JOURNAL OF COMBINATORIAL THEORY (A) 19, 51–65 (1975)

A Generalization of Cyclic Difference Sets I*

CLEMENT W. H. LAM

*Department of Mathematics, Statistics, and Computing Science,
University of Calgary, Calgary, Alberta, Canada*

Communicated by H. J. Ryser

Received October 1, 1974

This is the first of two papers on addition sets. In this paper, the basic properties of addition sets are given. It also contains examples of addition sets arising from natural central groupoids, (0, 1)-matrices satisfying the equation $M^2 = dI + \lambda J$ and Nth power residues. Their relationship with difference sets is also explained.

1. INTRODUCTION

A (v, k, λ)-*difference set* $D = \{d_1, ..., d_k\}$ is a collection of k residues modulo v, such that for *any* residue $\gamma \not\equiv 0 \pmod{v}$ the congruence

$$d_i - d_j \equiv \gamma \pmod{v} \tag{1.1}$$

has exactly λ solution pairs (d_i, d_j) with d_i and d_j in D.

Difference sets have been studied by many authors. I will just give the following comprehensive reference [1].

We will be mainly concerned with a generalization of the difference sets.

A (v, k, λ, g)-*addition set* $A = \{a_1, ..., a_k\}$, or simply an *addition set*, is a collection of k distinct residues modulo v, such that for any residue $\gamma \not\equiv 0 \pmod{v}$ the congruence

$$a_i + ga_j \equiv \gamma \pmod{v} \tag{1.2}$$

has exactly λ solution pairs (a_i, a_j) with a_i and a_j in A.

It is clear that when $g = v - 1$, the $(v, k, \lambda, v - 1)$-addition sets are difference sets. We sometimes write $g = -1$ instead of $g = v - 1$. It is also clear that we can restrict g to the range

$$0 \leqslant g \leqslant v - 1. \tag{1.3}$$

* This research was supported in part by the Army Research Office—Durham.

Given any positive integer v and g satisfying (1.3) there are certain obvious addition sets:

(i) the null set $A = \varnothing$;
(ii) $A = \{i\}$, where $(g + 1)\, i \equiv 0 \pmod{v}$;
(iii) $A = \{0, 1, \ldots, v - 1\}$;
(iv) $A = \{1, 2, \ldots, v - 1\}$, where $g = 0$; and
(v) $A = \{0, 1, \ldots, i - 1, i + 1, \ldots, v - 1\}$, where $(g, v) = 1$ and $(g + 1)\, i \equiv 0 \pmod{v}$.

These addition sets are said to be *trivial.* A nontrivial addition set will satisfy

$$1 < k < v - 1. \tag{1.4}$$

A simple nontrivial example is the set $\{1, 4\}$ which is a $(5, 2, 1, 2)$-addition set as well as a $(5, 2, 1, 3)$-addition set. Other examples will be given in Section 3.

It should be mentioned that the author has proved in [5] that there is no nontrivial addition set with $g = 1$.

2. Elementary Results

In this section, we will establish some elementary results about addition sets.

First of all, we will define a parameter d by letting $d + \lambda$ be the number of ways that 0 can be represented as $(a_i + ga_j)$ modulo v with a_i and a_j in the addition set A. The parameters v, k, λ, and d of an addition set satisfy some simple relations.

Theorem 2.1. *The parameters of a nontrivial addition set satisfy*

(i) $k^2 = d + \lambda v$,
(ii) $0 \leqslant d + \lambda \leqslant k$,
(iii) $0 < \lambda < k$, *and*
(iv) $-k < d < k$.

Proof. Relation (i) is established by counting. There is a total of k^2 pairs of the form (a_i, a_j). Thus (i) follows from the definitions of addition sets and the parameter d.

Relation (ii) is established by counting the number of solution pairs (a_i, a_j) in the congruence

$$a_j + ga_j \equiv 0 \pmod{v}.$$

By counting the number of solution pairs (a_i, a_j) in the congruence

$$a_i + ga_j \equiv \gamma \pmod{v},$$

where $\gamma \not\equiv 0 \pmod{v}$, we obtain

$$0 \leqslant \lambda \leqslant k. \tag{2.1}$$

Together with relation (ii), we have

$$-k \leqslant d \leqslant k. \tag{2.2}$$

In order to prove (iii) and (iv) we have to show that equality does not hold in (2.1) and (2.2).

If $d = -k$, then from (ii) we have $\lambda = k$. Substituting the values into (i) we have

$$k^2 = -k + kv. \tag{2.3}$$

Equation (2.3) implies that $k = 0$ or $k = v - 1$, contradicting the assumption that the addition set is nontrivial.

If $d = k$, then from (ii) we have $\lambda = 0$. Substituting the values into (i) we have

$$k^2 = -k. \tag{2.4}$$

Equation (2.4) implies that $k = 0$ or 1, again contradicting the assumption that the addition set is nontrivial. Hence we have established (iv).

If $\lambda = 0$, then (i) implies that

$$k^2 = d,$$

which is impossible because of (iv).

If $\lambda = k$, then (i) implies that

$$d = k(k - v). \tag{2.5}$$

Since $k - v \neq 0$, we have $k \mid d$, which is again impossible. Hence the theorem is proved.

Instead of the addition set itself, it is often convenient to deal with a polynomial derived from it.

A *Hall-polynomial* of a set A of residues modulo v is the polynomial

$$\theta(x) = x^{a_1} + \cdots + x^{a_k}, \tag{2.6}$$

where $a_i \in A$.

In terms of polynomials, the addition set property gives the following result.

THEOREM 2.2. *A set A of k distinct residues modulo v is a (v, k, λ, g)-addition set if and only if its Hall-polynomial satisfies*

$$\theta(x)\,\theta(x^g) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \qquad (\operatorname{mod} x^v - 1). \tag{2.7}$$

With the above observation, we can prove the following result.

THEOREM 2.3. *If* g.c.d. $(g, v) = w \neq 1$ *and* $d \neq 0$, *then the addition set is trivial.*

Proof. Let $\theta(x)$ be the Hall-polynomial of the addition set. Then it satisfies Eq. (2.7). Since $w \mid v$, Eq. (2.7) implies

$$\theta(x)\,\theta(x^g) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \qquad (\operatorname{mod} x^w - 1).$$

If ξ_w is any primitive wth root of unity, then this congruence gives

$$\theta(\xi_w)\,\theta(\xi_w{}^g) = d. \tag{2.8}$$

Since $w \mid g$, $\xi_w{}^g = 1$. Hence (2.8) gives

$$\theta(\xi_w) \cdot k = d. \tag{2.9}$$

Since we have assumed that $d \neq 0$, it follows from (2.9) that k divides d as integers. Because of inequality (iv) of Theorem 2.1, the last statement implies that the addition set is trivial.

COROLLARY 2.4. *Let A be a nontrivial addition set with v even. Then d is a square.*

Proof. Theorem 2.2 implies that the Hall-polynomial for A satisfies

$$\theta(x)\,\theta(x^g) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \qquad (\operatorname{mod} x^v - 1). \tag{2.10}$$

Substituting $x = -1$ into the above congruence, we have

$$\theta(-1)\,\theta((-1)^g) = d. \tag{2.11}$$

As A is nontrivial, Theorem 2.3 implies that g.c.d. $(g, v) = 1$. In particular, g is odd. Hence (2.11) implies that d is a square.

Given a set $A = \{a_1, ..., a_k\}$ mod v, then for any integer s the set $\{a_1 + s_1, ..., a_k + s\} \equiv A + s$ taken modulo v is a *shift* of A by s. It should be noted that a shift of an addition set need not be an addition set. However given an addition set $A = \{a_1, ..., a_k\}$ and any integer t, relatively prime to v, the set $\{ta_1, ..., ta_k\} \equiv tA$ taken modulo v is also an addition set with the same parameters. If t is relatively prime to v and if tA is some shift $A + s$ of the original addition set A, then t is called a ***multiplier*** of A. If $t \not\equiv 1 \pmod{v}$ then t is a nontrivial multiplier. If $tA \equiv A$ when taken modulo v, then t is a multiplier *fixing* the addition set A. Some well-known multiplier theorems for difference sets can be generalized to the case of addition sets. A proof of one will be given in [6].

The question as to whether every difference set must have a nontrivial multiplier is still open. For addition sets, there is a partial answer.

THEOREM 2.5. *Let A be a nontrivial (v, k, λ, g)-addition set with $d \neq 0$. Given any integer h prime to v, A is also a (v, k, λ, h)-addition set if and only if gh is a multiplier fixing A.*

Proof. Let us first assume that A is both a (v, k, λ, g)-addition set and a (v, k, λ, h)-addition set. By Theorem 2.2, it follows that the Hall-polynomial for A satisfies

$$\theta(x)\,\theta(x^g) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \pmod{x^v - 1}, \quad (2.12)$$

and

$$\theta(x)\,\theta(x^h) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \pmod{x^v - 1}. \quad (2.13)$$

Substituting x^h for x in (2.12), we have

$$\theta(x^h)\,\theta(x^{gh}) \equiv d + \lambda(1 + x^h + \cdots + x^{(v-1)h}) \pmod{x^{vh} - 1}. \quad (2.14)$$

Observe that $x^v - 1$ divides $x^{vh} - 1$. Furthermore, since h is prime to v, we have

$$1 + x^h + \cdots + x^{(v-1)h} \equiv 1 + x + \cdots + x^{v-1} \pmod{x^v - 1}.$$

Hence (2.14) implies

$$\theta(x^h)\,\theta(x^{gh}) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \pmod{x^v - 1}. \quad (2.15)$$

By multiplying $\theta(x)$ to both sides of (2.15), we obtain

$$\theta(x)\,\theta(x^h)\,\theta(x^{gh}) \equiv \theta(x)[d + \lambda(1 + x + \cdots + x^{v-1})] \pmod{x^v - 1}. \quad (2.16)$$

Now we use (2.13) and obtain

$$\theta(x^{gh})[d + \lambda(1 + x + \cdots + x^{v-1})] \equiv \theta(x)[d + \lambda(1 + x + \cdots + x^{v-1})] \pmod{x^v - 1}. \quad (2.17)$$

Next we expand both sides of (2.17) and cancel. Observe that

$$\theta(x^{gh})(1 + x + \cdots + x^{v-1}) \equiv k(1 + x + \cdots + x^{v-1}) \pmod{x^v - 1}.$$

A similar congruence is true for $\theta(x)$. Together with the assumption that $d \neq 0$, we have

$$\theta(x^{gh}) \equiv \theta(x) \qquad (\operatorname{mod} x^v - 1),$$

which is the same as saying that gh is a multiplier fixing the addition set A.

Conversely, we assume that gh fixes A, which is

$$\theta(x^{gh}) \equiv \theta(x) \qquad (\operatorname{mod} x^v - 1). \tag{2.18}$$

Since A is a (v, k, λ, g)-addition set, (2.12) still holds. Together with (2.18), we have

$$\theta(x^{gh})\,\theta(x^g) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \qquad (\operatorname{mod} x^v - 1). \tag{2.19}$$

Since A is nontrivial and $d \neq 0$, g is prime to v by Theorem 2.3. Hence there exists an integer f such that

$$g^f \equiv 1 \qquad (\operatorname{mod} v).$$

We substitute $x^{g^{f-1}}$ for x in (2.19) and obtain

$$\theta(x^h)\,\theta(x) \equiv d + \lambda(1 + x^{g^{f-1}} + \cdots + x^{(v-1)g^{f-1}}) \quad (\operatorname{mod} x^{vg^{f-1}} - 1). \tag{2.20}$$

However $x^v - 1$ divides $x^{vg^{f-1}} - 1$ and

$$1 + x^{g^{f-1}} + \cdots + x^{(v-1)g^{f-1}} \equiv 1 + x + \cdots + x^{v-1} \quad (\operatorname{mod} x^v - 1).$$

Thus (2.20) implies

$$\theta(x^h)\,\theta(x) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \qquad (\operatorname{mod} x^v - 1),$$

which means that A is also a (v, k, λ, h)-addition set.

The following corollary follows easily.

COROLLARY 2.6. *Let A be a nontrivial (v, k, λ, g)-addition set with $d \neq 0$. Then g^2 is a multiplier fixing A.*

Corollary 2.6 established the existence of multipliers for many addition sets. However, for difference sets, we have $g = -1$ and $g^2 \equiv 1$ (mod v), which gives us only the trivial multiplier.

In the example of Section 1, the set $A = \{1, 4\}$ has -1 as its only nontrivial multiplier. This is interesting to note because -1 is never a multiplier for a difference set [3].

Addition sets with $d \neq 0$ and $g^2 \equiv 1 \pmod{v}$ are interesting in another respect. They are closely related with a matrix equation first studied by Ryser [10].

Ryser investigated (0, 1)-matrices M of order v which satisfy the matrix equation $M^2 = D + \lambda J$, where D is a diagonal matrix and J is the matrix of all 1's. He showed that apart from certain exceptional matrices, M must satisfy

$$M^2 = dI + \lambda J, \tag{2.21}$$

where in (2.21) the matrix M has constant line sum k.

In [5], the author investigated solutions to (2.21) where M is a g-circulant. Here a *g-circulant* is a $v \times v$ matrix of rational numbers, in which each row (except the first) is obtained from the preceding row by shifting the elements cyclically g columns to the right. One can also define a Hall-polynomial for a g-circulant M by letting

$$\theta(x) = \sum_{i=0}^{v-1} m_i x^i,$$

where $(m_0, m_1, \ldots, m_{v-1})$ is the first row of M.

In particular, the following result was proved [5, p. 8].

THEOREM 2.7. *Let d and λ be rational numbers. A $v \times v$ g-circulant M satisfies* (2.21) *if and only if the following statements hold.*

(i) $d \neq 0$ *implies* $g^2 \equiv 1 \pmod{v}$, *and*

(ii) $\theta(x)\,\theta(x^g) \equiv d + \lambda(1 + x + \cdots + x^{v-1}) \pmod{x^v - 1}$.

If M is a (0, 1)-matrix, then d and λ are integers. Furthermore $\theta(x)$ is a polynomial with (0, 1) coefficients. In this case, condition (ii) of Theorem 2.7 is exactly the same as Eq. (2.7) of Theorem 2.2. Hence in the (0, 1) case, the following is true.

THEOREM 2.8. *Assume $d \neq 0$. Then the existence of a* (0, 1) *g-circulant M satisfying the matrix equation*

$$M^2 = dI + \lambda J$$

is equivalent to the existence of a (v, k, λ, g)-addition set with $g^2 \equiv 1$ $\pmod{v}$.

When $d = 0$, condition (i) of Theorem 2.7 is always true. In this case we do not even have the restriction that $g^2 \equiv 1 \pmod{v}$.

THEOREM 2.9. *The existence of a* (0, 1) *g-circulant M of size v satisfying the matrix equation*

$$M^2 = \lambda J \tag{2.22}$$

is equivalent to the existence of (v, k, λ, g)*-addition set with the same parameters.*

The (0, 1)-matrices satisfying the matrix equation

$$M^2 = J$$

correspond to central groupoids. In particular, (0, 1) g-circulants satisfying the equation correspond to natural central groupoids. For a discussion on central groupoids, please see [4].

Theorems 2.8 and 2.9 give us a few classes of addition sets, as will be seen in Section 3. Difference sets are, of course, a special class of addition sets. The following theorem shows that the value of the parameter d is important in determining whether an addition set is a difference set.

THEOREM 2.10. *Let A be a nontrivial addition set. If* $d = k - \lambda$, *then A is also a difference set.*

Proof. If $d = k - \lambda$, then 0 can be represented in k ways as $(a_i + ga_j)$ (mod v) with a_i and a_j in A. However, this implies that for all $a_i \in A$, there exists a_j in A such that

$$a_i \equiv (-g)\, a_j \qquad (\text{mod } v).$$

Thus $(-g)$ is a multiplier fixing A. By (iii) of Theorem 2.1, $k > \lambda$. Hence $d \neq 0$. As -1 is prime to v, Theorem 2.5 implies that A is also a $(v, k, \lambda, -1)$ addition set. In other words, A is a difference set.

If A is a difference set, then it is clear that $d = k - \lambda$. Thus the value of d characterizes whether or not an addition set is a difference set. From (ii) of Theorem 2.1, d satisfies

$$-\lambda \leqslant d \leqslant k - \lambda. \tag{2.23}$$

Hence, for difference sets, d attains its maximum allowed value. The case with $d = -\lambda$ also occurs as we will see in the next section.

3. EXAMPLES

In this section, we will investigate various classes of addition sets. Since difference sets are well known, we restrict our attention to addition sets which are not difference sets. That is, we are interested in addition set with d in the range.

$$-\lambda \leqslant d < k - \lambda.$$

The first class is derived from Theorem 2.9. Since they represent a slightly generalized version of natural central groupoids, we call them the Natural Central Groupoid type, or NCG type.

Natural Central Groupoid (NCG) Type

This type has parameters satisfying $k^2 = \lambda v$, $d = 0$, and $g = k$.

THEOREM 3.1. *The set $A = \{0, 1, 2,..., k - 1\}$ is a (v, k, λ, k)-addition set when $k^2 = \lambda v$.*

Proof. We will use Theorem 2.2. The Hall-polynomial for A is $\theta(x) = 1 + x + \cdots + x^{k-1}$. Observe that

$$(1 + x + \cdots + x^{k-1})(1 + x^k + \cdots + x^{k(k-1)}) = 1 + x + \cdots + x^{k^2-1}. \tag{3.1}$$

Since $k^2 = \lambda v$, Eq. (3.1) taken modulo $x^v - 1$ gives

$$\theta(x)\,\theta(x^k) \equiv \lambda(1 + x + \cdots + x^{v-1}) \qquad (\mathrm{mod}\, x^v - 1).$$

Hence the theorem is proved.

Ryser (R) Type

This type corresponds to a class of (0, 1)-matrices M satisfying

$$M^2 = I + \lambda J.$$

They were first given in [10]. The parameters satisfy $d = 1$ and $k^2 = 1 + \lambda v$.

THEOREM 3.2. *The set $A = \{0, 1,..., k - 1\}$ is a (v, k, λ, k)-addition set when $k^2 = 1 + \lambda \nu$.*

Proof. The proof is similar to the one for NCG type.

Shifted Ryser (SR) type

The parameters for this class satisfy $d = -1$, $k^2 = -1 + \lambda v$, and v odd.

THEOREM 3.3. *Let $A = \{0, 1, \ldots, k-1\}$ where $k^2 = -1 + \lambda v$ and v is odd. There exists an integer t such that $t + A$ modulo v is a (v, k, λ, k)-addition set.*

Proof. We will show that t is in fact the multiplicative inverse of $k + 1$ modulo v. First of all, we will show that $k + 1$ is relatively prime to v.

Let g.c.d. $(k + 1, v) = w$. Then we have $w \mid (k + 1)^2$. As $k^2 + 1 = \lambda v$, $w \mid k^2 + 1$. Hence $w \mid [(k + 1)^2 - (k^2 + 1)]$, which reduces to $w \mid 2k$. But v is odd. Hence w is odd. Thus we have $w \mid k$. But we also have $w \mid k + 1$. So $w = 1$. Hence, we can talk about the multiplicative inverse of $(k + 1)$ modulo v.

Let t be the multiplicative inverse of $(k + 1)$ modulo v. The Hall-polynomial for $t + A$ is

$$\theta(x) \equiv x^t(1 + x + \cdots + x^{k-1}) \qquad (\mathrm{mod}\, x^v - 1). \tag{3.2}$$

Hence

$$\theta(x)\, \theta(x^k) \equiv x^t x^{tk}(1 + x + \cdots + x^{k-1})(1 + x^k + \cdots + x^{k(k-1)}) \qquad (\mathrm{mod}\, x^v - 1). \tag{3.3}$$

Congruence (3.3) reduces to

$$\theta(x)\, \theta(x^k) \equiv -1 + \lambda(1 + x + \cdots + x^{v-1}) \qquad (\mathrm{mod}\, x^v - 1).$$

Hence the theorem is proved.

It should be noted that the condition v is odd is not restrictive at all. Since $d = -1$, Corollary 2.4 implies that any nontrivial addition set must have an odd v.

$A = \{2, 3\}$ is a $(5, 2, 1, 2)$-addition set, the first of this class. The set $\{1, 4\}$ given before is merely the set $\{2, 3\}$ multiplied by 2 and reduced modulo 5.

The remaining classes are all derived from Nth power residues modulo some prime v. So, we will first introduce some material from the theory of cyclotomy. (For a proof of some of the results quoted, please see [1] or [11].)

Let $v = Nf + 1$ be an odd prime and let α be a fixed primitive root of v. An integer R is said to belong to the *index class* l with respect to α if there exists an integer x such that

$$R \equiv \alpha^{Nx+l} \qquad (\mathrm{mod}\, v).$$

The *cyclotomic number* $(l, m)_N$ counts the number of times $R + 1$ belongs to the index class m when R belongs to index class l. That is, $(l, m)_N$ is the number of solutions x, y of the congruence

$$\alpha^{Nx+l} + 1 \equiv \alpha^{Ny+m} \qquad (\bmod\, v),$$

where the integers x, y are chosen from $0, 1,..., f - 1$.

Given an odd prime v and an integer N, the set of residues belonging to the index class 0 is called the set of Nth *power residues* modulo v. It should be noted that this set of Nth power residues does not depend on the choice of the primitive root and it forms a subgroup of the group of nonzero residues modulo v.

In 1953, Lehmer [7] gave the necessary and sufficient conditions for the existence of some difference set associated with Nth power residues. The following is a generalization of her results for addition sets.

THEOREM 3.4. *Let e be the index class to which g belongs. A necessary and sufficient condition that the* Nth *power residues of a prime $v = Nf + 1$ form a (v, k, λ, g)-addition set, is that*

$$(e, i)_N = \lambda \qquad \textit{for} \quad i = 0, 1,..., N - 1.$$

A necessary and sufficient condition that the Nth *power residues and zero for a prime $v = Nf + 1$ form a (v, k, λ, g)-addition set is that*

$$1 + (e, 0)_N = 1 + (e, e)_N = (e, i)_N = \lambda$$
$$\textit{for} \quad i = 1,..., e - 1, e + 1,..., N - 1.$$

Proof. Let $\{r_1, ..., r_f\}$ be the set of Nth power residues. Given any residue $\gamma \not\equiv 0 \pmod v$, the number of solution pairs (r_i, r_j) to the congruence

$$r_i + gr_j \equiv \gamma \qquad (\bmod\, v)$$

is the same as the number of solution pairs (r_i, r_j) to the congruence

$$1 + gr_jr_i^{-1} \equiv \gamma r_i^{-1} \quad (\bmod\, v),$$

which is also the same as the cyclotomic number $(e, i)_N$ where e is the index class to which g belongs and i is the index class to which γ belongs. Hence the Nth power residues form a (v, k, λ, g)-addition set if and only if $(e, i)_N = \lambda$ for $i = 0, 1,..., N - 1$.

When 0 is added to the set of Nth power residues the only effect is that the sums

$$r_i + g \cdot 0 = r_i \qquad \text{and} \qquad 0 + gr_i = gr_i$$

have to be counted too. Thus each r_i and gr_i is represented once more than the numbers $(e, 0)_N$ and $(e, e)_N$ indicate. Hence we have the rest of the theorem.

In this paper only the cases where $N = 2$ and $N = 4$ are considered. Hopefully, other values of N will give more addition sets.

Difference sets arising from Nth power residues are well known. In this section, we are interested in addition sets that are not difference sets. However these new addition sets are in many ways similar to their counterparts in difference sets. Together they give a much better picture of the role played by Nth power residues in the theory of addition sets. For this reason we will also quote, without proof, the corresponding results in difference sets. Before we do so, we will introduce a little more material from cyclotomy.

Theorem 3.4 established the special role played by the cyclotomic numbers. We define a *cyclotomic matrix* $C = (c_{ij})$ by letting c_{ij} be the cyclotomic number $(i, j)_N$ for the index classes i and j, where $0 \leqslant i, j \leqslant e - 1$. In terms of the cyclotomic matrix, Theorem 3.4 focuses our attention on the rows of the matrix.

Let v be an odd prime such that $v = 2f + 1$. If f is even, then the cyclotomic matrix is given in [11, p. 30] as

$$\begin{array}{c|c|c|} & 0 & 1 \\ \hline 0 & A & B \\ \hline 1 & B & B \\ \hline \end{array}\,, \qquad (3.4)$$

where $A = (f - 2)/2$ and $B = f/2$. Now we are ready to see another class of addition sets.

The next result was first communicated to me by James Shearer.

Negative Quadratic Residue (NQ) Type

THEOREM 3.5. *When $v = 4t + 1$ is a prime, the quadratic residues modulo v form an addition set with parameters $v, k, \lambda, d = 4t + 1, 2t, t, -t$ and g is any residue in the index class* 1.

Proof. When $v = 4t + 1$ is a prime, then $f = 2t$ is even. The cyclotomic matrix (3.4) implies that

$$(1, 0) = (1, 1) = t.$$

Hence if we take g to be any residue in index class 1, then Theorem 3.4 implies that the second power residues form a $(4t + 1, 2t, t, g)$-addition set. The value of d is then determined from the equation $k^2 = d + \lambda v$.

The corresponding difference set is due to Paley [9].

THEOREM 3.6 (Positive Quadratic Residue (PQ) type). *When $v = 4t - 1$ is a prime, the quadratic residues modulo v form a difference set with parameters $v, k, \lambda, d = 4t - 1, 2t - 1, t - 1, t$.*

Hence whenever v is an odd prime, the quadratic residues form an addition set. The sign of d determines whether it is a positive type or a negative type.

Let v be a prime of the form $4f + 1$. When f is even, the cyclotomic numbers are given in [11, p. 51] by the cyclotomic matrix

$$\begin{array}{c|c|c|c|c|}
 & 0 & 1 & 2 & 3 \\
\hline
0 & A & B & C & D \\
\hline
1 & B & D & E & E \\
\hline
2 & C & E & C & E \\
\hline
3 & D & E & E & B \\
\hline
\end{array} \tag{3.5}$$

together with the relations

$$\begin{aligned}
16A &= v - 11 - 6s, \\
16B &= v - 3 + 2s + 8t, \\
16C &= v - 3 + 2s, \\
16D &= v - 3 + 2s - 8t, \\
16E &= v + 1 - 2s,
\end{aligned}$$

where $v = s^2 + 4t^2$ with $s \equiv 1 \pmod 4$ is the proper representation of v; the sign of t is ambiguously determined. Here a representation $v = s^2 + 4t^2$ is said to be proper if $(v, s) = 1$. A proper representation of v with $s \equiv 1 \pmod 4$ uniquely identifies s [8, p. 123]. The value of t is also identified except for sign.

The case $N = 4$ gives us two types of addition sets.

Negative Biquadratic Residue (NB) Type

THEOREM 3.7. *The fourth power residues of a prime $v = 16t^2 + 1$ form an addition set with parameters $v, k, \lambda, d = 16t^2 + 1, 4t^2, t^2, -t^2$ and g is any residue in the index class 2.*

Proof. When $v = 16t^2 + 1$, then $s = 1$ and f is even. Hence the cyclotomic numbers C and E are equal in (3.5). Therefore $(2, 0) = (2, 1) = (2, 2) = (2, 3) = (v - 1)/16 = t^2$. Thus the theorem follows from Theorem 3.4.

The corresponding theorem in difference sets is due to Chowla [2].

THEOREM 3.8 (Positive Biquadratic Residue (PB) type). *The fourth power residues of primes $v = 4x^2 + 1$, x odd, form a difference set with parameters $v, k, \lambda, d = 4x^2 + 1, x^2, (x^2 - 1)/4, (3x^2 + 1)/4$.*

Negative Modified Biquadratic Residue (NBO) Type

THEOREM 3.9. *The set of biquadratic residues and zero of a prime $v = 16t^2 + 9$ form an addition set with parameters $v, k, \lambda, d = 16t^2 + 9, 4t^2 + 3, t^2 + 1, -t^2$ and g is any residue in the index class 2.*

Proof. When $v = 16t^2 + 9$, then $s = -1$ and f is even. Hence the cyclotomic numbers are $C = (v - 9)/16$ and $E = (v + 7)/16$. Thus

$$1 + (2, 0) = 1 + (2, 2) = (2, 1) = (2, 3) = (v + 7)/16 = t^2 + 1.$$

The theorem follows from Theorem 3.4.

The corresponding result in difference sets is attributed to M. Hall, Jr. It is for the case when $v = 4x^2 + 9$ is a prime with x odd.

The smallest addition set of the NQ (Negative Quadratic Residue) type is the (5, 2, 1, 2)-addition set given in Section 1. The smallest one of the NB (Negative Biquadratic Residue) type has parameters $v, k, \lambda, g = 17, 4, 1, 9$. The next smallest one has parameters $v, k, \lambda, g = 257, 64, 16, 9$. The smallest addition set of the NBO (Negative Modified Biquadratic Residue) type has parameters $v, k, \lambda, g = 73, 19, 5, 25$. The next one has parameters $v, k, \lambda, g = 409, 103, 26, 121$.

4. CONCLUSION

We have seen that addition sets are nontrivial generalizations of difference sets. They give rise to many new combinatorial objects. Their properties are very similar to those of the difference sets. Many results on difference sets can be generalized to the case of addition sets. In the next paper [6], we will see a generalization of the multiplier theorem and some nonexistence results. Using these results, a computer search for addition sets with small parameters was carried out. A list of these addition sets will also be given in [6].

References

1. L. D. Baumert, "Cyclic Difference Sets," Lecture Notes in Mathematics, Vol. 182, Springer-Verlag, Berlin, 1971.
2. S. Chowla, A property of biquadratic residues, *Proc. Nat. Acad. Sci. India, Sect. A* **14** (1944), 45–46.
3. E. C. Johnsen, The inverse multiplier for Abelian group difference sets, *Canad. J. Math.* **16** (1964), 787–796.
4. D. E. Knuth, Notes on central groupoids, *J. Combinatorial Theory* **8** (1970), 376–390.
5. C. W. H. Lam, Rational g-circulants satisfying the matrix equation $A^2 = dI + \lambda J$, Ph.D. Thesis, California Institute of Technology, 1974.
6. C. W. H. Lam, A Generalization of cyclic difference sets II, to appear.
7. E. Lehmer, On residue difference sets, *Canad. J. Math.* **5** (1953), 425–432.
8. I. Niven and H. S. Zuckerman, An Introduction to the Theory of Numbers, 2nd ed., Wiley, New York.
9. R. E. A. C. Paley, On orthogonal matrices, *J. Math. and Phys.* **12** (1933), 311–320.
10. H. J. Ryser, A generalization of the matrix equation $A^2 = J$, *Linear Algebra and Appl.* **3** (1970), 451–460.
11. T. Storer, "Cyclotomy and Difference Sets," Markham, Chicago, 1967.