Note added proof, April 1964. These twelve cases have also been disposed of by Yamamoto [3] in a recent paper which Professor M. Hall has just drawn to my attention.

References

[1] Marshall Hall, *A survey of difference sets*, Proc. American Math. Soc. 7 (1956), pp. 975-986.

[2] H. B. Mann, *Balanced incomplete block designs and abelian difference sets*, Illinois J. Math. (to appear).

[3] Koichi Yamamoto, *Decomposition fields of difference sets*, Pacific J. Math. 13 (1963), pp. 337-352.

THE UNIVERSITY OF GLASGOW

Reçu par la Rédaction le 24. 8. 1963

ACTA ARITHMETICA
IX (1964)

Waring's problem for $\mathfrak{p}$-adic number fields

by

B. J. Birch (Manchester)

To L. J. Mordell

1. As is well known, for any power d there is a number $g(d)$ such that every positive integer is a sum of $g(d)$ dth powers. Some time ago, Siegel ([7], [8]) generalised this to finite algebraic number fields. Let K be a finite algebraic number field; then the elements of K which are sums of dth powers of integers of K form a set which we may denote by $J(K, d)$. Siegel proved that there is a number $G(K, d)$ such that every large enough element of $J(K, d)$ is a sum of at most G dth powers. He conjectured that G should depend only on d and not on K; for instance, he proved that every large enough element of K which is a sum of squares is a sum of at most five squares.

In [2], it was shown that the circle method could be applied so long as the number of variables exceeded a certain bound independent of the field K; in particular, I proved

THEOREM. *Let $s \geqslant 2^d+1$; suppose that M is a large enough totally positive integer of K, which is a sum of at most s d-th powers in every $\mathfrak{p}$-adic completion of K. Then M is a sum of at most s totally positive d-th powers of integers of K.*

Siegel's conjecture was thus reduced to a $\mathfrak{p}$-adic problem. At the time, the best $\mathfrak{p}$-adic results available were due to Stemmler [9]; in particular, these were enough to prove the conjecture for prime d. Subsequently a result similar to but sharper than the above has been proved by Körner [3], and an 'elementary' approach has been given by Rieger [6]; Körner [4] has somewhat improved Mrs Stemmler's $\mathfrak{p}$-adic estimates. In this note I will prove

THEOREM 1. *If K is a $\mathfrak{p}$-adic field, then every element of K which is a sum of d-th powers of integers of K is a sum of at most d^{16d^2} such d-th powers.*

Combining this with my earlier theorem, we deduce a similar result for a finite algebraic number field, and hence also for a number field which is not necessarily of finite degree over the rationals. This confirms Siegel's conjecture.

Since this note was written, I have seen a paper by C. P. Ramanujam [11], in which he proves a theorem similar to Theorem 1 with d^{16d^2} replaced by $8d^5$. As our methods are different, and neither of our papers contains the other, I have made no substantial alterations.

2. From now on, K will be a $\mathfrak{p}$-adic field with ring of integers $\mathfrak{o}$ and prime ideal $\mathfrak{p} = (\pi)$. The rational prime above $\mathfrak{p}$ is p, the ramification index is e so that $(\pi)^e = (p)$, and the residue class field $\mathfrak{o}/\mathfrak{p} = k$ has p^f elements. We denote the set of n-tuples of any set E by E^n.

If $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathfrak{o}^n$ and j is any positive integer, $s_j(\boldsymbol{x})$ will denote the elementary symmetric function of weight j in $x_1, \ldots, x_n$ and $t_j(\boldsymbol{x})$ will be the sum of the jth powers of $x_1, \ldots, x_n$. It is convenient to take $s_0 = 1$, so that if $\boldsymbol{x}, \boldsymbol{y}$ are two sets of elements then

$$s_j(\boldsymbol{x}, \boldsymbol{y}) = \sum_{i=0}^{j} s_i(\boldsymbol{x}) s_{j-i}(\boldsymbol{y}). \tag{2.1}$$

The following is well known (see, for instance, [5], p. 151).

Lemma 1. *There are polynomials F_k with rational integer coefficients such that $t_k = F_k(s_1, \ldots, s_k)$ identically.*

In order to prove Theorem 1, it is convenient to prove a little more.

Theorem 2. *Given any set $\boldsymbol{x}$ of integers of K we can find a set $\boldsymbol{y}$ consisting of at most d^{16d^2} integers such that*

$$s_j(\boldsymbol{x}) = s_j(\boldsymbol{y}) \quad \textit{for} \quad j = 1, \ldots, d.$$

In view of Lemma 1, Theorem 1 is an immediate consequence of Theorem 2: given $\boldsymbol{x}$ we choose $\boldsymbol{y}$ so that $s_j(\boldsymbol{x}) = s_j(\boldsymbol{y})$ for $j = 1, \ldots, d$, and then by the lemma $t_d(\boldsymbol{x}) = t_d(\boldsymbol{y})$. In fact, we obtain a more general result without extra effort — if $\psi(x)$ is a polynomial in one variable over $\mathfrak{o}$ such that $\psi(0) = 0$, then any element of K which is a sum of values of ψ is a sum of at most d^{16d^2} values of ψ. The main gain in discussing symmetric functions rather than sums of dth powers is that we can now apply a version of Hensel's lemma, as in Lemmas 3 and 6 below. We are also able to bypass some of the difficulties in identifying $J(K, d)$.

The proof of Theorem 2 will be in three stages; first, in § 3, we prove a similar result for finite fields. Then in § 4 we prove Lemma 4 which deals with the case $d^4 \leqslant p^f$, and in § 5 we prove Lemma 9 which deals with the case $d^4 > p^f$. Putting together Lemmas 4 and 9 gives the theorem immediately.

This note solves the problem it set out to solve, but has several defects. The bad estimate d^{16d^2} for the number of variables needed has been improved by Ramanujam [11], so far as Theorem 1 is concerned; it is desirable to improve Theorem 2 and Lemma 2 as well. Bateman and Stemmler [1] and more particularly Ramanujam [11] tell us a lot about the identification of the set $J(K, d)$ of numbers which are sums of dth powers; but we have not identified the set $L(k, d)$ of possible values for the first d symmetric functions even in the apparently simple case where k is a finite field.

3. In this section, as elsewhere in the paper, k is a field with p^f elements. We wish to prove

Lemma 2. *Suppose that $p^f \geqslant d^4$. If $\boldsymbol{x}$ is any set of elements of k, then we can find a set $\boldsymbol{y}$ consisting of at most $\frac{1}{2}(5^d-1)$ elements of k such that*

$$s_j(\boldsymbol{x}) = s_j(\boldsymbol{y}) \quad \textit{for} \quad j = 1, \ldots, d.$$

(The condition $p^f \geqslant d^4$ is inessential but convenient — if $d^4 > p^f$, then the result remains essentially true for trivial but different reasons, see Lemma 8 below. Lemma 2 seems to be harder than it looks, though there is more than one way of proving it; in what follows, we use a suggestion of Davenport's.)

We will prove Lemma 2 by induction on d. The lemma is certainly true for $d = 1$; suppose it is true in the $(d-1)$ case, so that given any $\boldsymbol{x}$ we can find a $\frac{1}{2}(5^{d-1}-1)$-tuple $\boldsymbol{y}$ such that $s_i(\boldsymbol{x}) = s_i(\boldsymbol{y})$ for $i = 1, \ldots, d-1$. Write $\frac{1}{2}(5^{d-1}-1) = c$ for short.

We prove our induction step by easy stages.

In the first place, if $\boldsymbol{x}$ is any set of elements of k, then there is another set, which we may denote by $\overline{\boldsymbol{x}}$, such that $s_j(\boldsymbol{x}, \overline{\boldsymbol{x}}) = 0$ for $j = 1, \ldots, d$; for instance, we may take $\overline{\boldsymbol{x}}$ as $\boldsymbol{x}$ repeated (p^d-1) times.

Second, we may suppose in proving the lemma that there is a $\boldsymbol{w} \in k^{2c+1}$ such that

$$s_i(\boldsymbol{w}) = 0 \quad \text{for} \quad i = 1, \ldots, d-1, \quad s^d(\boldsymbol{w}) \neq 0.$$

In fact, there are two possibilities; either given any set of elements of k we can mimic its first d symmetric functions by means of a set of at most c elements, in which case our induction step is trivial, or else (as we will suppose) there is a $\boldsymbol{z}_1 \in k^{c+1}$ such that there is no $\boldsymbol{z}_2 \in k^c$ with $s_j(\boldsymbol{z}_1) = s_j(\boldsymbol{z}_2)$ for $j = 1, \ldots, d$. By the induction hypothesis we can certainly find $\boldsymbol{z}_2 \in k^c$ with $s_i(\boldsymbol{z}_1) = s_i(\boldsymbol{z}_2)$ for $i = 1, \ldots, d-1$, so we have found $\boldsymbol{z}_1 \in k^{c+1}$ and $\boldsymbol{z}_2 \in k^c$ with

$$s_i(\boldsymbol{z}_1) = s_i(\boldsymbol{z}_2) \quad \text{for} \quad i = 1, \ldots, d-1 \text{ and } s_d(\boldsymbol{z}_1) \neq s_d(\boldsymbol{z}_2).$$

Now we find $\boldsymbol{z}_3 \in k^c$ so that $s_i(\boldsymbol{z}_3) = s_i(\overline{\boldsymbol{z}}_1)$ for $i = 1, \ldots, d-1$, that is, so that $s_i(\boldsymbol{z}_1, \boldsymbol{z}_3) = 0$ for $i = 1, \ldots, d-1$; and we can take $\boldsymbol{w}$ as one of $(\boldsymbol{z}_1, \boldsymbol{z}_3)$ or $(\boldsymbol{z}_2, 0, \boldsymbol{z}_3)$.

Next we note that $p^f \geqslant d^4$ implies that every element of k is a sum of two dth powers (see, for instance, Weil [10], p. 502). We deduce that for every $\sigma \in k$ we can find $\boldsymbol{x} \in k^{4c+2}$ such that

$$s_i(\boldsymbol{x}) = 0 \quad \text{for} \quad i = 1, \ldots, d-1, \; s_d(\boldsymbol{x}) = \sigma.$$

In fact, we find $\lambda, \mu \in k$ so that $(\lambda^d + \mu^d) s_d(\boldsymbol{w}) = \sigma$, and then we take $\boldsymbol{x}$ as the union of the two sets $\lambda\boldsymbol{w}$, $\mu\boldsymbol{w}$ obtained by multiplying the elements of $\boldsymbol{w}$ by λ, μ respectively.

Finally, given any $\boldsymbol{x}$, we choose $\boldsymbol{y}_1 \in k^c$ so that $s_i(\boldsymbol{y}_1) = s_i(\boldsymbol{x})$ for $i = 1, \ldots, d-1$; and we choose $\boldsymbol{y}_2 \in k^{4c+2}$ so that $s_j(\boldsymbol{y}_2) = s_j(\boldsymbol{x}, \overline{\boldsymbol{y}}_1)$ for $j = 1, \ldots, d$; this we can do since $s_i(\boldsymbol{x}, \overline{\boldsymbol{y}}_1) = 0$ for $i = 1, \ldots, d-1$. So we have found $\boldsymbol{y} = (\boldsymbol{y}_1, \boldsymbol{y}_2) \in k^{5c+2}$ so that $s_j(\boldsymbol{x}) = s_j(\boldsymbol{y})$ for $j = 1, \ldots, d$; since $5c+2 = \frac{1}{2}(5^d - 1)$, our induction step is proved.

4. Write $D = \frac{1}{2}(5^d - 1)$ for short. In Lemma 4 we will show that if $d^4 \leqslant p^f$ then for any set $\boldsymbol{x}$ of elements of $\mathfrak{o}$ there are $y_1, \ldots, y_D, z_1, \ldots, z_d \in \mathfrak{o}$ such that $s_j(\boldsymbol{x}) = s_j(\boldsymbol{y}, \boldsymbol{z})$ for $j = 1, \ldots, d$. First, we prove a corollary of Hensel's lemma (a more complicated version of this will be used in the final section).

Lemma 3. *Let $r \geqslant 1$. Suppose that $\boldsymbol{a} \in \mathfrak{o}^d$, $\boldsymbol{y} \in \mathfrak{o}^D$, $\boldsymbol{z}^{(r)} \in \mathfrak{o}^d$ are such that*

$$z_i^{(r)} \not\equiv z_j^{(r)} \; (\pi) \quad \textit{for} \quad i \neq j \tag{4.1}$$

and

$$s_k(\boldsymbol{y}, \boldsymbol{z}^{(r)}) \equiv a_k \; (\pi^r) \quad \textit{for} \quad k = 1, \ldots, d. \tag{4.2}$$

Then we can find $\boldsymbol{z}^{(r+1)} \in \mathfrak{o}^d$ such that

$$\boldsymbol{z}^{(r+1)} \equiv \boldsymbol{z}^{(r)} \; (\pi^r) \tag{4.3}$$

and

$$s_k(\boldsymbol{y}, \boldsymbol{z}^{(r+1)}) \equiv a_k \; (\pi^{r+1}) \quad \textit{for} \quad k = 1, \ldots, d. \tag{4.4}$$

Proof. The congruence (4.3) is equivalent to $\boldsymbol{z}^{(r+1)} = \boldsymbol{z}^{(r)} + \pi^r \boldsymbol{t}$ with $\boldsymbol{t} \in \mathfrak{o}^d$, so it is enough to show that we can find $\boldsymbol{t}$ such that

$$s_k(\boldsymbol{y}, \boldsymbol{z}^{(r)} + \pi^r \boldsymbol{t}) \equiv a_k \; (\pi^{r+1}) \quad \text{for} \quad k = 1, \ldots, d.$$

But

$$s_k(\boldsymbol{y}, \boldsymbol{z}^{(r)} + \pi^r \boldsymbol{t}) \equiv s_k(\boldsymbol{y}, \boldsymbol{z}^{(r)}) + \pi^r \sum_{j=1}^{d} t_j \frac{\partial s_k}{\partial z_j}(\boldsymbol{y}, \boldsymbol{z}^{(r)}) \; (\pi^{2r});$$

so since $r \geqslant 1$, it is enough to solve the linear congruence

$$\sum_{j=1}^{d} t_j [\partial s_k / \partial z_j] \equiv \pi^{-r} [a_k - s_k(\boldsymbol{y}, \boldsymbol{z}^{(r)})] \; (\pi). \tag{4.5}$$

The determinant formed by the coefficients $\partial s_k / \partial z_j$ is of Vandermonde type; it has value $\pm \Pi(z_i - z_j)$ and so does not vanish mod π by (4.1); so (4.5) is certainly soluble.

Lemma 4. *Suppose $d^4 \leqslant p^f$, and write $\frac{1}{2}(5^d - 1) = D$. Then for any set $\boldsymbol{x}$ of elements of $\mathfrak{o}$ we can find $\boldsymbol{y} \in \mathfrak{o}^D$ and $\boldsymbol{z} \in \mathfrak{o}^d$ such that*

$$s_j(\boldsymbol{y}, \boldsymbol{z}) = s_j(\boldsymbol{x}) \quad \textit{for} \quad j = 1, \ldots, d.$$

Proof. First we choose $\boldsymbol{z}^{(1)} \in \mathfrak{o}^d$ so that

$$z_i^{(1)} \not\equiv z_j^{(1)} \; (\pi) \quad \text{for} \quad i \neq j;$$

this is possible since $d < p^f$.

Second, we choose $\boldsymbol{y} \in \mathfrak{o}^D$ so that

$$s_j(\boldsymbol{y}, \boldsymbol{z}^{(1)}) \equiv s_j(\boldsymbol{x}) \; (\pi) \quad \text{for} \quad j = 1, \ldots, d;$$

this is possible by Lemma 2.

Now we apply Lemma 3: for each $r \geqslant 1$ we find $\boldsymbol{z}^{(r)} \equiv \boldsymbol{z}^{(1)} (\pi)$ so that

$$s_j(\boldsymbol{y}, \boldsymbol{z}^{(r)}) \equiv s_j(\boldsymbol{x}) \; (\pi^r) \quad \text{for} \quad j = 1, \ldots, d.$$

Finally, we let $r \to \infty$. By the compactness of $\mathfrak{o}$, the sequence $\{\boldsymbol{z}^{(r)}\}$ has a limit point, call it $\boldsymbol{z}$, and then $s_j(\boldsymbol{y}, \boldsymbol{z}) = s_j(\boldsymbol{x})$ for $j = 1, \ldots, d$.

5. Finally, we deal with the case $d^4 > p^f$. This part of the proof, though not difficult, is distinctly messy.

Lemma 5. *There are forms $\varphi_{ij}(\boldsymbol{z})$ defined for $1 \leqslant i \leqslant j \leqslant d$, such that φ_{ij} has integral coefficients and degree $j - i$, $\varphi_{ii} = 1$ for $i = 1, \ldots, d$, and*

$$\sum_{k=1}^{d} \sum_{i=1}^{j} t_k \varphi_{ij}(\boldsymbol{z}) \frac{\partial s_i}{\partial z_k} = \sum_{k=j}^{d} t_k \prod_{i=1}^{j-1} (z_i - z_k)$$

identically in $\boldsymbol{z}$ for $j = 1, \ldots, d$.

This lemma is wholly trivial; it simply describes what happens when we triangularise the Vandermonde-type matrix $\partial s_i / \partial z_k$. We state it in order to establish notation.

Lemma 6. *Let $\boldsymbol{a} \in \mathfrak{o}^d$, $\boldsymbol{z}^{(r)} \in \mathfrak{o}^d$. Let the power of π dividing $\prod_{i=1}^{j-1} (z_i^{(r)} - z_j^{(r)})$ be $\pi^{v(j)}$ for each $j = 1, \ldots, d$, and suppose that*

$$\prod_{i=1}^{j-1} (z_k^{(r)} - z_i^{(r)}) \equiv 0 \; (\pi^{v(j)}) \quad \textit{for} \quad 2 \leqslant j \leqslant k \leqslant d$$

and

$$\sum_{i=1}^{j} \varphi_{ij}(\boldsymbol{z}^{(r)}) [s_i(\boldsymbol{z}^{(r)}) - a_i] \equiv 0 \; (\pi^{r+v(j)}). \tag{5.1}$$

Suppose that $r > \max[v(j)]$. Then we can find $\boldsymbol{z}^{(r+1)}$ such that

$$\boldsymbol{z}^{(r+1)} \equiv \boldsymbol{z}^{(r)}\ (\pi^r)$$

and

$$\sum_{i=1}^{j} \varphi_{ij}(\boldsymbol{z}^{(r+1)})[s_i(\boldsymbol{z}^{(r+1)}) - a_i] \equiv 0\ \ (\pi^{r+1+v(j)}). \tag{5.2}$$

Proof. First, note that since $\varphi_{ii} = 1$, we have

$$s_j(\boldsymbol{z}^{(r)}) - a_j \equiv 0\ \ (\pi^r) \quad \text{for} \quad j = 1, \ldots, d. \tag{5.3}$$

We try to solve (5.2) with $\boldsymbol{z}^{(r+1)} = \boldsymbol{z}^{(r)} + \pi^r \boldsymbol{t}$. Then by (5.3)

$$\sum_{i=1}^{j} \varphi_{ij}(\boldsymbol{z}^{(r)} + \pi^r \boldsymbol{t})[s_i(\boldsymbol{z}^{(r)} + \pi^r \boldsymbol{t}) - a_i]$$
$$\equiv \sum_{i=1}^{j} \varphi_{ij}(\boldsymbol{z}^{(r)})[s_i(\boldsymbol{z}^{(r)}) - a_i] + \pi^r \sum_{i=1}^{j}\sum_{k=1}^{d} \varphi_{ij}(\boldsymbol{z}^{(r)})\, t_k \frac{\partial s_i}{\partial z_k}(\boldsymbol{z}^{(r)})\ \ (\pi^{2r}).$$

So by Lemma 5,

$$\sum_{i=1}^{j} \varphi_{ij}(\boldsymbol{z}^{(r+1)})[s_i(\boldsymbol{z}^{(r+1)}) - a_i]$$
$$\equiv \sum_{i=1} \varphi_{ij}(\boldsymbol{z}^{(r)})[s_i(\boldsymbol{z}^{(r)}) - a_i] + \pi^r \sum_{k=j}^{d} t_k \prod_{i=1}^{j-1} (z_i - z_k)\ \ (\pi^{2r}).$$

Since $r \geqslant v(j)+1$, we get a solution of (5.2) by successively choosing $t_d, t_{d-1}, \ldots, t_1$ modulo π so that

$$t_j \equiv \pi^{-r} \prod_{i=1}^{j-1} (z_i - z_j)^{-1} \sum_{i=1}^{j} \varphi_{ij}(\boldsymbol{z}^{(r)})[s_i(\boldsymbol{z}^{(r)}) - a_i] - \sum_{k=j+1}^{d} t_k \prod_{i=1}^{j-1} \frac{z_i - z_k}{z_i - z_j}\ \ (\pi).$$

LEMMA 7. *We can find a sequence $\{z_j\}$ of elements of $\mathfrak{o}$ such that, whenever $2 \leqslant j \leqslant k$, $\prod_{i=1}^{j-1} (z_k - z_i)$ is divisible by at least as high a power of π as $\prod_{i=1}^{j-1} (z_j - z_i)$, and $\prod_{i=1}^{j-1} (z_j - z_i)$ is not divisible by π^{2j-2}.*

If now $\boldsymbol{a} \in \mathfrak{o}^d$ satisfies $a_j \equiv s_j(\boldsymbol{z})(\pi^{4d})$ for $j = 1, \ldots, d$, then we can find $\boldsymbol{w} \in \mathfrak{o}^d$ such that $s_j(\boldsymbol{w}) = a_j$ for $j = 1, \ldots, d$.

Proof. We choose $z_1, z_2, \ldots$ successively so as to make $\prod_{i=1}^{j-1} (z_j - z_i)$ divisible by as small a power of π as possible. Explicitly, we first choose $z_1, \ldots, z_{p^f}$ to be incongruent modulo π; then, for $j = j_0 + j_1 p^f + j_2 p^{2f} + \ldots$ in the scale of p^f, we take $z_{j+1} = \sum z_{j_u+1}\pi^u$. It is easy to verify $\pi^{2j-2} \nmid \prod_{i=1}^{j-1} (z_j - z_i)$. The hypotheses of Lemma 6 are now satisfied with $r = 2d$; so by Lemma 6 and induction, for each $r \geqslant 2d$ we can find $\boldsymbol{z}^{(r)}$ such that $\boldsymbol{z}^{(r)} \equiv \boldsymbol{z}\ (\pi^{2d})$ and $\sum_{i=1}^{j} \varphi_{ij}(\boldsymbol{z}^{(r)})[s_i(\boldsymbol{z}^{(r)}) - a_i] \equiv 0 (\pi^{r+v(j)})$; if $\boldsymbol{w}$ is a limit point of the sequence $\{\boldsymbol{z}^{(r)}\}$ then $s_j(\boldsymbol{w}) = a_j$ as required.

LEMMA 8. *For each integer m, let $L(d, \pi^{4d}, m)$ be the set of d-tuples $\boldsymbol{c}$ of residue classes modulo π^{4d} such that there exists $\boldsymbol{y} \in \mathfrak{o}^m$ with $s_j(\boldsymbol{y}) \equiv c_j(\pi^{4d})$ for $j = 1, \ldots, d$. Then*

$$L(d, \pi^{4d}) = \bigcup_m L(d, \pi^{4d}, m) \subseteq L(d, \pi^{4d}, p^{4d^2 f} - p^{4df} + 1).$$

Proof. Clearly $L(d, \pi^{4d}, m+1) \supseteq L(d, \pi^{4d}, m)$, and if $L(d, \pi^{4d}, m+1) = L(d, \pi^{4d}, m)$ then $L(d, \pi^{4d}, n) = L(d, \pi^{4d}, m)$ for all $n > m$. But there are only $p^{4d^2 f}$ possible values for the d-tuple $s_1, \ldots, s_d$ of residue classes modulo π^{4d}, and $L(d, \pi^{4d}, 1)$ accounts for p^{4df} of these since s_1 takes p^{4df} values. So the nested sequence of subsets L must terminate after at most $p^{4d^2 f} - p^{4df} + 1$ terms.

LEMMA 9. *For every set of integers $\boldsymbol{x}$, we can find a $p^{4d^2 f}$-tuple $\boldsymbol{y}$ such that $s_j(\boldsymbol{y}) = s_j(\boldsymbol{x})$ for $j = 1, \ldots, d$.*

Proof. By (2.1), for fixed $\boldsymbol{z} \in \mathfrak{o}^d$ there is a 1-1 correspondence between integer d-tuples $s_j(\boldsymbol{y}, \boldsymbol{z})$ and integer d-tuples $s_j(\boldsymbol{y})$ $(j = 1, \ldots, d)$; and for a fixed set of integers $\boldsymbol{y}$ there is a 1-1 correspondence between the $s_j(\boldsymbol{y}, \boldsymbol{z})$ and the $s_j(\boldsymbol{z})$.

First, fix $\boldsymbol{z} \in \mathfrak{o}^d$ as in Lemma 7.

Second, let $\bar{\boldsymbol{z}}$ denote $\boldsymbol{z}$ repeated $(p^{8d} - 1)$ times. Then by Lemma 8 we may choose a $(p^{4d^2 f} - d)$-tuple $\boldsymbol{y}_1$ so that $s_j(\boldsymbol{y}_1) \equiv s_j(\boldsymbol{x}, \bar{\boldsymbol{z}})$ (π^{4d}); and then $s_j(\boldsymbol{y}_1, \boldsymbol{z}) \equiv s_j(\boldsymbol{x})(\pi^{4d})$, as in the first step of the proof of Lemma 2.

Finally, by Lemma 7, we may choose $\boldsymbol{y}_2 \in \mathfrak{o}^d$ so that

$$s_j(\boldsymbol{y}_1, \boldsymbol{y}_2) = s_j(\boldsymbol{x}) \quad \text{for} \quad j = 1, \ldots, d.$$

This completes the proof of Lemma 9. Theorem 2 follows by combining Lemmas 4 and 9, and Theorem 1 is immediate from Theorem 2.

References

[1] P. T. Bateman and R. M. Stemmler, *Waring's problem for algebraic number fields, and primes of the form* $(p^r - 1)/(p^d - 1)$, Illinois J. Math. 6 (1962), pp. 142-156.

[2] B. J. Birch, *Waring's problem in algebraic number fields*, Proc. Cambridge Phil. Soc. 57 (1961), pp. 449-459.

[3] O. Körner, *Über Mittelwerte trigonometrischer Summen und ihre Anwendung in algebraischen Zahlkörpern*, Math. Annalen 147 (1962), pp. 205-239.

[4] — *Ganze algebraische Zahlen als Summen von Polynomwerten*, Math. Annalen 149 (1963), pp. 97-104.

[5] O. Perron, *Algebra* I, 3rd edition, Berlin 1951.

[6] G. J. Rieger, *Elementare Lösung des Waringschen Problems für algebraische Zahlkörper mit der verallgemeinerten Linnikschen Methode*, Math. Annalen 148 (1962), pp. 83-88.

[7] C. L. Siegel, *Generalisation of Waring's problem to algebraic number fields*, Amer. J. Math. 66 (1944), pp. 122-136.

[8] — *Sums of m-th powers of algebraic integers*, Ann. Math. 46 (1945), pp. 313-339.

[9] R. M. Stemmler, *The easier Waring problem in algebraic number fields*, Acta Arithmetica 6 (1961), pp. 447-468.

[10] A. Weil, *Numbers of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (1949), pp. 497-508.

[11] C. P. Ramanujam, *Sums of m-th powers in p-adic rings*, Mathematika 10 (1963), pp. 137-146.

UNIVERSITY OF MANCHESTER

Reçu par la Rédaction le 8. 10. 1963

ACTA ARITHMETICA
IX (1964)

Tauberian theorems for sum sets

by

P. Erdös (London), B. Gordon* (Los Angeles, Calif.),
L. A. Rubel (Urbana, Ill.) and E. G. Straus (Los Angeles, Calif.)

Introduction. The sums formed from the set of non-negative powers of 2 are just the non-negative integers. It is easy to obtain "abelian" results to the effect that if a set is distributed like the powers of 2, then the sum set will be distributed like the non-negative integers. We will be concerned here with converse, or "Tauberian" results. The main theme of this paper is the following question: if the set of sums formed from a given set of positive real numbers resembles an arithmetic progression, how much must the original set resemble a set of constant multiples of powers of 2?

If we denote the given set by $k_0, k_1, k_2, \ldots$, arranged in ascending order, and let $S(x)$ count the number of those sums of distinct k_j that do not exceed x, our problem is, roughly, that of showing that k_n is close to 2^n if $S(x)$ is close to x. Our first result gives sharp bounds for lim inf and lim sup of $2^n/k_n$ in terms of lim inf and lim sup of $S(x)/x$. In the next section, we show that if $S(x)-x$ is bounded, then k_n-2^n is bounded, and furthermore, $\sum|k_n-2^n|<\infty$, so that if the k_n are integers, then $k_n=2^n$ for all large n. We extend the method in the succeeding section to obtain estimates for k_n-2^n and $\sum_{n\leqslant N}|k_n-2^n|$ in terms of suitable bounds for $S(x)-x$, even if $S(x)-x$ is unbounded. Finally, on a slightly different note, we show that it is not possible for $S(x)$ to behave too much like x^a if $a<1$.

1. Asymptotic behavior. Let $K = k_0, k_1, k_2, \ldots$, $0<k_0\leqslant k_1\leqslant k_2\leqslant\ldots$, be any sequence of positive real numbers. Let $S(x)$ denote the number of choices of $\varepsilon_0, \varepsilon_1, \varepsilon_2, \ldots$ such that for each $j=0,1,2,\ldots$, either $\varepsilon_j=0$ or $\varepsilon_j=1$, and such that $\varepsilon_0 k_0+\varepsilon_1 k_1+\ldots\leqslant x$. Let

$$A = \liminf_{x\to\infty} S(x)/x, \qquad \alpha = \liminf_{n\to\infty} 2^n/k_n,$$

$$B = \limsup_{x\to\infty} S(x)/x, \qquad \beta = \limsup_{n\to\infty} 2^n/k_n.$$

* Alfred P. Sloan Fellow.