TITLES IN THE POPULAR LECTURES IN MATHEMATICS SERIES

Vol. 1 *The Method of Mathematical Induction*
By I. S. Sominskii

Vol. 2 *Fibonacci Numbers*
By N. N. Vorob'ev

Vol. 3 *Some Applications of Mechanics to Mathematics*
By V. A. Uspenskii

Vol. 4 *Geometrical Constructions using Compasses Only*
By A. N. Kostovskii

Vol. 5 *The Ruler in Geometrical Constructions*
By A. S. Smogorzhevskii

Vol. 6 *Inequalities*
By P. P. Korovkin

Vol. 7 *One Hundred Problems in Elementary Mathematics*
By H. Steinhaus

Vol. 8 *Complex Numbers and Conformal Mappings*
By A. P. Markushevich

Vol. 9 *The Cube Made Interesting*
By Aniela Ehrenfeucht

Vol. 10 *Mathematical Games and Pastimes*
By A. P. Domoryad

Vol. 11 *A Selection of Problems in the Theory of Numbers*
By W. Sierpiński

A SELECTION OF PROBLEMS
in the
THEORY OF NUMBERS

by

WACŁAW SIERPIŃSKI

TRANSLATED FROM THE POLISH BY

A. SHARMA

PERGAMON PRESS

OXFORD • LONDON • NEW YORK • PARIS

PWN—POLISH SCIENTIFIC PUBLISHERS

WARSZAWA

1964

PERGAMON PRESS LTD.
Headington Hill Hall, Oxford
4 & 5 Fitzroy Square, London W. 1

PERGAMON PRESS INC.
122 East 55th Street, New York 22, N. Y.

GAUTHIER-VILLARS ED.
55 Quai des Grands-Augustins, Paris 6e

PERGAMON PRESS G.m.b.H.
Kaiserstrasse 75, Frankfurt am Main

Distributed in the Western Hemisphere by
THE MACMILLAN COMPANY · NEW YORK
pursuant to a special arrangement with
PERGAMON PRESS LIMITED

Państwowe Wydawnictwo Naukowe
(PWN — POLISH SCIENTIFIC PUBLISHERS)
Warszawa

Library of Congress Catalog Card Number 63-22531

Printed in Poland (W.D.N.)

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).

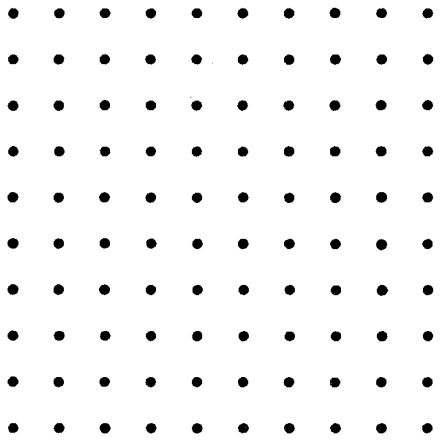

FIG. 1

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 $\leqq 1$, 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 $\leqq 2$, 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 $\leqq \frac{1}{2}$ and centre at the mid-point 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 $\frac{1}{2} < r \leqq \sqrt{5}/2$ 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 $\leqq \sqrt{2}/2$, then there would be no lattice points in its interior, but for a radius r such that $\sqrt{2}/2 < r \leqq \sqrt{10}/2$, 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 $(\sqrt{2}, \frac{1}{3})$, 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 square of their distances from p are equal. Hence by the theorem of Pythagoras we have the identity

$$(a-\sqrt{2})^2+(b-\tfrac{1}{3})^2 = (c-\sqrt{2})^2+(d-\tfrac{1}{3})^2,$$

whence

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

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

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

i.e.

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

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 $p(\sqrt{2}, \frac{1}{3})$.

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 lie 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 $p_1, p_2, \cdots, p_n, p_{n+1}, \cdots$ 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,

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

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 $(\sqrt{2}, \frac{1}{3})$ 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 $\geqq 0$, then the circle on whose circumference lie exactly n lattice points is the circle with centre $(\frac{1}{3}, 0)$ and radius $\frac{1}{3}5^k$, 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 $(\sqrt{2}, \sqrt{3}, \frac{1}{3})$. 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

$$n \leqq \pi\left(r+\frac{1}{\sqrt{2}}\right)^2.$$

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

$$\pi\left(r-\frac{1}{\sqrt{2}}\right)^2 \leqq n.$$

These inequalities give

$$\sqrt{\frac{n}{\pi}}-\frac{1}{\sqrt{2}} \leqq r \leqq \sqrt{\frac{n}{\pi}}+\frac{1}{\sqrt{2}},$$

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 $r > 1/\sqrt{2}$)

$$\frac{n}{\left(r+\frac{1}{\sqrt{2}}\right)^2} \leqq \pi \leqq \frac{n}{\left(r-\frac{1}{\sqrt{2}}\right)^2}.$$

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 π with arbitrary accuracy. This is interesting but in Analysis we know more convenient practical methods of calculating π 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 be 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 $\leqq 5$, 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 $\sqrt{5^{k-1}}$ 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

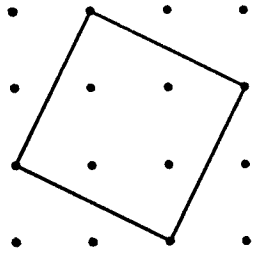

FIG. 2

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:

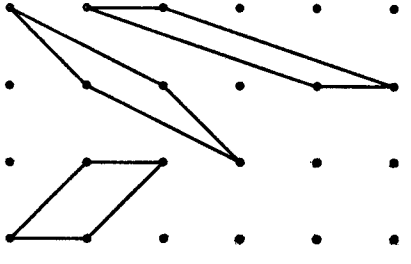

FIG. 3

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:

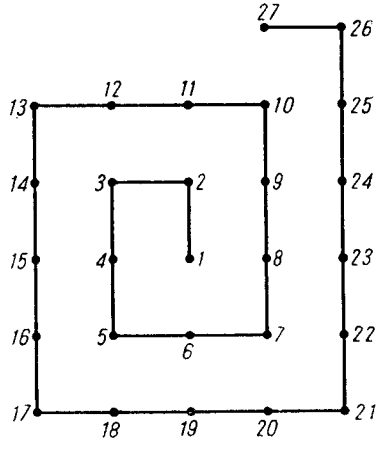

FIG. 4

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 $|x| \leqq |y|$, 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:

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:

For a natural number $n \geqq 3$, let us take n^2 lattice points (x, y) where x and y are natural numbers $\leqq n$; 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 $\leqq n$, 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 $k \leqq n$ 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 $m = 1, 2, \ldots$ and the set B is the set of all points with coordinates $(n+1, 0)$ where $n = 1, 2, \ldots$ 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 $\leqq 2r$, 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, $r = abc/4S$ 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 $\sqrt[3]{2}$ 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 $r^2 = l/m$ with l and m are natural numbers. Therefore $mr = \sqrt{lm} \geqq 1$, whence

$$4lm+1-4mr = (2mr-1)^2 \geqq 1,$$

so that

$$0 < \frac{4mr}{4lm+1} < 1.$$

There exists therefore an angle α such that $0 < \alpha < \pi/2$ and

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

We show that

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

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

$$\sin(k+2)\alpha = 2\sin(k+1)\alpha\cos\alpha - \sin k\alpha \quad \text{for} \quad k = 1, 2, \ldots \tag{3}$$

Let

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

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

$$\begin{aligned} t_1 &= (4lm+1)r\sin\alpha = 4mr^2 = 4l, \\ t_2 &= (4lm+1)^2 r \sin 2\alpha \\ &= 2(4lm+1)^2 r \sin\alpha\cos\alpha \\ &= 8mr^2(4lm-1) = 8l(4lm-1), \end{aligned} \tag{5}$$

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

$$t_{k+2} = 2(4lm-1)t_{k+1} - (4lm+1)^2 t_k \quad \text{for} \quad k = 1, 2, \ldots \tag{6}$$

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.