the corollary but not all its coefficients are divisible by \( p \). Let \( a_{n-k} \) denote the first coefficient not divisible by \( p \) and we suppose that \( k > 0 \). For every natural number \( x \) for which \( f(x) \) is divisible by \( p \), \( g(x) \) will be divisible by \( p \) where

\[
g(x) = a_{n-k}x^k + a_{n-k+1}x^{k+1} + \ldots + a_n.
\]

For a polynomial \( g(x) \) of degree \( k \), there would then exist more than \( n \) and, as \( k \leq n \), more than \( k \) natural numbers \( x < p \) for which \( p | g(x) \), contrary to Lagrange's theorem (because \( a_{n-k} \) is not divisible by \( p \)). Therefore \( k \) must be equal to 0, that is all the coefficients of the polynomial \( f \), except perhaps \( a_n \), are divisible by \( p \). But already there exists a number \( x \) for which \( f(x) \) is divisible by \( p \); so from (i) we immediately deduce that we must also have \( p | a_n \). In each case therefore our supposition that our corollary is not true leads to a contradiction.

18. Wilson's theorem

We now give some important applications of the corollary proved above. Let \( p \) be a prime number and let

\[
f(x) = (x-1)(x-2) \ldots (x-p+1) - x^{p-1} + 1
\]

be a polynomial of degree \( p-2 \) with integral coefficients. For \( x = 1, 2, \ldots, p-1 \) we have, by Fermat's theorem, \( p | x^p - x = x(x^{p-1} - 1) \), whence \( p | x^{p-1} - 1 \).

But for \( x = 1, 2, \ldots, p-1 \) we obviously also have

\[
p | (x-1)(x-2) \ldots (x-p+1),
\]

because for such \( x \) one of the factors of this product is zero. From the formula for \( f(x) \) (and considering that the difference of two numbers divisible by \( p \) is divisible by \( p \)) we deduce that \( p | f(x) \) for \( x = 1, 2, \ldots, p-1 \).

By the corollary to Lagrange's theorem (for \( n = p-2 \)) we then deduce that all coefficients of our polynomial, and thus also its constant term, are divisible by \( p \).

But for odd \( p \) (because \((-1)^{p-1} = 1\)) the constant term of the polynomial \( f(x) \) is the number \( 1 \cdot 2 \cdot 3 \ldots (p-1)+1 \), i.e. \( (p-1)!+1 \).
Therefore, if \( p \) is an odd prime number, \( p \mid (p-1)!+1 \); for \( p = 2 \), it is true because \( 1!+1 = 2 \). We have thus proved

**Theorem 14 (Wilson).** For every prime number \( p \) the number \((p-1)!+1\) is divisible by \( p \).

It is worth observing that if for a natural number \( n > 1 \) \((n-1)!+1\) is divisible by \( n \), then \( n \) must be a prime number. For if \( n \) were composite, then \( n = ab \), where \( a \) and \( b \) are natural numbers \( > 1 \) and \( < n \), and the number \( a \) would be one of the factors of the product \( 1.2.3 \ldots (n-1) \), and so the number \((n-1)!+1\), when divided by \( a \), would give the remainder 1, while being divisible by \( n \) it must of course be divisible by \( a \). Hence the contradiction, which proves that \( n \) must be prime.

Thus in order that the natural number \( n > 1 \) be prime it is necessary and sufficient that the number \((n-1)!+1\) be divisible by \( n \).

Theoretically, then, by only one division we can find out whether a number is prime or not. Practically, however, to apply this is impossible, because even for a number \( n \) of 3 digits the number \((n-1)!+1\) has more than a hundred digits.

In connection with Wilson's theorem the question is suggested whether or not there are primes for which the number \((p-1)!+1\) is divisible by \( p^2 \). For \( p \leq 50,000 \), there are only three such numbers: 5, 13 and 563 (Fröberg [1]). We do not know if such numbers \( p \) are infinitely many.

The theorems of Fermat and Wilson can be combined in the following theorem:

*If \( p \) is a prime number, then for every integer \( a \) the number \( a^p+(p-1)!a \) is divisible by \( p \).*

As a matter of fact, if \( p \) is prime number and \( a \) an arbitrary integer, then, by Fermat's theorem, \( a^p-a \) is divisible by \( p \), and, since by Wilson's theorem the number \( a+(p-1)!a = [1+\ldots+(p-1)!]a \) is divisible by \( p \), then their sum, i.e. the number \( a^p+(p-1)!a \), is divisible by \( p \). On the other hand, if this number is divisible by \( p \) for every integer \( a \), then for \( a = 1 \) we obtain Wilson's theorem, from which it follows that for an arbitrary integer \( a \) we have \( p \mid (p-1)!a+a \), which, because of \( p \mid a^p+(p-1)!a \),
gives $p|a^p+(p-1)!a-[(p-1)!a+a]$, i.e. $p|a^p-a$, which is the theorem of Fermat.

It is also easy to prove that the theorems of Fermat and Wilson can be combined into one theorem:

*If* $p$ *is a prime number and* $a$ *an integer, then* $(p-1)!a^p+a$ *is divisible by* $p$ *(Leo Moser).*

From the theorem of Wilson it is easy to deduce the following

**Theorem 15 (Leibniz).** *In order that the natural number* $p > 2$ *be prime, it is necessary and sufficient that the number* $(p-2)!-1$ *be divisible by* $p$.

*Proof.* If the number $p > 2$ is prime, then by Wilson's theorem the number $(p-1)!+1$ is divisible by $p$. But because $(p-1)! = (p-2)!(p-1)$ we have $(p-1)!+1 = (p-2)!p-[(p-2)!-1]$, whence from the divisibility of the left side by $p$ we deduce the divisibility by $p$ of the number $(p-2)!-1$.

On the other hand, if $p|(p-2)!-1$, then $p|(p-1)!-(p-1)$ and so $p|(p-1)!+1$, whence (as $p > 2$), as we have already proved above, it follows that $p$ must be a prime number.

We have thus proved the theorem of Leibniz.

If $p$ is a prime number $> 3$, then $(p-1)! > p$, because then $(p-1)! \geq 2(p-1) = p+(p-2) > p$ and so the number $(p-1)!+1$ is $> p$ and by Wilson's theorem is divisible by $p$; it is therefore a composite number.

Hence: if $p > 3$ is a prime number, then the number $(p-1)!+1$ is composite. It follows that there are infinitely many natural numbers $n$ for which $n!+1$ is composite. The question then arises whether there also exist infinitely many natural numbers $n$ for which $n!+1$ is prime. We do not know the answer to this problem.

The numbers $1!+1 = 2$, $2!+1 = 3$, $3!+1 = 7$ are prime; the next prime number of this form is $11!+1 = 39,916,801$. We do not know whether $27!+1$ is prime.

From the theorem of Leibniz it easily follows that there exist infinitely many natural numbers $n$ for which $n!-1$ is composite. We do not know, however, if there are infinitely many natural numbers $n$ for which $n!-1$ is prime.
The numbers \(3!-1 = 5\), \(4!-1 = 23\), \(6!-1 = 719\) are prime.

We also do not know if among the numbers \(p!+1\), where \(p\) is a prime number, there are infinitely many composite numbers. Similarly for the numbers \(p!-1\). Also we do not know the answer to the question whether there exist infinitely many natural numbers \(n\) for which the number \(p_1p_2\ldots p_n+1\) is prime (where \(p_n\) is the \(n\)th prime number) and also whether there is an infinity of natural numbers \(n\) for which the number \(p_1p_2\ldots p_n+1\) is composite.

The numbers \(p_1+1 = 3\), \(p_1p_2+1 = 7\), \(p_1p_2p_3+1 = 31\), \(p_1p_2p_3p_4+1 = 211\), \(p_1p_2p_3p_4p_5+1 = 2311\) are prime but the numbers \(p_1p_2\ldots p_n+1\) are composite for \(n = 6, 7,\) and \(8\), divisible respectively by \(59, 19,\) and \(347\).

We shall show that for natural \(n > 3\) the product \(Q_n\) of all prime numbers less than \(n\) is greater than \(n\).

We suppose that for some natural \(n > 3\) we have \(Q_n \leq n\). Therefore \(Q_n-1 < n\). But \(Q_n-1\) is not divisible by any prime number < \(n\) (because these numbers are divisors of \(Q_n\)) and, as \(n \geq 4\), the number \(Q_n-1 \geq Q_4-1 = 5 > 1\) has a prime divisor \(p\) which must be \(\geq n\). A fortiori, \(Q_n-1 \geq n\) which gives a contradiction. Therefore \(Q_n > n\) for \(n > 3\).

About the product \(P_n\) of all prime numbers \(\leq n\) we can prove that, for a natural number \(n\), \(P_n < 4^n\) (see Sierpiński [7], p. 396) and, for a natural number \(n \geq 29\), \(P_n > 2^n\).

It has also been proved that, for a natural number \(n > 2\), the sum of all prime numbers \(\leq n\) is \(> n\).

19. Decomposition of a prime number into the sum of two squares

Now let \(p\) be a prime number of the form \(4k+1\). Since \((p-1)/2 = 2k\) is even, we have

\[
1. 2. 3 \ldots \frac{p-1}{2} = (-1)(-2) \ldots \left(-\frac{p-1}{2}\right),
\]

which on division by \(p\) gives the same remainder as

\[
(p-1)(p-2) \ldots \left(p-\frac{p-1}{2}\right),
\]
which, if we reverse the order of the factors, can be written in the form

$$\frac{p+1}{2} \left( \frac{p+1}{2} + 1 \right) \cdots (p-2)(p-1).$$

Hence, multiplying by $$\left(\frac{p-1}{2}\right)!$$ and observing that

$$\frac{p+1}{2} = \frac{p-1}{2} + 1,$$ 

we deduce that the number $$\left(\left(\frac{p-1}{2}\right)!\right)^2$$ on dividing by $$p$$ gives the same remainder as $$(p-1)!$$. Now, as the last number increased by 1 is divisible by $$p$$ by Wilson's theorem, so also the number $$\left(\left(\frac{p-1}{2}\right)!\right)^2 + 1$$ is divisible by $$p$$. We have thus proved

**Theorem 16.** If $$p$$ is a prime number of the form $$4k+1$$, the number $$\left(\left(\frac{p-1}{2}\right)!\right)^2 + 1$$ is divisible by $$p$$.

In order to deduce a further corollary from this theorem, we prove the following

**Lemma.** If $$p$$ is a prime number and $$a$$ an integer not divisible by $$p$$, then there exist natural numbers $$x$$ and $$y$$, $$x < \sqrt{p}$$ and $$y < \sqrt{p}$$, such that for a suitable sign $$+$$ or $$-$$ the number $$ax \pm y$$ is divisible by $$p$$.

**Proof.** Let $$p$$ be a given prime number and let $$m$$ denote the greatest natural number $$\leq \sqrt{p}$$; then $$m+1 > \sqrt{p}$$ so that $$(m+1)^2 > p$$. We consider the integers $$ax - y$$, where $$x$$ and $$y$$ run through the values 0, 1, ..., $$m$$. There are $$(m+1)^2 > p$$ numbers of this type and since there are only $$p$$ possible remainders on dividing by $$p$$, for two different systems $$x_1$$, $$y_1$$ and $$x_2$$, $$y_2$$ where, for example, $$x_1 \geq x_2$$, the numbers $$ax_1 - y_1$$ and $$ax_2 - y_2$$ must give the same remainder when divided by $$p$$, so the number $$ax_1 - y_1 - (ax_2 - y_2) = a(x_1 - x_2) - (y_1 - y_2)$$ is divisible by $$p$$. We cannot have $$x_1 = x_2$$ because then the number $$y_1 - y_2$$ would be divisible by $$p$$, which, because of $$0 \leq y_1 \leq m \leq \sqrt{p} < p$$ and similarly $$0 \leq y_2 < p$$, is impossible when the systems $$x_1$$, $$y_1$$ and $$x_2$$, $$y_2$$ are different, as we supposed. Also $$y_1 \neq y_2$$, for otherwise the number $$a(x_1 - x_2)$$ would be divisible by $$p$$, and so from the non-divisibility of $$a$$ by $$p$$ it would follow that $$x_1 - x_2$$ is divisible by $$p$$,
which is impossible. Since \( x_1 \geq x_2 \) and \( x_1 \neq x_2 \), the number \( x_1 - x_2 \) is natural and the number \( y_1 - y_2 \) is an integer different from zero; so with a suitable sign the number \( y = \pm (y_1 - y_2) \) is natural and we have \( x = x_1 - x_2 \leq x_1 \leq m \leq \sqrt{p} \) and thus \( x < \sqrt{p} \) because the equation \( x^2 = p \) is not possible, the number \( p \) being prime. Similarly we get \( y < \sqrt{p} \). So the number \( ax \pm y \), which with a suitable sign is equal to the number \( a(x_1 - x_2) - (y_1 - y_2) \), is divisible by \( p \). The lemma is thus proved.

Now let \( p \) be a prime number of the form \( 4k+1 \) and let \( a = [(p-1)/2)!] \)---this will be a number not divisible by \( p \) (being a product of natural numbers less than \( p \) and by corollary to Theorem 7). By our lemma, there exist natural numbers \( x \) and \( y \) with \( x < \sqrt{p} \) and \( y < \sqrt{p} \) such that with a suitable sign + or − the number \( ax \pm y \) is divisible by \( p \). In each case then the number \( a^2x^2 - y^2 = (ax-y)(ax+y) \) will be divisible by \( p \). But, by Theorem 16 the number \( a^2 + 1 \) is divisible by \( p \), and so the number \( a^2x^2 + x^2 \) is also divisible by \( p \). As the numbers \( a^2x^2 + x^2 \) and \( a^2x^2 - y^2 \) are divisible by \( p \), their difference \( x^2 + y^2 \) is divisible by \( p \), so \( x^2 + y^2 = kp \) where \( k \) is a natural number. As \( x < \sqrt{p} \) and \( y < \sqrt{p} \), we have \( x^2 + y^2 < 2p \), that is \( kp < 2p \), whence \( k < 2 \), and, as \( k \) is a natural number, it follows that \( k = 1 \), i.e. \( x^2 + y^2 = p \). We have thus proved

**Theorem 17 (Fermat).** Every prime number of the form \( 4k+1 \) is the sum of the squares of two natural numbers.

Here for example \( 5 = 1^2 + 2^2 \), \( 13 = 2^2 + 3^2 \), \( 17 = 1^2 + 4^2 \), \( 29 = 2^2 + 5^2 \), \( 37 = 1^2 + 6^2 \), \( 41 = 4^2 + 5^2 \), \( 53 = 2^2 + 7^2 \), \( 61 = 5^2 + 6^2 \), \( 73 = 3^2 + 8^2 \).

We now prove that the decomposition of a prime number into the sum of two squares of natural numbers is unique if we disregard the order of the components. Indeed, we prove the more general

**Theorem 18.** If \( a \) and \( b \) are given natural numbers, then no prime number \( p \) can be written in two different ways in the form \( p = ax^2 + by^2 \) where \( x \) and \( y \) are natural numbers and where in case \( a = b = 1 \), we disregard the order of the components.
Proof. We suppose that the prime number $p$ has two decompositions

$$p = ax^2 + by^2 = a\xi_1^2 + b\eta_1^2$$

where $x, y, \xi_1, \eta_1$ are natural numbers. We thus have

$$p^2 = (ax\xi_1 + by\eta_1)^2 + ab(xy_1 - yx_1)^2$$

$$= (ax\xi_1 - by\eta_1)^2 + ab(xy_1 + yx_1)^2.$$

But

$$(ax\xi_1 + by\eta_1)(xy_1 + y\eta_1) = (ax^2 + by^2)\xi_1\eta_1 + (a\xi_1^2 + b\eta_1^2)xy$$

Therefore at least one of the factors on the left-hand side must be divisible by the prime number $p$.

If $p \mid ax\xi_1 + by\eta_1$, then from the first formula for $p^2$ it follows that $xy_1 - yx_1 = 0$; so $xy_1 = yx_1$ and we have $p = ax\xi_1 + by\eta_1$, whence $px = (ax^2 + by^2)\xi_1 = p\xi_1^2$; hence we have $x = \xi_1$ and also $y = \eta_1$.

Now, if $p \mid xy_1 + y\xi_1$, then from the second formula for $p^2$ it follows that $ax\xi_1 - by\eta_1 = 0$ and $p^2 = ab(xy_1 + y\xi_1)^2$, which, considering that the numbers $x, y, \xi_1$ and $\eta_1$ are natural, is possible only when $a = b = 1$, and then we have $p = xy_1 + y\xi_1$ and $xx_1 - y\eta_1 = 0$, which gives $px = (x^2 + y^2)y_1 = p\eta_1$, whence $x = y_1$, and, since $p = x^2 + y^2 = x_1^2 + y_1^2$, we have $y = x_1$ and our decompositions can differ only in the order of the components. Theorem 18 is thus proved.

From Theorem 18 it follows immediately that, if a natural number $n$ can be written in at least two different ways as the sum of squares of two natural numbers (if we do not regard as different those decompositions which differ only in the order of the components), then $n$ is not a prime number.

Thus for example from $2501 = 1^2 + 50^2 = 10^2 + 49^2$ we conclude that 2501 is not a prime.

If $m$ and $n$ are natural numbers, then we have $m^4 + 4n^4 = (m^2)^2 + (2n^2)^2 = (m^2 - 2n^2)^2 + (2mn)^2$. 
If $m = n$ or $m = 2n$, then our decompositions into the sum of squares are the same, but then we have either $m^4 + 4n^4 = 5n^4$, which is a prime number only for $m = n = 1$, or $m^4 + 4n^4 = 20n^4$, which is a composite number. If, however, $m \neq n$ and $m \neq 2n$, then it is easy to prove that our decompositions differ not only in the order of the components, and so the number $m^4 + 4n^4$ is composite. Thus:

*If $m$ and $n$ are natural numbers of which one at least is different from unity, then the number $m^4 + 4n^4$ is composite.*

In particular (for $m = 1$) it follows that the numbers $4n^4 + 1$, where $n$ is a natural number $> 1$, are all composite.

If we know two decompositions of a given natural number into the sum of two squares (differing not merely in the order of their components), then it can be shown that we can obtain the decomposition of this number as a product of two natural number greater than 1.

We observe, however, that, if a natural number gives only one decomposition into the sum of two squares of natural numbers, then it does not follow that it must be a prime number. For example, as is easy to see, the number 10 has only one such decomposition: $10 = 1^2 + 3^2$; the number 18 has only one decomposition: $18 = 3^2 + 3^2$. Similarly the number 45 has only one: $45 = 3^2 + 6^2$.

It can, however, be shown that if an odd natural number $n$ has only one decomposition into the sum of two squares of integers $\geq 0$ (where we do not regard as different those decompositions which differ only in the order of the components) and in this decomposition the components have no common factor $> 1$, then $n$ is a power of a prime number. In this connection, it has been computed on an electronic digital computer EMC (in the Department of Telecommunicational Constructions and Radiophony of the Polytechnic School, Warsaw) that the number $2^{39} - 7$ is a prime, because investigation has shown that there exists only one decomposition of this number, $2^{39} - 7 = 64,045^2 + 738,684^2$, into the sum of two squares, and in this decomposition the numbers have no common factor $> 1$.

—

(1) We have also the decomposition $m^4 + 4n^4 = (m^2 + 2mn + 2n^2) \times (m^2 - 2mn + 2n^2)$. 

---

*WHAT WE KNOW AND WHAT WE DO NOT KNOW*
Regarding the numbers $2^n - 7$ for $n = 4, 5, \ldots, 38$, we know that they are composite. The question whether all numbers $2^n - 7$ are, for a natural $n > 3$, composite was put in 1956 by P. Erdős. The answer is thus in the negative.

Numbers $2^n - 7$ are composite for $n = 40, 41, \ldots, 50$, because they are, as computed, divisible by 3, 5, 3, 107, 3, 5, 3, 11, 3, 61, 3, respectively. Thus, among the numbers $2^n - 7$ for a natural $n$, where $3 < n \leq 50$, there is only one prime (for $n = 39$).

It is easy to prove that among the numbers $2^p - 7$, where $p$ is a prime, infinitely many are composite. Namely, by Theorem 10, we have infinitely many primes of the form $4k+1$, and for every such prime $p$, since $5|2^4 - 1$, we have $5|2^{4k} - 1$, whence $5|2^{4k+1} - 2$, and so also $5|2^p - 7$.

We do not know if there is an infinity of natural numbers $n$ for which the number $2^n - 7$ is prime.

In connection with Theorem 17, the question arises as to what we can say about the decomposition of other prime numbers as a sum of two squares.

The number 2 has obviously only one decomposition as a sum of two squares of natural numbers: $2 = 1^2 + 1^2$. It remains therefore to inquire about prime numbers of the form $4k+3$ (where $k = 0, 1, 2, \ldots$). Now it is easy to prove that no natural number of this form can be written as the sum of the squares of two integers. Since natural number of the form $4k+3$ is odd, so in case $4k+3 = x^2 + y^2$, where $x$ and $y$ are integers, the numbers $x$ and $y$ cannot both be even or both be odd. Therefore, one of the numbers $x$ and $y$ must be even and the other odd. But the square of an even number gives the remainder 0 when divided by 4, and the square of an odd number—the remainder 1. The sum $x^2 + y^2$ would therefore give the remainder 1 when divided by 4, while the number $4k+3$ leaves the remainder 3. The formula $4k+3 = x^2 + y^2$ cannot hold for integers $k$, $x$ and $y$.

Thus, among primes only the number 2 and prime numbers of the form $4k+1$ decompose into the sum of two squares of natural numbers, each having only one such decomposition (if we do not consider them different when they differ only in the order of their components).
It would be more difficult to answer the question: which natural numbers are the sums of squares of two natural numbers. Even a necessary and sufficient condition for a natural number to be the sum of squares of natural numbers is quite complicated. It can be shown that in order that a natural number \( n \) be the sum of two squares of natural numbers it is necessary and sufficient that, in its prime factor decomposition, prime factors of the form \( 4k+3 \), if there are any, should occur in a power with an even exponent and further that either the number 2 should appear with an odd exponent or the number \( n \) should have at least one prime divisor of the form \( 4k+1 \).

It has also been investigated how many decompositions into the sum of squares of natural numbers has a given natural number \( n \). This depends on its decomposition into prime factors. It can be proved that there exist natural numbers having arbitrarily many decompositions into sums of squares of two natural numbers. The number 65 has two decompositions as sums of squares of two natural numbers: \( 65 = 1^2 + 8^2 = 4^2 + 7^2 \); the number 1105 has four decompositions: \( 1105 = 4^2 + 33^2 = 9^2 + 32^2 = 12^2 + 31^2 = 23^2 + 24^2 \).

20. Decomposition of a prime number into the difference of two squares and other decompositions

The question now arises whether a prime number can be expressed as the difference of two squares of natural numbers and in how many ways.

We suppose that a prime number is expressed as the difference of two squares of natural numbers, and that we have \( p = x^2 - y^2 \) where \( x \) and \( y \) are natural numbers; obviously \( x > y \). Hence \( p = (x-y)(x+y) \) and \( x-y \) and \( x+y \) are two natural divisors of the number \( p \), the first less than the second.

As \( p \) is prime, we deduce that \( x-y = 1 \), \( x+y = p \); so

\[
x = \frac{p+1}{2}, \quad y = \frac{p-1}{2}.
\]
The number $p$ must be odd and thus we have the only decomposition
\[ p = \left( \frac{p+1}{2} \right)^2 - \left( \frac{p-1}{2} \right)^2. \]

We have thus

**Theorem 19.** Every odd prime number is the difference of two squares of natural numbers, and this only in one way.

It is easy to prove that in order that the natural number $n > 1$ be the difference of two squares of natural numbers it is necessary and sufficient that after division by 4 it should not leave the remainder 2.

It can be shown that there exist numbers having arbitrarily many decompositions into differences of two squares. From Theorem 19 it follows that a natural number having more than one decomposition into the difference of two squares of natural numbers is not prime.

But it is also easy to prove that, if an odd number has only one decomposition into the difference of two squares of integers, then it is a prime number. For we suppose that the odd number $n$ is composite; we then have $n = ab$, where $a$ and $b$ are natural numbers $> 1$. We obviously have
\[ n = \left( \frac{n+1}{2} \right)^2 - \left( \frac{n-1}{2} \right)^2 = \left( \frac{a+b}{2} \right)^2 - \left( \frac{a-b}{2} \right)^2, \]
so that, if for example $a \geq b$, then $n - 1 = ab - 1 > a - b$ (because $b > 1$); our decompositions are then different. The odd composite number has therefore two different decompositions into the differences of two squares of integers. However, there are composite odd numbers having only one decomposition as a difference of two squares of natural numbers, for example the number 9. (It can be shown that squares of odd prime numbers are such numbers.)

We pass on next to the question of the representation of a prime number as a sum of three squares of natural numbers.

It can be shown that there exist infinitely many primes which are the sums of three squares of natural numbers as well as an infinity of primes which are not equal to such a sum. Among
primes < 100 those which are the sums of three squares of natural
numbers are only the following:

\[
\begin{align*}
3 &= 1^2 + 1^2 + 1^2; \\
11 &= 1^2 + 1^2 + 3^2; \\
17 &= 2^2 + 2^2 + 3^2; \\
19 &= 1^2 + 3^2 + 3^2; \\
29 &= 2^2 + 3^2 + 4^2; \\
41 &= 1^2 + 2^2 + 6^2 = 3^2 + 4^2 + 4^2; \\
43 &= 3^2 + 3^2 + 5^2; \\
53 &= 1^2 + 4^2 + 6^2; \\
59 &= 1^2 + 3^2 + 7^2; \\
61 &= 3^2 + 4^2 + 6^2; \\
67 &= 3^2 + 3^2 + 7^2; \\
73 &= 1^2 + 6^2 + 6^2; \\
83 &= 1^2 + 1^2 + 9^2 = 3^2 + 5^2 + 7^2; \\
89 &= 2^2 + 2^2 + 9^2 = 2^2 + 6^2 + 7^2 = 3^2 + 4^2 + 8^2; \\
97 &= 5^2 + 6^2 + 6^2.
\end{align*}
\]

We thus also see that there are primes which have more than
one decomposition into the sum of three squares of natural numbers,
for example 41, 83 and 89. However, it is easy to prove that every
integer can be written in the form \(x^2 + y^2 - z^2\) in an infinity of
ways, where \(x, y\) and \(z\) are natural numbers. It is enough to observe
that for integrals \(k\) and \(t\) we have the identity

\[
2k - 1 = (2t)^2 + (k - 2t^2)^2 - (k - 2t^2 - 1)^2, \\
2k = (2t + 1)^2 + (k - 2t^2 - 2t)^2 - (k - 2t^2 - 2t - 1)^2.
\]

As regards the representation of a prime number into the
sum of four squares of natural numbers, it can be proved that
all prime numbers have such a representation with the exception
of the numbers 2, 3, 5, 11, 17, 19 and 41. The proof, however,
is difficult.

It can also be proved that the only prime numbers which are
not the sums of five squares of natural numbers are the numbers
2, 3 and 7, and that for every natural number \(m > 3\) there exists
only a finite number of primes which are not the sums of \(m\) squares
of natural numbers.

I. Chowla has advanced the conjecture that if the number 1
is considered as a prime number (as some people did formerly),
then every natural numbers is the sum of eight or fewer squares of
prime numbers. This has been verified for natural numbers \( \leq 288,000. \)

In relation to Theorem 17 the question arises which prime numbers can be written in the form \( x^2 + 2y^2 \), or \( x^2 + 3y^2 \), where \( x \) and \( y \) are natural numbers. The following theorems hold:

In order that a prime number \( p \) be of the form \( x^2 + 2y^2 \), where \( x \) and \( y \) are natural numbers, it is necessary and sufficient that \( p \) be of the form \( 8k+1 \) or \( 8k+3 \). Every prime number of this form has only one representation of the form \( x^2 + 2y^2 \) (which follows from Theorem 18).

Thus, for example,

\[
3 = 1^2 + 2 \cdot 1^2, \quad 11 = 3^2 + 2 \cdot 1^2, \quad 17 = 3^2 + 2 \cdot 2^2, \quad 19 = 1^2 + 2 \cdot 3^2.
\]

The conjecture has been put forth that there are infinitely many primes \( p \) of the form \( 8k+1 \) as also of the form \( 8k+3 \) such that \( p = 1^2 + 2y^2 \), where \( y \) is a natural number, and likewise an infinity of numbers \( p \) for which \( p = x^2 + 2 \cdot 1^2 \), where \( x \) is a natural number. For example, \( 73 = 1^2 + 2 \cdot 6^2, \quad 83 = 9^2 + 2 \cdot 1^2. \)

In order that the prime number \( p \) be of the form \( p = x^2 + 3y^2 \), where \( x \) and \( y \) are natural numbers, it is necessary and sufficient that \( p \) be of the form \( 6k+1 \). Every prime number of this form has only one decomposition of the form \( x^2 + 3y^2 \).

Thus, for example, \( 7 = 2^2 + 3 \cdot 1^2, \quad 13 = 1^2 + 3 \cdot 2^2, \quad 19 = 4^2 + 3 \cdot 1^2, \quad 31 = 2^2 + 3 \cdot 3^2, \quad 37 = 5^2 + 3 \cdot 2^2 \). The conjecture has been advanced that there exist infinitely many primes \( p \) of the form \( 6k+1 \) such that \( p = 1 + 3y^2 \), where \( y \) is a natural number, as well as infinitely many primes \( p \) such that \( p = x^2 + 3 \cdot 1^2 \), where \( x \) is a natural number. We have, for example, \( 67 = 8^2 + 3 \cdot 1^2, \quad 103 = 10^2 + 3 \cdot 1^2, \quad 109 = 1^2 + 3 \cdot 6^2 \).

From Theorem 17 it follows immediately that in order that the prime number \( p \) be of the form \( x^2 + 4y^2 \), where \( x \) and \( y \) are natural numbers, it is necessary and sufficient that \( p \) be of the form \( 4k+1 \). The following theorem has also been proved:

In order that an odd prime number \( p \) be of the form \( x^2 - 2y^2 \), where \( x \) and \( y \) are natural numbers, it is necessary and sufficient that \( p \) be of the form \( 8k+1 \) or \( 8k+7 \).
Proofs of these theorems are to be found in Sierpiński [7], pp. 338 and 446.

We now occupy ourselves with the question which prime numbers are the sums of two cubes of natural numbers. It is easy to give the answer. For, if a prime number $p$ is the sum of two cubes of natural numbers, $p = x^3 + y^3$, then $x + y \mid p$, and, if at least one of the numbers $x, y$ is greater than 1, then $x + y < x^3 + y^3 = p$; the number $p$ would then have a natural divisor $x + y > 1$ and less than $p$, which is impossible. Therefore we must have $x = y = 1$, so that $p = 2$. Thus:

No prime number, except the number $2 = 1^3 + 1^3$, is the sum of two cubes of natural numbers.

Which prime numbers are the differences of two cubes of natural numbers? If $p$ is a prime number and $p = x^3 - y^3$, where $x$ and $y$ are natural numbers, then $x > y$, and we have $p = x^3 - y^3 = (x - y)(x^2 + xy + y^2)$, and, since the second factor is greater than the first, we must have $x - y = 1$ and $x^2 + xy + y^2 = p$, whence $p = x^3 - (x - 1)^3 = 3x^2 - 3x + 1$.

The prime number $p$, therefore, is the difference of two cubes of natural numbers if and only if it is of the form $3x(x - 1) + 1$, where $x$ is a natural number $> 1$, and then $p$ is the difference of the cubes of two successive natural numbers.

We do not know if there are infinitely many such prime numbers; the conjecture has been put forth that there are. For $x = 2, 3, 4, 5$, we obtain the prime numbers $7 = 2^3 - 1^3$, $19 = 3^3 - 2^3$, $37 = 4^3 - 3^3$, $61 = 5^3 - 4^3$; for $x = 6$, we obtain the composite number $91 = 7 \cdot 13$; for $x = 7$, we have the prime number $127 = 7^3 - 6^3$; for $x = 8$ and $x = 9$, we have composite numbers $169 = 13^2$ and $217 = 7 \cdot 31$; for $x = 10, 11, 12$, we have prime numbers $271 = 10^3 - 9^3$, $331 = 11^3 - 10^3$, $397 = 12^3 - 11^3$; for $x = 13$, we have the composite number $469 = 7 \cdot 67$; for $x = 14$ and $15$, we have prime numbers $547 = 14^3 - 13^3$ and $631 = 15^3 - 14^3$; for $x = 16$ and $x = 17$, we have composite numbers $721 = 7 \cdot 103$ and $817 = 19 \cdot 43$; for $x = 18$, we have the prime number $919 = 18^3 - 17^3$.

All prime numbers $< 1000$ which are the differences of two
cubes of natural numbers are thus the numbers: 7, 19, 37, 61, 127, 271, 331, 397, 547, 631 and 919.

However, it is easy to prove that there exist infinitely many primes which are not the differences of two cubes of natural numbers. As we have proved, each prime number which is the difference of two cubes of natural numbers is of the form $3x(x-1)+1$ where $x$ is a natural number $> 1$. But of the successive natural numbers $x-1$ and $x$ one is always even. Our prime number must therefore be of the form $6k+1$. But by Theorem 12, there exist infinitely many primes of the form $6k+5$, and obviously no such number is of the form $6k+1$ and therefore is not the difference of two cubes of natural numbers. However, there are composite numbers of the form $6k+5$ which are the differences of two cubes of natural numbers, for example the numbers $215 = 6\cdot35+5 = 6^3-1^3$. We can also prove, although it would be more difficult, that there exist infinitely many prime numbers of the form $6k+1$ which are not the differences of two cubes of natural numbers: such are, for example, the prime numbers 31, 67, 103, 139, 157.

Regarding prime numbers which are the sums of three cubes of natural numbers it has been conjectured that there are infinitely many such numbers. Indeed, a stronger conjecture has been made, namely, that there are infinitely many prime numbers of the form $x^3 + 2 = x^3 + 1^3 + 1^3$, where $x$ is a natural number. Such are, for example, the numbers $3 = 1^3 + 2$, $29 = 3^3 + 2$, $127 = 5^3 + 2$, $24,391 = 29^3 + 2$. It can be shown that there are infinitely many primes which are not the sums of three cubes of integers. However (as we have proved above for $n = 3$), it is easy to show that no prime number $> 2$ is the sum of two $n$th powers of natural numbers, where $n$ is an odd number $> 1$.

Moreover, we observe that K. F. Roth proved (in 1951) that every sufficiently large natural number is the sum of eight cubes of natural numbers of which at least seven are cubes of prime numbers.

21. Quadratic residues

If $p$ is a prime, every integer $r$ for which there exists an integer $x$ such that the number $x^2 - r$ is divisible by $p$ is called a quadratic
residue for \( p \). In other words, an integer \( r \) is called a quadratic residue for \( p \), if there exists a square of an integer which when divided by \( p \) leaves the remainder \( r \). Integers which are not quadratic residues for \( p \) are called quadratic non-residues for \( p \). For the number 2 obviously every integer is a quadratic residue because if \( r \) is an odd number then \( 2|1^2-r \), while if \( r \) is even then \( 2|0^2-r \).

Now, let \( p \) be an odd prime number. We find out how many numbers in the sequence 1, 2, 3, ..., \( p-1 \) are quadratic residues for \( p \).

Denote, in general, by \( r_x \) the remainder obtained on dividing \( x^2 \) by \( p \). For an integral \( x \) the numbers \( r_x \) will be all the quadratic residues for \( p \) (because \( p|x^2-r_x \)). In particular, each of the numbers
\[
(i) \quad r_1, r_2, \ldots, r_{(p-1)/2}
\]
will be a quadratic residue for \( p \). \( (p-1)/2 \) is a natural number because we have supposed that \( p \) is an odd prime. The numbers of the set (i) are obviously different from zero (because none of the numbers \( 1^2, 2^2, \ldots, [(p-1)/2]^2 \) is divisible by \( p \)); they are therefore numbers of the set 1, 2, 3, ..., \( p-1 \).

We observe that the numbers (i) are all different. Namely, suppose that for some natural \( i \) and \( j \) where \( i < j \leq (p-1)/2 \) we have \( r_i = r_j \). This would mean that the numbers \( i^2 \) and \( j^2 \) when divided by \( p \) give the same remainder, and therefore the number
\[
(j^2-i^2) = (j-i)(j+i)
\]
would be divisible by \( p \). But, because of the inequality which we have for \( i \) and \( j \), the numbers \( j-i \) and \( j+i \) are natural and both less than \( p \) (because \( j+i < 2j \leq p-1 < p \)) and the prime number \( p \) cannot be a divisor of the product of two natural numbers less than \( p \). We then prove that
\[
r_i \neq r_j \quad \text{for} \quad i < j \leq \frac{p-1}{2}.
\]

We have thus at least \( (p-1)/2 \) quadratic residues for \( p \) among the numbers 1, 2, 3, ..., \( p-1 \). We now show that in this set there are no more quadratic residues for \( p \) except the numbers of the set (i). To prove this let us suppose that \( r \) is a number in the set 1, 2, ..., \( p-1 \) which is a quadratic residue for
Thus there exists an integer $a$ such that $p|a^2 - r$. It follows that 
$p|(a^{p-1}/2 - r^{(p-1)/2})$. Since the number $r$ is not divisible by $p$, the
number $a$ is not divisible by $p$. By Fermat's theorem we have
$p|a^{p-1} - 1$. But from the preceding we get $p|a^{p-1} - r^{(p-1)/2}$. The
number $p$ thus divides the difference of the two sides of our
formula, that is $p|r^{(p-1)/2} - 1$. We thus have

$$p|r^{(p-1)/2} - 1 \quad \text{for} \quad i = 1, 2, \ldots, \frac{p-1}{2}.$$  

By Lagrange's theorem the polynomial $x^{(p-1)/2} - 1$ cannot be
divisible by $p$ for more than $(p-1)/2$ different values $x$ in the set
$0, 1, 2, \ldots, p-1$. It follows that besides the $(p-1)/2$ numbers
(i) we have in the sequence $1, 2, \ldots, p-1$ no other numbers $r$ for
which $p|r^{(p-1)/2} - 1$, i.e. we have in this set no other quadratic
residues for $p$. We have thus proved

**Theorem 20.** If $p$ is an odd prime number, then in the set
$1, 2, 3, \ldots, p-1$ we have exactly $(p-1)/2$ quadratic residues for $p$
and obviously as many quadratic non-residues for $p$ because

$$p-1 - \frac{p-1}{2} = \frac{p-1}{2}.$$  

From the proof of our theorem it follows immediately that
in order to get all the numbers of the set $1, 2, \ldots, p-1$ which are
quadratic residues for the odd prime $p$, it is enough to find the
remainders on dividing by $p$ the numbers

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$  

In this way we find, for example, that all positive quadratic
residues for number 13 which are less than 13 are the numbers
$1, 4, 9, 3, 12, 10$ and therefore (among the numbers $> 0$ and $< 13$)
non-residues for 13 are the numbers $2, 5, 6, 7, 8$ and 11.

As we have proved above, the number $r$ in the set $1, 2, \ldots, p-1$
is a quadratic residue for an odd prime $p$ if and only if the number
$r^{(p-1)/2} - 1$ is divisible by $p$. If the number $a$ of our set is a
quadratic non-residue for $p$, then the number $a^{(p-1)/2} - 1$ is not
What we know and what we do not know

Divisible by $p$. But, by Fermat's theorem, the number $a^{p-1} - 1$ is divisible by $p$, and, since $a^{p-1} - 1 = (a^{(p-1)/2} - 1)(a^{(p-1)/2} + 1)$, and as $p$ does not divide the first factor on the right-hand side, so it must divide the second factor, that is $p|a^{(p-1)/2} + 1$. Thus the number $a$ is a quadratic residue for the odd prime $p$ if $p|a^{(p-1)/2} - 1$ and a non-residue if $p|a^{(p-1)/2} + 1$.

We remark that for composite numbers it is otherwise. For example, for $n = 15$ among the natural numbers $< 15$ only five (and therefore less than $(n-1)/2 = 7$) are quadratic residues for the number 15, namely the numbers 1, 4, 6, 9 and 10, and the remaining 9 numbers are quadratic non-residues for the number 15. Among the natural numbers $< 8$ only two, namely 1 and 4, are quadratic residues for 8.

A. Valé Vins remarked that an odd number $n$ is prime if and only if none of the numbers

$$2^2, 3^2, 4^2, \ldots, \left(\frac{n-1}{2}\right)^2$$

give the remainder 0 or 1 when divided by $n$.

Cubic and biquadratic residues and residues of higher degree have also been examined. It can be proved that for every odd number $n$ there exist infinitely many primes $p$ for which every integer is an $n$th degree residue. For example, for the numbers 5 and 11 every integer is a cubic residue, and for the numbers 5 and 7 every integer is a fifth degree residue.

The proof that every integer is a fifth degree residue for the prime number 7 is an immediate consequence of the following formulae, which are easy to verify: $7|10^5 - 0$, $7|1^5 - 1$, $7|4^5 - 2$, $7|5^5 - 3$, $7|2^5 - 4$, $7|3^5 - 5$, $7|6^5 - 6$. It can be proved that for the primes 5 and 17 every integer is a residue of every odd degree. It can also be proved that in order that for a prime $p$ every integer be a residue of every odd degree it is necessary and sufficient that the prime number $p$ be of the form $2^{2k} + 1$, i.e. that it be a Fermat prime.

22. Fermat numbers

Fermat numbers are numbers of the form $F_k = 2^{2k} + 1$ where $k = 0, 1, 2, \ldots$. A famous mathematician of the seventeenth century,
P. Fermat, conjectured that all these numbers are prime. This is true for \( k = 0, 1, 2, 3, 4 \), but L. Euler in 1732 showed that the number

\[ F_5 = 2^{25} + 1 = 4,294,967,297 \]

having 10 digits is composite, divisible by 641. Today (in 1963) we know 38 composite numbers \( F_k \), namely for \( k = 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 23, 36, 38, 39, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 260, 267, 268, 284, 316, 452, 1945 \).

These 38 composite numbers \( F_k \) include those for which we know the prime factors (for example \( F_5 \) and \( F_6 \)), those whose prime factors we do not know, but for which we know the decomposition into products of two integers \( > 1 \) (such a number is \( F_{1945} \)), and those for which we do not know even the decomposition as products of two integers \( > 1 \), although we know that such a decomposition exists (\( F_7, F_8, F_{13} \) and \( F_{14} \)).

We begin with the greatest known composite Fermat number \( F_{1945} \). The number of digits of this number is \( > 10^{582} \) and therefore it is impossible to write all its digits. However, as has already been mentioned, we know the smallest prime divisor of this number, which is \( m = 5 \cdot 2^{1947} + 1 \). Now two questions arise: (1) how to obtain this divisor and (2) how it can be ascertained that the number \( m \), having 587 digits, is the divisor of the number \( F_{1945} \), whose digits we cannot write.

Obviously we will neither perform the division of the numbers \( F_{1945} \) by the number \( m \) nor find the quotient in the division, but in another way ascertain or rather explain how to determine that the number \( F_{1945} \) gives the remainder 0 when divided by \( m \).

For an integer \( t \) we denote by \( \bar{t} \) the remainder upon division of \( t \) by \( m \). From the definition of the number \( \bar{t} \) it follows that, for every integer \( t \), \( m|t - \bar{t} \). We now define a sequence \( r_k \) \((k = 1, 2, \ldots)\) by the conditions

\[ (i) \quad r_1 = 2^2, \quad r_{k+1} = \left( \frac{r_k}{2} \right)^2 \quad \text{for} \quad k = 1, 2, \ldots \]

We prove by induction that

\[ (ii) \quad m|2^{2^k} - r_k \quad \text{for} \quad k = 1, 2, \ldots \]
The formula (ii) is obviously true for \( k = 1 \), because \( 2^{2^1} - r_1 = 0 \). We suppose that it is true for a certain natural number \( k \). In view of (ii) we have a fortiori \( m|2^{k+1} - r_k^2 \), and since from \( m|t - \bar{t} \) for \( t = r_k^2 \), we have \( m|r_k^2 - \bar{r}_k^2, \ m|2^{k+1} - \bar{r}_k^2 \), so that by (i) \( m|2^{k+1} - r_{k+1}^2 \). Formula (ii) is thus proved by induction. For \( k = 1945 \) we get

\[ m|F_{1945} - r_{1945} + 1, \]

whence it follows that the number \( F_{1945} \) gives, when divided by \( m \), the same remainder as \( r_{1945} + 1 \). In order to find whether or not the number \( F_{1945} \) is divisible by \( m \) it is thus enough to find if \( r_{1945} + 1 \) is divisible by \( m \).

Now we reflect how to carry out the operation necessary for obtaining the number \( r_{1945} \). From formulae (i) it follows that the numbers \( r_2, r_3, \ldots, \) being the remainders left after division by \( m \), are all less than \( m \), so that each has less than 587 digits. From (i) it thus follows that to obtain the number \( r_{1945} \) it is necessary to square 1944 numbers having not more than 587 digits each and to divide the squares of those numbers (i.e. numbers having not more than 1175 digits each) by \( m \), having 587 digits. These are operations which an electronic computer today has been able to perform. In this way it has been computed that the number \( F_{1945} \) is divisible by the number \( m = 5,21947 + 1 \), and since, as is easy to show, \( F_{1945} > m \), the number \( F_{1945} \) is composite.

We now turn to the question how the prime divisor \( m \) of the number \( F_{1945} \) has been found. It is a well-known theorem that every natural divisor of the number \( F_n \) must be of the form \( 2^n + 2 \cdot k + 1 \), where \( k \) is an integer \( \geq 0 \). For \( n = 1945 \), it follows that the divisors of the number \( F_{1945} \) can only be numbers in the arithmetic progression \( 2^{1947}k + 1 \) (\( k = 0, 1, 2, \ldots \)). For \( k = 0 \), we obtain the trivial divisor 1. For \( k = 1 \), the number \( 2^{n+2} + 1 = 2^{1947} + 1 \) is obviously divisible by 3 and so is not a prime. For \( k = 2 \), the number \( 2^{n+2} \cdot 2 + 1 = 2^{1948} + 1 = (2^4)^{487} + 1 \) is divisible by \( 2^4 + 1 \) and so is not prime. For \( k = 3 \), the number \( 2^{n+2} \cdot 3 + 1 = 2^{1947} \cdot 3 + 1 \) is composite, divisible by 5 because \( 5|2^4 - 1 \), whence \( 5|2^{1944} - 1 \) and if we multiply the right side by \( 2^3 \), \( 5|2^{1947} \cdot 3 - 24 \), whence
$5|2^{1947} - 3 + 1$. For $k = 4$, the number $2^n+2.4+1 = 2^{1949} + 1$ is divisible by 3 and so is composite.

Thus trying to find the prime divisor of the number $F_{1945}$, we must divide it by $2^{1947} - 5 + 1 = m$. As the division turns out to be without remainder, it can be seen that $F_{1945}$ is composite. It follows at once, that the number $m$ as the smallest divisor of $F_{1945}$ greater than 1 is a prime.

Similarly one can investigate other Fermat numbers. For the number $F_5$, about which Fermat was convinced that it is a prime, the investigation is very simple. The divisors of the number $F_5$ must, as we know, take the form $2^k + 1$, that is, $128k + 1$. For $k = 1$, we obtain the number 129, divisible by 3 and therefore composite. For $k = 2$, we get the prime number 257, which is not a divisor of the number $F_5$, as can easily be ascertained by dividing of the number $F_5$ (containing 10 digits) by the number 257. For $k = 3$ we get the number 385, divisible by 5 and thus composite. For $k = 4$, we get the number 513 = $2^9 + 1$, divisible by 3 and thus composite. For $k = 5$, we get the prime number 641, about which it is easy to determine that it is a divisor of the number $F_5$. Hence with the help of only two divisions we can ascertain that 641 is the smallest prime divisor of the number $F_5$.

Dividing the number $F_5 = 4,294,967,297$ by 641 we obtain the quotient 6,700,417. The divisors of this number, being divisors of $F_5$, must be of the form $2^k + 1$ and if $F_5$ is composite, it must have a prime divisor not greater than its square root and so less than 2600. We thus have for $k$ the inequality $128k + 1 < 2600$, whence $k < 21$, and on the other hand we know that $k$ must be greater than 4 because the smallest prime divisors of the number $F_5$ is 641. Thus with the help of a few divisions it is verified that the number 6,700,417 is a prime, and the prime decomposition of the number $F_5$ into the product of two prime factors is obtained.

For the number $F_6$ the divisor $2^9.1071 + 1$ is obtained and thus the fact of its being composite is verified.

The quest for prime divisors of the number $F_n$ among the numbers of the arithmetic progression $2^n+2k+1$ leads to the discovery of such a divisor only when there exists not too large prime divisor of the number $F_n$. In the contrary case, putting for $k$
successively very large numbers, we are not able to encounter such a divisor. This holds, for example, for the numbers $F_7$ and $F_8$, of which the first has thirty-nine and the second seventy-eight digits. We know no prime divisor of these numbers, and no decomposition of it into a product of two natural numbers greater than 1; however, J. C. Morehead proved in 1905 that the number $F_7$ is composite and A. E. Western proved in 1909 that $F_8$ is composite. He proved this using the following

**Theorem 21.** If $F_n$ is prime, the number $3^{2^n} - 1 + 1$ is divisible by $F_n$.

We prove first the following

**Lemma.** If $k$ is a non-negative integer and if the number $p = 12k + 5$ is prime, then the number $3^{6k+2} + 1$ is divisible by $p$.

**Proof of the lemma.** The lemma is obviously true for the number $k = 0$; we may therefore say that $k$ is a natural number. Let $p = 12k + 5$. We consider the product of the first $6k+2$ natural numbers divisible by 3 and divide the factors of the product into three groups, putting in the first group the first $2k$ factors, in the second the next $2k+1$ factors and in the third the remaining $2k+1$ factors.

The factors of the first group give the product $3.6.9...6k$.

The factors of the second group give, after inverting the order of the factors, the product

$$(12k+3)12k(12k-3)...(6k+6)(6k+3),$$

which, since $p = 12k + 5$, can be written in the form

$$(p-2)(p-5)(p-8)...[p-(6k+2)].$$

Because the number of divisors is odd ($= 2k+1$), our product, after expanding and collecting the terms divisible by $p$, gives us the number $pu - 2.5.8...(6k+2)$, where $u$ is a certain integer.

The factors of the third group give the product

$$(12k+6)(12k+9)(12k+12)...(18k+6) = (p+1)(p+4)(p+7)...(p+6k+1) = pv+1.4.7...(6k+1),$$

where $v$ is a natural number.
We thus have

\[ 3.6.9 \ldots (18k+6) = 3.6.9 \ldots 6k(pu-2.5.8 \ldots (6k+2))(pv+1.4.7 \ldots (6k+1)) = pw-1.2.3.4.5.6 \ldots (6k+1)(6k+2) = pw-(6k+2)! \]

where \( w \) is an integer.

But \( 3.6.9 \ldots (18k+6) = (6k+2)!3^{6k+2} \). We deduce that the number \( pw \) is divisible by \( (6k+2)! \), and so \( pw = (6k+2)!t \), where \( t \) is an integer. But \( 6k+2 < 12k+5 = p \), and so the number \( (6k+2)! \) is not divisible by \( p \). As the product \( (6k+2)!t \) is divisible by \( p \), \( t \) must be divisible by \( p \), \( t = ps \), whence \( w = (6k+2)!s \), where \( s \) is an integer. We have therefore

\[ 3^{6k+2} = ps-1, \]

whence it follows that the number \( 3^{6k+2}+1 \) is divisible by \( p \). We have thus proved our lemma.

Proof of Theorem 21. Let \( n \) be a given natural number. We have \( 2^n = 2m \), where \( m \) is a natural number, hence \( F_n-1 = 4^m \), from which it follows that the number \( F_n-5 \) is divisible by 4. On the other hand, we have \( F_n-1 = 4^m = (3+1)^m = 3t+1 \), where \( t \) is a natural number. Hence \( F_n-5 = 3(t-1) \), which proves that the number \( F_n-5 \) is divisible by 3, and since, as we have shown, it is divisible by 4, it is divisible by 12, so that \( F_n = 12k+5 \), where \( k \) is an integer. From our lemma it thus follows that, if \( F_n \) is prime, then \( 3^{6k+2}+1 = 3^{(F_n-1)/2}+1 = 3^{2^{n-1}}+1 \) is divisible by \( F_n \).

This completes the proof. We also mention that it can be proved (which, however, will not be necessary for us) that the converse of Theorem 21 is true.

We now apply Theorem 21 to prove that the number \( F_7 \) is composite. It is enough to show that \( 3^{2^{127}}+1 \) is not divisible by

\[ F_7 = 340,282,366,920,938,463,463,374,607,431,768,211,457. \]

For this purpose it would be sufficient to calculate the remainder
of the division of $3^{2127}$ by $F_7$. The number $3^{2127}$ is so gigantic that we cannot write its digits, but in order to calculate the remainder which it gives when divided by $F_7$ we may proceed as follows. The number $3^{27}$ has 61 digits and so we can write it and calculate the remainder $r$ of its division by $F_7$. (Today it is not a difficult thing with the help of an electronic computer but in 1905, when Morehead worked, it was cumbersome but possible.) The remainder $r_1$ of the division of $r^2$ by $F_7$ will obviously be the remainder of the division of $3^{28}$ by $F_7$. Similarly the remainder $r_2$ of the division of $r_1^2$ by $F_7$ will be the remainder of the division of $3^{29}$ by $F_7$ and the remainder $r_3$ of the division of $r_2^2$ by $F_7$ is the remainder of the division $3^{210}$ by $F_7$. Proceeding in this manner we arrive at the remainder $r_{120}$ of the division of the number $3^{2127}$ by $F_7$. In this way it is found that $r_{120}$ $\neq$ $2^{27}$, whence it follows that the number $3^{2127} + 1$ is not divisible by $F_7$, so that, by Theorem 21, the number $F_7$ is not prime.

In a similar way it was also checked that the numbers $F_8$, $F_{13}$ and $F_{14}$ are not prime ($F_{13}$ and $F_{14}$ were investigated by means of electronic computers). For each of the numbers $F_n (n = 9, 10, 11$ and $12)$, which are composite, we know a prime divisor, namely $2^{16} \cdot 37 + 1 | F_9$, $2^{12} \cdot 11, 131 + 1 | F_{10}$, $2^{13} \cdot 39 + 1 | F_{11}$, $2^{14} \cdot 7 + 1 | F_{12}$. Further, it has been proved that the numbers $F_{15}$ and $F_{16}$ are composite and prime divisors are obtained:

$$2^{21} \cdot 573 + 1 | F_{15}, \quad 2^{18} \cdot 3150 + 1 | F_{16}.$$ 

However, the number $F_{17}$ has more than 30 thousand digits and existing computers are not able to perform several thousand divisions of numbers with several thousand digits by numbers having more than 30 thousand digits.

For the number $F_{16}$, the smallest prime divisor $2^{18} \cdot 3150 + 1$, was found in 1953, and thus the conjecture that all the numbers of the sequence

$$2 + 1, \quad 2^2 + 1, \quad 2^{2^2} + 1, \quad 2^{2^{2^2}} + 1, \ldots$$
are prime was disproved, because the number $F_{16}$ is the fifth term of this sequence. We do not know, however, if in this sequence there are infinitely many prime numbers or infinitely many composite numbers.

We observe that none of the numbers $2^{2^n} + 1$, where $n$ is a natural number, is prime, because they are $> 3$ and divisible by 3.

23. Prime numbers of the form $n^n + 1$, $n^n + 1$, etc.

In connection with Fermat numbers the question arises how many prime numbers there are of the form $n^n + 1$ where $n$ is a natural number. Suppose that $n$ is a natural number and that the number $n^n + 1$ is prime. Each natural number $n$ is, as we know, of the form $n = 2^k \cdot m$, where $k$ is an integer $\geq 0$, and $m$ is an odd number. If $m$ were $> 1$, then the number $n^{n+1} = (n^2)^m + 1$ would be $> n^{2k} + 1$ and divisible by $n^{2k} + 1$, i.e. it would be composite. Therefore $m$ must be equal to 1 and so $n = 2^k$.

If $k = 0$, then $n = 1$, and the number $n^n + 1$ is a prime. If $k > 0$, then $k = 2r \cdot s$, where $r$ is an integer $\geq 0$ and $s$ an odd number. If $s > 1$, then the number $n^n + 1 = 2^{2^n} \cdot s^n + 1 = (2^{2^n})^s + 1$, being $> 2^{2^n} + 1$ and divisible by this number, would be composite.

Therefore $s$ must be equal to 1, and so $k = 2^r$ and $n = 2^{2^r}$ and

$$n^{n+1} = 2^{2^r} \cdot 2^{2^r} + 1 = 2^{2^r+2^r} + 1 = F_{r+2^r}.$$

Hence the number $n^n + 1$, where $n$ is a natural number $> 1$, is a prime if and only if $n = 2^{2^r}$, where $r$ is an integer $\geq 0$, and the number $F_{r+2^r}$ is a prime.

For $r = 0$, since $F_1 = 5$ is prime, we get the prime number $2^2 + 1 = 5$. For $r = 1$, since $F_3 = 257$ is a prime, we get the prime number $4^4 + 1 = 257$. For $r = 2$, since the number $F_6$ is, as we know, composite, divisible by $2^8 \cdot 1071 + 1$, we do not get a prime number. Also for $r = 3$ we do not get a prime number because $F_{11}$ is composite, divisible by $2^{13} \cdot 39 + 1$. If, therefore, besides the number 2, 5 and 257 there exist prime numbers of
the form $n^n+1$, then they must be $\geq F_{20} > 2^{220} > 2^{106} > 10^{3.105}$, that is, they must have more than 300 thousand digits each.

Thus, among the numbers of the form $n^n+1$ (where $n$ is a natural number) having not more than 300 thousand digits there are only three primes: $1^1+1 = 2$, $2^2+1 = 5$, and $4^4+1 = 257$.

From this one may conjecture that there are no prime numbers of the form $n^n+1$, where $n$ is a natural number, except the three, 2, 5 and 257. It is, however, necessary to take into consideration that from such a conjecture it would follow that there exist infinitely many composite Fermat numbers; for such would be the $F_{r+2r}$ for $r = 4, 5, 6, \ldots$, that is the numbers $F_{20}$, $F_{37}$, $F_{70}$, $F_{135}$, $F_{264}$, $F_{521}$, $F_{1034}$, \ldots So far we have not been able to prove any of these numbers to be composite.

We next ask what we know about prime numbers of the form $n^n+1$. Now we have $1^1+1 = 2$, $2^2+1 = 17$. It is easy to prove that if the number $n^n+1$, where $n$ is a natural number $> 1$, is a prime, then for some integer $r \geq 0$, we must have $n = 2^r$, so that

$$n^n+1 = F_{r+2r+2r}.$$

For $r = 0$ we obtain the prime number $F_2 = 17$, for $r = 1$ the number $F_9$, which, as we know, is composite, divisible by $2^{16}.37+1$. For $r = 2$, we get the number $F_{66}$, which, as is easy to show, has more than $10^{18}$ digits. Hence the result that

*Among the numbers having not more than $10^{18}$ digits, there exist only two prime numbers of the form $n^n+1$, where $n$ is a natural number, viz. 2 and 17.*

It has also been investigated which of the numbers $n.2^n+1$, where $n = 1, 2, 3, \ldots$, are prime (these are known as Cullen's numbers). Besides the number 3 (for $n = 1$) we know only one such prime number, for $n = 141$ (see Robinson [3]). The question about the number of such primes remains open.

As is easy to prove, there are no prime numbers of the form $2^n+1$ except the Fermat primes. For if $n = 2^r.m$, where $m$ is an odd number $> 1$, then the number $2^n+1 = (2^r)^m+1$ is divis-
ible by a smallest number $2^{2r}+1 > 1$ and so is composite. Among prime numbers of the form $2^n+1$, where $n = 1, 2, \ldots$, we thus know only five: for $n = 1, 2, 4, 8, 16$, and the smallest number of this form of which we do not know whether it is prime or not is the number $2^{131,072}+1$. We therefore know only four prime numbers of the form $2.2^n+1$, where $n$ is a natural number, namely for $n = 1, 3, 7$ and 15. However, we know 19 prime numbers of the form $3.2^n+1$, viz. for $n = 1, 2, 5, 6, 8, 12, 18, 30, 36, 41, 66, 189, 201, 209, 276, 353, 408, 438, 534$. We know only three prime numbers of the form $4.2^n+1$, where $n = 1, 2, \ldots$, namely for $n = 2, 6$ and 14. But we know 12 prime numbers of the form $5.2^n+1$ (where $n = 1, 2, \ldots$): for $n = 1, 3, 7, 13, 15, 25, 39, 55, 75, 85, 127, 1947$.

For each natural number $k \leq 100$ we know at least one natural number $n$ such that the number $k.2^n+1$ is prime. However, one can show that there exist infinitely many odd natural numbers $k$, for which each of the numbers $k.2^n+1$ ($n = 1, 2, \ldots$) is composite (see Sierpiński [6]).

Prime numbers of the form $2^m+2^n+1$, where $m$ and $n$ are natural numbers and $m > n$, have also been investigated. We know such prime numbers, for example $2^2+2+1 = 7.2^3+2+1 = 11, 2^3+2^2+1 = 13, 2^4+2+1 = 19$.

We do not know if there are infinitely many such prime numbers. However, it is easy to show that there exist infinitely many composite numbers of the form $2^m+2^n+1$, where $m$ and $n$ are natural numbers, $m > n$. This follows, for example, immediately from the equality

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

or from the fact that for $k = 1, 2, \ldots$ the number $2^{4k}+2^l+1$ is always divisible by 5, and the number $2^{2k}+2^l+1$ is for natural $k$ and $l$ always divisible by 3. We have also the decomposition

$$2^{4k}+2^{2k}+1 = (2^{2k}+2^k+1)(2^{2k}-2^k+1).$$

A. Richner checked that the numbers $2^n+3$ for $n < 24$ are prime only for $n = 1, 2, 3, 4, 6, 7, 12, 15, 16, 18$. It is easy to prove that
among the numbers $2^{2n} + 3$ there are infinitely many which are composite, viz. the numbers $2^{2(3k+1)} + 3$ for $k = 0, 1, 2, \ldots$ are all divisible by 19. However, the numbers $2^{2k+1} + 3$ for $k = 0, 1, 2, \ldots$ are all divisible by 7.

We have also $13 | 2^{2^k} - 3$ for $k = 1, 2, 3, \ldots$, whence it follows that each of the numbers

$$2^{2^2} - 3, \quad 2^{2^{2^2}} - 3, \ldots$$

is divisible by 13 and so is composite.

However, we do not know whether among the numbers

$$2 + 3, \quad 2^2 + 3, \quad 2^{2^2} + 3, \quad 2^{2^{2^2}} + 3, \ldots$$

there is only a finite number of primes.

But among the numbers

$$2^{2^2} + 5, \quad 2^{2^2} + 5, \ldots$$

there are no primes, because each of these numbers is divisible by 7. The proof of this is easy. For a natural $k$, the number $2^{2k} = (3+1)^k$ when divided by 3 gives the remainder 1; so $2^{2k} = 3t + 1$, where $t$ is a natural number. Hence $2^{2^k} + 5 = 2^{3t+1} + 5 = (7+1)^t \cdot 2 + 5$, which is obviously divisible by 7.

It is not known if there exist natural numbers $k$ for which there are infinitely many prime numbers of the form $2^{n_1} + 2^{n_2} + \ldots + 2^{n_k} + 1$, where $n_1, n_2, \ldots, n_k$ are natural numbers.

We do not know if there exist infinitely many prime numbers of the form $2^n + n^2$, where $n$ is a natural number. The smallest four such numbers are the prime numbers $3 = 2^1 + 1^2$, $17 = 2^3 + 3^2$, $593 = 2^9 + 9^2$ and $32,993 = 2^{15} + 15^2$.

A. Schinzel proved that for every positive integer $a$ satisfying the inequalities $2 \leq a \leq 2^{27}$ there exists at least one positive integer $n \leq 15$ such that the number $a^{2^n} + 1$ is composite. If the conjecture that for every integer $a > 1$ there exists at least one positive integer $n$ such that the number $a^{2^n} + 1$ is composite were stated, it would imply that there exist infinitely many composite Fermat numbers. In fact, for $a = 2^k$ ($k = 1, 2, \ldots$) we have
\[ a^{2^n} + 1 = F_{n+k}. \] For \( a = 2^{21945} \) we cannot show that there exists at least one positive \( n \) such that \( a^{2^n} + 1 \) is composite.

It is easy to prove that there exist infinitely many positive integers \( a \), for which all numbers \( a^{2^n} + 1 (n = 1, 2, \ldots) \) are composite, for example, the number \( b^m \) where \( b \) is an integer > 1 and \( m \) an odd integer > 1. On the other hand, we cannot find any positive integer \( a > 1 \) for which all numbers \( a^{2^n} + 1 (n = 1, 2, \ldots) \) are prime. From the conjecture of Schinzel (it will be considered in § 29) it follows that for every positive integer \( m \) there exists an integer \( a > 1 \) such that the \( m \) numbers \( a^{2^n} + 1 (n = 1, 2, \ldots, m) \) are prime. For \( m = 4 \) one can put \( a = 2 \). It may be difficult to find such a number for \( m = 5 \).

24. Three false propositions of Fermat

P. Fermat stated the following three theorems (in his letter to Mersenne in 1641):

1. No prime number of the form \( 12k + 1 \) is a divisor of any number of the form \( 3^n + 1 \).
2. No prime number of the form \( 10k + 1 \) is a divisor of any number of the form \( 5^n + 1 \).
3. No prime number of the form \( 10k - 1 \) is a divisor of any number of the form \( 5^n + 1 \).

It is easy to verify that none of the three theorems is true; the first because, for example, \( 61|3^5 + 1 \), \( 241|3^{60} + 1 \), the second because \( 521|5^5 + 1 \), the third because \( 29|5^7 + 1 \). A. Schinzel proved in [4] that for each of these theorems there exist infinitely many prime numbers for which it is false.

Therefore the situation here is somewhat different from that of Fermat's theorem stating that each of the numbers \( 2^{2^n} + 1 \) (where \( n = 1, 2, 3, \ldots \)) is prime, where we know only a finite number of examples which show that it is false.

Besides the three above theorems Fermat also stated the theorem that none of the prime numbers of the form \( 12k - 1 \) is a divisor of any number of the form \( 3^n + 1 \), which was proved later (see Pillai [1]).
25. Mersenne numbers

Mersenne numbers are numbers of the form $M_n = 2^n - 1$, where $n = 1, 2, 3, \ldots$. They are interesting in two respects. Firstly, the greatest known prime numbers are Mersenne numbers and secondly with the help of Mersenne numbers we discover what are called perfect numbers, that is those which are equal to the sum of all their natural divisors less than those numbers themselves. (Perfect numbers were investigated in antiquity.)

One can express the $n$th Mersenne number as the sum of the first $n$ terms of the geometric progression $1, 2, 2^2, 2^3, 2^4, \ldots$

We have therefore

\[ M_1 = 1, \quad M_2 = 3, \quad M_3 = 7, \quad M_4 = 15, \]
\[ M_5 = 31, \quad M_6 = 63, \quad M_7 = 127, \ldots \]

It is easy to prove, if the index $n$ of the number $M_n$ is composite, then the number $M^n$ is composite; for if $n = ab$ where $a$ and $b$ are natural numbers $> 1$, then $2^a - 1 > 1$ and $2^n - 1 = 2^{ab} - 1 > 2^a - 1$, and the number $2^{ab} - 1$ is divisible by $2^a - 1$, and so is composite.

Therefore if the number $M^n$, where $n > 1$, is prime, then the number $n$ must be prime, but the converse is not necessarily true because, for example,

\[ M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89. \]

It has been proved that, if $p$ is a prime number, then each natural divisor of the number $M_p$ must be of the form $2kp + 1$, where $k$ is an integer $\geq 0$. Thus, for example, the divisors of the number $M_{11}$ are the numbers $22k + 1$, where $k = 0, 1, 4$ and 93.

In particular, therefore, it follows that the divisors of the number $M_{101} = 2^{101} - 1$ must be of the form $202k + 1$. Unfortunately none of the prime divisors of the number $M_{101}$ has been found so far (evidently the number $k$ is very large), although by other methods (of which we speak later) it has been verified that $M_{101}$ is composite (cf. page 92).

It has also been proved that if $p$ is a prime number of the form $8k + 7$, then $q | M_{(q-1)/2}$. This allows us to confirm that many
of the numbers $M_p$, where $p$ is a prime number, are composite. For example

$$47|M_{23}, 167|M_{83}, 263|M_{131}, 359|M_{179},$$

$$383|M_{191}, 479|M_{239}.$$

The conjecture has been advanced (so far not proved) that among the numbers $M_p$, where $p$ is a prime number, there exist infinitely many which are composite.

We know only 20 Mersenne primes so far; they are the numbers $M_n$ for $n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253$ and 4423. The eight greatest prime numbers of Mersenne were discovered (with the help of electronic computers) in the last ten years.

We now explain how it could be verified that these large Mersenne numbers are prime. This was possible only with the aid of the following theorem:

**Theorem (E. Lucas-D.H. Lehmer).** The number $M_p$, where $p$ is an odd prime, is a prime if and only if $M_p$ is a divisor of the $(p-1)$-th term of the sequence $u$ $(n = 1, 2, ...)$, defined by the conditions:

$$\begin{align*}
u_1 &= 4, \\
u_{n+1} &= \nu_n^2 - 2 \quad \text{for} \quad n = 1, 2, ... \end{align*}$$

(and thus the sequence whose first few terms are the numbers 4, 14, 194, 37,634, ...).

It is easy to prove that in order that $M_p | u_{p-1}$ it is necessary and sufficient that $M_p$ be a divisor of the $(p-1)$-th term of the sequence $r_n (n = 1, 2, ...)$ depending on $M_p$ and defined by the conditions:

$$r_1 = 4, \quad \text{and} \quad r_{n+1} \text{ is the remainder on division of the number} \quad r_n^2 - 2 \text{ by } M_p.$$

Thus in order to find whether or not the number $M_p$ is a prime we have only to square and then to divide $M_p$ numbers less than $M_p$. In particular, in order to find whether $M_{101}$ is a prime number it is necessary to determine that the divisibility $M_{101} | r_{100}$ holds where the number $M_{101}$ has thirty-one digits. These calculations have been performed and it has been found that $r_{100}$ is not
divisible by $M_{101}$; hence the result that $M_{101}$ is a composite number.

In order to verify that the number $M_{3217}$ having 969 digits is a prime, it has been necessary to show that the number $r_{3216}$ (corresponding to $M_{3217}$) is divisible by $M_{3217}$. It has required about several thousands squaring operations and then dividing the squares obtained, having not more than 969 digits, by the number $M_{3217}$, which the existing electronic computers have made possible.

We write here only the first and the last few digits of this number. It is $M_{3217} = 259,117,0...09,315,071$. All the 969 digits of this number are given in the journal *Mathematical Tables and other Aids to Computation* 12(1958), p. 60. It is also mentioned there that verification that the number $M_{3217}$ is a prime, took the Swedish electronic computer BESK 5½ hours.

The conjecture has been advanced that if the Mersenne number $M_n$ is a prime then the number $M_{M_n}$ is also a prime. This is true for the four smallest Mersenne numbers, but for the fifth Mersenne prime number, i.e. for the number $M_{13} = 8191$, as D. H. Wheeler calculated in 1953, it is not true, because $N_{M_{13}} = 2^{8191} - 1$ (having 2466 digits) is composite (see Robinson [1]). The verification of this (with the help of the theorem of Lucas–Lehmer) required one hundred hours work on an electronic computer. We do not know any of the prime divisors of this composite number. However, in 1957 it was discovered (see Robinson [2]) that although the number $M_{17}$ is prime, the number $M_{M_{17}}$ is composite, being divisible by $1768(2^{17} - 1) + 1$, and also that, although the number $M_{19}$ is prime, the number $M_{M_{19}}$ is composite, being divisible by $120(2^{19} - 1) + 1$.

The conjecture has also been advanced (and so far not disproved) that the numbers $q_0, q_1, q_2, ...$ where $q_0 = 2$ and $q_{n+1} = 2^{q_n} - 1$ for $n = 0, 1, 2, ...$ are all prime. This is true for the numbers $q_n$ where $n \leq 4$, but the number $q_5$ has, as is easy to calculate, more than $10^{37}$ digits, and so we are not able to write it, let alone verifying whether or not it is prime.

We remember in connection with Mersenne numbers the
finding of even perfect number. Originally Euclid gave the following method of obtaining even perfect numbers: we calculate the sum of the successive terms of the geometric progression \(1, 2, 2^2, 2^3, \ldots\) If such a sum is a prime number, we multiply it by the last term. We have thus obtained a perfect number. Euler proved that this method allows us to get all even perfect numbers.

In other words, this shows that all even perfect numbers are of the form \(2^{p-1} M_p\), where \(M_p\) is a prime number.

It follows that we know as many even perfect numbers as there are known Mersenne primes, namely at present 20.

The smallest perfect number is \(2M_2 = 6\), the greatest known perfect number is \(2^{4422}(2^{4423}-1)\). We do not know odd perfect numbers, we only know (Kanold [1]) that, if they exist, they are very large (greater than \(10^{20}\)).

As for Mersenne numbers, we further mention that F. Jakóbczyk has advanced the conjecture that, if \(p\) is a prime number, then the number \(M_p\) is not divisible by any square of a prime number. A. Schinzel has put the question whether there exist infinitely many Mersenne numbers which are the products of different prime numbers.

26. Prime numbers in several infinite sequences

The question whether or not a given infinite sequence, defined in even a simple way, will contain infinitely many primes is in general very difficult. As we have already said, we do not know if sequences like \(n^2+1\), \(n!+1\), \(n!-1\), \(2^n+1\), \(2^n-1\) (for \(n = 1, 2, \ldots\)) contain infinitely many primes. We also do not know if the infinite sequence 1, 11, 111, 1111, ... contains an infinity of primes. Similar is the case of the so-called Fibonacci numbers \(u_n\) \((n = 1, 2, \ldots)\), defined by the conditions

\[ u_1 = u_2 = 1 \quad \text{and} \quad u_{n+2} = u_n + u_{n+1} \quad \text{(for \(n = 1, 2, \ldots\)).} \]

The first few terms of this sequence are the numbers

\[ u_1 = 1, \ u_2 = 1, \ u_3 = 2, \ u_4 = 3, \ u_5 = 5, \ u_6 = 8, \]

\[ u_7 = 13, \ u_8 = 21, \ldots \]
It has been found that the numbers $u_n$ are prime for $n = 3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47$. Other prime numbers $u_n$ are not known so far. We can prove that if $n \neq 4$ and the number $u_n$ is prime, then $n$ must be prime, but the converse is not necessarily true because, for example,

$$u_2 = 1, \quad u_{19} = 4181 = 37 \cdot 113, \quad u_{34} = 1,346,269 = 557 \cdot 2417.$$

We do not know if among the numbers $u_p$, where $p$ is a prime number, there are infinitely many composite numbers.

The sequence $v_n$ ($n = 1, 2, \ldots$), defined by the conditions

$$v_1 = 1, \quad v_2 = 3, \quad v_{n+2} = v_n + v_{n+1} \text{ for } n = 1, 2, \ldots,$$

has also been investigated. The first few terms are 1, 3, 4, 7, 11, 18, \ldots The numbers $v_n$ are prime for $n = 2, 4, 5, 7, 8, 11, 13, 17, 19, 31, 37, 41, 47, 53, 61, 71$. The greatest known prime number $v_n$ is the number $v_{71} = 688,846,502,588,399$. We do not know if the number of primes $v_n$ is infinite.

We give one more sequence, which in the last few years has occupied the attention of some mathematicians. Consider the sequence of all successive odd numbers: 1, 3, 5, 7, 9, 11, 13, 15, \ldots We put $u_1 = 1$; in this sequence the smallest number $> u_1$ is $u_2 = 3$. We erase from our sequence every third number (i.e. numbers occupying the third, sixth, ninth places, etc.). We obtain in this manner a new sequence: 1, 3, 7, 9, 13, 15, 19, 21, 25, 27, \ldots The smallest number of our sequence $> 3$ is 7, which we denote by $u_3$; now we omit every seventh number in the last sequence, which gives us the sequence 1, 3, 7, 9, 13, 15, 21, 25, 27, \ldots The smallest number of this sequence $> u_3$ is 9, which we denote by $u_4$. We will now remove from the sequence so obtained every ninth number. If we carry on this procedure further, we obtain the infinite sequence $u_1, u_2, \ldots$, whose terms less than one hundred are

$$1, 3, 7, 9, 13, 15, 21, 25, 31, 33, 37, 43, 49, 51, 63, 67, 69, 73, 75, 79, 87, 93, 99.$$

The terms of our sequence are called lucky. We do not know if there are infinitely many primes among them. It has been calcu-
lated that among the lucky numbers less than 98,600 there are 715 prime numbers.

27. Solution of equations in prime numbers

We know many simple equations (even of the first degree) about which we do not know whether they have infinitely many solutions in prime numbers. Such is, for example, the equation \( x + y = z \). It is easy to show that the question whether this equation has infinitely many solutions in prime numbers \( x, y, z \) is equivalent to the question whether there exist infinitely many pairs of twin primes, for, if \( p, q \) and \( r \) are prime numbers such that \( p + q = r \), then obviously the prime numbers \( p \) and \( q \) cannot both be odd (because then their sum would be an even number \( > 2 \) and so composite). Therefore one of the numbers \( p \) and \( q \), say \( q \), is even and so equal to 2. The numbers \( p \) and \( r = p + 2 \) would then be a pair of twin primes. On the other hand, if the numbers \( p \) and \( r = p + 2 \) are a pair of twin primes, then the numbers \( x = p, y = 2, z = p + 2 \) are prime and give the solution of the equation \( x + y = z \).

We do not know if the equation \( 2x + 1 = y \) or the equation \( 2x - 1 = y \) have infinitely many solutions in prime numbers \( x, y \), although we know many such solutions for the equation \( 2x + 1 = y \), \( (x, y) = (2, 5), (3, 7), (5, 11), (11, 23) \), and for the equation \( 2x - 1 = y \), \( (x, y) = (2, 3), (3, 5), (7, 13), (19, 37) \).

The conjecture has been advanced that each of our equations has infinitely many solutions.

However, it has been proved that the equation \( x + y = z + t \) has infinitely many solutions in distinct primes \( x, y, z, t \) and that the same holds for the equation \( x^2 + y^2 = z^2 + t^2 \). For example, \( 7^2 + 19^2 = 11^2 + 17^2 \). It is, on the other hand, easy to show that the equation \( x^2 + y^2 + z^2 = t^2 \) has no solution in prime numbers \( x, y, z, t \).

We do not know if there exist infinitely many right-angled triangles with integral sides, two of which are prime numbers. It can be proved that this problem is equivalent to the question whether the equation \( p^2 = 2q - 1 \) has infinitely many solutions.
in prime numbers \(p\) and \(q\). Examples of such triangles are the triangles with sides \((3, 4, 5)\), \((5, 12, 13)\), \((11, 60, 61)\), \((19, 180, 181)\), \((29, 240, 241)\), \((61, 1860, 1861)\).

It is easy to obtain all solutions of the equation \(x^2 - 2y^2 = 1\) in prime numbers \(x, y\). For, if the natural numbers \(x, y\) satisfy the equation \(x^2 = 2y^2 + 1\), then \(x\) is obviously an odd number, \(x = 2k + 1\), where \(k\) is an integer, so that \(x^2 = 4k^2 + 4k + 1\), whence \(y^2 = 2k(k + 1)\) and \(y\) is even. Therefore, if \(y\) is a prime number, then \(y = 2\), whence we deduce that our equation has only one solution in prime numbers: \(x = 3, y = 2\).

But we do not know how many solutions in prime numbers \(x, y\) there exist for the equation \(x^2 - 2y^2 = -1\). We know such solutions, for example, \(x = 7, y = 5\) or \(x = 41, y = 29\).

It is easy to prove that if \(n\) is a natural number \(> 1\), then the equation \(p^n + q^n = r^n\) has no solutions in prime numbers.

However, so far Fermat’s conjecture has not been proved, viz. that, if \(p\) is an odd prime number, the equation \(x^p + y^p = z^p\) has no solutions in natural numbers \(x, y, z\). This has been proved for odd prime numbers \(p < 4002\) (see Selfridge, Nicol and Vanlinder [1]).

28. Magic squares formed from prime numbers

A magic square with \(n\) rows is a table formed of \(n^2\) different natural numbers written in \(n\) rows (and as many columns) such that the sum of the numbers of each row, the sum of the numbers in each column, and the sum of the numbers in each of the two principle diagonals are equal. We know magic squares with three or four rows formed only from prime numbers.

These are the squares:

\[
\begin{array}{ccc}
569 & 59 & 449 \\
239 & 359 & 479 \\
269 & 659 & 149 \\
\end{array}
\]

\[
\begin{array}{cccc}
17 & 317 & 397 & 67 \\
307 & 157 & 107 & 227 \\
127 & 277 & 257 & 137 \\
347 & 47 & 37 & 367 \\
\end{array}
\]
In the first of these squares the sums of which we spoke are all equal to 1077 and in the second they are equal to 798.

In the October 1961 issue of the *Recreational Mathematics Magazine* (p. 28) there is given a magic square formed from 169 different primes.

The conjecture has been advanced that for every natural number \( n \geq 3e \) there exist infinitely many magic squares formed from \( n^2 \) distinct primes.

29. Hypothesis of A. Schinzel

We say that a polynomial in the variable \( x \) with integral coefficients is *irreducible* if it is not the product of two polynomials (of lesser degree) with integral coefficients.

Regarding the polynomial \( f(x) \) in the variable \( x \) with integral coefficients, the question arises whether such a polynomial for all natural values of \( x \) gives infinitely many prime numbers.

It is easy to show that a necessary condition for this is that the polynomial be irreducible. This property, however, is not sufficient, for, as is easy to see, the polynomial \( x^2 + x + 2 \) is irreducible and does not give a prime number for any natural numbers \( x \), because for every natural number \( x \) its value is an even number > 2.

It is also easy to prove that in addition to irreducibility, the polynomial \( f(x) \) must also have the following property:

*There is no natural number > 1 which is a divisor of the number \( f(x) \) for each integral value of \( x \).*

Are these properties sufficient for the polynomial \( f(x) \) with integral coefficients, where the coefficient of the highest power of \( x \) is positive, to give infinitely many primes for natural \( x \)?

In the last century W. Buniakowski advanced the conjecture that this is so. From this conjecture it follows immediately that there exist infinitely many prime numbers of the form \( x^2 + 1 \), where \( x \) is a natural number.

From the aforementioned conjecture it follows that there exist infinitely many natural numbers \( x \) for which \( x^2 \mid x + 41 \) is a prime number.
A. Schinzel has advanced (see Schinzel and Sierpiński [2]) the following more general hypothesis H.

**H. If s is a natural number and \( f_1(x), f_2(x), \ldots, f_s(x) \) are polynomials with integral coefficients, having positive coefficients for the highest power of \( x \), irreducible and satisfying the following property S:**

**S. There is no natural number \( > 1 \) which is a divisor of the product \( f_1(x) f_2(x) \ldots f_s(x) \) for every integral value of \( x \), then there exist infinitely many natural numbers \( x \) for which each of the numbers \( f_1(x), f_2(x), \ldots, f_s(x) \) is prime.**

In particular, let \( s = 2, f_1(x) = x, f_2(x) = x+2k \), where \( 2k \) is a given even number. We have

\[
f_1(1)f_2(1) = 1 - 2k \quad \text{and} \quad f_1(-1)f_2(-1) = 1-2k.
\]

If there were a natural number \( d > 1 \) such that \( d|f_1(x)f_2(x) \) for every integer \( x \), then we would have \( d|2k-1 \) and \( d|2k+1 \), which is impossible because, as we know, two successive odd numbers \( 2k-1 \) and \( 2k+1 \) have no common factor greater than unity. Property S is thus satisfied, and from the hypothesis H it follows that there exist infinitely many natural numbers \( x \) such that the numbers \( f_1(x) \) and \( f_2(x) \) are prime; hence \( x = p, x+2k = q \), where \( p \) and \( q \) are prime numbers, whence \( 2k = q-p \). From the hypothesis it then follows that every even natural number can be written in an infinity of ways as the difference of two primes. In particular, for \( k = 1 \) it follows that there exist infinitely many pairs of twin primes.

Many other theorems on prime numbers (which have not been proved so far) can be deduced from the hypothesis H of A. Schinzel.
Often in mathematics there arise in a natural way simple questions the answer to which is difficult or even yet unknown. We have many such questions in arithmetic.

The unsolved problems of arithmetic can be classified into two kinds. The problems of the first kind are problems for which we know how to obtain the complete solution, and the only difficulty is that we are not in a position to perform all the necessary computations, because of their length, even with the assistance of the biggest calculating machines that exist at present. This difficulty is therefore purely technical. All other unsolved problems are classified as problems of the second kind. As regards each of these problems, no method is known that could lead to a solution, even after extremely long and most tiresome calculations that possibly exceed our capabilities of today.

For example, a problem of the first kind is to find all the natural divisors of \(2^{101} - 1\). To obtain them it is sufficient to divide our number successively by the numbers 1, 2, 3, ..., up to \(2^{101} - 1\) and to ascertain which of them divide our number without remainder. However, this would require computations exceeding our present powers. We obviously know two natural divisors of our number: 1 and \(2^{101} - 1\). It is curious that, leaving aside the problem of proving that there exist other divisors of our number (this in itself would not be easy), we do not even now know any of them.

It is worth noting that for the number greater than ours by 1, the number \(2^{101}\), we know all the natural divisors; there are 102 of them, namely the first 102 terms of the geometric progression (with common ratio 2) 1, 2, 4, 8, 16, ..., \(2^{100}\), \(2^{101}\). Thus an in-
quiry into a neighbouring number may present quite a different degree of difficulty.

Another example of a problem of the first kind is finding a decomposition of the number 10 into the sum of a finite number of distinct rational numbers with numerator 1. The method of finding such a decomposition is known for every given rational number. But it is proved that in each decomposition of the number 10 into the sum of a finite number of different fractions of the form $\frac{1}{n}$ (where $n$ is a natural number) the number of components is $> 12,366$, so that it is not practically possible to obtain such a decomposition (see Lyness [1]).

A problem of the second kind is the question whether the equation $x^3 + y^3 + z^3 = 3$ has integral solutions $x, y, z$ other than the four known solutions:

$$x = y = z = 1; \quad x = 4, \quad y = 4, \quad z = -5;$$

$$x = 4, \quad y = -5, \quad z = 4; \quad x = -5, \quad y = 4, \quad z = 4.$$  

It has happened that a problem which was at one time of the second kind is later solved. For example, in the year 1845, J. Bertrand made the conjecture that, if $n$ is a natural number $> 1$, then between $n$ and $2n$ there is at least one prime number. At that time the question whether the conjecture is correct was a problem of the second kind. But five years later, Chebyshev proved that the conjecture (known by the name of Bertrand's postulate) is correct. The proof of Chebyshev was not elementary. An elementary proof was obtained after the year 1930 (see, e.g. Sierpiński [7], p. 395-400).

In the days of P. Fermat (1601–1655) it was a problem of the second kind whether the conjecture of Fermat is true: that for the every natural number $n$ the number $F_n = 2^{2^n} + 1$ (known as the $n$th Fermat number) is prime (i.e., has no other natural divisor except 1 and itself). Then in 1732 L. Euler proved that the conjecture of Fermat is false since the number

$$F_n = 2^{2^5} + 1 + 2^{32} + 1 = 4,294,967,297$$

is not prime, being divisible by 641.
In this case the disproving of Fermat's conjecture was not, strictly speaking, difficult. Fermat knew that the numbers $F_n$ are prime for $n < 5$. The number $F_5$ has ten digits in the decimal scale. One cannot help wondering why Fermat, while stating his conjecture, did not try to divide the number $F_5$ by successive primes less than a thousand: if he had done so (which in the days of Fermat when there were no calculating machines, would be burdensome but practicable), it would have established the fact that the number $F_5$ is composite.

At present the question whether or not $F_{17}$ is prime is a problem of the first kind (because it would be sufficient to divide $F_{17}$ by successive prime numbers less than this number in order to ascertain if it is prime or not) but in a few years' time with the help of electronic computers, it may be settled. To prove that the above numbers $F_n$ are not prime is not easy.

In view of the fact that we know only a few Fermat numbers $F_n$ which are prime, and only those which are the smallest, while knowing as many as 38 composite numbers, it has been lately conjectured that all numbers $F_n$ for $n \geq 5$ are composite. This conjecture is now a problem of the second kind.

A problem of the second kind has been, until recently, the question whether there exist natural numbers $n > 1$ for which the number $n \cdot 2^n + 1$ (known as Cullen's number) is prime. It was only a short time ago that such smallest prime number for $n = 141$ was discovered.

After the rejection of Fermat's conjecture about the numbers $F_n$ the following two questions suggest themselves:

(i) Do there exist infinitely many prime numbers among the numbers $F_n (n = 1, 2, \ldots)$?

(ii) Are there infinitely many composite numbers among the numbers $F_n (n = 1, 2, \ldots)$?

Each of these questions is nowadays a problem of the second kind. Even for a long time it would have remained a problem of the second kind whether all numbers of the sequence

$$2 + 1, \ 2^2 + 1, \ 2^{2^2} + 1, \ 2^{2^{2^2}} + 1, \ldots$$
are prime. In 1953 (cf. Selfridge [1]), with the help of an electronic computer, proved that the answer to this question is negative, namely it was shown that the fifth term of this sequence, the number $F_{16} = 2^{216}+1$ having 19,729 digits, is composite; the smallest prime factor of this number was obtained: it is $2^{18}.3150+1$. Thus several difficult problems of arithmetic, posed long ago, have been solved during recent years.

It also happens that problems of the second kind later become problems of the first kind. This was the case, for example, with the question whether every odd number $> 7$ is the sum of three odd prime numbers. For some time it was a problem of the second kind until I. Vinogradov proved that every sufficiently large odd number is the sum of three odd prime numbers. Later it was proved that every odd integer $> a = 3^{315}$ is the sum of three odd primes.

Consequently the question whether every odd number $> 7$ is the sum of three odd prime numbers is today a problem of the first kind, because it would be enough to find out whether every number $> 7$ and $\leq a$ is the sum of three odd prime numbers (and to obtain for every natural number its decomposition into the sum of three odd prime numbers or to confirm that such a decomposition does not exist is, as is easy to see, a problem of the first kind or a solvable problem).

We give below a series of problems of the first and the second kind. Problems of the first kind will be denoted by $P_k^1$ (where $k = 1, 2, \ldots$), those of the second kind by $P_k^2$ and problems for which answers are known by $P_k^3$.

$P_1^2$. **Do there exist infinitely many prime numbers among the numbers** $2^n-1$, **where $n$ is a natural number?**

So far we know 20 prime numbers of this form, of which the greatest is $2^{4423}-1$ (see Hurwitz and Selfridge [1]). This is the greatest prime number yet known.

$P_2^2$. **Do there exist infinitely many prime numbers $p$ for which** $2^p-1$ **is composite?**

$P_3$. **If** $2^n-1$ **is a prime number, is** $2^{2^n-1}-1$ **prime?**

This problem had been for a long time of the second kind. It was only in 1953 that D. J. Wheeler proved (by means of an
electronic computer) the number \( m = 2^{213-1} - 1 \) (having 2466 digits) to be composite, the number \( 2^{13} - 1 \) being prime (Robinson [2]). However, we still do not know any divisor of \( m \) other than 1 and \( m \). Yet in 1957 it was shown that the numbers \( 2^{217-1} - 1 \) and \( 2^{19-1} - 1 \) are composite while \( 2^{17} - 1 \) and \( 2^{19} - 1 \) are prime and that \( 2^{217-1} - 1 \) is divisible by \( 1768.(2^{17} - 1)+1 \) and \( 2^{219-1} - 1 \) is divisible by \( 120.(2^{19} - 1)+1 \).

**P4.** Do there exist infinitely many prime numbers of the form \( 2^m + 2^n - 1 \) where \( m \) and \( n \) are natural numbers?

If the answer to the problem P4 were negative, then the answer to problem P2 would also be negative (because \( 2^{m+1} - 1 = 2^m + 2^m - 1 \)) and the number of prime Fermat numbers would also then be finite (as \( 2^m + 1 = 2^m + 2 - 1 \)).

**P5.** Is it true that, if \( 2^n - 1 \) is prime, then \( 2^n - 1 + 100 \) is a prime number?

For several years nothing was done to decide this. It was only in 1957 that J. L. Selfridge showed that it is not true, for the number \( 2^{31} - 1 \) is prime but the number \( 2^{31} + 99 \) is divisible by 1933.

**P6.** Do there exist infinitely many prime numbers of the form \( 2^m + 3^n - 1 \) where \( m \) and \( n \) are positive integers?

If the number of Fermat primes were infinite, the answer to problem P6 would of course be affirmative. T. Kulikowski has listed some scores of prime numbers of the form \( 2^m + 3^n + 1 \); the greatest of the numbers listed by him is \( 3.2^{534} + 1 \), having 162 digits.

**P7.** Does there exist, besides 2 = 1 + 1, 5 = 2^2 + 1, 257 = 4^4 + 1, a prime number of the form \( n^n + 1 \) where \( n \) is a natural number?

**P8.** Does there exist, besides 2 and 17, a prime number of the form \( n^n + 1 \) where \( n \) is a natural number?

**P9.** Does there exist a prime number \( p \) such that the number \( 2^p - 1 \) has factors which are squares of natural numbers > 1?

**P10.** Do there exist infinitely many natural numbers \( n \) for which the number \( 2^n - 1 \) is not divisible by any square of a natural number > 1?

This question was put by A. Schinzel. If the answer to this question were negative, then the answer to P10 would be positive.
P_{11}. Do there exist infinitely many prime numbers whose digits (in the decimal scale) are all unities?

P_{12}. Do there exist infinitely many prime numbers of the form \( x^2 + 1 \) where \( x \) is a natural number?

However, it has been proved that there exist infinitely many natural numbers \( x \) for which \( x^2 + 1 \) is the product of not more that three different prime numbers. The proof of this is difficult.

P_{13}. Do there exist infinitely many prime numbers of the form \( x^2 + y^2 + 1 \) where \( x \) and \( y \) are natural numbers?

This problem had been for a long time of the second kind. It was solved recently by Bredihin [1].

P_{14}. Do there exist infinitely many prime numbers of the form \( x^2 + y^2 + z^2 + 1 \) where \( x, y \) and \( z \) are natural numbers?

The answer to this question is in the affirmative, but the proof is difficult. However, it is easier to prove that there exist infinitely many prime numbers of the form \( x^2 + y^2 \) where \( x \) and \( y \) are natural numbers.

We know prime numbers of the form \( x^4 + 1 \), where \( x \) is a natural number, for example \( 17 = 2^4 + 1, 257 = 4^4 + 1 \), but we do not know if they are infinitely many.

P_{15}. Do there exist infinitely many prime numbers among the numbers \( n! + 1 \) where \( n \) is a natural number?

P_{16}. Does there exist an even number \( > 2 \) which is not the sum of two prime numbers?

The conjecture that the answer to this question is in the negative was made by Ch. Goldbach in 1742. The slightly stronger conjecture has been made that every even number \( > 6 \) is the sum of two different prime numbers. It is true for even positive integers \( \leq 100,000 \) (Pipping [1], [2]).

P_{17}. Does there exist an even number which is not the difference of two prime numbers?

In connection with the question \( P_{17} \), it has been conjectured that the answer to the question \( P_{18} \) is in the affirmative.

P_{18}. Can every even number be represented in infinitely many ways as the difference of two prime numbers?
As regards questions \( P_{16} \) and \( P_{17} \), we further observe that for every given natural number \( n \) we are able (disregarding the length of the necessary calculations) to decide whether or not it is the sum of two prime numbers, but we do not know any suitable method to decide the question whether or not any given number is the difference of two prime numbers. For odd numbers we are able to investigate, although for some odd numbers it is still a problem of the first kind, for example for the number \( 2^{217} - 1 \).

Two prime numbers whose difference is 2 are called twin prime numbers.

If the answer to question \( P_{18} \) were positive, then so also would be the answer to the question:

\( P_{19} \). Do there exist infinitely many twin primes?

There are more than 8000 such pairs of numbers smaller than one million; the greatest known pair of such prime numbers are \( p \) and \( p+2 \), for \( p = 1,000,000,009,649 \).

\( P_{20} \). Do there exist, for every natural number \( m \), only a finite number of prime number pairs \( p \) and \( q > p \) such that \( q - p < m \)?

If the answer to problem \( P_{19} \) were in the affirmative, then the answer to the problem \( P_{20} \) would be in the negative (even for \( m = 3 \)).

\( P_{21} \). Do there exist arbitrarily long arithmetic progressions formed of different prime numbers?

We do not know if there exists an arithmetic progression formed from one hundred different prime numbers. It has been proved that if such an arithmetic progression exists, then the number of digits in each term (except perhaps the first) must be more than ten.

\( P_{22} \). Do there exist infinitely many arithmetic progressions formed of three prime numbers?

It has been proved that the answer to this problem is in the affirmative, but the proof is difficult (see van der Corput [1]). Examples of such progressions are 3, 5, 7 and 11, 17, 23 and also 47, 53, 59. In the last progression we have three successive prime numbers (i.e. such that between any two there lies no prime number).

The following question arises:
P23. Do there exist infinitely many arithmetic progressions formed of three successive prime numbers?

We also know arithmetic progressions having four successive prime numbers, for example:

251, 257, 263, 269 or 1741, 1747, 1753, 1759.

According to the conjecture of A. Schinzel (see Schinzel and Sierpiński [2]), there exist arbitrarily long arithmetic progressions formed of successive prime numbers. So far we do not know any arithmetic progressions formed of five successive prime numbers and we do not know if such a progression exists.

It is easy to prove that there exist infinitely many arithmetic progressions consisting of three different squares of natural numbers, which follows immediately from the identity.

$$(n^2 - 2n - 1)^2 + (n^2 + 2n - 1)^2 = 2(n^2 + 1)^2.$$ 

The following question arises:

P24. Do there exist infinitely many arithmetic progressions formed of three different squares of prime numbers?

We know such progressions, for example 7², 13², 17² or 7², 17², 23². Several hundred years ago the following question was put:

P25. Do there exist arithmetic progressions formed of four different squares of natural numbers?

Fermat proved that such a progression does not exist, but the proof is difficult. It is also difficult to prove that the answers to the following questions are negative:

P26. Do there exist arithmetic progressions formed of three different cubes of natural numbers? (Cf. A. Wakulicz [1]).

P27. Do there exist arithmetic progressions formed of three different fourth powers of natural numbers?

As early as the first half of the nineteenth century the question was raised about those arithmetic progressions of integers which contain infinitely many prime numbers.

P28. Does every progression $a + kr$ ($k = 0, 1, 2, \ldots$) where $a$ and $r$ are relatively prime contain infinitely many prime numbers?
In 1837 Dirichlet proved that the answer to the problem is in the affirmative, but its proof was not elementary. It is true that during the last ten years an elementary proof was obtained, but it was long and complicated.

\( P_29. \) Is the following conjecture of Schinzel true: if \( a \) and \( r \) are relatively prime natural numbers, \( a < r \), then there exist an integer \( k \) such that \( 0 \leq k < r \) and \( a + kr \) is a prime number?

\( P_{30}. \) Find a prime number having five hundred digits.

\( P_{31}. \) Does there always lie at least one prime number between \( n^2 \) and \( (n+1)^2 \) for every natural number \( n \)?

\( P_{32}. \) Does there always lie at least one prime number between \( n^2 \) and \( n^2 + n \) for each natural number \( n > 1 \)?

Obviously if the answer to the problem \( P_{32} \) were in the affirmative, then the answer to \( P_{31} \) would also be in the affirmative.

\( P_{33}. \) If, for a natural number \( n > 1 \), the numbers \( 1, 2, 3, \ldots, n^2 \) are written successively in \( n \) rows with \( n \) numbers in each row:

\[
\begin{array}{cccc}
1, & 2, & 3, & \ldots, n \\
2n+1, & 2n+2, & 2n+3, & \ldots, 3n \\
2n+1, & 2n+2, & 2n+3, & \ldots, 3n \\
\vdots \\
n^2-n+1, & n^2-n+2, & n^2-n+3, & \ldots, (n-1)n \\
n^2-n+1, & n^2-n+2, & n^2-n+3, & \ldots, n^2,
\end{array}
\]

will each row contain at least one prime number?

This is how our table looks for \( n = 5 \) for example (the prime numbers being underlined):

\[
\begin{array}{ccccccc}
1, & 2, & 3, & 4, & 5 \\
6, & 7, & 8, & 9, & 10 \\
11, & 12, & 13, & 14, & 15 \\
16, & 17, & 18, & 19, & 20 \\
21, & 22, & 23, & 24, & 25
\end{array}
\]
A. Schinzel has proved that the answer to the question \( P_{33} \) is in the affirmative for \( 1 < n \leq 4500 \).

It can easily be proved that an affirmative answer to problem \( P_{32} \) would follow from an affirmative answer to problem \( P_{33} \).

\( \textbf{P}_{34} \). Can every rational number be put in the form

\[
\frac{(p+1)}{(q+1)},
\]

where \( p \) and \( q \) are prime numbers?

\( \textbf{P}_{35} \). Can every rational number be put in the form

\[
\frac{(p-1)}{(q-1)},
\]

where \( p \) and \( q \) are prime numbers?

The conjecture has been put forward that every rational number can be written in infinitely many ways in the form \( \frac{(p+1)}{(q+1)} \) and also in the form \( \frac{(p-1)}{(q-1)} \), where \( p \) and \( q \) are prime numbers. We do not know how to prove it even for number 2. The theorem stating that 2 can be put in the form \( \frac{(p+1)}{(q+1)} \) (\( p, q \) prime) in an infinity of ways is obviously equivalent to the theorem stating that the equation \( p-2q = 1 \) has infinitely many solutions in prime numbers \( p \) and \( q \). Thus, for certain very simple equations of the first degree in two unknowns, not only do we not know how to obtain all solutions in prime numbers, but also how to answer the question whether there are infinitely many such solutions.

It is easy to prove that the question whether the equation \( p+q = r \) has infinitely many solutions in prime numbers, \( p, q \) and \( r \) is equivalent to problem \( P_{19} \). But the question whether the equation \( p+q = 2r \) has infinitely many solutions in different prime numbers \( p, q, r \) is equivalent to the (solved) problem \( P_{22} \).

In some cases it is easy to obtain all solutions in prime numbers of an equation of the second degree in two unknowns; for example it is easy to prove that the equation \( p^2-2q^2 = 1 \) has only one solution in prime numbers: \( p = 3 \) and \( q = 2 \).

However, we do not know whether the equation \( p^2-2q^2 = -1 \) has infinitely many solutions in prime numbers \( p \) and \( q \). Such solutions, for example, are \( p = 7, q = 5 \) and \( p = 41, q = 29 \).
It is also easy to prove that the equation \( p^2 + q^2 = r^2 \) has no solutions in prime numbers \( p, q, r \), but to prove (as has been done by P. Erdös) that the equation \( p^2 + q^2 = r^2 + s^2 \) has infinitely many solutions in different prime numbers \( p, q, r, s \) is difficult.

That the equation \( p + q + r = s \) has infinitely many solutions in prime numbers \( p, q, r, s \) follows from the theorem of Vinogradov.

\[ P_{36}. \text{Do there exist infinitely many natural numbers } n \text{ for which each of the numbers } n \text{ and } n+1 \text{ have only one prime divisor?} \]

We know only twenty-six such numbers so far. The smaller of them are \( n = 2, 3, 4, 7, 8, 16, 31, 127, 256 \), the largest known: \( n = 2^{4423} - 1 \). We can prove that of any three successive natural numbers greater than seven at least one has more than one prime divisor.

\[ P_{37}. \text{Do there exist infinitely many natural numbers } n \text{ such that each of the numbers } n, n+1, n+2 \text{ is the product of two different prime numbers?} \]

As is easy to verify, such numbers are, for example, the numbers \( n = 33, 93, 141 \).

\[ P_{38}. \text{Do there exist infinitely many natural numbers } n \text{ such that the number } n \text{ and } n+1 \text{ have the same number of natural divisors?} \]

If the answer to question \( P_{37} \) were in the affirmative, then the answer to question \( P_{38} \) would also be in the affirmative.

It has been conjectured that there exist arbitrarily long sequences of successive natural numbers having the same number of natural divisors. If this conjecture were correct, then the answer to question \( P_{38} \) would be in the affirmative.

A sequence of four successive natural numbers having the same number of natural divisors (namely six) is exemplified by the sequence with first term 241; a sequence of five successive natural numbers having the same number of natural divisors (namely eight) is exemplified by the sequence with first term 40,311.

\[ P_{39}. \text{Do there exist infinitely many prime numbers of the form } x^3 + y^3 + z^3 \text{ where } x, y, z \text{ are integers?} \]

G. H. Hardy and J. E. Littlewood conjectured in [1] that there exist infinitely many prime numbers which are sums of three cubes of natural numbers. We can prove that there exist infinitely
many prime numbers of the form $x^3+y^3+z^3+t^3$ where $x$, $y$, $z$ and $t$ are integers.

The proof follows immediately from the theorem of Dirichlet of which we have spoken above, and the identity

$$18k+1 = (2k+14)^3 + (3k+30)^3 - (2k+23)^3 - (3k+26)^3.$$  

$P_{40}$. Do there exist infinitely many prime numbers $p$ such that for all natural numbers $n < p-1$, the number $2^n$ when divided by $p$ leaves a remainder other than 1?

Such numbers are, for example, $p = 3, 5, 11, 13, 19, 29, 37, 53, 59, 61, 67, 83, 101, 107, 131, 139, 149$.

$P_{41}$. Do there exist infinitely many composite numbers $n$ which are simultaneously divisors of the numbers $2^n-2$ and $3^n-3$?

$P_{42}$. Do there exist infinitely many composite numbers $n$ which are divisors of the numbers $a^n-a$ for every integer $a$?

Such numbers are Carmichael numbers; the smallest of them is 561. If the answer to problem $P_{42}$ were in the affirmative, then so would be the answer to problem $P_{41}$.

$P_{43}$. Do there exist infinitely many natural numbers $n$ for which $2^n-2$ is divisible by $n^2$?

Such (prime) numbers $n$ exist, for example 1093 and 3511, but we do not know any composite number $n$ of this kind.

$P_{44}$. Is every natural number the sum of eight or fewer squares of prime numbers (including 1 as a prime number)?

$P_{45}$. Does there exist an odd number $n$ such that the sum of all its natural divisors is equal to $2n$?

Natural numbers $n$ the sum of whose divisors is equal to $2n$ are called perfect numbers.

So far we know 20 perfect numbers, all of them even, namely the numbers $2^{n-1}M_n$, where $M_n = 2^n-1$ is a prime number. We do not know if there exists an odd perfect number — "Perfect numbers like perfect men are very rare" — said Descartes.

A stronger conjecture than the above has been made, namely the conjecture that there is no odd number whose product by the number of its divisors is divisible by the sum of
its divisors. This conjecture has been verified for numbers \( n < 10^{20} \) (H. J. Kanold [1]).

\[ P_{46}. \] Do there exist natural numbers \( n \) for which the sum of all their natural divisors is \( 2n+1 \)?

Such a natural number would be equal to the sum of all its non-trivial natural divisors other than 1 and \( n \).

However, it is easy to prove that there exist infinitely many natural numbers \( n \) for which the sum of all their natural divisors is \( 2n-1 \); such numbers are all powers (with the natural exponent) of 2. We do not know if there are other such numbers.

\[ P_{47}. \] Do there exist infinitely many natural numbers \( n \) such that the numbers \( n \) and \( n+1 \) have the same sum of natural divisors?

We know such numbers, e.g. 14, 206, 957, 1334, 1634, 1634, 2685, 2974 and 4364.

Natural numbers \( m \) and \( n \neq m \) are called amicable if the sum of the divisors of each is \( m+n \).

\[ P_{48}. \] Do there exist infinitely many pairs of amicable numbers?

We know many pairs of amicable numbers; the smallest such pair is 220 and 284, both numbers are even. We also know a pair of odd amicable numbers; for example, \( 3^3 \cdot 5 \cdot 7 \cdot 13 \) and \( 3 \cdot 5 \cdot 7 \cdot 139 \).

\[ P_{49}. \] Does there exist a pair of amicable numbers one of which is even and the other odd?

We are not yet able to answer the question whether there exist pairs of amicable numbers having no common factor greater than 1. It has been shown that if \( m \) and \( n \) are such a pair, then each of them must be greater than \( 10^{23} \) and the number \( mn \) must have more than 20 prime divisors.

\[ P_{50}. \] Is every sufficiently large natural number which is not the square of a natural number, the sum of a prime number and a square of integer?

The conjecture that the answer to this question is in the affirmative was made by G. H. Hardy and J. E. Littlewood [1].

\[ P_{51}. \] Is every sufficiently large natural number the sum of a prime number and two squares of integers?

This problem was recently answered affirmatively by Yu. V. Linnik [1].
It has been shown that every sufficiently large natural number is the sum of two prime numbers and the square of an integer, but the proof of this is difficult.

P\textsuperscript{2}\textsubscript{52}. Does there exist a composite number \( n \) which is a divisor of the number

\[1^{n-1} + 2^{n-1} + 3^{n-1} + \ldots + (n-1)^{n-1} + 1?\]

It is easy to prove that if \( p \) is a prime number, then

\[1^{p-1} + 2^{p-1} + \ldots + (p-1)^{p-1} + 1\]

is divisible by \( p \).

P\textsuperscript{2}\textsubscript{53}. Does there exist a natural number \( n > 7 \) for which the number \( n! + 1 \) is the square of a natural number?

Such numbers \( n \leq 7 \) exist: they are 4, 5, and 7. M. Kraitchik in his book [1], vol. I, pp. 38–41 proved that if \( n! + 1 \) is a perfect square and \( n > 7 \) then \( n > 1020 \).

P\textsuperscript{2}\textsuperscript{54}. If \( \pi(x) \) denotes the number of all prime numbers \( x \), then does the inequality \( \pi(x+y) \leq \pi(x)+\pi(y) \) hold for every \( x > 1, y > 1 \)?

A. Schinzel has proved that the answer to this question is in the affirmative if \( \min(x, y) \leq 146 \) and S. L. Segal has verified the inequality for \( x, y \leq 101,081 \).

P\textsuperscript{2}\textsubscript{55}. We denote by \( \pi_1(x) \) the number of all prime numbers \( \leq x \) which when divided by 4 leave the remainder 1, and by \( \pi_3(x) \) the number of all those prime numbers \( \leq x \) which when divided by 4 leave the remainder 3. Find natural number \( x \) such that \( \pi_3(x) < \pi_1(x) \).

It was only in 1957 that the smallest such number \( x = 26,861 \) was discovered by J. Leech [1]. For this number we have \( \pi_1(x) = 1473, \pi_3(x) = 1472 \). But as early as 1914 Littlewood proved that there are infinitely many such natural numbers, and that there are also infinitely many natural numbers \( x \) for which \( \pi_3(x) > \pi_1(x) \). Thus it was known for over forty years that there exist natural numbers having a certain property but none of them was found. We also have, for \( x = 623,681, \pi_1(x) - \pi_3(x) = 8 \).

Numerous straightforward but difficult problems are met with in finding solutions of equations in integers.
Difficulties may appear even in the solution, in terms of integers, of equations of the second degree in two unknowns (which, moreover, are linear with respect to each of the unknowns). For example, the problem of finding all the integral solutions of the equation \( xy + 1 = 2^{101} \) is a problem of the first kind.

It would be difficult also to discover natural numbers \( x \) and \( y \) for which the sum \( x + y \) is the square of a natural number but the sum of the squares \( x^2 + y^2 \) is the fourth power of a natural number. Fermat found such a number \( x = 1,061,652,393,520, \ y = 4,565,486,027,761, \) and declared that there are no smaller numbers, which was proved later.

P56. Obtain all solutions of the equation \( x^3 - y^2 = 18 \) in integers.

It has been proved that such solutions are finite in number, but we do not know how many there are.

P57. Does the equation \( x^2 - y^3 = 1 \) have other solutions in positive integers except \( x = 3, \ y = 2? \)

It has been proved that the answer to question P57 is in the negative, but the proof is not easy.

P58. Does the system of four equations of the second degree in seven unknowns

\[
x_1^2 + x_2^2 = x_4^2, \quad x_1^2 + x_3^2 = x_5^2, \quad x_2^2 + x_3^2 = x_6^2, \quad x_1^2 + x_2^2 + x_3^2 = x_7^2
\]

have a solution in natural numbers \( x_1, x_2, \ldots, x_7? \)

The geometrical meaning of this question will be found on p. 24.

However, we are able to prove that the first three of our equations have infinitely many solutions in natural numbers. The solution \( x_1 = 117, \ x_2 = 44, \ x_3 = 240, \ x_4 = 125, \ x_5 = 267, \ x_6 = 244 \) was known at the beginning of the eighteenth century.

P59. Do there exist integers \( x, y, \ z \) other than zero satisfying the equation

\[ x^3 + y^3 + z^3 = xyz? \]

We can prove that question P59 is equivalent to each of the following two questions, proposed by W. Mnich:

\[
\text{P56.} \quad \text{Obtain all solutions of the equation } x^3 - y^2 = 18 \text{ in integers.}
\]

\[
\text{P57.} \quad \text{Does the equation } x^2 - y^3 = 1 \text{ have other solutions in positive integers except } x = 3, y = 2?.
\]

\[
\text{P58.} \quad \text{Does the system of four equations of the second degree in seven unknowns}
\]

\[
x_1^2 + x_2^2 = x_4^2, \quad x_1^2 + x_3^2 = x_5^2, \quad x_2^2 + x_3^2 = x_6^2, \quad x_1^2 + x_2^2 + x_3^2 = x_7^2
\]

\[
\text{have a solution in natural numbers } x_1, x_2, \ldots, x_7?
\]

\[
\text{P59.} \quad \text{Do there exist integers } x, y, z \text{ other than zero satisfying the equation}
\]

\[ x^3 + y^3 + z^3 = xyz? \]
P₆₀. Do there exist three rational numbers whose sum is equal to 1 and whose product is equal to 1?

P₆₁. Do there exist integers x, y, z satisfying the equation

\[ \frac{x}{y} + \frac{y}{z} + \frac{z}{x} = 1? \]

These problems were solved negatively by J. W. S. Cassels in 1960. For a more elementary proof, see Sansone and Cassels [1].

It is easy to prove that for each natural number s > 1 the equation \( x_1 + x_2 + x_3 + \ldots + x_s = x_1 x_2 \ldots x_s \) has at least one solution \( x_1, x_2, \ldots, x_s \) in natural numbers (for proving this it is enough to put \( x_1 = x_2 = \ldots = x_{s-2} = 1, \ x_{s-1} = 2, \ x_s = s \). We do not know, however, if, for all sufficiently large values of s, the number of solutions of the equation is arbitrarily large.

P. Erdős has made the conjecture that its truth would answer the question:

P₆₂. Do there exist for every natural number \( n > 1 \), natural numbers x, y, z such that

\[ \frac{4}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}? \]

R. Obláth and S. A. Rosati have proved that the conjecture of Erdős is true for all natural numbers \( n > 1 \), and < 141,648.

P₆₃. Do there exist, for every natural \( n > 1 \), natural numbers x, y, z such that

\[ \frac{5}{n} = \frac{1}{x} + \frac{1}{y} + \frac{1}{z}? \]

G. Palamà proved in [1] that the answer to the question is in the affirmative for all natural numbers \( n > 1 \) and \( \leq 922,321 \).

P₆₄. Does the equation \( x^3 + y^3 = 2z^3 \) have integral solutions x, y, z where \( x \neq z \), and \( z \neq 0 \) (cf. P₂₆)?

P₆₅. Does there exist a natural number n other than 1 and 24 for which \( 1^2 + 2^2 + \ldots + n^2 \) is the square of a natural number?
It has been shown that the answer to problems $P_{64}$ and $P_{65}$ is negative, but the proof is difficult.

It would also be difficult to answer the question:

$P_{66}$. How many integral solutions $x, y$ does the equation $2x^4 - y^2 = 1$ have?

W. Ljunggren proved in [1] that this equation has only two solutions in positive integers $x, y$:

$$x = y = 1 \quad \text{and} \quad x = 13, \quad y = 239.$$

$P_{67}$. Is the conjecture of Euler correct, namely that there are no natural numbers $x, y, z, t$ such that

$$x^4 + y^4 + z^4 = t^4?$$

Euler stated even the more general conjecture that the equation $x_1^n + x_2^n + \ldots + x_r^n = y^n$ has no solution in positive integers $x_1, x_2, \ldots, x_r, y$ for $1 < s < n$.

$P_{68}$. Is each natural number the sum of four cubes of integers?

The author has voiced the conjecture that for every integer there are infinitely many ways of breaking it into $x^3 + y^3 - z^3 - t^3$ where $x, y, z$ and $t$ are natural numbers.

This conjecture is proved for all natural numbers $\leq 1000$ and for infinitely many others (for proof for numbers $\leq 350$ see Schinzel and Sierpiński [1] and Mąkowski [1]).

However, we are able to prove that there exist infinitely many natural numbers which are not sums of cubes of three integers (for example, all numbers which when divided by 9 leave the remainder 4 or 5) and that every integer is, in an infinity of ways, the sum of five cubes of integers. The proof of the last theorem is easy; it follows immediately from the observation that each integer divisible by 6 is the sum of four cubes of integers, because for integral $k$ we have the identity:

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

and from the fact that for integral $t$ and $n$ each of the numbers

$$6t - (6n)^3, \quad 6t + 1 - (6n+1)^3, \quad 6t + 2 - (6n+2)^3,$$

$$6t + 3 - (6n+3)^3, \quad 6t + 4 - (6n-2)^3, \quad 6t + 5 - (6n-1)^3$$

is divisible by 6.
P_69. Does the equation $x^3 + y^3 + z^3 - t^3 = 1$ have infinitely many integral solutions $x, y, z, t$?

We know such solution, for example $4^3 + 4^3 + 6^3 - 7^3 = 1$, $4^3 + 38^3 + 58^3 - 63^3 = 1$. J. A. Gabovitch proved in 1962 that this equation has infinitely many solutions in positive integers $x, y, z, t$. However, it is easy to prove that the equation $x^3 - y^3 - z^3 - t^3 = 1$ has infinitely many solutions in natural numbers $x, y, z, t$, which follows immediately from the identities:

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

P_70. Can every natural number be put in the form $x^3 + y^3 + 2z^3$ where $x, y, z$ are integers?

The smallest natural number about which we are undecided is the number 76; an other is 99. For other numerical results on this topic, see Chao Ko [1] and Mąkowski [1]. K. Moszyński and J. Swianiewicz have found that $113 = -133^3 - 46^3 + 2.107^3$.

P_71. Is every natural number which leaves a remainder other than 4 or 5 when divided by 9 the sum of three cubes of integers?

In particular, we do not know if the number 30 is the sum of three cubes of integers (see Miller and Woollett [1]).

The numbers 0, 1 and 2 are the sums of three cubes of integers in an infinity of ways, which follows immediately from the identities:

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

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

However, we do not know if the number 3 is the sum of three cubes of integers in an infinity of ways.

We do not know any number which leaves a remainder different from 4 or 5 when divided by 9 and for which we are able to prove that it has a finite number $\geq 0$ of decompositions into the sum of three cubes of integers.

P_72. Do there exist natural numbers $n > 2$ and $x, y, z$ for which $x^n + y^n = z^n$?
Fermat gave without proof the theorem stating that there are no such numbers. This theorem has been proved (see Selfridge, Nicol and Vandiver [1]) for all integers $n$ where $2 < n \leq 4002$ and for infinitely many others. Even the proof for $n = 3$ is every difficult. The proof for $n = 4$ is easier.

$P_7^2$. Does the equation $x^n + y^n = z^n + t^n$ have solutions in natural numbers $x, y, z, t$ where $x \neq z$ and $x \neq t$ for every natural number $n > 4$?

For $n < 5$ we know, for example, the following solutions:

$$1^2 + 8^2 = 4^2 + 7^2, \quad 1^3 + 12^3 = 9^3 + 10^3, \quad 133^4 + 134^4 = 59^4 + 158^4.$$

$P_7^3$. Do there exist natural numbers which can be expressed, in at least three different ways, as the sums of two fourth powers of integers? (If we disregard the order of components.)

$P_7^4$. Is every natural number the sum of nineteen fourth powers of integers?

Waring made the conjecture that the answer to this question is in the affirmative. F. C. Auluck [1] has proved, using the method of Hardy and Littlewood, that every integer $> 10^{1089}$ is the sum of nineteen biquadrates. It has been proved that every sufficiently large natural number is the sum of sixteen fourth powers of integers (Davenport [1]).

$P_7^5$. For every natural exponent $s$, does there exist a natural number $k$ such that every natural number $n$ is the sum of $k$ terms each of which is the $s$-th power of a non-negative integer?

The theorem that the answer to this question is affirmative was stated without proof by Waring in 1782, the discovery of the proof was regarded for a hundred years as very difficult; it was found in 1909 by D. Hilbert. However, his proof is difficult. An elementary proof is given in Khinchin [1].

$P_7^6$. Do there exist successive natural numbers (except $8 = 2^3$ and $9 = 3^2$) each of which is the power of a natural number with natural exponent $1$?

E. Catalan made the conjecture that there is no such number. For some results and other references see e.g. J. W. S. Cassels [1].
P78. For every natural number \( m \), is the number of all systems of natural numbers \( x, y, z, t \) greater than 1 satisfying the inequality \( 0 < x^y - z^t < m \) finite?

S. Pillai in [2] made a conjecture equivalent to an affirmative answer to question P78.

P79. Do there exist three successive natural numbers each of which is the power of a natural number with natural exponent > 1?

This problem was answered (negatively) by A. Mąkowski [2].

However, it is easy to prove that no four successive natural numbers exist, each of them a power of a natural number with exponent > 1. In fact, out of four successive natural numbers one always leaves the remainder 2 when divided by 4 and therefore cannot be the power of a natural number (an even one of course) with exponent > 1.

P80. Do there exist natural numbers \( m \) and \( n > 1 \) such that

\[ 1^n + 2^n + 3^n + \ldots + (m-1)^n = m^n? \]

P. Erdős made the conjecture that the answer to this question is negative. L. Moser proved in [2] that there are no such numbers \( m \) and \( n > 1 \) when \( m \leq 10^{10^6} \).

P81. For any given natural numbers \( k \) and \( l \), does there always exist a natural number \( n \) such that, if the set of numbers 1, 2, 3, ..., \( n \) is broken into \( k \) or fewer sets having no common elements, then at least one of these sets will contain an arithmetic progression with \( l \) different terms?

This question used to be regarded as very difficult. In 1928, van der Waerden proved that the answer to question P81 is in the affirmative. The proof, although elementary, was complicated. It may be found in Khinchin [1].

P82. Can we obtain a prime number from every natural number \( \geq 10 \) by changing two of its digits?

We observe that a prime number cannot be obtained from every natural number by changing one of its digits: we can show that 200 is the smallest natural number from which we cannot obtain a prime number by changing one digit.
Do there exist natural numbers $a > 41$ such that the numbers $x^2 + x + a$ are prime for $x = 0, 1, 2, \ldots, a-2$?

It has been proved (Lehmer [2]) that if such a number $a$ exists, then it is the only one and that it is $> 125 \cdot 10^7$.

We call numbers of the form $t_n = \frac{1}{2}n(n+1)$, where $n$ is a natural number, triangular numbers. For a long time we did not know how to answer the question:

Does there exist a triangular number other than 1 and 6 whose square is also a triangular number?

W. Ljunggren proved in 1946 that the answer to question $P_{84}$ is negative. The proof is difficult.

However, it is easy to prove that there exist infinitely many triangular numbers which are also squares of natural numbers. To prove this it is enough to show that such numbers exist (for example $1 = 1.2/2 = 1^2$) and that for each number with this property (i.e., that of being triangular and also a perfect square) we can obtain a greater number with this property. For this it is enough to verify the identity

$$(3x+4y+1)(3x+4y+2) - 2(2x+3y+1)^2 = x^2 + x - 2y^2,$$

from which it immediately follows that if the number $t_x = \frac{1}{2}x(x+1)$ is a square, $t_x = y^2$, then the number $t_{3x+4y+1}$ is also a square and is equal to $(2x+3y+1)^2$.

As $t_1 = 1$, we obtain from this that $t_6 = 6^2$, whence further $t_{49} = 35^2$, and next $t_{288} = 204^2$ and so on.

Does the equation $x^2 y^2 = z^2$ have solutions in odd numbers $x, y, z$ greater than 1?

It would be easy to obtain solutions of this equation in even integers. Such is, for example, the solution $x = 2^{12} \cdot 3^6, y = 2^8 \cdot 3^8, z = 2^{11} \cdot 3^7$. It has been proved that such solutions are infinitely many.

Chao Ko proved that, if the natural numbers $x, y, z > 1$ satisfy our equation, then the numbers $x$ and $y$ must have a common factor $> 1$, but A. Schinzel, in [3], proved that in each such solution, either each prime divisor of $x$ is a divisor of $y$ or each prime divisor of $y$ is a divisor of $x$, and proposed the question:
P_{86}. If \( x, \ y \) and \( z \) are natural numbers > 1 such that \( x^y = z \) then is it true that \( x \) and \( y \) must have the same prime factors?

P_{87}. Is the conjecture of R. D. Carmichael true, viz. that for each natural number \( m \) there exists a natural number \( n \) not equal to \( m \) such that the number of natural numbers not greater than \( m \) and relatively prime to \( m \) is equal to the number of natural numbers not greater than \( n \) and relatively prime to \( n \)?

P_{88}. Do there exist infinitely many natural numbers \( n \) such that the number of natural numbers \( \leq n \) and relatively prime to \( n \) is equal to the number of natural numbers \( \leq n+1 \) and prime to \( n+1 \)?

P_{89}. Does there exist a composite number \( n \) such that the number of all natural numbers \( \leq n \) and relatively prime to \( n \) is a divisor of the number \( n-1 \)?

The conjecture that there is no such composite number was made by D. H. Lehmer in [1].

P_{90}. Do there exist infinitely many pairs of natural numbers \( m \) and \( n \) such that the number of all natural numbers < \( m \) and relatively prime to \( m \) is equal to the sum of all the natural divisors of the number \( n \)?

It is easy to show that the answer to question P_{90} would be in the affirmative if the answer to problems P_{1} or P_{19} were in the affirmative.

P_{91}. Do there exist infinitely many natural numbers which are not, for any natural number \( n \), the sum of all natural divisors of \( n \), that are smaller than \( n \)?

This problem was set by P. Erdös. We know some such numbers, for example 2 and 5.

P_{92}. If we denote by \( f(n) \) the sum of all natural divisors of \( n \) less than \( n \), then is it true that the sequence

\[ n, f(n), ff(n), \ldots \]

for all natural numbers \( n > 1 \), is either periodic or stops at the number 1?

E. Catalan has made the conjecture that the answer to this question is in the affirmative. Not only we are unable to prove
this, but even the verification of it for individual natural numbers \( n \) is tedious. For example, as P. Poulet has calculated for \( n = 936 \) we obtain the sequence

\[
936, 1794, 2238, 2250, \ldots, 74, 40, 50, 43, 1
\]
of 189 terms, the greatest of which has fifteen digits.

**P93.** For every natural number \( n > 90 \) is the number of all natural numbers prime to \( n \) and less than \( n \), greater than or equal to the number of all prime numbers \( \leq n \)?

L. Moser in [1] gave a proof that the answer to this question is in the affirmative. Another proof was given by P. Erdős. These proofs are not easy.

**P94.** For every natural number \( n \) do there exist \( n \) different natural numbers such that the sum of any two of them is the square of a natural number?

This problem was set by L. Moser.

**P95.** Do there exist natural numbers \( n > 3 \) for which the number \( 2^n - 7 \) is prime?

T. Kulikowski proved in 1960 that number \( 2^{39} - 7 \) is prime.

**P96.** Do there exist infinitely many natural numbers which cannot be put in any of the four forms \( 6xy \pm x \pm y \) where \( x \) and \( y \) are natural numbers?

It can be shown that question P96 is equivalent to question P19.

We call an infinite sequence a *Fibonacci sequence* if its first two terms are equal to number 1 and every term is the sum of the preceding two terms, and hence the sequence:

\[
1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \ldots
\]

**P97.** Do there exist infinitely many prime numbers in a Fibonacci sequence?

*Fibonacci sequence* are numbers of the form

\[
P_n = \frac{n(n+1)(n+2)}{6}
\]

where \( n \) is a natural number. The name is derived from the number

Tetrahedral numbers are numbers of the form
of balls used in forming a pile in the shape of a tetrahedron. The first ten such numbers are 1, 4, 10, 20, 35, 56, 84, 120, 165, 220. The nineteenth century was occupied with marking out all the tetrahedral numbers which were also squares. E. Lucas conjectured in 1875 that there are only three such numbers: $P_1 = 1$, $P_2 = 2^2$ and $P_{48} = 140^2$. G. N. Watson proved it in 1918 but the proof is not easy.

$P_{98}$. How many tetrahedral numbers are also triangular?

We know such numbers. According to E. B. Escott and H. Sendacka such numbers $< 10^9$ are the numbers 1, 10, 120, 1540, and 7140, for which

$$P_1 = t_1, \quad P_3 = t_4, \quad P_8 = t_{15}, \quad P_{20} = t_{55}, \quad P_{34} = t_{119}.$$ 

This raises the conjecture that except for these five numbers there are no other tetrahedral numbers which are also triangular.

Many unsolved problems arise from inquiring into the decimal expansion of the square root of a natural number which is not a perfect square. As we know, elementary methods are known for calculating an arbitrary number of successive digits in this expansion.

Now if we come to the decimal expansion of the number $\sqrt{2}$ (which in 1950 was calculated for more than one thousand places) we do not really know the law of the succession of digits in this expansion. For example, we have the question:

$P_{95}$. Does the digit 1 occur infinitely many times in the decimal expansion of the number $\sqrt{2}$?

The digit 1 can be replaced in this question by any other digit.

The same is the case with the decimal expansion of many other known irrational numbers, for example $e$ and $\pi$. However, with regard to the expression of these numbers in continued fractions, the situation is somewhat different. We know the law of the succession of denominators in the expansion of irrational square roots of natural numbers and also for the number $e$ (the base of natural logarithms), but we do not know this for the number $\pi$, where we do not know if the denominator 1 occurs infinitely many times.
$P_{100}$. Does the sequence of nine digits 123456789 directly following one another occur at least once in the decimal expansion of $\pi$?

There are a lot more unsolved problems in arithmetic. Their number continually increases with time. This is because the new problems arise more rapidly than those already established are solved, and plenty of them have remained unsolved for centuries(1). But the progress of our knowledge of numbers is advanced not only by what we already know about them, but also by realizing what we yet do not know about them.

(1) When I said this in my lecture at the University of Rennes, a prominent mathematician of that university, Professor L. Antoine, said: “Certain problems will therefore never be solved”. I answered that this was of course possible but if humanity would last infinitely long, the situation might be paradoxical because although the number of unsolved problems would constantly and indefinitely increase, every problem would eventually be solved. In fact, suppose that ten new problems are posed every year and only one of the already posed ones is solved. Already the number of unsolved problems will increase indefinitely, namely after $n$ years there will remain $9n$ unsolved problems. But if the problems posed are marked with successive numbers and each year the problem marked with the lowest number (of those already posed) is solved, then the $n$th problem will be solved after $n$ years and thus, in time every one of the problems posed will be solved.
REFERENCES

W. H. Aning and P. Erdős

F. C. Auluck

N. G. W. H. Beeger

J. Brillhart and G. D. Johnson

B. M. Bredihin

M. Cantor

J. W. S. Cassels

Chao Ko

J. G. van der Corput

H. Davenport

C.-E. Fröberg

H. Hadwiger

G. H. Hardy and J. E. Littlewood
G. H. HARDY and E. M. WRIGHT

A. HURWITZ and J. L. SELFRIDGE

C. HYLTÉN-CAVALLIUS

A. E. INGHAM

H. J. KANOLD

A. Y. KHINCHIN

R. B. KILLGROVE and K. E. RALSTON

M. KRAITCHIK

T. KULIKOWSKI

J. LEECH

D. H. LEHMER

YU. V. LINNIK

W. LJUNGGREN

R. C. LYNNESS

A. MAKOWSKI
REFERENCES

H. Meschkowski

J. C. P. Miller and M. F. C. Woollett

L. Moser
[1] On the equation $\varphi(n) - \pi(n)$, Pi Mu Epsilon Journal. 1951, pp. 177-180.
[2] On the diophantine equation $1^n + 2^n + 3^n + \ldots + (m - 1)^n = m^n$, Scripta Math. 19 (1953), pp. 84-88.

G. Palamà

S. S. Pillai
[1] On the divisors of $a^n + 1$, J. Indian Math. Soc. 6 (1942), pp. 120-121.

N. Pipping

R. M. Robinson

G. Sansone and J. W. S. Cassels

A. Schinzel
REFERENCES

A. SCHINZEL and W. SIERPIŃSKI

J. L. SELFRIDGE

J. L. SELFRIDGE, C. A. NICOL and H. S. VANDIVER

D. SHANKS

W. SIERPIŃSKI

A. WAKULICZ

YIN WEN-LIN