(ii) On the converse of Cauchy's theorem; (iii) Direct proof of a new criterion for the summability of a Fourier series; (iv) The summation of Denjoy-Fourier series : S. Pollard.

Note on an expansion of Neumann type in a special class of hypergeometric functions : J. Proudman.

On the oscillations of a rotating mechanical system with infinite freedom : J. Proudman and F. Edith Mercer.

Waves in canals and basins—II : Periodic motion in basins : B. M. Sen.

Motion referred to moving frames : F. Tavani.

(i) A note on Hankel transforms; (ii) The mean value of the zeta function on the critical line : E. C. Titchmarsh.

On isotropic polyadics : P. du Val.

A reduction formula for certain integrals of cylinder functions : J. Vint.

Computations concerning numbers representable by four or five cubes : A. E. Western.

THE FOUR SQUARE THEOREM

J. H. GRACE*.

1. The theorem that every positive integer is the sum of four or a smaller number of squares is so very familiar and has been so often proved that it will not be easy for a new demonstration to excite any interest : yet I venture to hope that the ensuing argument, based mainly on the theory of lattices, may deserve attention.

2. If two integers can each be expressed as the sum of four squares (some of which may be zero) the same is true of their product†; it follows that the theorem need be proved only for prime numbers. The number 2 presents no difficulty.

* Received 16 February, 1926; read 11 March, 1926.

† To recall the composition formula, observe that if, in the ordinary notation of quaternions,

$$(d+ai+bj+ck)(\delta+\alpha i+\beta j+\gamma k) = D+Ai+Bj+Ck,$$

then $$(a^2+b^2+c^2+d^2)(\alpha^2+\beta^2+\gamma^2+\delta^2) = A^2+B^2+C^2+D^2.$$

3. Suppose that p is a prime number of the form $4n+1$, then, as is well known, there exists an integer a such that

$$a^2+1 \equiv 0 \pmod p.$$

Consider now the points whose coordinates x, y referred to a set of rectangular axes are integers and satisfy the congruence

$$ax \equiv y \quad \text{or} \quad ay \equiv -x \pmod p.$$

Since the set is discrete and possesses the additive* property it forms a lattice†; further, when x is given y is determinate *modulo* p, and hence of the integer points in a very large area a fraction asymptotically $1/p$ belongs to the lattice. It follows that the area of a unit cell is p units.

Now let ξ, η be one of the lattice-points nearest the origin and call this A. The point B whose coordinates are $-\eta$, ξ also belongs to the lattice. The lines OA, OB are equal and at right angles, and the square $OACB$ having them for adjacent sides is a unit cell of the lattice. In

* By this is meant that, if x, y and x', y' belong to the set, so also do $x \pm x'$, $y \pm y'$: as Dedekind justly remarked, subtractive is the more proper word, for the additive case can be deduced.

† Poincaré, *Journal de l'Ecole Polytechnique*, cahier 47 (1880), 177, called this the theorem of Bravais; for two dimensions it is familiar in elliptic functions, being equivalent to the fact that a function of one complex variable cannot be more than doubly periodic; for higher dimensions there is an analogous theorem originally proved by Weierstrass and Riemann. I venture to sketch a proof which is at once simple and general.

Theorem. *If a set of points in n-dimensions is discrete and has the additive property it forms a lattice.*

There is a lower limit to the distance between two points of the set, so that there cannot be a limiting point, and hence a solid of finite content contains a finite number only of members of the set: if the points whose coordinates are

$$x_1, x_2, \ldots, x_n; \quad y_1, y_2, \ldots, y_n$$

belong to the set so also do the two points whose coordinates are

$$x_1+y_1, x_2+y_2, \ldots, x_n+y_n; \quad x_1-y_1, x_2-y_2, \ldots, x_n-y_n,$$

though the second hypothesis includes the first.

The data are independent of choice of axes, *i.e.* they persist after a change of axes, as is obvious for the part involving distance, and as for the other, it is really a vector statement. Alternatively its invariance follows from the linearity of the transformation equations from one set of axes to another.

The theorem is easily proved for $n = 1$, when the points are all on a straight line, since if P is a variable member of the set, the distance OP has either a lower limit or a minimum: the first alternative is inconsistent with discreteness and the second leads at once to the desired result.

We now proceed inductively from n dimensions to $n+1$. Without loss of generality, it may be assumed that the set in $n+1$ dimensions does not entirely belong to an n-flat.

Suppose that $P_1, P_2, \ldots, P_n$ are n points of the set not lying on an $(n-1)$-flat through O: we may take the n-flat π containing these $n+1$ points for $x_{n+1} = 0$, and, since the additive profact, its corners belong to the lattice, and no other point of it does, for any point of a square is certainly distant from at least one corner by less than the length of a side of the square, which is the minimum distance between two lattice points. The area of the square $OACB$ must consequently be p and we have

$$\xi^2+\eta^2 = p,$$

which proves the theorem for primes of this form.

4. Next let p be a prime of the form $4n+3$. It is easy to see (and has been many times proved) that there exist two integers a and b such that

$$a^2+b^2+1 \equiv 0 \pmod{p}. \tag{1}$$

---

perty is independent of axes, it follows by agreement that the points of the set lying in π form a lattice.

Let the coordinates $x_1, x_2, \ldots, x_n$ be measured parallel to the edges of a unit cell of this lattice: the points of the set for which $x_{n+1} = 0$ have for coordinates

$$\lambda_1 a_1, \lambda_2 a_2, \ldots, \lambda_n a_n, 0,$$

where the λ's are integers and the a's the lengths of the edges of the cell. Now let

$$x_1, x_2, \ldots, x_{n+1}$$

be a point of the set for which $x_{n+1} \neq 0$: either x_{n+1} has a minimum or a lower limit. In the first alternative we may take the minimum to belong to the point whose coordinates are

$$x_r = 0 \quad (r = 1, 2, \ldots, n), \qquad x_{n+1} = a_{n+1},$$

and an easy argument shows that the general point of the set is

$$\lambda_1 a_1, \lambda_2 a_2, \ldots, \lambda_n a_n, \lambda_{n+1} a_{n+1},$$

where the λ's are again integers. This is the lattice theorem.

In the second alternative, let

$$x_r = 0 \quad (r = 1, 2, \ldots, n), \qquad x_{n+1} = a_{n+1},$$

be a point of the system not in $x_{n+1} = 0$; then for an infinite number of values of x_{n+1} less than a_{n+1} there are points

$$x_1, x_2, \ldots, x_{n+1}$$

belonging to the set. Fixing attention on one such, we derive from it a point for which

$$0 \leqslant x_r < a_r \quad (r = 1, 2, \ldots, n), \qquad 0 \leqslant x_{n+1} < a_{n+1}$$

by compounding with a suitable point

$$x_r = \lambda_r a_r \quad (r=1, 2, \ldots, n), \qquad x_{n+1} = 0.$$

We thus obtain an infinite set σ of points of the system belonging to the solid bounded by

$$x_r = 0, a_r \quad (r = 1, 2, \ldots, n+1),$$

and this, as already remarked, is contrary to the assumption of discreteness in the set.

The theorem of Bravais is now completely established.

Consider the points whose coordinates referred to rectangular axes in four dimensions are integers and satisfy the congruence

$$(a+bi)(x+yi)-(z+wi) \equiv 0 \pmod{p},$$

this being really equivalent to two congruences. From (1) we deduce

$$(a-bi)(z+wi)+(x+yi) \equiv 0 \pmod{p},$$

and thence it is easy to see that if x, y, z, w belongs to the set so also do

$$w, z, -y, -x; \quad -z, w, x, -y; \quad y, -x, w, -z.$$

The lines joining the origin to these four associated points are equal in length and mutually at right angles.

Since the set is discrete and possesses the additive property it forms a lattice; moreover, when x, y are given, z, w are determinate modulo p, so that of the integer points within a hypersolid of large content a fraction asymptotically $1/p^2$ belongs to the lattice. It follows that the content of a unit cell is p^2.

Now let ξ, η, ζ, ϖ be one of the lattice-points nearest to the origin O; call that A, and let the associated points alluded to above be B, C, D. The lines OA, OB, OC, OD are equal in length and mutually at right angles, so that they are adjacent edges of a regular solid S in four dimensions. The centre of this solid S is G, and of the points belonging to S only G besides the corners can possibly belong to the lattice, because any other point of S is distant from at least one of the sixteen corners by less than the length of an edge, which is the minimum distance between two lattice-points. Of course, OG is equal to an edge. The question now is whether the solid S is a unit cell of the lattice.

It is quite easy to see that the cube σ whose edges are OA, OB, OC is a unit cell for the part of the lattice in the three-flat $OABC$, which I call π. If there are no other lattice-points nearer to π than D, it is easy to infer that S is a unit cell. Suppose, *per contra*, that P is a lattice-point nearer to π than D, and let π' be the three-flat through P parallel to π. In π' there will be a subsidiary part of the lattice exactly like that in π, and since the section σ' of the solid S by π' is just like the cube σ, and so derived from a unit cell of the part of the lattice in π' by a motion of translation, at least one point of σ', which is entirely in S, belongs to the lattice. It follows that the only possible position of π' is through G, the only point of S that can be a lattice-point. In the alternative case, then, G is one of the nearest points of the lattice to π and OG, OA, OB, OC are edges of a unit cell. The content of a unit cell is thus either

$$(\xi^2+\eta^2+\zeta^2+\varpi^2)^2 \quad \text{or} \quad \tfrac{1}{2}(\xi^2+\eta^2+\zeta^2+\varpi^2)^2,$$

and hence either $$(\xi^2+\eta^2+\zeta^2+\varpi^2)^2 = p^2$$

or $$(\xi^2+\eta^2+\zeta^2+\varpi^2)^2 = 2p^2.$$

Since the symbols all denote integers, the second relation is impossible; the first gives

$$\xi^2+\eta^2+\zeta^2+\varpi^2 = p,$$

and the proof is complete.

5. I add some remarks on a question which has occurred to me in connexion with the foregoing argument, viz. "are the shortest lines of a lattice the edges of a unit cell?" Or, in precise statement, say, for three dimensions : "O is a point of a lattice, A one of the nearest points to O, B one of the nearest not on the line OA, and C one of the nearest not in the plane OAB; are OA, OB, OC the edges of a unit cell?"

For two dimensions the answer is "Yes", a fact of some importance in the theory of crystals and elliptic functions; for three dimensions this answer also holds good, but in four dimensions it does not. In fact, referring to § 4, consider the lattice having for unit cell a solid with OA, OB, OC, OG for coterminous edges : it is easy to see that, since O, A, B, C, G are all lattice-points, so also is D, and the points A, B, C, D satisfy the conditions of the query; yet the solid S, which has OA, OB, OC, OD for edges, is not a unit cell.

6. In two dimensions the above result admits of an easy proof which serves to establish the fundamental theorem of Bravais. Consider a circle whose centre is at the origin O and which encloses at least two points of the set not collinear with O : if the circle encloses an infinite number of points of the set there will be a limiting point, and this is contrary to the condition of discreteness; thus there are only a finite number of points inside the circle. Let A be one of the nearest to O and B one of the nearest not on the line OA, so that, for any other point P of the set,

$$OP \geqslant OB \geqslant OA.$$

The corners of the triangle OAB thus belong to the set, and beyond them this area is clear of the set, as very simple reasoning shows. If we complete the parallelogram $OACB$, the triangle CAB has the same properties in regard to the set as the triangle OAB, from the additive property; it follows that it and the whole parallelogram are free of points of the set.

The points of the lattice having $OACB$ for unit cell all belong to the set, and no other point does, because if there were any such the figure $OACB$ would contain some by the additive property. The theorem is thus proved.

As far as I know there is no such simple argument in higher dimensions, and I rely on the following lemma, which perhaps is interesting in itself:

Suppose that Γ is a hypersolid in n dimensions bounded by n pairs of parallel $(n-1)$-flats, and that d is the distance of a point of Γ from a corner, then, for at least one of the corners,

$$d^2 \leqslant a_1^2 + a_2^2 + \ldots + a_n^2,$$

where $2a_1, 2a_2, \ldots, 2a_n$, are the lengths of the edges.

The sign of equality obtains when and only when the solid is rectangular and the point is its centre.

The truth of the lemma can be seen by induction, it being clear for $n = 1$. I content myself with indicating the proof roughly. The solid is divided into 2^n solids by $(n-1)$-flats through the centre parallel to the original faces. Any one of the new solids Γ' is partially bounded by n faces of the original, and the projection γ of any point of Γ' on one at least of these faces is internal to that face regarded as belonging to Γ. Applying the assumed result for $n-1$ dimensions to the projection, the truth of the general theorem for the part Γ' of the solid Γ follows, and a similar argument applies to each of the other parts.

7. There is no difficulty now in proving the "shortest-edge" theorem of § 5 for three dimensions, and in seeing that the exception to it, above mentioned, is the only possible one in four dimensions. For higher dimensions there are naturally more failures.*

---

* Cf. Bachmann, *Die Arithmetik der quadratischen Formen*, Zweite Abteilung (1923), 144 and 180. I owe this reference to the kindness of a referee. It may be added that the query of § 5, as regards two dimensions, is fully discussed in the original memoir of Bravais, *Journal de l'Ecole Polytechnique*, cahier 33 (1850), 1–128.