DECOMPOSITION FIELDS OF DIFFERENCE SETS

KOICHI YAMAMOTO

1. Preliminaries from cyclotomic fields. In this paper we denote the rational number field by Q, and its subring of all rational integers by Z. All algebraic quantities are to be contained in a "sufficiently large" cyclotomic field over Q. We also denote by ζ_m an unspecified primitive mth root of unity.

If $\mathfrak{p}$ is a prime ideal, α an integer $\neq 0$ of a cyclotomic field $Q(\zeta_m)$, then the $\mathfrak{p}$-*component* of α is, by definition, the power of $\mathfrak{p}$ which exactly divides α. If $\mathfrak{a}$ is an ideal $\neq 0$ of $Q(\zeta_m)$, then the $\mathfrak{a}$-component of α is defined as the product of the $\mathfrak{p}$-components of α extended over all prime ideal divisors of $\mathfrak{a}$.

Theorem 1 below will be frequently used later, and is essentially based on the well-known theorem in the theory of cyclotomic fields: The set of all integers of the cyclotomic field $Q(\zeta_m)$ is identical with the ring $Z[\zeta_m]$.

Let C be a number-theoretic function, whose values are contained in the ring $Z[\zeta_m]$. We define the difference operator $\Delta(\rho)$ by

$$\Delta(\rho)C(i) = C(i + \rho) - C(i) .$$

Here ρ is a rational number not necessarily an integer. But we make the convention that $C(\rho) = 0$ if ρ is not an integer, so $-\Delta(\rho)$ will be an identity operator if ρ is not an integer. We say that C is a periodic function with a period n if $\Delta(n)C(i) = 0$ for all i.

THEOREM 1. *Let $n = p_1^{t_1} \cdots p_s^{t_s}$ be the prime-power decomposition of n. Let m be relatively prime to n, C be a periodic number-theoretic function, with period n whose values $C(i)$ are integers of the cyclotomic field $Q(\zeta_m)$, and $f(x) = \sum_{i=0}^{n-1} C(i)x^i$. Moreover let d be a divisor of n and α be an integer of $Q(\zeta_m)$.*

Then, in order that $f(\zeta_n^r) \equiv 0 \pmod{\alpha}$ for all divisors r of d, it is necessary and sufficient that

$$p_1^{t_1} \cdots p_s^{t_s} \Delta(np_1^{-t_1-1}) \cdots \Delta(np_s^{-t_s-1})C(i) \equiv 0 \pmod{\alpha}$$

for all i and for all $t_1, \cdots, t_s$ such that $p_1^{t_1} \cdots p_s^{t_s} \mid d$.

Proof. (1) We can assume $s > 0$, so we first consider the case $s = 1$. Put $n = p^t$, $d = p^u$, and we proceed by an induction on u. Now we have

Received March 7, 1962.

$$f(\zeta_n) = \sum_{i=0}^{p^{l-1}-1} \sum_{j=0}^{p-1} C(i + p^{l-1}j)\zeta_n^{i+p^{l-1}j}$$
$$= \sum_{i=0}^{p^{l-1}-1} \sum_{j=1}^{p-1} (C(i + p^{l-1}j) - C(i))\zeta_n^{i+p^{l-1}j} ,$$

by using the fact that $\zeta_n^{p^{l-1}} = \zeta_p$ is a primitive pth root of unity, or that $\sum_{j=0}^{p-1} \zeta_p^j = 0$. The $p^{l-1}(p-1)$ integers $\zeta_n^{i+p^{l-1}j}$ for $0 \leqq i < p^{l-1}$, $1 \leqq j < p$ form a $Z[\zeta_m]$-basis of the ring $Z[\zeta_{mn}]$, and we have $f(\zeta_n) \equiv 0 \pmod{\alpha}$ if and only if $C(i + p^{l-1}j) - C(i) \equiv 0 \pmod{\alpha}$ for all choices of i, j above. This condition is equivalent to

$$\Delta(np^{-1})C(i) \equiv 0 \pmod{\alpha}$$

for all i. This shows the validity of our assertion for $u = 0$.

(2) Assume therefore $s = 1$, $u > 0$ and assume the validity of the assertion for smaller values of u. Now we have

$$f(x^p) \equiv \sum_{i=0}^{p^l-1} C(i)x^{ip} \equiv \sum_{i=1}^{p^{l-1}-1} \left(\sum_{j=0}^{p-1} C(i + p^{l-1}j)\right)x^{ip} \pmod{1 - x^n} .$$

As was proved in (1) above, it follows from $f(\zeta_n) \equiv 0 \pmod{\alpha}$ that $C(i) \equiv C(i + p^{l-1}j) \pmod{\alpha}$. Thus if we define

$$g(x) = p \sum_{i=0}^{p^{l-1}-1} C(i)x^{ip} ,$$

then

$$f(x^p) \equiv g(x) \pmod{\alpha, 1 - x^n} .$$

The condition $f(\zeta_n^{p^t}) \equiv 0 \pmod{\alpha}$ for all t such that $0 \leqq t \leqq u$ is equivalent to $f(\zeta_n^{p^t}) \equiv 0 \pmod{\alpha}$ and $g(\zeta_n^{p^t}) \equiv 0 \pmod{\alpha}$ for all t such that $0 \leqq t \leqq u - 1$. The last is equivalent to, by the induction hypothesis, that $p^t\Delta(p^{l-t-1})C(i) = 0 \pmod{\alpha}$ and $p^{t+1}\Delta(p^{l-1-t-1})C(i) \equiv 0 \pmod{\alpha}$ for all $0 \leqq t \leqq u - 1$, namely to $p^t\Delta(p^{l-t-1})C(i) \equiv 0 \pmod{\alpha}$ for all t such that $0 \leqq t \leqq u$. This shows the validity of the theorem for $s = 1$.

(3) Now assume $s > 1$ and assume the validity of the theorem for smaller values of s. Put $n = n_1n'$, $n_1 = p_1^{l_1}$, $n' = p_2^{l_2} \cdots p_s^{l_s}$, $d = d_1d'$, $d_1 = (n_1, d)$, $d' = (n', d)$. Any divisor r of d is written uniquely as $r = r_1r'$ where $r_1 \mid d_1$, $r' \mid d'$. For a given i there are j, k such that

$$i \equiv n'j + n_1k \pmod{n} ,$$

and j, k are determined $\pmod{n_1}$ and $\pmod{n'}$ respectively. Hence

$$f(x) \equiv \sum_{j=0}^{n_1-1} \sum_{k=0}^{n'-1} C(n'j + n_1k)x^{n'j+n_1k} \pmod{1 - x^n} ,$$

$$f(\zeta_n^r) = \sum_{j=0}^{n_1-1} \sum_{k=0}^{n'-1} C(n'j + n_1k)\zeta_n^{n'rj}\zeta_n^{n_1rk}$$
$$= \sum_{j=0}^{n_1-1} C^*(\zeta_n^{n_1r}, j)$$

where

$$C^*(y, j) = \sum_{k=0}^{n'-1} C(n'j + n_1k)y^k .$$

Now $\zeta_n^{n'} = \xi$ is a primitive n_1th root of unity and $\zeta_n^{n_1} = \eta$ is a primitive n'th root of unity. And the condition $f(\zeta_n^r) \equiv 0 \pmod{\alpha}$ for some ζ_n implies of course the same congruence for all primitive nth roots of unity. Thus $f(\zeta_n^r) \equiv 0 \pmod{\alpha}$ for some ζ_n implies that

$$\sum_{j=0}^{n_1-1} C^*(\eta^{r'}, j)\xi^{r_1j} \equiv 0 \pmod{\alpha}$$

for all primitive n_1th roots of unity ξ and for all n'th roots of unity η. Note that $C^*(\eta^{r'}, j)$ are integers of $Q(\zeta_m, \eta) = Q(\zeta_{mn'})$ with $(mn', n) = 1$. Applying the already established case $s = 1$ of the Theorem to the polynomial $\sum_{j=0}^{n_1-1} C^*(\eta^{r'}, j)x^j$, we see that $f(\zeta_n^r) \equiv 0 \pmod{\alpha}$ for all r such that $r \mid d$ if and only if

$$p_1^{t_1}\Delta_j(n_1p_1^{-t_1-1})C^*(\eta^{r'}, j) \equiv 0 \pmod{\alpha}$$

for all t_1 such that $p_1^{t_1} \mid d_1$ and for all r' such that $r' \mid d'$. Here $\Delta_j(\rho)$ denotes the difference operator to apply on the argument j. The above condition may be stated as

$$p_1^{t_1} \sum_{k=0}^{n'-1} \Delta_j(n_1p_1^{-t-1})C(n'j + n_1k)\eta^{r'k} \equiv 0 \pmod{\alpha}$$

for all t_1 and r' such that $p_1^{t_1} \mid d_1$ and $r' \mid d'$. Now we can apply the induction hypothesis to the polynomial $p_1^{t_1}\sum_{k=0}^{n'-1}\Delta_j(n_1p_1^{-t_1-1})C(n'j + n_1k)x^k$, because the coefficients are integers of $Q(\zeta_m)$, $(m, n') = 1$ and n' has $s - 1$ distinct prime divisors. Thus we see that the last condition is true if and only if

$$p_1^{t_1}p_2^{t_2} \cdots p_s^{t_s}\Delta_j(n_1p_1^{-t_1-1})\Delta_k(n'p_2^{-t_2-1}) \cdots \Delta_k(n'p_s^{-t_s-1})C(n'j + n_1k)$$
$$= p_1^{t_1} \cdots p_s^{t_s}\Delta(np_1^{-t_1-1}) \cdots \Delta(np_s^{-t_s-1})C(i) \equiv 0 \pmod{\alpha}$$

for all i and for all $t_1, \cdots, t_s$ such that $p_1^{t_1} \cdots p_s^{t_s} \mid d$.

COROLLARY. *Under the same notations as in Theorem* 1, *let furthermore* S *be a set of divisors of* n *such tnat* $r \in S$ *and* $r' \mid r$ *implies* $r' \in S$. *Then in order that* $f(\zeta_n^r) \equiv 0 \pmod{\alpha}$ *for all* $r \in S$, *it is necessary and sufficient that*

$$p_1^{t_1} \cdots p_s^{t_s}\Delta(np_1^{-t_1-1}) \cdots \Delta(np_s^{-t_s-1})C(i) \equiv 0 \pmod{\alpha}$$

for all i and for all $p_1^{t_1} \cdots p_s^{t_s} = r \in S$.

2. Difference sets. Let $D = \{a_1, \cdots, a_k\}$ be a (v, k, λ)-difference set. We denote the quantity $k - \lambda$ by n. We associate with D its *generating polynomial* $g_D(x) = g(x)$ defined by $g(x) = \sum_{i=1}^{k} x^{a_i}$, which is determined (mod $1 - x^v$). As is well known the condition

$$(*) \qquad g(x)g(x^{v-1}) \equiv n + \lambda(1 + x + \cdots + x^{v-1}) \pmod{1 - x^v}$$

characterizes the difference set property of the set D. The above implies that

$$(1) \qquad g(\zeta)g(\zeta^{\tau}) = n$$

for all vth roots of unity $\zeta \neq 1$, where τ denotes the complex conjugation of the field $Q(\zeta_v)/Q$. As is easily verified, the condition (1) implies conversely the relation (*). This is the reason why the two parameters v and n are the most fundamental to a number-theoretic study of difference sets. If v is even, then n is a square as seen from (1) for $\zeta = -1$. Also k is determined by the quadratic equation

$$(2) \qquad k(v - k) = n(v - 1) ,$$

and λ by

$$(3) \qquad \lambda(v - 2n - \lambda) = n(n - 1) .$$

From (3) follows that $n + (n - 1) \leqq v - 2n \leqq n(n - 1) + 1$ or

$$(4) \qquad 4n - 1 \leqq v \leqq n^2 + n + 1 .$$

The two extreme cases $v = 4n - 1$ and $v = n^2 + n + 1$ correspond to the difference sets of Hadamard type and to the difference sets of projective planes.

If we fix n then there are $\tau(n)\tau(n - 1)$ ways of choosing parameters (v, k, λ) satisfying the relations $k(k - 1) = (v - 1)\lambda$ and $k - \lambda = n$, where $\tau(m)$ denotes the number of divisors of m. Similarly, if we fix v, then there are $2^{\omega(v-1)}$ ways of choosing these parameters, where $\omega(m)$ denotes the number of distinct prime divisors of m.

The difference set D will be called nontrivial if $v > 1$ and $n > 1$. We consider nontrivial difference sets exclusively in this paper.

There are several difference sets closely related to a given difference set D. If D is a (v, k, λ)-difference set, u and β are integers such that $(\beta, v) = 1$, then $D + u = \{a_1 + u, \cdots, a_k + u\}$ and $\beta D = \{\beta a_1, \cdots, \beta a_k\}$ are (v, k, λ)-difference sets, *similar* to D. The difference set $(-1)D$ will be denoted by $-D$. Furthermore the residual set $D^* = \{0, 1, \cdots, v - 1\} - D$ of D is a $(v, v - k, v - 2n - \lambda)$-difference set, which is called the *residual* difference set of D. Note

that D^* has the parameters $v^* = v$, $k^* = v - k$, $\lambda^* = v - 2n - \lambda$, $n^* = n$, and that the relations (2) and (3) may be written as $kk^* = n(v-1)$, $\lambda\lambda^* = n(n-1)$ together with $k + k^* = v$, $\lambda + \lambda^* = v - 2n$. As for the generating polynomials we note that

$$
\begin{aligned}
& g_{D+u}(x) \equiv x^u g_D(x) && (\mathrm{mod}\ 1 - x^v)\ , \\
(5)\qquad & g_{\beta D}(x) \equiv g_D(x^\beta) && (\mathrm{mod}\ 1 - x^v)\ , \\
& g_D(x) + g_{D^*}(x) \equiv 1 + x + \cdots + x^{v-1} && (\mathrm{mod}\ 1 - x^v)\ .
\end{aligned}
$$

In particular we see that for any vth root of unity $\zeta \neq 1$ that

$$
(6)\qquad g_{-D}(\zeta) = g_D(\zeta)^\tau\ , \qquad g_{D^*}(\zeta) = -g_D(\zeta)\ .
$$

Besides the generating polynomial $g_D(x) = g(x)$, it is sometimes useful to consider the *d-generating polynomial* $g_d(x)$ for a divisor d of v. This is, by definition, the generating polynomial $g(x)$ reduced $(\mathrm{mod}\ 1 - x^d)$, or

$$
g_d(x) \equiv \sum_{i=0}^{d-1} C(i)x^i \quad (\mathrm{mod}\ 1 - x^d)\ ,
$$

where $C(i)$ is the number of elements a_j of the set D satisfying $a_j = i \ (\mathrm{mod}\ d)$. It is to be noted that

$$
(7)\qquad 0 \leqq C(i) \leqq \frac{v}{d}
$$

for all i. The congruences (5) are true when $g(x)$ are replaced by d-generating polynomials, and the modulus by $1 - x^d$. Similarly the equations (6) remain true when $g(x)$ are replaced by d-generating polynomials, for any dth root of unity $\zeta \neq 1$.

3. Decomposition field of a difference set. Let p be a prime, $\mathfrak{p}$ be any prime ideal divisor of p in $Q(\zeta_v)/Q$. Then the set of all automorphisms θ of $Q(\zeta_v)/Q$ satisfying $\mathfrak{p}^\theta = \mathfrak{p}$ constitutes the decomposition group $\mathfrak{Z}_\mathfrak{p}$ of $\mathfrak{p}$. Because $Q(\zeta_v)/Q$ is an abelian extension, the group $\mathfrak{Z}_\mathfrak{p}$ is the same for all $\mathfrak{p}$, called the *decomposition group* of p in $Q(\zeta^v)/Q$, and denoted by $\mathfrak{Z}_p$. It is generated by the set of all Frobenius automorphisms $F = (\zeta_{v'} \to \zeta_{v'}^p)$ where $v = p^l v' \ (v', p) = 1$, the effect of F on ζ_{p^l} being arbitrary. The subfield K_p corresponding to $\mathfrak{Z}_p$ is called the *decomposition field* of p in $Q(\zeta_v)/Q$. If d is a divisor of v, then it is known that the decomposition field of p in $Q(\zeta_d)/Q$ is equal to the intersection $K_p \cap Q(\zeta_d)$.

If D is a (v, k, λ)-difference set, then the intersection $\mathfrak{Z}$ of all decomposition groups $\mathfrak{Z}_p$ in $Q(\zeta_v)/Q$ with $p \mid n$ will be called the *decomposition group* of the difference set D, the subfield of $Q(\zeta_v)/Q$ corresponding to it the *decomposition field* of D. Note that these concepts

are completely determined by the parameters v and n, so are the same for all difference sets similar to D, and also for D^*.

THEOREM 2. *Assume that there exists a (v, k, λ)-difference set D. Let p be a prime divisor of n, d be a divisor of v such that $d \neq 1$, $(p, d) = 1$ and that the decomposition field of p in $Q(\zeta_d)/Q$ is real. Then the exponent of the p-component of n is even.*

Proof. The complex conjugation τ of $Q(\zeta_d)/Q$ belongs to the decompostion group $\mathfrak{Z}_p$ of p by assumption. Namely $\mathfrak{p}^\tau = \mathfrak{p}$ for all prime ideal divisors $\mathfrak{p}$ of p. This means that $g(\zeta_d)$ and $g(\zeta_d)^\tau$ have the same $\mathfrak{p}$-component for all these prime ideal divisors $\mathfrak{p}$ of p, and so they have the same p-component, say $\mathfrak{b}$. Since $d \neq 1$ it follows from (1) that the p-component p^e of n is $= \mathfrak{b}^{1+\tau} = \mathfrak{b}^2$. Therefore $\mathfrak{b}$ is divisible by all the prime ideal divisors $\mathfrak{p}$ of p with the same exponent. But because p is unramified in $Q(\zeta_d)/Q$, $\mathfrak{b}$ is a power of (p) and e is even.

COROLLARY 1. *If there exists a (v, k, λ)-difference set with real decomposition field, then n must be a square.*

Proof. The decomposition group $\mathfrak{Z}_p$ of p in $Q(\zeta_d)/Q$ contains the complex conjugation τ for all prime divisors p of n and for all divisors d of v. Thus if v has a divisor d such that $(d, p) = 1$, $d \neq 1$, then it follows from Theorem 2 that the p-component of n is a square. If on the contrary v is a power of p, say p^l, then from (2) or $(p^l - 1)n = k(p^l - k)$ follows that k is divisible by p. Therefore if p^m is the p-component of k, then $l > m$ and both k and $p^l - k$ have the same p-component p^m, so the p-component of n is p^{2m}.

REMARK. The condition in the hypothesis of Theorem 2 is that p is a prime divisor of n, d a divisor of v such that $d \neq 1$, and that there exists an exponent h such that $p^h \equiv -1 \pmod{d}$.

COROLLARY 2. *Assume that there exists a (v, k, λ)-difference set. Define for an odd integer q, $q^* = (-1)^{(q-1)/2}q$. If p is a prime, p^e the p-component of n, and if q is an odd divisor of v, then*

$$\chi(r) = \left(\frac{p^e, q^*}{r}\right) = 1$$

for all rational prime spots r, the symbol being the Hilbert norm residue symbol. Or, then there exists a nonzero solution for the Diophantine equation

$$p^e x^2 + (-1)^{(q-1)/2} q y^2 = z^2 .$$

Proof. Because of the relation $(q_1 q_2)^* = q_1^* q_2^*$ for odd integers q_1, q_2, and of the bihomomorphic property of the Hilbert residue symbol, we can assume that q is an odd prime divisor of v. The symbol $\chi(r) = 1$ except possibly $r = p_\infty$ (the rational infinite spot), $r = 2$, $r = p$ and $r = q$. Now $\chi(p_\infty) = 1$ since $p > 0$. Moreover $\chi(q) = 1$ or $= (p/q)$ with the Legendre symbol according as $p = q$ or not. The Legendre symbol represents -1 only for p which is a quadratic nonresidue of q. But in this case $p^{(q-1)/2} \equiv -1 \pmod q$ and e must be even by Theorem 2. We have seen that $\chi(p_\infty) = \chi(q) = 1$. Now if $p = 2$, then we have $\chi(2) = 1$ by the product formula of the Hilbert symbol. If $p \neq 2$, then we have $\chi(2) = 1$ since $q^* \equiv 1 \pmod 4$. So we have (in case $p \neq q$) that $\chi(p) = 1$ by the product formula.

THEOREM 3. (1) *Under the same assumptions as Theorem 2, let furthermore p^e and p^l be the p-components of n and v. Then we have $p^{e/2} \leqq (v/d)p^{-l}$.*

(2) *Assume that there exists a (v, k, λ)-difference set. Let p be a prime divisor of n, p^e and p^l be the p-components of n and v. If e is even, then we have $p^{e/2} \leqq vp^{-1}$.*

Proof. Put $w = dp^l$ in (1) and put $w = p^l$ in (2). Denote the generating polynomial of D by $g(x)$. Then the decomposition group of p in $Q(\zeta_w)/Q$ contains the complex conjugation τ of $Q(\zeta_w)/Q$, because the restriction of τ in $Q(\zeta_d)/Q$ is a power of the Frobenius automorphism F of $Q(\zeta_d)/Q$, as was shown in Proof of Theorem 2. This means that any prime ideal divisor $\mathfrak{p}$ of p in $Q(\zeta_w)/Q$ is invariant under τ, and the p-component $\mathfrak{b}$ of $g(\zeta_w)$, being invariant under τ, satisfies $(p^e) = \mathfrak{b}^{1+\tau} = \mathfrak{b}^2$ as seen from (1). It follows from Theorem 2 that e is even under assumption of 1), and e is assumed even for (2). This implies in particular that $g(\zeta_w) \equiv 0 \pmod{p^{e/2}}$. The same is true for all divisors $r \neq 1$ of w, because the decomposition group of p in $Q(\zeta_r)/Q$ contains the complex conjugation. We have seen that $g(\zeta) \equiv 0 \pmod{p^{e/2}}$ for all wth roots of unity $\zeta \neq 1$.

On the other hand $g(1) = k$ is not necessarily divisible by $p^{e/2}$. But we see from (2) that $k(v - k) \equiv 0 \pmod{p^e}$, or at least one of the two numbers $g_D(1) = k$ and $g_{D^*}(1) = v - k$ is $\equiv 0 \pmod{p^{e/2}}$. Thus, by replacing D by D^* if necessary, we can assume that $g(\zeta) \equiv 0 \pmod{p^{e/2}}$ for all wth roots of unity ζ.

Consider the w-generating polynomial $g_w(x) = \sum_{i=0}^{w-1} C(i)x^i$ of D. Since $g_w(\zeta) = g(\zeta) \equiv 0 \pmod{p^{e/2}}$ for all wth roots of unity ζ, we can apply Theorem 1. Thus we conclude, if $d = q_1^{t_1} \cdots q_r^{t_r}$ is the prime-power decomposition of d in (1) that

$$q_1^{t_1} \cdots q_r^{t_r} \Delta(wq_1^{-t_1-1}) \cdots \Delta(wq_r^{-t_r-1}) \Delta(wp^{-1}) C(i) \equiv 0 \pmod{p^{e/2}} .$$

Because $(d, p) = 1$ and because $\Delta(wq_j^{-t_j-1})$ for $j = 1, \cdots, r$ are all identity operators, we have $\Delta(wp^{-1})C(i) \equiv 0 \pmod{p^{e/2}}$ for all i. In the case (2) the last congruence follows immediately from Theorem 1.

Now I assert that there is an i such that $\Delta(wp^{-1})C(i) \neq 0$. Indeed, if $\Delta(wp^{-1})C(i) = 0$ for all i, then we would have

$$\Delta(wq_1^{-1}) \cdots \Delta(wq_r^{-1}) \Delta(wp^{-1}) C(i) = 0$$

for all i, which implies, again by Theorem 1 (by taking $\alpha = 0$), that $g_w(\zeta_w) = g(\zeta_w) = 0$, and $n = 0$ by (1), a contradiction. This applies to the case (1), and the same argument is applies to the case (2).

We have seen that $C(i + wp^{-1}) - C(i) \equiv 0 \pmod{p^{e/2}}$, but $\neq 0$ for some i. Then it follows from (7) that

$$p^{e/2} \leqq | C(i + wp^{-1}) - C(i) | \leqq \frac{v}{w} = \frac{v}{d} p^{-l}$$

for the case (1), and we have only to take $d = 1$ in the above for the case (2).

COROLLARY. *The decomposition field of a nontrivial difference set cannot be real.*

Proof. This follows immediately from Corollary 1 to Theorem 2 and the assertion (2) of Theorem 3.

Similarly it is proved that if there exists a (v, k, λ)-difference set, d is a divisor $\neq 1$ of v, $p_1, \cdots, p_s$ are distinct prime divisors of n such that $p_j \nmid d$ and that the decomposition fields of p_j in $Q(\zeta_d)/Q$ are real, then $p_1^{e/2} \cdots p_s^{es/2} \leqq v/d$, where $p_j^{e_j}$ are the p_j-components of n.

EXAMPLE. There does not exist a difference set for which both v and n are powers of the same prime. For instance (16, 6, 2)-, (64, 28, 12)- and (256, 120, 56)-difference sets.

REMARK. If a and m are relatively prime integers $\neq 0$, then the *order* of $a \pmod m$ is the smallest positive integer z such that $a^z \equiv 1 \pmod m$, and is denoted by $z = \mathrm{ord}_m a$. Theorem 2 implies in particular that if there exists a (v, k, λ)-difference set, and if q is an odd prime divisor of v, p is a prime such that $\mathrm{ord}_q p$ is even, then p is contained in n with an even exponent. The same is true if $4 | v$ and if $\mathrm{ord}_4 p = 2$ or $p \equiv -1 \pmod 4$. The criterion is useful for smaller v's since we can use the tables in [4] for $\mathrm{ord}_q p$, $q < 1000$. The assertion (1) of Theorem 3 may be stated as: If there exists a (v, k, λ)-difference

set, $d \neq 1$ a divisor of v, and if p is a prime such that $p^h \equiv -1 \pmod{d}$ for some h, then $p^{e/2} \leqq (v/d)p^{-l}$, where p^e and p^l are the p-components of n and v.

Hall [2] listed 12 choices of (v, k, λ) such that $3 \leqq k \leqq 50$, $k < v/2$, for which the existence of corresponding difference sets had not been decided by the method of multipliers. For all of these Theorem 3 establishes the non-existence very simply.

4. Difference sets with imaginary quadratic decomposition fields. In view of Theorem 3 and its Corollary, it would be a natural step to consider next those difference sets whose decomposition fields may be imaginary quadratic.

THEOREM 4. *Let q be a prime divisor of v such that $q \equiv -1 \pmod{4}$, q^l be the q-component of v. Assume that any prime divisor p of n satisfies*

(i) $\operatorname{ord}_q p \equiv 0 \pmod{2}$,

(ii) $\operatorname{ord}_{q^l} p = \frac{1}{2} q^{l-1}(q-1)$, *or*

(iii) $p = q$.

If there exists a (v, k, λ)-difference set D, then the Diophantine equation

$$4n = x^2 + qy^2, \quad 0 \leqq x, \quad 0 \leqq y \leqq \frac{v}{q^l}, \quad x + y \leqq \frac{2v}{q^l}$$

has a solution.

Proof. Denote by σ a generator of the Galois group of $Q(\zeta_{q^l})/Q$, and by $g(x)$ the generating polynomial of D. Denote the p-component of $g(\zeta_{q^l})$ by $\mathfrak{b}_p$. If p satisfies (i), then it follows from Theorem 2 and Remark to it that $\mathfrak{b}_p$ is rational, $\mathfrak{b}_p = (p)^e$ for some positive integer e. If p satisfies (ii), then p is decomposed into a product of two different prime ideal divisors $\mathfrak{p}, \mathfrak{p}^\tau$ in $Q(\zeta_{q^l})/Q$, and the decomposition group of p in $Q(\zeta_{q^l})/Q$ is equal to $\{\sigma^2\}$. Thus σ^2 leaves $\mathfrak{p}$ and $\mathfrak{p}^\tau$ fixed, and so $\mathfrak{b}_p$ fixed. The last statement is true for the case (iii), too.

Summarizing we have that $\mathfrak{b}_p^{\sigma^2} = \mathfrak{b}_p$ for all prime divisors p of n. This means that if we put $\gamma = g(\zeta_{q^l})$ then $(\gamma)^{\sigma^2} = (\gamma)$, or $\gamma^{1-\sigma^2} = \eta$ is a unit of $Q(\zeta_{q^l})$. We have $\eta^{1+\tau} = \gamma^{(1-\sigma^2)(1+\tau)} = \gamma^{(1+\tau)(1-\sigma^2)} = n^{1-\sigma^2} = 1$, or $|\eta| = 1$. Because $Q(\zeta_{q^l})/Q$ is totally imaginary and abelian, this implies that η is a root of unity in $Q(\zeta_{q^l})$, or $\eta = \varepsilon\zeta_{q^l}^j$ for some j, where $\varepsilon = 1$ or $= -1$.

Now I assert that $\varepsilon = 1$. Indeed if we put $N = q^{l-1}(q-1)$ then

$$1 = \eta^{1+\sigma^2+\cdots+\sigma^{N-2}} = \varepsilon^{N-2}\zeta_{q^l}^{j(1+\sigma^2+\cdots+\sigma^{N-2})}$$

shows firstly that $\varepsilon^{N/2} = \varepsilon$ since $\frac{1}{2}N$ is odd, and secondly that ε is a q^lth root of unity, therefore $\varepsilon = 1$. Moreover if $\zeta_{q^l}^\sigma = \zeta_{q^l}^s$ for an

integer s, then the above shows also that $(1-s^N),/(1-s^2)\,j \equiv 0 \pmod{q^l}$. This implies that there is an integer u such that $-j \equiv (1-s^2)u \pmod{q^l}$. In fact $1-s^2 \not\equiv 0 \pmod{q}$ if $q \neq 3$, and if $q=3$ then the 3-component of $1-s^2$ and $1-s^N$ are 3 and 3^l respectively, so $j \equiv 0 \pmod 3$ and there is an integer u such that $-j \equiv (1-s^2)u \pmod{3^l}$.

Replace the difference set D by $D+u$. Then $\eta = (g(\zeta_{q^l}))^{1-\sigma^2}$ is replaced by $(\zeta_{q^l}^u g(\zeta_{q^l}))^{1-\sigma^2} = \zeta_{q^l}^{u(1-\sigma^2)}\eta = \zeta_{q^l}^{(1-s^2)u+j} = 1$. Namely we can assume that $g(\zeta_{q^l})^{\sigma^2} = g(\zeta_{q^l})$, by replacing D by $D+u$ if necessary. Then $g(\zeta_{q^l}) = \gamma$ is an integer of the quadratic subfield $Q(\sqrt{-q})$ of $Q(\zeta_{q^l})$ and $n = \gamma^{1+\tau}$ is the norm of an integer γ of $Q(\sqrt{-q})$.

More precisely there exist integers a, b such that $\gamma = a + b\omega$, where $\omega = (-1+\sqrt{-q})/2$, so we have $4n = (2a-b)^2 + qb^2$. Note that $g_{D^*}(\zeta_{q^l}) = -a - b\omega$, $g_{-D}(\zeta_{q^l}) = a + b\omega^\tau = a - b - b\omega$, $g_{-D^*}(\zeta_{q^l}) = -a + b + b\omega$, as seen from (6). Thus we can assume $a \geqq 0$ and $b \geqq 0$, by replacing D by D^*, $-D$, or $-D^*$ if necessary. We know that ω is a Gauss's sum

$$\omega = \sum_{i=1}^{q-1} \psi(i)\zeta_q^i = \pm \sum_{i=1}^{q-1} \psi(i)\zeta_{q^l}^{q^{l-1}i} .$$

where $\psi(i) = 1$ or 0 according as i is a quadratic residue or nonresidue of q, ζ_q is a suitably chosen primitive qth root of unity, and the sign $\pm$ is that of (j/q) for the j such that $\zeta_{q^l}^{q^{l-1}} = \zeta_q^j$. If $g_{q^l}(x) = \sum_{i=0}^{q^l-1} C(i)x^i$ is the q^l-generating polynomial of D, then $g_{q^l}(x) - (a \pm b\sum_{i=1}^{q-1}\psi(i)x^{q^{l-1}i})$ has a zero point $x = \zeta_{q^l}$, so applying Theorem 1 (by taking $\alpha = 0$), we obtain

$$C(0) - a = C(q^{l-1}i) \mp b\psi(i) \qquad (i = 1, \cdots, q-1) .$$

In particular $C(0) - a = C(q^{l-1}) \mp b = C(-q^{l-1})$. Comparing this with (7) we find $a \leqq vq^{-l}$, $b \leqq vq^{-l}$. Note that a similar treatment on $g_{-D^*}(\zeta_{q^l}) = -a + b + b\omega$ yields $|a-b| \leqq vq^{-l}$. The Theorem is now proved by taking $x = |2a-b|$, $y = b$.

REMARK. The condition (ii) in Theorem 4 is the same as $\mathrm{ord}_q\, p = \frac{1}{2}(q-1)$ if $p^{q-1} \not\equiv 1 \pmod{q^2}$.

COROLLARY. *If $v = q^l$, q being a prime with $q \equiv -1 \pmod 4$, and if any prime divisor p of n has an even order or the order $\frac{1}{2}(q-1) \pmod q$, $p^{q-1} \not\equiv 1 \pmod{q^2}$, then a nontrivial (v, k, λ)-difference set exists only if $l = 1$, $q > 3$, i.e., $v = q > 3$. In this case there are exactly two difference sets with the parameters $v = q$, $n = \frac{1}{4}(q+1)$, namely the set of all quadratic residues of q, and its residual set, in the sense of similarity.*

Proof. The Diophantine equation $4n = x^2 + qy^2$, $0 \leqq x$, $0 \leqq y \leqq 1$,

$x + y \leqq 2$ has only one solution $x = y = 1$, and $n = \frac{1}{4}(q + 1)$. Then $q > 3$ from $n > 1$. From (4) follows that $q^l = v \leqq n^2 + n + 1 = 1/16 (q^2 + 6q + 23) < q^2$, or $l = 1$. Also if $g(\zeta_q) = a + b\omega$ as in Proof of Theorem 4, then there are four possibilities for a, b, of which we have only to consider the case $a = 0$, $b = \pm 1$ such that we would have $g(\zeta_q) = \pm\omega = \sum_{i=1}^{q-1} \psi(i)\zeta_q^i$. Then $C(0) = C(i) - \psi(i)$ for $i = 1, \cdots, q - 1$ or $C(0) = 0$, $C(i) = \psi(i)$, since $C(i)$ and $\psi(i)$ are non-negative. Thus D is the set of all quadratic residues of q, and any difference set with the parameters $v = q$, $n = \frac{1}{4}(q + 1)$ is similar either to D or to D^*.

In the following two Theorems, n is necessarily a square.

THEOREM 5. *Let q and r be distinct prime divisors of v, q^l and r^m be the q-components and r-components of v respectively, and let $q \equiv -1 \pmod 4$, $(\varphi(q^l), \varphi(r^m)) = 2$. Assume that any prime divisor p of n satisfies one of the conditions*:

(i) $\operatorname{ord}_q p \equiv 0 \pmod 2$ *and* $\operatorname{ord}_r p \equiv 0 \pmod 2$, $\not\equiv 0 \pmod 4$,

(ii) $\operatorname{ord}_{q^l} p = \frac{1}{2}\varphi(q^l)$ *and* $\operatorname{ord}_{r^m} p = \varphi(r^m)$,

(iii) $p = q$ *and* $\operatorname{ord}_{r^m} p = \varphi(r^m)$.

If there exists a (v, k, λ)-difference set D, then there is a solution for the Diophantine equation

$$4n = x^2 + qy^2, \quad 0 \leqq x, \quad 0 \leqq y \leqq \frac{2v}{q^l r^m}, \quad x + y \leqq \frac{4v}{q^l r^m}.$$

Proof. (1) Denote the generating polynonial of D by $g(x)$ and put $w = q^l r^m$. Then $Q(\zeta_w)/Q$ is the direct composite of $Q(\zeta_{q^l})$ and $Q(\zeta_{r^m})$ over Q, and the Galois group of $Q(\zeta_w)/Q$ is generated by two automorphisms σ and ρ such that σ is a generator of the Galois group of $Q(\zeta_{q^l})/Q$ acting as an identity on $Q(\zeta_{r^m})$, and ρ is a generator of the Galois group of $Q(\zeta_{r^m})/Q$ acting as an identity on $Q(\zeta_{q^l})$. Now if p satisfies (i), then $p^z \equiv -1 \pmod w$ for some z, and the p-component $\mathfrak{b}_p$ of $g(\zeta_w)$ is rational by Theorem 2. If p satisfies (ii), then $\operatorname{ord}_w p$ is the LCM of $\operatorname{ord}_{q^l} p$ and $\operatorname{ord}_{r^m} p$, which is $= \frac{1}{2}\varphi(w)$ by assumption. The decomposition field of p in $Q(\zeta_w)/Q$ is the quadratic field $Q(\sqrt{-q})$. This means that any prime ideal divisor $\mathfrak{p}$ of p in $Q(\zeta_w)$ is originated in $Q(\sqrt{-q})$. Finally if p satisfies (iii), then $p = q = \mathfrak{q}^{\varphi(q^l)}$ in $Q(\zeta_w)/Q$ for the prime ideal divisor $\mathfrak{q}$ of q in $Q(\zeta_w)/Q$. The q-component $\mathfrak{b}_q$ of $g(\zeta_w)$ is rational, since it is a power of $\mathfrak{q}$ and the q-component of n is a square by Theorem 2.

(2) Summarizing we see that for any prime divisor p of n, $\mathfrak{b}_p$ is an ideal originated in $Q(\sqrt{-q})$, and so is the ideal $(g(\zeta_w))$. If we put $\gamma = g(\zeta_w)$ then $\gamma^{1-\sigma^2} = \eta$ and $\gamma^{1-\rho} = \theta$ are units of $Q(\zeta_w)$. Then $\eta^{1+\tau} = \theta^{1+\tau} = 1$, or η and θ are roots of unity in $Q(\zeta_w)$, just as in Proof of

Theorem 4. Hence η^{1-p} is a q^lth root of unity and $\theta^{1-\sigma^2}$ is an r^mth root of unity. But both are $=\gamma^{(1-\sigma^2)(1-\rho)}$, and we see that $\eta^{1-\rho} = \theta^{1-\sigma^2} = 1$, or that η is a root of unity in $Q(\zeta_{q^l})$ and θ is a root of unity in the subfield K fixed by σ^2. K is the composite of $Q(\zeta_{r^m})$ and $Q(\sqrt{-q})$, of absolute degree $2\varphi(r^m)$, and θ is a root of unity in $Q(\zeta_{r^m})$ except for the case $q = 3$; θ if $q = 3$, may be a $6r^m$th root of unity. We have seen that $\eta = \varepsilon\zeta_{q^l}^i$, $\theta = \varepsilon'\zeta_{r^m}^g$ (for $q \neq 3$) or $\theta = \varepsilon'\zeta_{r^m}^j\zeta_3^a$ (for $q = 3$), where i, j, a are integers and $\varepsilon, \varepsilon'$ are either 1 or -1. Just as in Proof of Theorem 4, we verify that $\varepsilon = 1$, and that by replacing D by $D + ur^m$ for some u if necessary, we can assume $\eta = 1$. This process does not affect θ, and again by replacing D by $D + u'q^l$ for some u' if necessary, we can assume also that $\theta = \varepsilon'$ (for $q \neq 3$) or $\theta = \varepsilon'\zeta_3^a$ (for $q = 3$).

(3) First consider $q \neq 3$. I assert that $\varepsilon' = 1$. Indeed from $\gamma^{1-\sigma^2} = 1$, $\gamma^{1-\rho} = \varepsilon' = \pm 1$ follows that γ^2 belongs to $Q(\sqrt{-q})$. If we put $\mathfrak{O} = Z[\zeta_w]$, $\mathfrak{o} = Z[\omega]$, $\omega = (-1 + \sqrt{-q})/2$, then $\gamma\mathfrak{O} = \mathfrak{c}\mathfrak{O}$ for some ideal $\mathfrak{c}$ of $\mathfrak{o}$, since $\gamma\mathfrak{O}$ was originated in $Q(\sqrt{-q})$. On the other hand $\gamma^2 \in \mathfrak{o}$ and so $\mathfrak{c}^2 = \gamma^2\mathfrak{o}$ is a principal ideal of $\mathfrak{o}$, which implies that $\mathfrak{c}$ itself is principal, because the class number of $Q(\sqrt{-q})$, an imaginary quadratic field of a prime discriminant, is odd. Thus if $\mathfrak{c} = \gamma_0\mathfrak{o}$, $\gamma_0 \in \mathfrak{o}$, then $\gamma^2 = \gamma_0^2\eta_0$ for a unit η_0 of $Q(\sqrt{-q})$. Such a unit must be ± 1. But $\eta_0 = -1$ is screened out, since otherwise $\gamma\gamma_0^{-1} = \sqrt{-1}$ belongs to $Q(\zeta_w)$, which is impossible. So $\eta_0 = 1$ and $\gamma = \pm\gamma_0$ belongs to $Q(\sqrt{-q})$.

(4) Next let $q = 3$. Then γ^2 satisfies $\gamma^{2(1-\sigma^2)} = 1$, $\gamma^{2(1-\rho)} = \zeta_3^{2a}$. I assert first that $a \equiv 0 \pmod 3$. Indeed otherwise γ^2 determines a subfield K over $Q(\sqrt{-q})$ of degree 3. Note that this is possible only for $r \equiv 1 \pmod 3$. Moreover K is uniquely determined as the subfield of $Q(\zeta_w)/Q(\zeta_3)$ of relative degree 3. A relative basis of integers of K with respect to $Z[\zeta_3]$ is furnished by the three integers $\xi, \xi^\rho, \xi^{\rho^2}$ where $\xi = \sum_{i=0}^{(1/3)(r-1)-1} \zeta_r^{\rho^{3i}}$. The condition $(\gamma^2)^{1-\rho} = \zeta_3^{-a}$ implies that γ^2 has the form $\gamma^2 = \alpha_0(\xi + \zeta_3^a\xi^\sigma + \zeta_3^{2a}\xi^{\sigma^2}) = \alpha_0\Lambda$, $\alpha_0 \in Z[\zeta_3]$, where $\Lambda = \xi + \zeta_3^a\xi^\sigma + \zeta_3^{2a}\xi^{\sigma^2}$ is the Lagrange resolvent of $Q(\zeta_{3r})/Q(\zeta_3)$. It is known that $\Lambda^{1+\tau} = r$. Thus we would have $n^2 = \gamma^{2(1+\tau)} = \alpha_0^{1+\tau}r$, which is impossible because $(n, r) = 1$ was assumed in (i), (ii), (iii).

We have seen that γ^2 belongs to $Q(\sqrt{-3})$. But in fact γ itself belongs to $Q(\sqrt{-3})$. Indeed if we put $\mathfrak{o} = Z[\zeta_3]$, $\mathfrak{O} = Z[\zeta_w]$, then we know in (2) that $\gamma\mathfrak{O} = \mathfrak{c}\mathfrak{O}$ for some ideal $\mathfrak{c}$ of $\mathfrak{o}$. But $\mathfrak{c}$ is a principal ideal because the class number of $Q(\sqrt{-3})$ is 1. Thus we have $\gamma\mathfrak{O} = \gamma_0\mathfrak{O}$ for $\gamma_0 \in \mathfrak{o}$. On the other hand $\gamma^2 \in \mathfrak{o}$, and $\gamma^2 = \gamma_0^2\eta_0$ for some unit η_0 of $\mathfrak{o}$. η_0 is a 6th root of unity, and $\eta_0^{1/2} = \gamma\gamma_0^{-1}$ is a root of unity in $Q(\zeta_w)$. This is possible only when η_0 is a third root of unity. This means that $\gamma = \eta_0^{1/2}\gamma_0 \in Q(\sqrt{-3})$.

(5) We have seen that $\gamma = g(\zeta_w)$ is an integer of $Q(\sqrt{-q})$. If $\gamma = a + b\omega$, where $\omega = (-1 + \sqrt{-q})/2$ is the Gauss's sum, and if $g_w(x) = \sum_{i=0}^{w-1} C(i)x^i$ then the polynomial $g_w(x) - (a \pm b \sum_{i=1}^{q-1} \psi(i)x^{q^{l-1}r^m i})$ where $\psi(i) = \frac{1}{2}((i/q) + 1)$ has a zero point $x = \zeta_w$, and it follows from Theorem 1 that

$$C(0) - a - C(q^{l-1}r^m i) \mp b\psi(i) = C(q^l r^{m-1} j) - C(q^l r^{m-1} j + q^{l-1} r^m i)$$

for $i = 1, \cdots, q-1; j = 1, \cdots, r-1$. By comparing with (7) we see that $|a| \leqq 2v/w$, $|b| \leqq 2v/w$, and also $|a - b| \leqq 2v/w$ by a similar consideration on $-D$. Thus we have $4n = 4\gamma^{1+\tau} = x^2 + qy^2$, $0 \leqq x$, $0 \leqq y \leqq 2v/w$, $x + y \leqq 4v/w$ for $x = |2a - b|$, $y = |b|$.

COROLLARY. *If in particular* $v = q^l r^m$ *in Theorem* 5, *then we have only one possibility* $v = 21$, $n = 4$. D *is similar to* $\{1, 2, 4, 7, 14\}$ *or its residual set.*

Proof. If we consider that n is a square $\geqq 4$, the Diophantine equation in Theorem 5 implies $x = 3$, $y = 1$, $n = 4$, $q = 7$, $v = 21$. We may assume $a = -1$, $b = 1$ in Proof of Theorem 5 above. Thus $g(\zeta_{21}) = \gamma = -1 + \omega = -1 + \zeta_7 + \zeta_7^2 + \zeta_7^4$, from which it follows that $D = \{1, 2, 4, 7, 14\}$.

THEOREM 6. *Let* q *and* r *be prime divisors of* v *such that* $q \equiv -1 \pmod 4$, $r \equiv 1 \pmod 4$, $(q/r) = -1$ *and that* $(\varphi(q^l), \varphi(r^m)) = 2$ *for the* q*-component* q^l *and the* r*-component* r^m *of* v. *Assume that any prime divisor* p *of* n *satisfies either* (i) $\operatorname{ord}_q p \equiv 0 \pmod 2$ *and* $\operatorname{ord}_r p = 0 \pmod 2$, $\not\equiv 0 \pmod 4$, *or* (ii) $\operatorname{ord}_{q^l} p = \varphi(q^l)$ *and* $\operatorname{ord}_{r^m} p = \varphi(r^m)$. *Then, if there exists a* (v, k, λ)*-difference set* D, *there is a solution to the Diophantine equation*

$$4n = x^2 + qry^2, \quad 0 \leqq x, \quad 0 \leqq y \leqq \frac{2v}{q^l r^m}, \quad x + y \leqq \frac{4v}{q^l r^m} - 2.$$

Proof. (1) Let $g(x)$ be the generating polynomial of D and put $w = q^l r^m$. Then the p-component $\mathfrak{b}_p$ of $g(\zeta_w)$ is rational for p satisfying (i), by Theorem 2. If p satisfies (ii) then the decomposition field of p in $Q(\zeta_w)/Q$ is $Q(\sqrt{-qr})$ by the assumption. The Galois group of $Q(\zeta_w)/Q$ is generated by σ and ρ such that σ generates the Galois group of $Q(\zeta_{q^l})/Q$ acting as an identity on $Q(\zeta_{r^m})$, and ρ generates the Galois group of $Q(\zeta_{r^m})/Q$ acting as an identity on $Q(\zeta_{q^l})$. Thus if we put $\gamma = g(\zeta_w)$, then $\eta = \gamma^{1-\sigma\rho}$ satisfies $\eta^{1+\tau} = 1$ and hence is a root of unity in $Q(\zeta_w)$. Moreover we can assume $\eta = \pm 1$ by replacing D by $D + uq^l + u'r^m$ if necessary. By the same argument as in Proofs of Theorems 4 and 5, it is easy to verify that $\gamma^{1-\sigma^2} = \gamma^{1-\rho^2} = 1$. This

means that γ^2 belongs to the subfield of $Q(\zeta_w)/Q$ fixed by $\{\sigma^2, \rho^2, \sigma\rho\}$, i.e. to $Q(\sqrt{-qr})$.

(2) I assert that γ itself belongs to $Q(\sqrt{-qr})$. Indeed otherwise $\gamma^{1-\sigma\rho} = -1$, and $\gamma = \frac{1}{2}(c\sqrt{-q} + d\sqrt{r})$ for some rational integers c, d such that $c \equiv d \pmod 2$. Then $4n = 4\gamma^{1+\tau} = qc^2 + rd^2$, which is impossible since n is a square and $(q/r) = -1$ by assumption. Now γ belongs to $Q(\sqrt{-qr})$ and $\gamma = a + b\omega$ for some a, b where $\omega = \frac{1}{2}(-1 + \sqrt{-qr})$. Note that ω is the Gauss's sum $\sum_{i=1}^{qr-1} \psi(i)\zeta_{qr}^i$ for $\psi(i) = \frac{1}{2}((i/qr) + 1)$ where (i/qr) is the Jacobi symbol, and ζ_{qr} is a suitably chosen primitive qrth root of unity. If we denote the w-generating polynomial of D by $g_w(x)$, then $g_w(x) - (a \pm b\sum_{i=1}^{qr-1} \psi(i)x^{q^{l-1}r^{m-1}i})$ has a zero point $x = \zeta_w$. We can apply Theorm 1 by taking $\alpha = 0$. Note that the coefficients of the last polynomial are not necessarily integers, and we must apply Theorem 1 to the twice of this polynomial, but the conclusion is of course the same because $\alpha = 0$. We have

$$C(0) - a - (C(q^{l-1}r^m i) - \tfrac{1}{2}) = C(q^l r^{m-1} j) - \tfrac{1}{2} - (C(q^{l-1}r^m i + q^l r^m j) \mp b\psi(ri + qj))$$

or

$$C(0) - a + 1 - C(q^{l-1}r^m i) = C(q^l r^{m-1} j) - C(q^{l-1}r^m i + q^l r^{m-1} j) \mp b\psi(ri + qj)$$

for $i = 1, \cdots, q-1$; $j = 1, \cdots, r-1$. Comparing with (7) we see that $|a - 1| \leqq 2v/w$, $|b| \leqq 2v/w$, By considering D^* we have also $|-a - 1| \leqq 2v/w$, or $|a| \leqq 2v/w - 1$. Similarly $|a - b| \leqq (2v/w) - 1$ by considering $-D$. Thus $4n = 4\gamma^{1+\tau} = x^2 + qy^2$, $x = |2a - b|$, $y = |b|$, for which $0 \leqq x$, $0 \leqq y \leqq 2v/w$, $x + y \leqq 4v/w - 2$.

COROLLARY. *If in particular $v = q^l r^m$ in Theorem 6, then q and r are twin primes, $l = m = 1$, and the difference set D is similar to the Stanson-Sprott difference set* [5], *consisting of all i such that $0 < i < qr$, $(i/qr) = 1$ and of all multiples lying between 0 and $qr - 1$ of the larger of the twin primes q, r, or to its residual set.*

Proof. (1) The only solution of the Diophantine equation in Theorem 6, for which $n > 1$ and $(n, qr) = 1$, is given by $x = y = 1$, $4n = qr + 1$. In view of the fact that n is a square, say ν^2, the above is pssible only when q and r are twin primes $q_1 = 2\nu - 1$, $r_1 = 2\nu + 1$ in some order.

Now I assert that qr is the only value of v, which is a multiple of qr and for which (3) has integral solutions. Indeed $v = 2n + \lambda + n(n-1)\lambda^{-1} \equiv 0 \pmod{q_1 r_1}$ implies that $\lambda \equiv n \pmod{q_1}$ or

$\lambda \equiv n - 1 \pmod{q_1}$, and similarly $\lambda \equiv n \pmod{r_1}$ or $\lambda \equiv n - 1 \pmod{r_1}$. Then we must have $\lambda \equiv n \pmod{q_1 r_1}$ or $\lambda \equiv n - 1 \pmod{q_1 r_1}$, i.e., $\lambda = n$ or $\lambda = n - 1$. For $\lambda \equiv n \pmod{q_1}$ and $\lambda \equiv n - 1 \pmod{r_1}$ implies that $\lambda \equiv n + \frac{1}{2}(r_1 + 1)q_1 \pmod{q_1 r_1}$ hence $\lambda > n$, and similarly $\lambda^* > n$, which is impossible since $\lambda\lambda^* = n(n-1)$. We have seen that $\lambda + \lambda^* = 2n - 1$, $v = 4n - 1 = q_1 r_1$, i.e., $l = m = 1$.

(2) Besides $x = y = 1$, we can even assume that $a = 0$, $b = \pm 1$ in Proof of Theorem 6 in such a way that $g(\zeta_v) = \pm\omega = \sum_{i=1}^{v-1} \psi(i)\zeta_v^i$, or that

$$(8) \qquad C(0) + 1 + C(r_1 i + q_1 j) - \psi(r_1 i + q_1 j) = C(r_1 i) + C(q_1 j)$$

for $i = 1, \cdots, q_1 - 1$; $j = 1, \cdots, r_1 - 1$. Define $C^*(i) = \sum_{j=0}^{r_1-1} C(i + q_1 j)$, $C_*(j) = \sum_{i=0}^{q_1-1} C(j + r_1 i)$. These are the coefficients of the q_1- and r_1-generating polynomials of D. Applying Theorem 2 we find that $(g_{q_1}(\zeta_{q_1}))$ is rational and hence $(g_{q_1}(\zeta_{q_1})) = (\nu)$ or $g_{q_1}(\zeta_{q_1}) \equiv 0 \pmod{\nu}$. By Theorem 1 it follows that $C^*(i) \equiv C^*(0) \pmod{\nu}$ for all i. Similarly $C_*(j) \equiv C_*(0) \pmod{\nu}$ for all j. By making summations of (8) over $i = 1, \cdots, q_1 - 1$ or over $j = 1, \cdots, r_1 - 1$ respectively we find that

$$\begin{aligned}(r_1 - 1)(C(0) + 1) + (C^*(r_1 i) - C(r_1 i)) - \tfrac{1}{2}(r_1 - 1) \\ = (r_1 - 1)C(r_1 i) + C^*(0) - C(0)\,, \\ (q_1 - 1)(C(0) + 1) + (C_*(q_1 j) - C(q_1 j)) - \tfrac{1}{2}(q_1 - 1) \\ = (q_1 - 1)C(q_1 j) + C_*(0) - C(0)\,.\end{aligned}$$

Recalling $r_1 - 1 \equiv 0$, $q_1 - 1 \equiv -2 \pmod{\nu}$, and $C^*(i) \equiv C^*(0)$, $C_*(j) \equiv C_*(0) \pmod{\nu}$, we have that

$$C(r_1 i) \equiv C(0) \pmod{\nu}\,, \qquad C(q_1 j) \equiv C(0) + 1 \pmod{\nu}\,,$$

from which it follows immediately that $C(0) = 0$, $C(q_1 j) = 1$, $C(r_1 i) = 0$, $C(r_1 i + q_1 j) = \psi(r_1 i + q_1 j)$ for $i = 1, \cdots, q_1 - 1$; $j = 1, \cdots, r_1 - 1$. This means that the set D consists of all i such that $(i/q_1 r_1) = 1$ and of all nonzero multiple of q_1, the smaller of the twin primes. The Stanson-Sprott difference set is precisely $-D^*$.

NUMERICAL DATA. There are 373 choices of v, n such that $2 \leqq n \leqq 50$, and that (2) has a solution. In 273 of these, Theorems 2 to 6 establish the nonexistence of the corresponding difference sets, and in 58 of these examples of the corresponding difference sets are known. The remaining 42 case are not convered by our Theorems, and in fact have decomposition fields of higher degrees than 2.

REFERENCES

1. S. Chowla and H. J. Ryser, *Combinatorial problems*, Canad. J. Math., **2** (1950), 93-99.
2. M. Hall, *A survey of difference sets*, Proc. Amer. Math. Soc., **7** (1956), 975-986.
3. D. Hilbert, *Die Theorie der algebraischer Zahlkörper*, Jahresber. Deut. Math.-Ver., **4** (1897), 175-546.
4. K. G. J. Jacobi, *Canon Arithmeticus*, Akademie-Verlag, Berlin, 1956.
5. R. G. Stanson and D. A. Sprott, *A family of difference sets*, Canad. J. Math., **10** (1958), 73-77.

UNIVERSITY OF SOUTHERN CALIFORNIA