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


THE UNIVERSITY OF GLASGOW

Reçu par la Rédaction le 21. 3. 1964

ACTA ARITHMETICA
IX (1964)

Waring’s problem for 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 \( g(d) \) \( d \)-th 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 \( d \)-th 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 \( G \) \( d \)-th 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 \( s \geq 2^a + 1 \); 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 \( p \)-adic completion of \( K \). Then \( M \) is a sum of at most \( s \) totally positive \( d \)-th powers of integers of \( K \).

Siegels conjecture was thus reduced to a \( p \)-adic problem. At the time, the best \( p \)-adic results available were due to Stegler [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 [8]; Körner [4] has somewhat improved Mrs Stegler’s \( p \)-adic estimates. In this note I will prove

**Theorem 1.** If \( K \) is a \( p \)-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 \( d^a \) 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 \( d = d^e \) replaced by \( 8d^2 \). 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 \( p \)-adic field with ring of integers \( \mathcal{O} \) and prime ideal \( p = \pi \); the rational prime above \( p \) is \( p \), the ramification index is \( e \) so that \( (\pi)^e = (p) \), and the residue class field \( \mathcal{O}/p = k \) has \( p^e \) elements. We denote the set of \( n \)-tuples of any set \( E \) by \( E^n \).

If \( x = (x_1, \ldots, x_n) \in \mathcal{O}^n \) and \( j \) is any positive integer, \( s_j(x) \) will denote the elementary symmetric function of weight \( j \) in \( x_1, \ldots, x_n \) and \( t_j(x) \) will be the sum of the \( j \)th powers of \( x_1, \ldots, x_n \). It is convenient to take \( s_1 = 1 \), so that if \( x, y \) are two sets of elements then

\[
s_j(x, y) = \sum_{x_1, \ldots, x_j} s_j(x) s_{j-1}(y).
\]

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

**Lemma 1.** There are polynomials \( F_n \) with rational integer coefficients such that \( s_n = F_n(s_1, \ldots, s_n) \) identically.

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

**Theorem 2.** Given any set \( E \) of integers of \( K \) we can find a set \( E \) consisting of at most \( d^e \) elements such that

\[
s_j(x) = s_j(y) \quad \text{for} \quad j = 1, \ldots, d.
\]

In view of Lemma 1, Theorem 1 is an immediate consequence of Theorem 2: given \( x \) we choose \( y \) so that \( s_j(x) = s_j(y) \) for \( j = 1, \ldots, d \), and then by the lemma \( t_j(x) = t_j(y) \).

The proof of Theorem 2 is 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 \( d \leq p^e \), and in § 5 we prove Lemma 9 which deals with the case \( d > p^e \). 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 \( d^e \) 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 Stemmer [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 \( d \)th 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 \( p^e \) elements. We wish to prove

**Lemma 2.** Suppose that \( p^e > d^e \). If \( x \) is any set of elements of \( k \), then we can find a set \( y \) consisting of \( \frac{1}{2}(5^{d-1}-1) \) elements of \( k \) such that

\[
s_j(x) = s_j(y) \quad \text{for} \quad j = 1, \ldots, d.
\]

(The condition \( p^e > d^e \) is essential, and convenient — if \( d^e > p^e \), then the result remains essentially true for trivial but different reasons, see Lemma 5 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.)

We will prove Lemma 3 by induction on \( d \). The lemma is certainly true for \( d = 1 \); suppose it is true in the \((d-1)\)st case, so that any \( x \) can we find a \( \frac{1}{2}(5^{d-1}-1) \)-tuple \( y \) such that \( s_i(x) = s_i(y) \) for \( i = 1, \ldots, d-1 \). Write \( \frac{1}{2}(5^{d-1}-1) = e \) for short.

We prove our induction step by easy stages.

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

Second, we may suppose in proving the lemma that there is a \( \varphi \) \( \mathcal{E}^{2e+1} \) such that \( s_i(\varphi) = 0 \) for \( i = 1, \ldots, d-1 \), \( \varphi(\varphi) \neq 0 \).

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 \( e \) elements, in which case our induction step is trivial, or else (as we will suppose) there is a \( s_i \mathcal{E}^{2e+1} \) such that there is no \( s_i \mathcal{E}^{2e+1} \) with \( s_i(x) = s_i(y) \) for \( j = 1, \ldots, d \). By the induction hypothesis we can certainly find \( s_i \mathcal{E}^{2e+1} \) with \( s_i(x) = s_i(y) \) for \( i = 1, \ldots, d-1 \), so we have found \( x \mathcal{E}^{2e+1} \) and \( y \mathcal{E}^{2e+1} \) with

\[
s_i(x) = s_i(y) \quad \text{for} \quad i = 1, \ldots, d-1 \text{ and } s_i(x) \neq s_i(y).
\]

Now we find \( s_i \mathcal{E}^{2e} \) so that \( s_i(x) = s_i(y) \) for \( i = 1, \ldots, d-1 \), that is, so that \( s_i(x, x) = 0 \) for \( i = 1, \ldots, d-1 \); and we can take \( x \) as one of \( x, x \) or \( x, 0, x \).
Next we note that $p' > d'$ 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 $x \in k$ we can find $x_0 \in c^d_k$ such that

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

In fact, we find $\lambda, \mu \in k$ so that $(x^2 + p') s_i(x) = \sigma$, and then we take $x$ as the union of the two sets $\lambda x, \mu x$ obtained by multiplying the elements of $\sigma$ by $\lambda, \mu$ respectively.

Finally, given any $x$, we choose $y_i \in c^d$ so that $s_i(y_i) = s_i(x)$ for $i = 1, \ldots, d - 1$; and we choose $y_d \in c^{d+1}$ so that $s_d(y_d) = s_d(x)$ for $j = 1, \ldots, d - 1$. So we have found $y = (y_1, y_d) \in c^{d+1}$ so that $s_i(y) = s_i(x)$ for $j = 1, \ldots, d$; since $5d + 2 = \frac{1}{2}(5d - 1)$, our induction step is proved.

4. Write $D = \frac{1}{2}(5d - 1)$ for short. In Lemma 4 we will show that if $d' < p'$ then for any set $x$ of elements of $c$ there are $y_1, \ldots, y_d, z_1, \ldots, z_d$, such that $s_i(x) = \sigma_i(y, z)$ for $j = 1, \ldots, d$. First, we prove a corollary of Hendel's lemma (a more complicated version of this in the final section).

**Lemma 3.** Let $r \geq 1$. Suppose that $a \in c^d$, $y \in c^d$, $z \in c^d$ are such that

$$(4.1) \quad \sigma_i^r \neq \sigma_j^r \quad (\pi) \quad \text{for} \quad i \neq j$$

and

$$(4.2) \quad s_k(y, z^r) = s_k(x) \quad (\pi) \quad \text{for} \quad k = 1, \ldots, d.$$ 

Then we can find $x^{r+1} \in c^d$ such that

$$(4.3) \quad x^{r+1} = \sigma_i^{r+1} \quad (\pi)$$

and

$$(4.4) \quad s_k(y, x^{r+1}) = s_k(x) \quad (\pi+1) \quad \text{for} \quad k = 1, \ldots, d.$$ 

**Proof.** The congruence (4.3) is equivalent to $x^{r+1} = \sigma_i + \pi t$ with $t \in c^d$, so it is easy to show that we can find $t$ such that

$$s_k(y, x^{r+1}) = s_k(x) \quad (\pi+1) \quad \text{for} \quad k = 1, \ldots, d.$$ 

But

$$s_k(y, x^{r+1}) = s_k(y, \sigma_i + \pi t) = s_k(y, \sigma_i) + \pi \sum_{j=1}^d t_j \frac{\partial s_k}{\partial q_j}(y, \sigma_i) (\pi r);$$

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

$$\sum_{j=1}^d t_j \frac{\partial s_k}{\partial q_j}(y, \sigma_i) = \pi \sigma_k(s_k(y, \sigma_i)) (\pi).$$

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

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

$$s_i(y, z) = s_i(x) \quad (\pi) \quad \text{for} \quad j = 1, \ldots, d.$$ 

**Proof.** First we choose $z^{r+1} \in c^d$ such that

$$z^{r+1} \neq \sigma_j^r \quad (\pi) \quad \text{for} \quad i \neq j;$$

this is possible since $d' < p'$.

Second, we choose $y \in c^d$ so that

$$s_k(y, z^{r+1}) = s_k(x) \quad (\pi) \quad \text{for} \quad j = 1, \ldots, d;$$

this is possible by Lemma 2.

Now we apply Lemma 3: for each $r \geq 1$ we find $x^{r+1} \in c^{d+1}$ such that

$$s_k(y, z^{r+1}) = s_k(x) \quad (\pi+1) \quad \text{for} \quad j = 1, \ldots, d.$$ 

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

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

**Lemma 5.** There are forms $q_i(x)$ defined for $1 \leq i \leq j \leq d$, such that $q_i$ has integral coefficients and degree $j - i$, $q_i = 1$ for $i = 1, \ldots, d$, and

$$\sum_{j=i}^d \sum_{k=1}^d b_{jk}q_j(x) = \sum_{j=k}^d \sum_{k=1}^d b_{jk}q_k(x) \quad \text{for} \quad i = 1, \ldots, d,$$

identically in $x$ for $j = 1, \ldots, d$.

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

**Lemma 6.** Let $a \in c^d$, $z \in c^d$. Let the power of $\pi$ dividing $\prod_{j=1}^{d-1} (z^{r+1} - z^r)$ be $\pi^r$ for each $j = 1, \ldots, d$, and suppose that

$$\prod_{j=1}^{d-1} (z^{r+1} - z^r) \equiv 0 \quad (\pi^r) \quad \text{for} \quad 2 \leq j \leq k \leq d$$

and

$$\sum_{j=1}^{d-1} p_{jk}(x) \cdot (z_k - z^r) \equiv 0 \quad (\pi^{r+1}).$$
Suppose that \( r > \max\{n(j)\} \). Then we can find \( z^{r+1} \) such that

\[
s(z^{r+1}) = n(z^{r+1})
\]

and

\[
\sum_{j=1}^{f} \phi_j(\alpha^{r+1}) = n(z^{r+1})
\]

(5.3)

\[
\sum_{j=1}^{f} \phi_j(\alpha^{r+1}) [s_j(\alpha^{r+1}) - a_j] = 0 \quad (\alpha^{r+1} + \alpha^0),
\]

Proof. First, note that since \( \phi_j = 1 \), we have

\[
s_j(z) - a_j = 0 \quad (\alpha^r) \quad \text{for} \quad j = 1, \ldots, d.
\]

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

\[
\sum_{j=1}^{f} \phi_j(\alpha^{r+1}) [s_j(\alpha^{r+1}) - a_j] = \pi \sum_{j=1}^{d} \phi_j(\alpha^{r+1}) \int_0^{\frac{1}{\alpha^0}} (\alpha^{r+1}) (\alpha^{r+1}).
\]

So by Lemma 5,

\[
\sum_{j=1}^{f} \phi_j(\alpha^{r+1}) [s_j(\alpha^{r+1}) - a_j] = \pi \sum_{j=1}^{d} \phi_j(\alpha^{r+1}) \int_0^{\frac{1}{\alpha^0}} (\alpha^{r+1}),
\]

Since \( r > n(j) + 1 \), we get a solution of (5.2) by successively choosing \( t_1, t_2, \ldots, t_k \) modulo \( \pi \) so that

\[
t_j = \pi^{-1} \sum_{i=1}^{j-1} (z_i - z_{i+1}) \sum_{j=1}^{f} \phi_j(\alpha^{r+1}) [s_j(\alpha^{r+1}) - a_j] - \sum_{k=1}^{d} t_k \sum_{j=1}^{j-1} (z_i - z_{i+1}) (\alpha^{r+1}).
\]

Lemma 7. We can find a sequence \( \{z_j\} \) of elements of \( \mathfrak{c} \) such that, whenever \( 2 \leq j \leq k \), \( \prod_{i=1}^{j-1} (z_i - z_j) \) is divisible by at least as high a power of \( \pi \) as \( \prod_{i=1}^{j-1} (z_i - z_j) \), and \( \prod_{i=1}^{j-1} (z_i - z_j) \) is not divisible by \( \pi^{r+1} \).

If now \( \alpha \) satisfies \( a_j = s_j(\alpha^{r+1}) \) for \( j = 1, \ldots, d \), then we can find \( \alpha \) such that \( s_j(\alpha^{r+1}) = a_j \) for \( j = 1, \ldots, d \).

Proof. We choose \( z_1, z_2, \ldots \) successively so as to make \( \prod_{i=1}^{j-1} (z_i - z_j) \) divisible by as small a power of \( \pi \) as possible. Explicitly, we first choose \( z_1, \ldots, z_d \) to be congruent modulo \( z_1 \); then, for \( j = 2, 3, \ldots \), we choose \( z_j + 1 \) to be congruent to \( z_j \) modulo \( z_j \); if \( j = 1 \), we take \( z_1 = s_1 \), \( z_2 = s_2 \). It is easy to verify that \( s_j(\alpha^{r+1}) = a_j \) for \( j = 1, \ldots, d \).

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

Tauberian theorems for sum sets

by

P. Erdős (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 \( k_1, k_2, k_3, \ldots \), arranged in ascending order, and let \( S(x) \) count the number of those sums of distinct \( k_i \) 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 \( \liminf \) and \( \limsup \) of \( 2^n/k_n \) in terms of \( \liminf \) and \( \limsup \) 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 \( \sum |k_n - 2^n| \) 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 \( a^x \) if \( a < 1 \).

1. Asymptotic behavior. Let \( K = k_0, k_1, k_2, \ldots, \) be any sequence of positive real numbers. Let \( S(x) \) denote the number of choices of \( \epsilon_j, \epsilon_1, \epsilon_2, \ldots \) such that for each \( j = 0, 1, 2, \ldots \), either \( \epsilon_j = 0 \) or \( \epsilon_j = 1 \), and such that \( \epsilon_0 k_0 + \epsilon_1 k_1 + \ldots \leq x \). Let

\[
A = \liminf_{x \to \infty} S(x)/x, \quad a = \liminf_{x \to \infty} 2^n/k_n, \\
B = \limsup_{x \to \infty} S(x)/x, \quad \beta = \limsup_{x \to \infty} 2^n/k_n.
\]

* Alfred P. Sloan Fellow.