ACTA ARITHMETICA
IX (1964)

Difference sets

by

R. A. Rankin (Glasgow)

1. Let v, k, λ be positive integers, with $k < v$. A set $D(v, k)$ of k distinct residues $d_1, d_2, \ldots, d_k$ modulo v is called a (v, k, λ) *difference set*, if every residue $m \not\equiv 0 \pmod{v}$ can be expressed in exactly λ different ways in the form

$$m \equiv d_\mu - d_\nu \pmod{v}.$$

Then $k(k-1) = \lambda(v-1)$ and we put $n = k - \lambda$, so that

$$k^2 = n + \lambda v.$$

With each difference set $D(v, k)$ there is associated a complementary difference set $D(v, v-k)$, whose members are the complementary set of residues modulo v; $D(v, v-k)$ is a (v^*, k^*, λ^*) difference set with the parameters

$$v^* = v, \qquad k^* = v - k, \qquad \lambda^* = v - 2k + \lambda, \qquad n^* = k^* - \lambda^* = n.$$

It follows that we may, if we wish, suppose that $0 < k \leqslant v/2$.

With the difference set $D(v, k)$ we associate the polynomial

$$\theta(x) = \sum_{\nu=1}^{k} x^{d_\nu},$$

where we may suppose that $0 \leqslant d_\nu < v$, and we then have the fundamental identity

$$\theta(x)\,\theta(1/x) \equiv n + \lambda(1 + x + x^2 + \ldots + x^{v-1}) \big(\operatorname{mod}\,(x^v - 1)\big). \tag{1.1}$$

Our object is to find criteria that are necessary for the existence of difference sets, and these are given in Theorems 1-4 and are applied to certain unsettled cases given by Marshall Hall [1]. For this purpose we consider factorization into ideal factors in a suitable cyclotomic field $K(N)$ generated by $\omega = \exp(2\pi i/N)$, where N is a divisor of v. We write, for any integer s,

$$\xi_s = \theta(\omega^s) = \sum_{\nu=1}^{k} \omega^{d_\nu s} = \sum_{q=0}^{N-1} a_q \omega^{qs},$$

where a_q is the number of different d_ν congruent to q modulo N. It follows that

$$(1.2) \qquad 0 \leqslant a_q \leqslant V = v/N \qquad (0 \leqslant q < N),$$

and, by (1.1),

$$(1.3) \qquad \xi_s \bar{\xi}_s = n \ \ (0 < s < N), \qquad \xi_0 = k.$$

If a is any algebraic integer in $K(N)$, we denote by $[a]$ the principal ideal that it generates.

2. In this section $D(v, k)$ is a given (v, k, λ) difference set and N is a fixed divisor of v. We put $n = n_0 n_1$, where $(n_0, n_1) = 1$ and every rational prime p dividing n_1 is such that

$$(2.1) \qquad p^t \equiv -1 \pmod N$$

for some integer t, while n_0 contains no such primes p.

THEOREM 1. *$n_1 = m^2$ for some positive integer m and $\xi_s \equiv 0 \pmod m$ if $0 < s < N$.*

Proof. That n_1 is a perfect square is known; see [2], Theorem 3, for example.

Suppose that $0 < s < N$; since $\xi_s \bar{\xi}_s = n_0 n_1$, by (1.3), it follows that

$$[\xi_s] = \mathfrak{n}_0 \mathfrak{n}_1,$$

where the ideals $\mathfrak{n}_0$, $\mathfrak{n}_1$ are prime to each other and

$$\mathfrak{n}_0 \bar{\mathfrak{n}}_0 = [n_0], \qquad \mathfrak{n}_1 \bar{\mathfrak{n}}_1 = [n_1].$$

Now $(n_1, N) = 1$, so that every rational prime $\mathfrak{p}$ dividing n_1 splits up into a number of distinct prime ideal factors $\mathfrak{p}$. If $\mathfrak{p}^{(\nu)}$ denotes the conjugate ideal under the isomorphism $\omega \to \omega^\nu$, where $(\nu, N) = 1$, then $\mathfrak{p}^{(\nu)} = \mathfrak{p}$ whenever ν is congruent to a power of p modulo N. In particular, by (2.1),

$$\bar{\mathfrak{p}} = \mathfrak{p}^{(-1)} = \mathfrak{p},$$

and this holds for every prime ideal factor of n_1, so that $\bar{\mathfrak{n}}_1 = \mathfrak{n}_1$, and therefore

$$[n_1] = \mathfrak{n}_1^2.$$

Since the prime ideal factors of each rational prime divisor of n_1 are distinct, it follows that $n_1 = m^2$, for some positive integer m. Also $\mathfrak{n}_1 = [m]$, so that $\xi_s \equiv 0 \pmod m$.

Since $(N, n_1) = 1$, it follows that the congruence

$$Na \equiv k \pmod m$$

has a unique solution a satisfying $0 \leqslant a < m$.

Our next theorem gives some information about the number m and the coefficients a_q.

THEOREM 2. (i) *$a_q \equiv a \pmod m$ $(0 \leqslant q < N)$. (ii) $a < V$. (iii) $k \geqslant Na + \sqrt{n}$. (iv) $m(k - Na) \leqslant \lambda V + n + a(Na - 2k)$.*

We deduce immediately the

COROLLARY. *If $N = v$, then $m = 1$; i.e. n has no prime divisors p satisfying* (2.1). *A similar conclusion holds if $v = 2N$ and $k \leqslant N$.*

For then $a = 0$, by (iii), and (iv) gives $m \leqslant 1$. The first part of the corollary is a particular case of Theorem 3 of [2].

Proof of Theorem 2. By Theorem 1, we have for $0 \leqslant q < N$,

$$Na_q = \sum_{s=0}^{N-1} \xi_s \omega^{-qs} \equiv \xi_0 = k \pmod m,$$

so that (i) follows and therefore $a \leqslant a_q \leqslant V$, by (1.2). However, if $a = V$, then $a_q = a$ for all q, and so $n = 0$ and $k = v$, which is false; thus (ii) holds.

Write $a_q = a + mA_q$ $(0 \leqslant q < N)$, so that A_q is a non-negative integer and

$$(2.2) \qquad m \sum_{q=0}^{N-1} A_q = k - Na.$$

It follows that

$$\sqrt{n} = |\xi_1| = m \Big| \sum_{q=0}^{N-1} A_q \omega^q \Big| \leqslant k - Na,$$

which gives (iii).

Finally,

$$n(N-1) + k^2 = \sum_{s=0}^{N-1} |\xi_s|^2 = N \sum_{q=0}^{N-1} a_q^2$$

$$= N \Big\{ Na^2 + 2ma \sum_{q=0}^{N-1} A_q + m^2 \sum_{q=0}^{N-1} A_q^2 \Big\}.$$

Since $A_q \leqslant A_q^2$, (iv) follows from this and (2.2).

Theorem 2 enables us to dispose of the sixth of Hall's twelve unsettled cases [1]. Here

$$v = N = 171, \quad k = 35, \quad \lambda = 7, \quad n = 28, \quad n_0 = 7, \quad n_1 = 4.$$

Thus, by Theorem 1, $m = 2$, which contradicts the Corollary. No difference set with these parameters can therefore exist.

3. In several of Hall's unsettled cases it turns out that, for a suitable choice of N, $[\xi_s] = [r]$ $(0 < s < N)$, where r is a positive rational integer whose square is n; hence

$$\xi_s = r\delta(s) \quad (0 < s < N), \tag{3.1}$$

where $\delta(s)$ is a unit in $K(N)$ of unit modulus, and therefore

$$\delta(s) = \pm\omega^l$$

for some integer l depending on s. We suppose that these conditions are satisfied for a difference set $D(v, k)$ and deduce some information about the integer l, which enables us to evaluate the coefficients a_q.

Let $N = N_1N_2$, where N_1 is the greatest factor of N that is prime to $2r$. We then have the following theorem.

THEOREM 3. *If* $0 < s < N$ *and* $d = (s, N_2)$, *then*

$$\delta(s) = \varepsilon(d)\,\omega^{sa(d)}, \tag{3.2}$$

where, for each divisor d *of* N_2, $\varepsilon(d) = \pm 1$ *and* $a(d)$ *is a rational integer depending only on* d. *If* r *is odd,* N_2 *is even and* d_1 *and* d_2 *are divisors of* N_2 *with* $d_2 = 2^t d_1 < N$, *where* d_1 *is odd and* t *is a positive integer, then* $a(d_2) = a(d_1)$ *and* $\varepsilon(d_1)$ *may be taken to be* 1.

Proof. Let d be any divisor of N_2 and suppose that $d \neq N$. Then, since $\xi_d \epsilon K(N/d)$, it is clear that

$$\delta(d) = \varepsilon(d)\,\omega^{da(d)}, \tag{3.3}$$

where $\varepsilon(d) = \pm 1$ and $a(d)$ is a rational integer.

Let p be a rational prime number that does not divide r. Then, for any s,

$$\xi_s^p = \Big\{\sum_{q=0}^{N-1} a_q\,\omega^{qs}\Big\}^p \equiv \sum_{q=0}^{N-1} a_q^p\,\omega^{pqs} (\operatorname{mod} p)$$
$$\equiv \sum_{q=0}^{N-1} a_q\,\omega^{pqs} (\operatorname{mod} p) \equiv \xi_{ps} (\operatorname{mod} p).$$

Hence, for $0 < s < N$ and $ps \neq N$,

$$\delta^p(s)r \equiv \delta^p(s)r^p \equiv \delta(ps)r (\operatorname{mod} p),$$

so that

$$\delta(ps) - \delta^p(s) \equiv 0 (\operatorname{mod} p). \tag{3.4}$$

Now the left-hand side of (3.4) is of the form

$$\pm\omega^b(1 \pm \omega^c),$$

and so is either (a) zero, (b) a unit, (c) divisible by 2 (for $\pm\omega^c = 1$), or (d) a *proper* algebraic divisor of one of the rational odd prime factors of N. If $p \neq 2$, only (a) can hold and we deduce that

$$\delta(ps) = \delta^p(s) \tag{3.5}$$

whenever $(p, 2r) = 1$, $0 < s < N$, $ps \neq N$.

Write, for $0 < s < N$,

$$f = (s, N) = de, \quad s = ft, \tag{3.6}$$

where $d = (s, N_2)$, $e = (s, N_1)$. Then, since $(e, 2r) = 1$,

$$\delta(f) = \delta^e(d) = \varepsilon(d)\,\omega^{dea(d)} = \varepsilon(d)\,\omega^{fa(d)},$$

by (3.3) and (3.5). Also, since $\sigma = \omega^f$ generates $K(N/f)$ and $(t, N/f) = 1$, an application of the isomorphism $\sigma \to \sigma^t$ to the equation

$$\xi_f = r\varepsilon(d)\,\omega^{fa(d)}$$

gives

$$\xi_s = r\varepsilon(d)\,\omega^{sa(d)},$$

so that (3.2) follows.

Finally, suppose that r is odd, N_2 is even and that d_1 and d_2 are divisors of N_2 with $d_2 = 2^t d_1 < N$, where d_1 is odd and t is a positive integer. Take $p = 2$ in (3.4) and apply this congruence t times, giving

$$\delta(d_2) - \delta^{2^t}(s) \equiv 0 (\operatorname{mod} 2).$$

Hence

$$\varepsilon(d_2)\,\omega^{d_2\{a(d_2) - a(d_1)\}} \equiv 1 (\operatorname{mod} 2). \tag{3.7}$$

The left-hand side of (3.7) must be ± 1; i.e.

$$d_2\{a(d_2) - a(d_1)\} \equiv 0 (\operatorname{mod} N/2). \tag{3.8}$$

Now, whenever N/d is even, an odd multiple of $N/(2d)$ may be added to $a(d)$ in (3.2), provided that the sign of $\varepsilon(d)$ is changed and *vice versa*. This shows that we may assume that $\varepsilon(d_1) = 1$ and we then change $\varepsilon(d_2)$, if necessary, to make (3.8) hold modulo N, so that we may take $a(d_2) = a(d_1)$.

This completes the proof of Theorem 3.

For our next theorem we require Ramanujan's function

$$c(d, t) = \frac{1}{N_1} \sum_{\substack{s=0 \\ (s, N_2) = d}}^{N-1} \omega^{st} = \sum_{\delta | (N_2/d,\, t/N_1)} \delta\mu(N_2/d\delta). \tag{3.9}$$

The notation is as before and t is any rational integer. The number $c(d, t)$ is a rational integer and is zero when t is not divisible by N_1. Also

$$|c(d, t)| \leqslant c(d, 0) = \varphi(N_2/d), \tag{3.10}$$

where $\varphi(N_2/d)$ is Euler's function.

THEOREM 4. *For* $0 \leqslant q < N$,

$$Na_q = k - r\varepsilon(N_2) + rN_1 \sum_{d|N_2} \varepsilon(d) c\bigl(d, \alpha(d) - q\bigr). \tag{3.11}$$

In particular, if $q = \alpha(1)$,

$$|Na_q - k + r\varepsilon(N_2) - \varepsilon(1) rN_1 \varphi(N_2)| \leqslant rN_1\{N_2 - \varphi(N_2)\}. \tag{3.12}$$

Proof. We have

$$Na_q = \sum_{s=0}^{N-1} \xi_s \omega^{-qs} = k + r \sum_{s=1}^{N-1} \delta(s) \omega^{-qs}$$

$$= k + r \sum_{d|N_2} \varepsilon(d) \sum_{\substack{s=1 \\ (s,N_2)=d}}^{N-1} \omega^{s\{\alpha(d)-q\}}.$$

(3.11) follows from this and (3.9), and (3.12) is an immediate deduction from (3.10) and (3.11).

Theorem 4 can be used to dispose of possible difference set parameters by showing that (1.2) is incompatible with (3.11) or (3.12) .

Eight of Hall's unsettled cases satisfy the conditions of this section, the relevant parameters being given in the following table:

Case	1	2	3	4	5	7	8	9
v	45	36	96	64	175	120	288	100
k	12	15	20	28	30	35	42	45
λ	3	6	4	12	5	10	6	20
n	9	9	16	16	25	25	36	25
N	45	36	96	64	175	30	36	25
N_1	5	1	3	1	7	3	1	1
N_2	9	36	32	64	25	10	36	25
r	3	3	4	4	5	5	6	5

By applying (3.12) we can show that Cases 1, 5 and 9 cannot occur. For example, in Case 1, with $N = 45$ and $\sigma = e^{2\pi i/9}$,

$$[3] = \mathfrak{p}^6,$$

where $\mathfrak{p} = [1-\sigma]$ and is prime since 3 is a primitive root modulo 5. It follows that $[\xi_s] = [3]$ for $0 < s < 45$. Since

$$Na_q = k - r\varepsilon(N_2) (\operatorname{mod} rN_1),$$

by (3.11), $\varepsilon(N_2) = -1$ and (3.12) gives, for $q = \alpha(1)$,

$$|45a_q - 105| \leqslant 45,$$

which is impossible for $a_q = 0, 1$.

Cases 2, 3, 4 and 7 can be ruled out by use of (3.11). For example, in Case 7 with $N = 30$, $[5] = \mathfrak{p}^2$, where $\mathfrak{p} = [1 - e^{2\pi i/5}]$ and is prime, so that $[\xi_s] = [5]$ for $0 < s < 30$. Thus $r = 5$ and, by (3.11), for $0 \leqslant q < 30$,

$$a_q = 1 + \tfrac{1}{2} \sum_{d|10} \varepsilon(d) c\bigl(d, \alpha(d) - q\bigr), \tag{3.13}$$

where we can take

$$\varepsilon(1) = \varepsilon(5) = 1, \quad \alpha(2) = \alpha(1), \quad \alpha(10) = \alpha(5),$$

by Theorem 3. Write

$$c_1(t) = c(1, t) + \varepsilon(2) c(2, t), \quad c_5(t) = c(5, t) + \varepsilon(10) c(10, t).$$

Then, for $t = 0, 1, 2, \ldots, 29$, $c_1(t)$ and $\pm c_5(t)$ are cyclic permutations of

$$200000200000200000200000200000$$

and

$$800000\bar{2}00000\bar{2}00000\bar{2}00000\bar{2}00000,$$

respectively, where $\bar{2}$ stands for -2. This shows that $c_1(t)$ is periodic with period 6 and that, for certain pairs of values of t differing by 6, $c_2(t)$ takes values differing by 10. Hence, by (3.13), for some q,

$$a_{q+6} - a_q = \pm 5.$$

This contradicts the fact that $0 \leqslant a_q \leqslant 4$ for all q.

The criteria given in this paper have therefore disposed of Hall's cases 1-7 and 9. In a recent paper [2], Mann has used different methods to dispose of the ten cases 1-6, 8 and 10-12; I am indebted to him for sending me an earlier report of his work written for The Boeing Company. He informs me that eight of his ten cases, together with Case 9, have been disposed of by R. Turyn. Accordingly, it is now known that none of Hall's twelve cases can give rise to a difference set.

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 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 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 𝔭-adic problem. At the time, the best 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 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^{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