Sum Sequences Modulo n

Fan Chung*† Jon Folkman Ron Graham*

Abstract

A sum sequence modulo n is a sequence $S = (s_1, s_2, \ldots, s_d)$ of elements in $\mathbb{Z}/n\mathbb{Z}$ such that every $x \in \mathbb{Z}/n\mathbb{Z}$ can be represented as $s_i + s_j,\ i < j$, in the same number λ of ways. For example, $(0, 1, 2, 4)$ is a sum sequence modulo 6 with $\lambda = 1$. We examine polynomials associated with sum sequences using tools from number theory, combinatorics and Galois theory. In particular, we give a complete characterization of sum sequences and their associated polynomials. We also describe some variations on these ideas and mention several possible generalizations to arbitrary finite groups.

1 Introduction

Given a finite group G of order n, an (n, d, λ) difference set is a d element subset $D \subseteq G$ such that every *non-identity* element of G can be expressed as gh^{-1} with $g, h \in D$ in exactly λ ways. Difference sets have a long and distinguished history in combinatorics and an extensive literature is available (e.g., see [9]). However there are still many fundamental questions concerning difference sets which remain unanswered. Difference sets with $\lambda = 1$ correspond to finite projective planes and even here we know relatively little. For example, it is conjectured that the order of any finite projective plane must be a prime power, and while projective planes of orders 6 and 10 have

*University of California, San Diego.

†Research supported in part by AFSOR FA9550-09-1-0090

been ruled out, the existence of a finite projective plane of order 12 is still unresolved (see [5]).

In this paper we will investigate a related concept which we call sum sequences. In the most general setting, we start with some finite group G. A sequence $S = (s_1, s_2, \ldots, s_d)$ with $s_k \in G$ for $1 \leq k \leq d$ will be called a (G, d, λ) *sum sequence* if *every* element $g \in G$ can be represented in exactly λ ways as a product $s_i s_j$ with $i < j$. Since we are going to restrict our attention in this paper to the case that G is the cyclic group $\mathbb{Z}/n\mathbb{Z}$, we will write our group operation as addition. We will usually just say that S is a (n, d, λ) sum sequence or just a sum sequence modulo n when the parameters d and λ are understood. Of course, since $\mathbb{Z}/n\mathbb{Z}$ is abelian, the order of the entries in S doesn't matter.

Here are a few examples of sum sequences:

$$(0) \pmod 1;$$
$$(0, 1, 2) \pmod 3;$$
$$(0, 1, 2, 4) \pmod 6;$$
$$(0, 0, 1, 2, 3, 4) \pmod 5;$$
$$(0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 3, 3, 3, 3, 3, 3) \pmod 4.$$

Incidentally, the last example is the smallest sum sequence modulo 4.

An outline of the paper is as follows. In the first few sections we describe some background and preliminary material. In Section 3, we recast our problem in terms of a polynomial $P^{(S)}(x) = \sum_{i=0}^{n-1} a_i x^i$ over the rational field $\mathbb{Q}$. Here, a_i is defined to be the number of indices j such that $s_j = i$. In Sections 4, 5 and 6, we characterize these polynomials. In particular, we show that S is a sum sequence modulo n if and only if $P^{(S)}(\theta)^2 = P^{(S)}(\theta^2)$ for all θ satisfying $\theta^n = 1$ with $\theta \neq 1$ (i.e., the non-unity n^{th} roots of unity). In Section 7, we describe the relationship between two related families of polynomials corresponding to the sum sequences. In Section 8, we translate our results back into polynomials over $\mathbb{Z}$ which then can be applied to our original problem of sum sequences in $\mathbb{Z}/n\mathbb{Z}$. In Section 9, we consider a variation of sum sequences in which we allow the additional sums $s_i + s_i$. Finally, in Sections 10–11 we make some concluding remarks.

We point out some related work that appears in papers of Lam [3, 6], and Isbell [2] in the late 70's. Here, an (n, d, λ, μ) *addition set* is a subset

$T = \{t_1, t_2, \ldots, t_d\} \subseteq \mathbb{Z}/n\mathbb{Z}$ such that every nonzero residue has exactly λ representations as $t_i + t_j,\ i < j$, while 0 has exactly μ such representations. These concepts were also applied to finite groups by Sumner and Butson [11, 12] around the same time. More recently, in the past few years, Coulter and Gutekunst [1] have developed these ideas even further. In particular, for a group G of order n, they call a subset $T = \{t_1, t_2, \ldots, t_d\} \subseteq G$ an (n, d, λ) *sum set* if every element of G can be expressed as a product $t_i t_j,\ i < j$, in exactly λ ways. They then derive various necessary conditions on these parameters for sum sets to exist, and give examples when they do.

The point is that in these definitions you are only allowed to form pair sums from a *subset* of the group. For our results, a sum sequence S can have many copies of the same element. This allows for a much greater variety of sum sequences, at least in the case when the group is $\mathbb{Z}/n\mathbb{Z}$, which is the only case we consider.

We should remark that this work was begun as a project of the last two authors more than 50 years ago. Unfortunately, the untimely death of Jon Folkman in 1969 (see https://en.wikipedia.org/wiki/Jon_Folkman) delayed completion of this work until now. We are pleased that we were finally able to complete it.

2 Preliminary remarks

An obvious restriction on the parameters of an (n, d, λ) sum sequence is that

$$\binom{d}{2} = \lambda n. \tag{1}$$

Thus, for $n = 4$, for example, the only values of d for which an (n, d, λ) sum sequence could exist are for $n \equiv 0$ or $1 \pmod 8$. Suppose we tried a brute force approach for determining all sum sequences $\pmod 4$. Denote the hypothesized sum sequence by $S = (0^x, 1^y, 2^z, 3^w)$, where s^t denotes t copies of the value s. Thus, the example of the sum sequence in the previous section is denoted by $(0^3, 1^4, 2^3, 3^6)$. Computing the number of times each

residue modulo 4 occurs for S, we have

$$\begin{aligned}
\binom{x}{2} + \binom{z}{2} + yw \quad &\text{for } 0 \pmod 4;\\
xy + zw \quad &\text{for } 1 \pmod 4;\\
\binom{y}{2} + \binom{w}{2} + xz \quad &\text{for } 2 \pmod 4;\\
xw + yz \quad &\text{for } 3 \pmod 4.
\end{aligned}$$

These expressions must all be equal, so subtracting the 4th expression from the 2nd, and factoring, we obtain

$$(x - z)(y - w) = 0.$$

Now (w.l.o.g) setting $z = x$, we have $x^2 - x + yw = x(y + w) = x^2 + \frac{1}{2}(y^2 - y + w^2 - w)$. Finally, eliminating w from the two equations, we obtain the quartic Diophantine equation

$$x^4 - (4y + 1)x^3 + (6y^2 + y + 2)x^2 - (4y^3 - y^2 + y)x + y^4 - y^3 = 0. \qquad (2)$$

Actually, this doesn't look like much fun to solve! In fact, not only is $(x, y) = (3, 4)$ a solution, but so is $(x, y) = (18, 21), (x, y) = (60, 66)$, and more generally, the one-parameter family $(x, y) = (\frac{1}{4}(t^4 - t^2), \frac{1}{4}(t^4 + t^2 - 2t))$ for $t \in \mathbb{Z}$. (This is not the only one-parameter family of solutions to (2)). It would appear that this method is not going to be very helpful in trying to classify all possible sum sequences modulo n for general n. So instead, we will take a different approach.

The following definitions and facts will be needed later. (These can be found in any standard text on algebraic number theory such as [7]). The nth cyclotomic polynomial, denoted by $\Phi_n(x)$, is defined by

$$\Phi_n(x) = \prod_{\substack{1 \le k \le n \\ gcd(k,n)=1}} \left(x - e^{2\pi i k/n}\right).$$

For all n, $\Phi_n(x)$ is irreducible over $\mathbb{Q}$. The degree of $\Phi_n(x)$ is just $\phi(n)$, Euler's totient function which counts the number of integers less than or equal to n and relatively prime to n.

Euler's theorem [8] states that if a and n are relatively prime then

$$a^{\phi(n)} \equiv 1 \quad mod\ n.$$

A basic fact concerning cyclotomic polynomials is the following:

$$x^n - 1 = \prod_{d|n} \prod_{\substack{1 \le k \le n \\ gcd(k,n)=d}} \left(x - e^{2\pi i k/n}\right) = \prod_{d|n} \Phi_d(x). \tag{3}$$

Here are some examples of cyclotomic polynomials.

$$\begin{aligned}
\Phi_1(x) &= x - 1, \\
\Phi_{2^n}(x) &= 1 + x^{2^{n-1}},\ n \ge 1, \\
\Phi_{p^k}(x) &= \sum_{j=0}^{p-1} x^{jp^{k-1}} \qquad \text{if } p \text{ is an odd prime}, \\
\Phi_{2^h p^k}(x) &= \sum_{j=0}^{p-1} (-1)^j x^{j2^{h-1}p^{k-1}},\ n \ge 1, k \ge 1.
\end{aligned}$$

For a prime p and $p \nmid n$,

$$\Phi_n(x^p) = \Phi_n(x)\Phi_{np}(x).$$

3 The polynomial $P^{(S)}(x)$

Suppose $n \ge 2$ and $S = (s_1, s_2, \ldots s_d)$ is a sum sequence modulo n. We now introduce a polynomial $P^{(S)}(x)$ associated with S. To do this, define a_i by

$$a_i = |\{j : s_j = i\}|. \tag{4}$$

Then define

$$P^{(S)}(x) = \sum_{i=0}^{n-1} a_i x^i. \tag{5}$$

We will usually just write $P(x)$ instead of $P^{(S)}(x)$ when the set S is clear. For example, the sum sequence $(0, 0, 0, 1, 1, 1, 1, 2, 2, 2, 3, 3, 3, 3, 3, 3)$ modulo 4

has the associated polynomial $P(x) = 6x^3+3x^2+4x+3$. If $P(x)$ corresponds to some sum sequence modulo n, we will say that $P(x)$ is *balanced* modulo n (or just *balanced* if the value of n is clear).

Observe that if $S = (s_1, s_2, \ldots, s_d)$ is a sum sequence modulo n, then so is the sequence $S + c = (s_1 + c, s_2 + c, \ldots, s_d + c)$. Hence, the corresponding *shifted* polynomial $P^{(S+c)}(x) = x^c P^{(S)}(x) \pmod{(x^n - 1)}$ is balanced modulo n.

Theorem 1 *Suppose $n \geq 2$ is an integer and $S = (s_1, s_2, \ldots, s_d)$ is a sequence of residues modulo n. Let $P(x) = \sum_{i=0}^{n-1} a_i x^i$ be the associated polynomial where a_i is the number of indices j such that $s_j = i$. Then S is a sum sequence modulo n if and only if $P(\lambda)^2 = P(\lambda^2)$ for each complex number λ satisfying $\lambda^n = 1, \lambda \neq 1$.*

Proof: Let N_k denote the number of sums congruent to $k \bmod n$. Then

$$N_k = \begin{cases} \displaystyle\sum_{\substack{0 \leq i < j \leq n-1 \\ i+j \equiv k \pmod{n}}} a_i a_j + \frac{a_{\hat{k}}(a_{\hat{k}} - 1)}{2} & \text{where } 2\hat{k} \equiv k \pmod{n} \text{ if } n \text{ is odd,} \\ \displaystyle\sum_{\substack{0 \leq i < j \leq n-1 \\ i+j \equiv k \pmod{n}}} a_i a_j & \text{if } k \text{ is odd and } n \text{ is even,} \\ \displaystyle\sum_{\substack{0 \leq i < j \leq n-1 \\ i+j \equiv k \pmod{n}}} a_i a_j + \frac{a_{k/2}(a_{k/2} - 1)}{2} + \frac{a_{k/2+n/2}(a_{k/2+n/2} - 1)}{2} & \text{if } k \text{ is even and } n \text{ is even.} \end{cases}$$

Regarding subscripts modulo n (in the remainder of this proof), we have

$$\sum_{i=0}^{n-1} a_i a_{k-i} = \begin{cases} 2N_k + a_{\hat{k}} & \text{where } 2\hat{k} \equiv k \pmod{n} \text{ if } n \text{ is odd,} \\ 2N_k & \text{if } k \text{ is odd and } n \text{ is even,} \\ 2N_k + a_{k/2} + a_{k/2+n/2} & \text{if } k \text{ is even and } n \text{ is even.} \end{cases}$$

We write

$$P(x)^2 = A(x) + x^n B(x)$$
$$P(x^2) = C(x) + x^n D(x)$$

where A, B, C, D are polynomials of degree at most $n-1$. Let

$$A(x) + B(x) = \sum_{k=0}^{n-1} b_k x^k$$
$$C(x) + D(x) = \sum_{k=0}^{n-1} c_k x^k$$

Then

$$b_k = \sum_{i=0}^{n-1} a_i a_{k-i}$$
$$c_k = \begin{cases} a_{\hat{k}} & \text{where } 2\hat{k} \equiv k \pmod{n} \text{ if } n \text{ is odd,} \\ 0 & \text{if } k \text{ is odd and } n \text{ is even,} \\ a_{k/2} + a_{k/2+n/2} & \text{if } k \text{ is even and } n \text{ is even.} \end{cases}$$

By setting

$$N(x) = \sum_{k=0}^{n-1} N_k x^k,$$

we have

$$A(x) + B(x) = C(x) + D(x) + 2N(x).$$

Thus we conclude that $(s_1, s_2, \ldots, s_d)$ is a sum sequence modulo n if and only if all the N_k are constant, and that this is equivalent to $N(\lambda) = 0$ for all non-unity n^{th} roots of unity λ. This is in turn equivalent to $P(\lambda)^2 = P(\lambda^2)$. □

4 A useful lemma

The following lemma will be needed for the proof of Theorem 2 in Section 5.

Lemma 1 *Suppose p is an odd prime and $P(x)$ is a polynomial with integer coefficients. Suppose there are polynomials $K_d(x)$ and $K_{pd}(x)$ satisfying*

$$\begin{aligned} P(x) &= K_d(x)\Phi_d(x) + \mu_d x^{\alpha_d} \\ &= K_{pd}(x)\Phi_{pd}(x) + \mu_{pd} x^{\alpha_{pd}} \end{aligned}$$

where α_d, α_{pd} are integers and μ_d, μ_{pd} are either 0 or 1. Then

$$\mu_d = \mu_{pd} \text{ and } \alpha_d \equiv \alpha_{pd} \ (mod\ d).$$

Proof: Note that since P and Φ_d have integer coefficients and Φ_d has no integer factor except for ± 1, then K_d has integer coefficients (by using a well known result of Gauss, e.g., see [10]).

For the remainder of the argument we will regard all polynomials as elements of $\mathbb{Z}_p[x]$. Note that

$$\Big(\Phi_d(x)\Big)^p = \Phi_d(x^p) = \begin{cases} \Phi_d(x)\Phi_{pd}(x) & \text{if } p \nmid d, \\ \Phi_{pd}(x) & \text{if } p \mid d. \end{cases}$$

Therefore, if $p \nmid q$ and $r \geq 1$, we have

$$\Phi_{p^r q}(x) = \big(\Phi_q(x)\big)^{(p-1)p^{r-1}}.$$

Suppose $p \nmid r, p \nmid s, r \neq s$. Let $\varphi(x)$ be a prime factor of $\Phi_r(x)$. Then $\varphi \nmid \Phi_s$ and $\varphi^2 \nmid \Phi_r$. Suppose not. Then $\varphi^2 \mid \Phi_r \Phi_s$. Since $\Phi_r \Phi_s \mid x^{rs} - 1$, we get $\varphi^2 \mid x^{rs} - 1$. Then $x^{rs} - 1$ and rsx^{rs-1} have a common factor, which is a contradiction.

Let $d = p^s q$ where $p \nmid q$. We consider

$$\begin{aligned} \mu_{pd} x^{\alpha_{pd}} - \mu_d x^{\alpha_d} &= K_d(x)\Phi_d(x) - K_{pd}(x)\Phi_{pd}(x) \\ &= \begin{cases} K_d(x)\Phi_d(x) - K_{pd}(x)\Phi_d(x)^{p-1} & \text{if } s = 0, \\ K_d(x)\Phi_d(x) - K_{pd}(x)\Phi_d(x)^p & \text{if } s > 0. \end{cases} \end{aligned}$$

If $\mu_{pd} \neq \mu_d$, then $\Phi_d(x)$ divides a power of x which is impossible. If $\mu_{pd} = \mu_d = 0$, we are done. Suppose $\mu_{pd} = \mu_d = 1$. Then $\Phi_d(x) \mid x^{\alpha_{pd}} - x^{\alpha_d}$ so $\Phi_d(x) \mid x^{|\alpha_{pd} - \alpha_d|} - 1$.

Let $|\alpha_{pd} - \alpha_d| = ld + r$, $0 \leq r < d$. We then have

$$x^{|\alpha_{pd} - \alpha_d|} - 1 = (x^d - 1)\big(1 + x^d + \ldots + x^{(l-1)d}\big)x^r + x^r - 1.$$

Since $\Phi_d(x) \mid x^d - 1$, we have $\Phi_d(x) \mid x^r - 1$. Suppose $r > 0$. $x^r - 1$ is a product of powers of $\Phi_\delta(x)$, for all $\delta \mid r, p \nmid \delta$.

If $q \nmid r$, then $\Phi_q(x)$ and $x^r - 1$ are relatively prime. However, $\Phi_q \mid \Phi_d \mid x^r - 1$ since $d = p^s q$. Hence $q \mid r$. Let $r = p^t q r'$. We consider

$$\begin{aligned} x^r - 1 &= \prod_{\delta \mid r} \Phi_\delta(x) \\ &= \prod_{k=0}^{t} \Phi_{p^k q}(x) \prod_{\substack{\delta \mid qr' \\ \delta \neq q}} \prod_{k=0}^{t} \Phi_{p^k \delta}(x) \\ &= \Phi_q(x)^{p^t} \prod_{\substack{\delta \mid qr' \\ q \neq q}} \Phi_\delta(x)^{p^t}. \end{aligned}$$

Since $\Phi_d(x)$ is a power of $\Phi_q(x)$ and $\Phi_q(x)$ is relatively prime to $\Phi_\delta(x)$ for $\delta \mid qr', \delta \neq q$, so $\Phi_d(x) \mid \Phi_q(x)^{p^t}$.

If $s = 0$, we have $d = q$ and $r = p^t q r' \geq q = d$, which is impossible. So, $s \neq 0$. Therefore, we have

$$\begin{aligned} \Phi_d(x) = \Phi_{p^s q}(x) &= \Phi_q(x)^{(p-1)p^{s-1}} \\ \text{and} \qquad \Phi_q(x)^{(p-1)p^{s-1}} &\mid \Phi_q(x)^{p^t} \end{aligned}$$

which implies $(p-1)p^{s-1} \leq p^t$.

If $s > t$, then

$$p^{s-1} \geq p^t \geq 2p^{s-1}$$

so $s \leq t$. Hence

$$d = p^s q \leq p^t q \leq p^t q r' = r,$$

which is impossible. Thus, we must have $r = 0$ and therefore $\alpha_{pd} \equiv \alpha_d \pmod{d}$. The lemma is proved. □

5 The next reduction

In this section we derive a strong restriction for polynomials that satisfy the conclusion of Theorem 1.

Theorem 2 *Suppose $n = m2^r \geq 2$ where m is odd and $P(x) \in \mathbb{Z}[x]$. Further, suppose*

$$P(\lambda)^2 = P(\lambda^2) \text{ for all } \lambda \text{ with } \lambda^n = 1, \lambda \neq 1. \tag{6}$$

Then

$$P(x) = \frac{(1 - x^{m2^r})}{(1 - x^{2^r})} K(x) + \mu x^{\alpha} \tag{7}$$

where $\mu = 0$ or 1, α is a non-negative integer and $K(x) \in \mathbb{Q}[x]$ with $deg(K(x)) < 2^r$.

Proof: If $m = 1$, the theorem is trivially true. Assume $m > 1$. Let $d > 1$ and $d \mid m$. Suppose λ is a primitive dth root of unity. Hence $\lambda \neq 1$ and

$$\lambda^n = \left(\lambda^d\right)^{2^r m/d} = 1.$$

From Euler's theorem, we have

$$2^{\phi(d)} = sd + 1$$

for some s odd. Note that d is also odd.

Since $P(\lambda)^2 = P(\lambda^2)$, iteratively we have

$$\begin{aligned} P(\lambda)^{sd+1} = P(\lambda)^{2^{\phi(d)}} &= P\left(\lambda^{2^{\phi(d)}}\right) \\ &= P(\lambda^{sd+1}) = P(\lambda). \end{aligned}$$

Thus we have $P(\lambda)^{sd} = 0$ or $P(\lambda)^{sd} = 1$. If $P(\lambda)^{sd} = 1$, $P(\lambda)$ is a root of unity. Let $P(\lambda)$ have order e. Then e divides sd so e is odd. Let f be the least common multiple of d and e. Note that both λ and $P(\lambda) \in \mathbb{Q}[\lambda]$ so $\mathbb{Q}[\lambda]$ contains a primitive root of unity of order f. Hence $\mathbb{Q}[\lambda]$ contains a subfield of degree $\phi(f)$ over $\mathbb{Q}$. Since $\mathbb{Q}[\lambda]$ is of degree $\phi(d)$ over $\mathbb{Q}$, then $\phi(d) \geq \phi(f)$. However $d \mid f$ and f is odd, so $d = f$. Hence $e \mid d$ and therefore $P(\lambda)$ is a power of λ. Thus for $\mu_d = 0, 1$, we have $P(\lambda) = \mu_d \lambda^{\alpha_d}$. Therefore,

$$P(x) = K_d(x)\Phi_d(x) + \mu_d x^{\alpha_d}$$

for $d > 1, d \mid m$ and $\mu_d = 0, 1$.

Now let ξ be a 2^{sd}th root of unity, where $0 \le s \le r$. We may assume $\xi^{2^s} = \lambda$. ξ and its powers are nth roots of unity so we may iterate the relation $P(\xi)^2 = P(\xi^2)$ to obtain

$$P(\xi)^{2^s} = P(\xi^{2^s}) = P(\lambda) = \mu_d \lambda^{\alpha_d}.$$

Hence,

$$P(\xi)^{2^s d} = \mu_d \lambda^{d\alpha_d} = \mu_d = 0 \text{ or } 1,$$

so $P(\xi) = \mu_{2^s d}\xi^{\alpha_{2^s d}}$ is 0 or a 2^{sd}th root of unity, i.e.,

$$P(\xi) = \mu_{2^s d}\xi^{\alpha_{2^s d}}.$$

Thus,

$$P(x) = K_{2^s d}(x)\Phi_{2^s d}(x) + \mu_{2^s d}x^{\alpha_{2^s d}}.$$

We can now relax the definition of d and by using Lemma 1 we have, for $d \mid n, d \nmid 2^r$,

$$P(x) = K_d(x)\Phi_d(x) + \mu_d x^{\alpha_d}, \qquad \mu = 0 \text{ or } 1.$$

For p an odd prime, $pd \mid n, d \nmid 2^r$, we have $\mu_d = \mu_{pd}$ and $\alpha_d \equiv \alpha_{pd} \pmod d$ by Lemma 1. If $2d \mid n, d \nmid 2^r$ and ξ is a primitive $2d$th root of unity, then

$$\left(\mu_{2d}\xi^{\alpha_{2d}}\right)^2 = P(\xi)^2 = P(\xi^2) = \mu_d \xi^{2\alpha_d}.$$

Therefore $\mu_d = \mu_{2d}$ and $2d \mid 2\alpha_{2d} - 2\alpha_d$ and $\alpha_d \equiv \alpha_{2d} \pmod d$.

Iterating these relations we have $\mu_d = \mu_n$ and $\alpha_d \equiv \alpha_n \pmod d$. Since $x^{t+d} = x^t + x^t(x^d - 1)$ and $\Phi_d(x) \mid x^d - 1$, we may change α_d by any multiple of d by altering $K_d(x)$. Since $\alpha_d \equiv \alpha_n \pmod d$ we may assume that $\alpha_d = \alpha_n$.

We now have $\Phi_d(x) \mid P(x) - \mu_n x^{\alpha_n}$ for $d \mid n, d \nmid 2^r$. Since $\Phi_d(x), \Phi_{d'}(x)$ are distinct irreducible polynomials for $d \ne d'$. $P(x) - \mu_n x^{\alpha_n}$ is divisible by

$$\prod_{\substack{d \mid n \\ d \nmid 2^r}} \Phi_d(x) = 1 + x^{2^r} + x^{2^r \cdot 2} + \ldots + x^{2^r(m-1)}$$

$$= \frac{x^{2^r m} - 1}{x^{2^r} - 1}.$$

This completes the proof of Theorem 2. □

A consequence of Theorem 2 is the following.

Theorem 3 *Let n be an odd integer. A sequence S is a sum sequence modulo n if and only if it can be shifted to a sequence with "coordinates" $a_0, a_1, \ldots, a_{n-1}$ where either $a_i = a$ for $i = 0, \ldots, n-1$ or*

$$a_i = \begin{cases} a+1 & \text{if } i = 0, \\ a & \text{if } i = 1, \ldots, n-1. \end{cases}$$

Proof: Let S have coordinates $a_0, a_1, \ldots, a_{n-1}$ (where, as usual, a_i denotes the number of terms in S that are congruent to i modulo n). Let $P(x) = a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$. By Theorem 1, S is a sum sequence modulo n if and only if $P(\lambda)^2 = P(\lambda^2)$ for $\lambda^n = 1, \lambda \neq 1$. By Theorem 2 this condition implies

$$P(x) = K(x)(1 + x + \ldots + x^{n-1}) + \mu x^{\alpha}.$$

For λ satisfying $\lambda^n = 1$ if $\lambda \neq 1$, we have

$$P(\lambda)^2 = \mu^2 \lambda^{2\alpha} = \mu \lambda^{2\alpha} = P(\lambda^2).$$

Since the degree of $P(x)$ is at most $n-1$, the polynomial $K(x)$ is a constant. Hence the sequence is a sum sequence if and only if all the entries are equal with the possible exception of one coordinate which is one larger than the others.

By a suitable shifting, the exceptional coordinate can be assumed to be a_0. This proves Theorem 3. □

6 Characterizing $P(x) \in \mathbb{Q}[x]$.

In this section we will allow our polynomial $P(x)$ to have rational coefficients. This makes it more convenient to apply the results from Galois theory that we will need.

For a given integer $n \geq 2$, we wish to characterize those polynomials $P(x) \in \mathbb{Q}[x]$ which satisfy the equations:

$$P(\theta)^2 = P(\theta^2) \text{ for all } \theta \text{ with } \theta^n = 1, \theta \neq 1. \tag{8}$$

We will assume $deg(P) \leq n-1$. For the rest of this section, we will assume that λ is a fixed primitive $2^r th$ root of unity, i.e., $\lambda^{2^{r-1}} + 1 = 0$. Note that $P(x) = 0$ and $P(x) = 1$ are trivial solutions to (8).

Thus, we can set $\alpha = 0$ in (7) and rewrite it as follows. Suppose $n = m2^r$ where m is odd, and suppose that $P(x)$ satisfies (8). Then (up to a shifting factor of x^α), we have

$$P(x) = \frac{(1-x^{m2^r})}{(1-x^{2^r})}K(x) + \mu \tag{9}$$

where $\mu = 0$ or 1, and $K(x) \in \mathbb{Q}[x]$ with the $deg(K(x)) < 2^r$. Our goal then is to characterize the polynomials $K(x)$ so that $P(x)$ satisfies (8).

We first make some preliminary remarks.

Let

$$1 - x^{2^r} = \Phi_1(x)\Phi_2(x)\Phi_3(x)\ldots\Phi_{r+1}(x) \tag{10}$$

be the factorization of $1 - x^{2^r}$ into the (unique) irreducible cyclotomic polynomials $\Phi_k(x)$ where

$$\Phi_1(x) = 1 - x \text{ and } \Phi_k(x) = 1 + x^{2^{k-2}},\ 2 \leq k \leq r+1. \tag{11}$$

Then there is a unique expansion

$$\frac{K(x)}{1-x^{2^r}} = \sum_{k=1}^{r+1} \frac{b_k(x)}{\Phi_k(x)} = \frac{b_1(x)}{1-x} + \frac{b_2(x)}{1+x} + \ldots + \frac{b_k(x)}{1+x^{2^{k-2}}} + \ldots + \frac{b_{r+1}(x)}{1+x^{2^{r-1}}} \tag{12}$$

where $b_1(x) \in \mathbb{Q}$ is a constant, $b_k(x) \in \mathbb{Q}[x]$ and $deg(b_k(x)) < 2^{k-2}$ for $2 \leq k \leq r+1$. The proof for this expansion is the method of partial fractions taught to college algebra students. Note that in fact, b_1 and b_2 are constant, and do not depend on x.

Theorem 4 *Let $n = m2^r \geq 2$ be given where m is odd. Suppose $P(x) \in \mathbb{Q}[x]$ satisfies*

$$P(\theta)^2 = P(\theta^2) \text{ for all } \theta \text{ with } \theta^n = 1, \theta \neq 1.$$

where $deg(P(x)) < 2^n$. *From (9) and (12) we can write*

$$P(x) = (1 - x^{m2^r}) \sum_{k=1}^{r+1} \frac{b_k(x)}{\Phi_k(x)} + \mu \tag{13}$$

where $\mu = 0$ *or* 1. *Then* $P(x)$ *lies in one of two types of one-parameter families of polynomials (up to shifting by a power of* x*).*

Type I. *Choose* $t \in \mathbb{Q}$, *and define*

$$\begin{aligned} c_{r+1} = t,\ c_{k-1} = c_k^2, \quad b_k = \frac{1}{m2^{r+2-k}}(c_k - \mu),\ 2 \le k \le r+1, \\ b_1 = \frac{1}{m2^r}(c_1 - \mu). \end{aligned} \tag{14}$$

Type II. *For* $r \ge 3$, *choose* $t \in \mathbb{Q}$ *and define*

$$\begin{aligned} c_{r+1} = t\sqrt{\pm 2}, \quad b_{r+1} = t(x^{2^{r-3}} \mp x^{3\cdot 2^{r-3}} - \mu) \\ c_{k-1} = c_k^2, \quad b_k = \frac{1}{m2^{r+2-k}}(c_k - \mu),\ 2 \le k \le r+1, \\ b_1 = \frac{1}{m2^r}(c_1 - \mu). \end{aligned} \tag{15}$$

Note that in both cases, these choices define $P(x)$.

Proof: With $n = m2^r$, m odd, suppose $\theta^{2^k} + 1 = 0$ with $0 \le k \le r-1$. Then we have the

Claim.

$$P(1) = m2^r b_1 + \mu,\ P(\theta) = m2^{r-k} b_{k+2}(\theta) + \mu,\ \text{for } 0 \le k \le r-1. \tag{16}$$

To see this, note that

$$\begin{aligned} P(\theta) &= \frac{(1 - x^{m2^r})}{(1 - x^{2^r})} K(x)\Big|_{x=\theta} + \mu = \frac{(1 - x^{m2^r})}{(1 + x^{2^k})} b_{k+2}(x)\Big|_{x=\theta} + \mu \\ &= \frac{-m2^r \theta^{m2^r - 1}}{2^k \theta^{2^k - 1}} b_{k+2}(\theta) + \mu \\ &= m2^{r-k} b_{k+2}(\theta) + \mu \end{aligned}$$

since all the other terms $\frac{1-x^{m2^r}}{1+x^{2j}} b_{j+2}(x), j \neq k$, in the expansion of $P(x)$ are 0 when $x = \theta$ and $\theta^{2^k} + 1 = 0$. Similarly,

$$\begin{aligned} P(1) &= \frac{(1-x^{m2^r})}{(1-x^{2^r})} K(x)\Big|_{x=1} + \mu = \frac{(1-x^{m2^r})}{(1-x)} b_1\Big|_{x=1} + \mu \\ &= m2^r b_1 + \mu \end{aligned}$$

This proves the Claim.

Since θ^2 satisfies $(\theta^2)^{2^{k-1}} + 1 = 0$, we find by (16),

$$P(\theta^2) = m2^{r-k+1} b_{k+1}(\theta^2) + \mu. \tag{17}$$

Hence, if $P(x)$ satisfies (8) then we have

$$b_{k+1}(\theta^2) = m2^{r-k-1} b_{k+2}^2(\theta) + \mu b_{k+2}(\theta), \tag{18}$$

where we use the fact that $\mu^2 = \mu$. For b_1 we have the (slightly different) relation

$$b_1 = m2^r b_2^2 + 2\mu b_2. \tag{19}$$

Thus, for example, since $\lambda^{2^{r-1}} + 1 = 0$, then $b_r = b_r(\lambda^2) = 2mb_{r+1}(\lambda)^2 + \mu b_{r+1}(\lambda)$. More generally, once the value of $b_{r+1}(\lambda) \in \mathbb{Q}(\lambda)$ is fixed, then the values of all the other $b_k(x), 1 \leq k \leq r$, are determined by (18) and (19).

Let us make the substitutions

$$c_1 = m2^r b_1 + \mu,\ c_k = m2^{r-k+2} b_k + \mu,\ 2 \leq k \leq r+1. \tag{20}$$

Then (18) and (19) imply

$$c_k = c_{k+1}^2,\ 1 \leq k \leq r. \tag{21}$$

Since $c_1 = m2^r b_1 + \mu = P(1) \in \mathbb{Q}$ is formed by starting with $c_{r+1} = 2mb_{r+1} + \mu \in \mathbb{Q}(\lambda)$ and repeatedly squaring r times then we must have $c_{r+1} = \tau\lambda^d$ for some choice of $\tau \in \mathbb{Q}(\lambda)$ and some integer $d \geq 0$. In other words, if we write $c_{r+1} = \tau \exp(\alpha i)$ and we square it r times, then we get $c_1 = c_{r+1}^{2^r} = \tau^{2^r} \exp(2^r \alpha) \in \mathbb{Q}$. This implies that α is an integer multiple of $\frac{2\pi}{2^r}$ and consequently, an integral power of λ. Let s be the *largest* index such that c_s

is a rational multiple of a power of λ.

Claim. $s \geq r$.

Proof. If $\tau \in \mathbb{Q}$ then $s = r + 1$ and the Claim holds in this case. There are several more possibilities:

Case 1. $s = r$. Then $c_r = u\lambda^{2d}$ with $u \in \mathbb{Q}$. By (21), $c_{r+1} = \sqrt{u}\lambda^d$ for some d where by hypothesis, $\sqrt{u} \notin \mathbb{Q}$. Now the polynomial $z^2 - u$ is irreducible over $\mathbb{Q}$ since the only possible factorization is $z^2 - u = (z - \sqrt{u})(z + \sqrt{u})$. Hence, the field extension $\mathbb{Q}(z^2 - u)$ is a quadratic extension of $\mathbb{Q}$. However, it is well known from Galois theory (e.g., see [10]) that there are only three quadratic extensions of $\mathbb{Q}$, namely $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$. Thus, we must be able to express the roots of $z^2 - u$ as elements of one of these fields. That is, we can write $\sqrt{u} = a + ib$, $\sqrt{u} = a + b\sqrt{2}$ or $\sqrt{u} = a + b\sqrt{-2}$ for rationals $a, b \in \mathbb{Q}$. But if $\sqrt{u} = a + ib$, for example, then $u = (a + ib)^2 = a^2 - b^2 + 2iab \in \mathbb{Q}$. This implies that $ab = 0$. However, $b = 0$ implies that $\sqrt{u} = a \in \mathbb{Q}$ which is a contradiction. Hence we must have $a = 0$ and $\sqrt{u} = bi = b\lambda^{2^r}$. But then c_{r+1} is a rational multiple of a power of λ, contradicting our hypothesis.

In the case that $\sqrt{u} = a + b\sqrt{2}$, then $u = a^2 + 2b^2 + 2ab\sqrt{2} \in \mathbb{Q}$. Thus, $ab = 0$. If $b = 0$ then $\sqrt{u} = a \in \mathbb{Q}$ which is a contradiction. Hence, we have $a = 0$ and $\sqrt{u} = b\sqrt{2}$ for some $b \in \mathbb{Q}$. The same argument applies in the remaining case that $\sqrt{u} = a + b\sqrt{-2}$ and there we have $\sqrt{u} = b\sqrt{-2}$.

Note that for this case we must have $r \geq 3$, since if $r \leq 2$ then $\sqrt{2} \notin \mathbb{Q}$, and $\sqrt{-2} \notin \mathbb{Q}$. However, $\lambda^{2^{r-3}} - \lambda^{3 \cdot 2^{r-3}} = \sqrt{2}$ and $\lambda^{2^{r-3}} + \lambda^{3 \cdot 2^{r-3}} = \sqrt{-2}$. Thus, for Case 1 we have the two choices $c_{r+1} = t(\lambda^{2^{r-3}} \pm \lambda^{3 \cdot 2^{r-3}})\lambda^d$ for some $t \in \mathbb{Q}$ and some integer $d \geq 0$.

Case 2. Suppose that $s = r - 1$. Thus, $r \geq 3$ and $c_{r-1} = u\lambda^{4d}$ where $u \in \mathbb{Q}$. Consider the term $c_r = \sigma\lambda^{2d}$ so that $u = \sigma^2$. Since by hypothesis, σ is not a rational multiple of a power of λ, then the polynomial $z^2 - u$ is irreducible over $\mathbb{Q}$. Thus, the field $\mathbb{Q}[z^2 - u]$ is quadratic extension of $\mathbb{Q}$ and the roots $\pm\sqrt{u}$ must lie in one of $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$.

For the first case, suppose that the root $\sqrt{u} \in \mathbb{Q}(i)$, i.e., $\sigma = \sqrt{u} = a + bi$ for some $a, b \in \mathbb{Q}$. Therefore,

$$u = (a + bi)^2 = a^2 - b^2 + 2abi.$$

This implies that $ab = 0$. However, if $b = 0$ then $\sigma = a \in \mathbb{Q}$ which is a

contradiction. On the other hand, if $a = 0$ then $\sigma = bi$ which is a rational multiple of a root of unity which is also a contradiction.

For the second case, suppose that $\sigma\sqrt{u} = a + b\sqrt{2}$. Then,

$$u = (a + b\sqrt{2})^2 = a^2 + 2b^2 + 2iab\sqrt{2}.$$

Again, we must then have $ab = 0$. If $b = 0$ then $\sigma = a$ which is a contradiction. However, if $a = 0$ then $\sigma = b\sqrt{2}$ for some $b \in \mathbb{Q}$.

For the third case that $\sigma\sqrt{u} = a + b\sqrt{-2}$, the same argument shows that we must have $\sigma = b\sqrt{-2}$ for some $b \in \mathbb{Q}$.

Now consider the term $c_{r+1} = \tau\lambda^d$ where $\sigma = \tau^2$. Since $z^2 - \sigma$ is irreducible over $\mathbb{Q}$, then its roots must lie in one of $\mathbb{Q}(i), \mathbb{Q}(\sqrt{2})$ or $\mathbb{Q}(\sqrt{-2})$. However, $\sqrt{\sigma}$ cannot belong to any of these three fields. For example, suppose that $\sqrt{b\sqrt{2}} = p + qi$ for rationals $p, q \in \mathbb{Q}$. Then $b\sqrt{2} = (p + qi)^2 = p^2 - q^2 + 2pqi$ which is impossible. Similarly, suppose that $\sqrt{b\sqrt{2}} = p + q\sqrt{\pm 2}$ for rationals $p, q \in \mathbb{Q}$. Then

$$b\sqrt{2} = (p + q\sqrt{\pm 2})^2 = p^2 \pm 2q^2 + 2pq\sqrt{\pm 2}$$

which implies $p = q = 0$, The remaining cases are similar. This concludes Case 2.

Case 3. $s < r - 1$. The same argument as in Case 2 shows that in general if c_{w+1} is not a rational multiple of a power of λ, then c_w must be. Thus, this case also leads to a contradiction.

So we know that the only possible values for $c_{r+1} = 2mb_{r+1} + \mu$ are either $c_{r+1} = t\lambda^d(\lambda^{2^{r-3}} \pm \lambda^{3\cdot 2^{r-3}})$ or $c_{r+1} = t\lambda^d$ for $t \in \mathbb{Q}$ and some integer d. In either case, c_r is a rational multiple of a power of λ.

As we have seen, once the value of c_{r+1} is fixed, the values of all the other c_k (and therefore, the values of all the b_k) are determined. However, the polynomial $P(x)$ is required to have rational coefficients. So if $c_{r+1} \notin \mathbb{Q}$, and we use the recurrence (21) to generate the remaining values of c_k, then the values of the b_k might be rational, and so we might have $P(x) \notin \mathbb{Q}[x]$. The remedy for this problem is simple. We just replace the occurrence of λ in c_{r+1} by x to get the corresponding value for b_{r+1}. For example, if $c_{r+1} = t\lambda^d$ then we would define $b_{r+1} = \frac{1}{2m}(tx^d - \mu)$. Now, to get the earlier values of

b_s, $s \leq r$, we compute the value of c_s iteratively and then replace the power of λ by the *same* term x^d. Just as we always reduce large powers λ by the relation $\lambda^{2^{r-1}}+1=0$, we also reduce each polynomial $b_{k+2}(x)$ by the relation $x^{2^k}+1=0$. This is the equation satisfied by the power of λ that occurs when computing the contribution to $P(x)$ of the term $\frac{b_{k+2}(x)}{1+x^{2^k}}$. In particular, this will guarantee that $deg(b_{k+2}(x)) < 2^k$. Since we eventually reach a value of $c_k \in \mathbb{Q}$, the variable x will not occur in the corresponding terms b_k.
For example, for the Type I solutions, if $c_{r+1} = t\lambda^d$ then we set $b_{r+1} = \frac{1}{2m}(tx^d - \mu)$. In general, for $2 \leq s \leq r$, we define $b_s = \frac{1}{m2^{r-s+2}}(t^{2^{r-s+1}}x^d - \mu)$. The case of $s=1$ is slightly different. For this we have $b_1 = \frac{1}{m2^r}(c_1 - \mu)$.

On the other hand, for the Type II solutions, if $c_{r+1} = t\lambda^d(\lambda^{2^{r-3}} \pm \lambda^{3\cdot 2^{r-3}}) = t\lambda^d\sqrt{\mp 2}$ then we set $b_{r+1} = \frac{1}{2m}x^d(x^{2^{r-3}} \pm x^{3\cdot 2^{r-3}} - \mu)$ and $b_r = \frac{1}{4m}x^d(c_{r+1}^2 - \mu) = \frac{1}{4m}x^d(2t^2 - \mu)$. We then compute the values of the remaining $b_k(x)$ as above.

We also point out that the choice of the factor λ^d in the definition of c_{r+1} just corresponds to shifting $P(x)$ by a factor of x^d, and so has no essential effect on the solution. Thus, in our statements of the Type I and Type II solutions, we have taken $d=0$. □

7 $\mu = 0$ versus $\mu = 1$

From (12) and (14), we see that the corresponding coefficients of $P(x)$ when $\mu = 0$ and when $\mu = 1$ are quite similar. In fact, if we detach the $-\mu$ terms from each of the b_k and add them up, we get

$$
\begin{aligned}
&-\frac{1}{m2^r(1-x)} - \frac{1}{m2^r(1+x)} - \frac{1}{m2^{r-1}(1+x^2)} - \frac{1}{m2^{r-2}(1+x^4)} - \dots \\
&\dots - \frac{1}{4m(1+x^{2^{r-2}})} - \frac{1}{2m(1+x^{2^{r-1}})} = -\frac{1}{m(1-x^{2^r})} \\
&= -\frac{1}{m}(1 + x^{2^r} + x^{2\cdot 2^r} + x^{3\cdot 2^r} + \dots + x^{(m-1)2^r}).
\end{aligned}
$$

Thus, we see that the coefficients of $P(x)$ using $\mu = 1$ agree with those of $P(x)$ using $\mu = 0$ with the exception of the coefficients of $x^{k\cdot 2^r}$, $k \geq 0$, for which we have to subtract $\frac{1}{m}$. For the constant term with $k=0$, we also have to add the term $\mu = 1$.

As an example, consider the case that $n = 24 = 3 \cdot 2^3$ so that $\lambda^4 + 1 = 0$. Then

$$P(x) = (1 - x^{24}) \left(\frac{b_1}{1-x} + \frac{b_2}{1+x} + \frac{b_3(x)}{1+x^2} + \frac{b_4(x)}{1+x^4} \right) + \mu. \qquad (22)$$

The Type I choice is $c_4 = t \in \mathbb{Q}$. Thus $c_3 = t^2, c_2 = t^4, c_1 = t^8$. Taking $\mu = 0$, we find:

$$b_4 = \frac{1}{2}t, b_3 = \frac{1}{4}t^2, b_2 = \frac{1}{8}t^4, b_1 = \frac{1}{8}t^8. \qquad (23)$$

Thus, for the choice of $t = 2, \mu = 0$, for example, the coefficients of $P(x)$ (starting with the constant term) are:

$$[\ 12, 10, 11, 10, 34/3, 10, 11, 10, 12, 10, 11, 10,$$
$$34/3, 10, 11, 10, 12, 10, 11, 10, 34/3, 10, 11, 10\ ].$$

For $t = 3, \mu = 0$, the coefficients of $P(x)$ are:

$$[\ 278, 270, 276, 270, 277, 270, 276, 270, 278, 270, 276, 270,$$
$$277, 270, 276, 270, 278, 270, 276, 270, 277, 270, 276, 270\ ]$$

On the other hand, if we take $\mu = 1$ we find:

$$b_4 = \frac{1}{2}(t-1), b_3 = \frac{1}{4}(t^2-1), b_2 = \frac{1}{8}(t^4-1), b_1 = \frac{1}{8}(t^8-1).$$

For this case with $t = 2, \mu = 1$, the coefficients of $P(x)$ are:

$$[\ 38/3, 10, 11, 10, 34/3, 10, 11, 10, 35/3, 10, 11, 10,$$
$$34/3, 10, 11, 10, 35/3, 10, 11, 10, 34/3, 10, 11, 10\ ],$$

while for $t = -2, \mu = 0$, we have the coefficient vector for $P(x)$:

$$[\ 12, 10, 11, 10, 12, 10, 11, 10, 11, 10, 11, 10,$$
$$12, 10, 11, 10, 11, 10, 11, 10, 12, 10, 11, 10\ ].$$

One Type II choice for $P(x)$ is $c_4 = t(\lambda - \lambda^3) = t\sqrt{2}$. In this case $c_3 = 2t^2, c_2 = 4t^4, c_1 = 16t^8$. Thus, with $\mu = 0$, we have

$$b_4(x) = \frac{1}{2}t(x - x^3), b_3(x) = \frac{2}{4}t^2, b_2(x) = \frac{4}{8}t^4, b_1 = \frac{16}{8}t^8.$$

For the choice $t = 1, \mu = 0$, for example, we find the coefficient vector for $P(x)$ is:

$$[\ 1, 2/3, 2/3, 1/3, 1, 1/3, 2/3, 2/3, 1, 2/3, 2/3, 1/3,$$
$$1, 1/3, 2/3, 2/3, 1, 2/3, 2/3, 1/3, 1, 1/3, 2/3, 2/3\ ].$$

For $P(x)$ with $t = 3, \mu = 0$, we have the coefficient vector:

$$[\ 4389, 4361, 4386, 4360, 4389, 4360, 4386, 4361, 4389, 4361, 4386, 4360,$$
$$4389, 4360, 4386, 4361, 4389, 4361, 4386, 4360, 4389, 4360, 4386, 4361\ ].$$

If we had made the other Type II choice $c_4 = t(\lambda + \lambda^3) = t\sqrt{-2}$, then the corresponding values of the b_k would be

$$b_4(x) = \frac{1}{2}t(x + x^3), b_3(x) = -\frac{2}{4}t^2, b_2(x) = \frac{4}{8}t^4, b_1 = \frac{16}{8}t^8$$

and would have the coefficient vectors for $P(x)$ with $t = 1, \mu = 0$ and $P(x)$ with $t = 3, \mu = 0$ being:

$$[\ 2/3, 2/3, 1, 2/3, 2/3, 1/3, 1, 1/3, 2/3, 2/3, 1, 2/3,$$
$$2/3, 1/3, 1, 1/3, 2/3, 2/3, 1, 2/3, 2/3, 1/3, 1, 1/3\ ]$$

and

$$[\ 4386, 4361, 4389, 4361, 4386, 4360, 4389, 4360, 4386, 4361, 4389, 4361,$$
$$4386, 4360, 4389, 4360, 4386, 4361, 4389, 4361, 4386, 4360, 4389, 4360\ ],$$

respectively. These are both just translates of the corresponding vectors for the Type I solutions for $P(x)$.

For the case that $\mu = 1$, the calculations are similar. Thus, for the Type II solution $c_4 = t\sqrt{2}$ we find $c_3 = 2t^2, c_2 = 4t^4, c_1 = 16t^8$ and

$$b_4 = \frac{1}{2}(x - x^3 - 1), b_3 = \frac{1}{4}(2t^2 - 1), b_2 = \frac{1}{8}(t^4 - 1), b_1 = \frac{1}{8}(t^8 - 1)$$

and we have the coefficient vector for $P(x)$ with $t = 3, \mu = 1$ is:

$$[\ 13169/3, 4361, 4386, 4360, 4389, 4360, 4386, 4361, 13166/3, 4361, 4386, 4360,$$
$$4389, 4360, 4386, 4361, 13166/3, 4361, 4386, 4360, 4389, 4360, 4386, 4361\ ].$$

As we will see in the next section, there is no value of t so that with $\mu = 1$ $P(x)$ has all integer coefficients.

8 When is $P(x) \in \mathbb{Z}[x]$?

Let us examine the contributions to the coefficients of $P(x)$ from the various terms of the expansion (12) more carefully.

We first consider the Type I solution. It follows from (12) that for $k \geq 1$, the coefficient a_k in $P(x) = \sum_{k=0}^{m2^r-1} a_k x^k$ satisfies the following:

$$a_k = \sum_{1 \leq i \leq d+1} b_i - b_{d+2} \tag{24}$$

where d is the largest integer power of 2 dividing k. If $d = r$, we define $b_{r+2} = 0$. For $k = 0$, we have $a_0 = \sum_{i=1}^{r+1} b_i$. Thus, for example, when $n = 3 \cdot 2^3$, $a_1 = b_1 - b_2,\ a_2 = b_1 + b_2 - b_3, a_4 = b_1 + b_2 + b_3 - b_4, a_0 = a_8 = b_1 + b_2 + b_3 + b_4$, etc.

In general, if all the a_k are to be integers, then the difference of any two a_k's must be an integer. In particular $a_0 - a_{2^{r-1}} = 2b_{r+1}$ must be an integer. But by (20), $b_{r+1} = \frac{1}{2m}(t - \mu)$. Hence, a *necessary* condition for $P(x) \in \mathbb{Z}[x]$ is that $2b_{r+1} = \frac{t-\mu}{m} \in \mathbb{Z}$, i.e.,

$$t \equiv \mu \pmod{m}. \tag{25}$$

Let us now show that (25) is also *sufficient* for $P(x) \in \mathbb{Z}[x]$. The plan is to show that $a_{2^k} - a_{2^{k-1}} \in \mathbb{Z}$ for $1 \leq k \leq r+1$, and then show that $a_1 \in \mathbb{Z}$. This will imply that all the coefficients are integers. We are assuming that $t \equiv \mu \pmod{m}$ so that $a_0 - a_{2^{r-1}} = 2b_{r+1} = \frac{t-\mu}{m} \in \mathbb{Z}$. Now consider the diffference $a_{2^{r-1}} - a_{2^{r-2}} = 2b_r - b_{r+1}$. By (14), we have

$$2b_r - b_{r+1} = \frac{1}{2m}(t^2 - t). \tag{26}$$

If $t = cm + \mu$ then $t^2 - t = c^2m^2 + 2cm\mu - cm$ (since $\mu^2 = \mu$) which is clearly a multiple of m. Also, $t^2 - t = t(t-1)$ is always even. Thus, since m is odd then $\frac{1}{2m}(t^2 - t) \in \mathbb{Z}$.

In general, for $1 \leq k \leq r-1$, we consider the difference

$$\begin{aligned} a_{2^k} - a_{2^{k-1}} = 2b_{k+1} - b_{k+2} &= \frac{2}{m2^{r+1-k}}(c_{k+1} - \mu) - \frac{1}{m2^{r-k}}(c_{k+2} - \mu) \\ &= \frac{1}{m2^{r-k}}(t^{2^{r-k}} - t^{2^{r-k-1}}). \end{aligned} \tag{27}$$

It is easily checked that the final expression in (27) is an integer. (Consider the cases that t is even and odd, and write $m = at + \mu$ and expand, using the fact that $\mu^2 = \mu$). Finally, we consider the coefficient

$$a_1 = b_1 - b_2 = \frac{1}{m2^r}(c_1 - \mu) - \frac{1}{m2^r}(c_2 - \mu) = \frac{1}{m2^r}(t^{2^r} - t^{2^{r-1}}).$$

The same arguments as above show that this is also an integer. Hence, we can conclude that for the Type I solution, $P(x) \in \mathbb{Z}[x]$ provided only that $t \equiv \mu \pmod{m}$.

For the Type II solutions, there is a slight but crucial difference. For these solutions, b_{r+1} contributes to twice as many coefficients as in the Type I solution (because of the occurrence of the term $x^{2^{r-3}} \pm x^{3\cdot 2^{r-3}}$ in $b_{r+1}(x)$). In particular, the contributions b_{r+1} to the a_k have been shifted by 2^{r-3} (and there are twice as many). More precisely, the expressions for a_k in terms of sums of the b_i are unchanged from those in (24) except for $k \equiv 0, 2^{r-3}, 3\cdot 2^{r-3}, 2^{r-3} + 2^{r-1}, 3\cdot 2^{r-3} + 2^{r-1} \pmod{2^r}$. For $k \equiv 0 \pmod{2^r}$ we omit the final summand b_{r+1}. For $k \equiv 2^{r-3} \pmod{2^r}$ we add the additional term b_{r+1} and we add $-b_{r+1}$ for $k \equiv 2^{r-3} + 2^{r-1}$. Finally, if the Type II solution has $b_{r+1} = \frac{1}{2m}(x^{2^{r-3}} + x^{3\cdot 2^{r-3}} - \mu)$ then for $k \equiv 3\cdot 2^{r-3}$, we add the term b_{r+1} to the sum for a_k and for $k \equiv 3\cdot 2^{r-3} + 2^{r-1}$ we add $-b_{r+1}$ to the sum for a_k. On the other hand, if the Type II solution has the form $b_{r+1} = \frac{1}{2m}(x^{2^{r-3}} - x^{3\cdot 2^{r-3}} - \mu)$ then we add $-b_{r+1}$ to the sum for a_k when $k \equiv 3\cdot 2^{r-3} \pmod{2^r}$ and we add b_{r+1} to the sum for a_k when $k \equiv 3\cdot 2^{r-3} + 2^{r-1} \pmod{2^r}$.

We show here a specific example for the case $n = 16$. First we show column contributions to a_k for the Type I solution.

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}
b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1
b_2	$-b_2$	b_2	$-b_2$	b_2	$-b_2$	b_2	$-b_2$	b_2	$-b_2$	b_2	$-b_2$	b_2	$-b_2$	b_2	$-b_2$
b_3		$-b_3$		b_3		$-b_3$		b_3		$-b_3$		b_3		$-b_3$	
b_4				$-b_4$				b_4				$-b_4$			
b_5								$-b_5$							

Next, we show the column contributions for the Type II solutions.

a_0	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}	a_{11}	a_{12}	a_{13}	a_{14}	a_{15}
b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1	b_1
b_2	$-b_2$	b_2	$-b_2$	b_2	$-b_2$	b_2	$-b_2$	b_2	$-b_2$	b_2	$-b_2$	b_2	$-b_2$	b_2	$-b_2$
b_3		$-b_3$		b_3		$-b_3$		b_3		$-b_3$		b_3		$-b_3$	
b_4				$-b_4$				b_4				$-b_4$			
		b_5				$\pm b_5$				$-b_5$				$\mp b_5$	

In the column for a_6, we choose $+b_5$ for the solution $b_5 = \frac{1}{2}(x^2 + x^6 - \mu)$ and $-b_5$ for the solution $b_5 = \frac{1}{2}(x^2 - x^6 - \mu)$.

In general, for $b_{r+1} = \frac{1}{2m}\left(x^{2^{r-3}} + x^{3\cdot 2^{r-3}} - \mu\right)$ we have

$$a_k = \begin{cases} \displaystyle\sum_{1\le i\le r} b_i & \text{if } k \equiv 0 \pmod{2^r} \\ \displaystyle\sum_{1\le i\le r-2} b_i - b_{r-1} + b_{r+1} & \text{if } k \equiv 2^{r-3} \pmod{2^r} \\ \displaystyle\sum_{1\le i\le r-2} b_i - b_{r-1} - b_{r+1} & \text{if } k \equiv 2^{r-3} + 2^{r-1} \pmod{2^r} \\ \displaystyle\sum_{1\le i\le r-2} b_i - b_{r-1} + b_{r+1} & \text{if } k \equiv 3\cdot 2^{r-3} \pmod{2^r} \\ \displaystyle\sum_{1\le i\le r-2} b_i - b_{r-1} - b_{r+1} & \text{if } k \equiv 3\cdot 2^{r-3} + 2^{r-1} \pmod{2^r} \\ \displaystyle\sum_{1\le i\le d+1} b_i - b_{d+2} & \text{otherwise} \end{cases}$$

where d denotes the largest power of 2 that divides k.

For $b_{r+1} = \frac{1}{2m}\big(x^{2^{r-3}} - x^{3\cdot 2^{r-3}} - \mu\big)$, we have

$$a_k = \begin{cases} \sum\limits_{1\le i\le r} b_i & \text{if } k \equiv 0 \pmod{2^r} \\ \sum\limits_{1\le i\le r-2} b_i - b_{r-1} + b_{r+1} & \text{if } k \equiv 2^{r-3} \pmod{2^r} \\ \sum\limits_{1\le i\le r-2} b_i - b_{r-1} - b_{r+1} & \text{if } k \equiv 2^{r-3} + 2^{r-1} \pmod{2^r} \\ \sum\limits_{1\le i\le r-2} b_i - b_{r-1} - b_{r+1} & \text{if } k \equiv 3\cdot 2^{r-3} \pmod{2^r} \\ \sum\limits_{1\le i\le r-2} b_i - b_{r-1} + b_{r+1} & \text{if } k \equiv 3\cdot 2^{r-3} + 2^{r-1} \pmod{2^r} \\ \sum\limits_{1\le i\le d+1} b_i - b_{d+2} & \text{otherwise.} \end{cases}$$

In a sense, the b_r contributions are now "unprotected". This means that in addition to the requirement that $a_0 - a_{2^{r-1}} = 2b_{r+1} \in \mathbb{Z}$, we also have the requirement that $a_0 - a_{2^{r-2}} = 2b_r \in \mathbb{Z}$. By (15), this implies that in addition to $t \equiv \mu \pmod{m}$ we also have $2b_r = \frac{1}{2m}(2t^2 - \mu) \in \mathbb{Z}$ which means $2t^2 - \mu \equiv 0 \pmod{2m}$.

Let us first consider the case $\mu = 0$. In this case the latter condition is implied by $t \equiv 0 \pmod{m}$. To see this, we consider the same differences that we did in the Type I solution, except that instead of $a_0 - a_{2^{r-1}}$ we use $a_{2^{r-3}} - a_{2^{r-3}+2^{r-1}} = 2b_{r+1}$. The only changes in this case are because the sums for $a_{2^{r-2}}$ and $a_{2^{r-3}}$ have been changed (because the term b_{r+1} has been shifted over by 2^{r-3} places). The new values now are (by (15)):

$$a_{2^{r-2}} - a_{2^{r-3}} = 2b_{r-1} - b_r - b_{r+1} = \frac{1}{2m}(2t^4 - t^2 - t), \text{ and}$$
$$a_{2^{r-3}} - a_{2^{r-4}} = 2b_{r-2} - b_{r-1} + b_{r+1} = \frac{1}{2m}(4t^8 - t^4 + t)$$

Since both of these new values (together with the other differences) are in $\mathbb{Z}$ if $t \equiv 0 \pmod{m}$, then the case of $\mu = 0$ is finished.

However, for $\mu = 1$, there is a difference. For the Type II solutions, in this case the two necessary conditions mentioned above now become $t \equiv 1 \pmod{m}$ and $t^2 \equiv 1 \pmod{2m}$, which are clearly contradictory. Hence, none

of the Type II polynomials with $\mu = 1$ can lie in $\mathbb{Z}[x]$ for any rational value of t.

We summarize these results in the following:

Theorem 5 *Let $n = m2^r \geq 2$ with m odd. Then any sum sequence S modulo n can be constructed as follows. Let $P^{(S)}(x)$ be the polyomial associated with S as described in Theorem 4. Then $P^{(S)}(x)$ must either come from a Type I solution with the choice of $t \equiv \mu \pmod{m}$ and $\mu = 0$ or 1, or from a Type II solution with the choice of $t \equiv 0 \pmod{m}$ and $\mu = 0$. We are then allowed to shift S by adding an arbitrary integer d modulo n to each element of S.*

We list a few small sum sequences below, using the corresponding polynomials.

$$3x^3 + 4x^2 + 3x + 6 \pmod 4,$$
$$x^4 + x^3 + x^2 + x + 2 \pmod 5,$$
$$x^4 + x^2 + x + 1 \pmod 6,$$
$$x^5 + 2x^4 + x^3 + 2x^2 + x + 2 \pmod 6,$$
$$2x^5 + 3x^4 + 2x^3 + 3x^2 + 2x + 4 \pmod 6,$$
$$x^7 + 3x^6 + x^5 + 2x^4 + 2x^3 + 3x^2 + 2x + 2 \pmod 8$$
$$2x^9 + x^8 + 2x^7 + x^6 + 2x^5 + x^4 + 2x^3 + x^2 + 2x + 2 \pmod{10}.$$

Notice that although $P(x)$ has $n = m2^r$ coefficients, these coefficients can take on at most $r + 2$ *different* values. Furthermore, for the normalized form in which the largest coefficient is a_0, no two coefficient values can differ by more than $O(\sqrt{a_0})$. From this perspective, in any sum sequence each residue occurs roughly the same number of times.

9 Augmented sum sequences

A natural extension of a sum sequence is that of an *augmented* sum sequence modulo n. If $S = (s_1, s_2, \ldots, s_d)$ is a sequence of residues modulo n, we say

that S is an *augmented* sum sequence if every $x \in \mathbb{Z}/n\mathbb{Z}$ can be represented in the same number λ of ways as a sum $s_i + s_j$ for $i \leq j$. The difference from the usual definition of a sum sequence is that now we allow the sums $s_i + s_i$. Thus, since there are now $\binom{d+1}{2}$ sums to consider, we have the necessary condition that $\binom{d+1}{2} = \lambda n$ in order that S could be an augmented sum sequence modulo n. For example, the multisets $(0, 0, 1, 1, 2)$ and $(0, 1, 2, 3, 4)$ are augmented sum sequences modulo 3, and modulo 5, respectively.

One could easily imagine that this slight extension in the definition of a sum sequence would only result in a minor change in the characterization of augmented sum sequences. However, this is definitely not the case! In fact, the two examples just listed (suitably generalized to odd moduli n) are all there are.

Theorem 6 *Let S be an augmented sum sequence modulo n. Then:*

(1) *n must be odd;*

(2) *Every residue modulo n must occur the same number of times in S with the possible exception that one residue may occur one fewer time than all the others.*

Proof of **(1)**. Suppose $n \geq 2$ is even and S is an augmented sum sequence modulo n. Let N_i denote the number of elements in S which are congruent to i modulo 2, for $i = 0, 1$. Then the number of pair sums from S which are *even* is just $\binom{N_0+1}{2} + \binom{N_1+1}{2}$ (since n is even). On the other hand, the number of pair sums which are *odd* is $N_0 N_1$. Since these two quantities must be equal, we have

$$\binom{N_0 + 1}{2} + \binom{N_1 + 1}{2} = \frac{1}{2}(N_0^2 + N_0 + N_1^2 + N_1) = N_0 N_1$$

which implies that $(N_0 - N_1)^2 + N_0 + N_1 = 0$, i.e., $N_0 = N_1 = 0$ which is a contradiction. This proves **(1)**.

Proof of **(2)**. Suppose $n \geq 3$ is odd and $S = \{s_1, s_2, \ldots, s_d\}$ is an augmented sum sequence modulo n. As in Section 3, we introduce a polynomial

$$Q^{(S)}(x) = \sum_{i=0}^{n-1} a_i x^i$$

where a_i denotes the number of indices j such that $s_j = i$.

Observe that if $S = \{s_1, s_2, \ldots, s_d\}$ is an augented sum sequence modulo n, then so is the sequence $S + c = (s_1 + c, s_2 + c, \ldots, s_d + c)$. Hence, the corresponding *shifted* polynomial $Q^{(S+c)}(x) = x^c Q^{(S)}(x) \mod (x^n - 1)$ is balanced. We will ordinarily omit the superscript (S) on $Q^{(S)}(x)$ and just write $Q(x)$ when S is understood. In order to prove **(2)**, we first need the following result.

Theorem 7 *Suppose $n \geq 3$ is an odd integer and $S = (s_1, s_2, \ldots, s_d)$ is a sequence of residues modulo n. Let $Q(x) = \sum_{i=0}^{n-1} a_i x^i$ be the associated polynomial where a_i is the number of indices j such that $s_j = i$. Then S is an augmented sum sequence modulo n if and only if $Q(\lambda)^2 = -Q(\lambda^2)$ for each complex number λ satisfying $\lambda^n = 1, \lambda \neq 1$.*

Proof: The proof is quite similar to that of Theorem 1. Let N_k denote the number of pair sums congruent to k mod n. Then

$$N_k = \begin{cases} \displaystyle\sum_{\substack{0 \leq i \leq j \leq n-1 \\ i+j \equiv k \pmod{n}}} a_i a_j - \frac{a_{\hat{k}}(a_{\hat{k}} - 1)}{2} & \text{where } 2\hat{k} \equiv k \pmod{n} \text{ if } n \text{ is odd,} \\ \displaystyle\sum_{\substack{0 \leq i \leq j \leq n-1 \\ i+j \equiv k \pmod{n}}} a_i a_j & \text{if } k \text{ is odd and } n \text{ is even,} \\ \displaystyle\sum_{\substack{0 \leq i \leq j \leq n-1 \\ i+j \equiv k \pmod{n}}} a_i a_j - \frac{a_{k/2}(a_{k/2} - 1)}{2} - \frac{a_{k/2+n/2}(a_{k/2+n/2} - 1)}{2} & \\ & \text{if } k \text{ is even and } n \text{ is even.} \end{cases}$$

Regarding subscripts modulo n, we have

$$\sum_{i=0}^{n-1} a_i a_{k-i} = \begin{cases} 2N_k - a_{\hat{k}} & \text{where } 2\hat{k} \equiv k \pmod{n} \text{ if } n \text{ is odd,} \\ 2N_k & \text{if } k \text{ is odd and } n \text{ is even,} \\ 2N_k - a_{k/2} - a_{k/2+n/2} & \text{if } k \text{ is even and } n \text{ is even.} \end{cases}$$

Suppose

$$Q(x)^2 = A(x) + x^n B(x)$$
$$Q(x^2) = C(x) + x^n D(x)$$

where A, B, C, D are of degree at most $n-1$. Similar to the proof in Theorem 1, we have

$$A(x) + B(x) = 2N(x) - C(x) - D(x)$$

where

$$N(x) = \sum_{k=0}^{n-1} N_k x^k.$$

We conclude that $(s_1, s_2, \ldots, s_d)$ is an augmented sum sequence modulo n if and only if $N(\lambda) = 0$ for λ satisfying $\lambda^n = 1$ and $\lambda \neq 1$, which is equivalent to

$$Q(\lambda)^2 = -Q(\lambda^2) \tag{28}$$

for all λ with $\lambda^n = 1, \lambda \neq 1$. This proves Theorem 7. □

To complete the proof of **(2)**, suppose that $Q(x)$ satisfies (28).
Define $P(x) = -Q(x)$. Then by (28), $P(x)$ satisfies

$$P(\lambda)^2 = P(\lambda)^2, \text{ for all } \lambda^n = 1, \lambda \neq 1.$$

Now we can apply Theorem 3 to $P(x)$. This implies that

$$Q(x) = a\left(\frac{1-x^n}{1-x}\right) - \mu x^\alpha$$

for some a where $\mu = 0$ or 1 and $0 \leq \alpha \leq n-1$. Of course, we can always normalize $Q(x)$ to have $\alpha = 0$. Interpreting the coefficients of $Q(x)$ in terms of the multiset S, we have proved Theorem 6. □

In particular, the two examples $\{0, 0, 1, 1, 2\}$ and $\{0, 1, 2, 3, 4\}$ presented at the beginning of the section are examples of the only two kinds of augmented sum sequences!

We point out that is not difficult to produce polynomials which satisfy (28) which have irrational or complex coefficients. For example, the following polynomials are balanced :

$$\frac{1}{2}x^4 - \left(\frac{1}{2}\sqrt{\frac{-3}{5}}\Big(x^3 - x^2 - x + 1\Big)\right) \pmod 5;$$

$$\frac{1}{2}x^{10} - \left(\frac{1}{2}\sqrt{\frac{3}{11}}\Big(x^9 - x^8 + x^7 + x^6 + x^5 - x^4 - x^3 - x^2 + x - 1\Big)\right) \pmod{11}.$$

10 Concluding remarks.

There are a number of questions we haven't addressed in the previous sections. For example, what are the possible *simple* sum sequences? These are sum sequences S having multiplicity $\lambda = 1$, i.e., each element of $\mathbb{Z}/n\mathbb{Z}$ has a unique representation as a sum of two distinct elements of S? We saw two examples of such sets in the introduction, namely $S = \{0, 1, 2\} \pmod 3$ and $S = \{0, 1, 2, 4\} \pmod 6$. It turns out that these are all there are (up to cyclic shifts)! This follows easily from our characterization of those $P(x) \in \mathbb{Z}$ together with the constraint that for these sets to exist, n must be an *even* triangular number.

Another problem which arises is to characterize those sum sequences that have no repeated elements, i.e., are actual subsets of $\mathbb{Z}/n\mathbb{Z}$. For example, all of $\mathbb{Z}/n\mathbb{Z}$ for any odd n is such a set. It is not hard to show that these together with $\{0, 1, 2, 4\} \pmod 6$ are all there are of these, as well.

Of course, a natural direction to explore is to address these same questions for finite abelian groups. For *sum sets* this has already been started in [11, 12, 1], for example. However, it remains to be explored for sum *sequences*. For example, consider the group $\mathbb{Z}_2 \times \mathbb{Z}_2$ with the four elements $(i, j),\ i, j = 0 \text{ or } 1$. Then the infinite family of sequences consisting of $4t^2 + t$ copies of three of these elements together with $4t^2 + 5t + 1$ copies of the fourth element (in some order) is a sum sequence for this group for any value of $t \geq 1$.

While there are relatively few augmented sum sequences for $\mathbb{Z}/n\mathbb{Z}$, there may be more for other abelian groups. For example, if G has odd order then the sequence consisting of α copies of G but with one element of G removed is an augmented sum sequence for G. In fact, there is no reason to restrict our attention to abelian groups. For example, for S_3, the permutation group on the set $\{1, 2, 3\}$, the sequence $S = (s_1, s_2, s_3, s_4) = (id, (1, 2), (1, 2, 3), (1, 3, 2))$ is an example of a simple sum sequence for S_3. That is, every element of S_3 can be represented uniquely as $s_i s_j,\ i < j$. (where the product is composition of permutations). We think that these more general questions are quite interesting and we hope to return to some of them in the near future.

11 Acknowledgements

The authors would like to acknowledge helpful discussions with Joe Buhler and Daniel Kane during the course of writing this paper as well as the useful comments of several anonymous referees.

References

[1] R. S. Coulter and T. Gutekunst, Subsets of finite groups exhibiting additive regularity, *Discrete Math.* **313** (2013), 236–248.

[2] J. R. Isbell, Perfect addition sets, *Discrete Math.* **24** (1978), 13–18.

[3] C. W. H. Lam, A generalization of cyclic difference sets, I, II, *J. Combin. Theory* (A) **19A** (1975). 51–65; 177–191.

[4] C. W. H. Lam, Cyclotomy and addition sets, *J. Combin. Theory* (A) **22A** (1977) 43–60.

[5] C. W. H. Lam, The Search for a Finite Projective Plane of Order 10, *Amer. Math. Monthly* **98** (1991), 305–318.

[6] C. W. H. Lam, S. L. Ma and M. K. Siu, The existence and nonexistence of perfect addition sets, *J. Combin. Theory* (A) **35** (1983), 67–78.

[7] S. Lang, *Algebraic Number Theory* second edition, Graduate Texts in Mathematics **110**. Springer Verlag, New York, (1994) xiv + 357pp.

[8] W. J. Leveque, *Elementary Theory of Numbers*, Dover Books on Advanced Mathematics, Dover, New York, (1990) viii + 132 pp.

[9] E. H. Moore and H. S. Pollatsek, *Difference Sets*, Student Mathematical Library vol. 47, Amer. Math. Soc., Providence, RI, (2013), xiii + 298 pp.

[10] I. Stewart, *Galois Theory* second edition, Chapman and Hall, New York, (1989) x+202 pp.

[11] J. S. Sumner, Generalized Addition Sets, Ph.D. Thesis, University of Miami, Coral Gables, Fla., 1980.

[12] J. S. Sumner and A. T. Butson, Addition sets in a finite group, *J. Combin. Theory* (A) **32** (1982), 350–369.