CYCLOTOMIES AND DIFFERENCE SETS MODULO A PRODUCT OF TWO DISTINCT ODD PRIMES

Thomas Storer

1. INTRODUCTION

A theory of cyclotomy modulo a product of two distinct odd primes was developed in [5], where it was used in the construction of a family $\{W_e\}$ of difference sets. Necessary and sufficient conditions for the existence of W_e-difference sets were given, with a detailed analysis of the cases $e = 2, 4$. In [1] it was shown that W_6- and W_8-difference sets do not exist, and it has been conjectured that those of type W_{2n} exist for no $n > 2$.

The purpose of the present paper is to investigate some other cyclotomies modulo a product of two distinct odd primes, and to determine necessary and sufficient conditions that certain subsets of the above residue systems constitute difference sets.

2. CYCLOTOMY MODULO A PRODUCT OF PRIMES

Throughout the paper, p and q denote distinct odd primes, ζ and η divisors of $p - 1$ and $q - 1$, respectively, and g an integer modulo pq that belongs to the exponents $\frac{p-1}{\zeta}$ modulo p and $\frac{q-1}{\eta}$ modulo q. Further, we define

$$e = \text{g.c.d.}\,(p - 1, q - 1), \quad \varepsilon = \text{g.c.d.}\left(\frac{p-1}{\zeta}, \frac{q-1}{\eta}\right), \quad f = \frac{p-1}{e}, \quad f' = \frac{q-1}{e}, \quad d = eff'.$$

If g has d distinct powers modulo pq, we call g a *generator* (or, alternately, a *quasi-primitive root*) of pq; when $\zeta = \eta = 1$, g is called a *primitive root* of pq. We shall be concerned with the special case $\zeta = 1$.

LEMMA 1. *If* g' *is a primitive root of* q, *and if* g *is a generator of* pq *and*

$$x \equiv 1 \pmod p \quad \textit{and} \quad x \equiv g' \pmod q,$$

then the de *integers*

$$g^s x^i \quad (s = 0, 1, \cdots, d - 1;\ i = 0, 1, \cdots, e - 1)$$

constitute a reduced residue system modulo pq.

This lemma (as well as further lemmas whose proofs we suppress) can be proved by techniques developed in [5]. We remark that, if η is odd, then g is a nonsquare modulo q. Also, $\alpha = \text{g.c.d.}\,(\eta, f') = 1$, since otherwise $g^{d/\alpha} \equiv 1 \pmod{pq}$.

COROLLARY 1. *There is an integer* μ: $0 \le \mu \le d - 1$ *such that* $x^e \equiv g^\mu \pmod{pq}$.

Received June 2, 1966.

Supported by a National Science Foundation Post-doctoral Research Grant.

COROLLARY 2. *There is an integer* ν: $0 \leq \nu \leq d - 1$ *such that*

$$-1 \equiv \begin{cases} g^{d/2} \pmod{pq} & \text{if } ff'\eta \text{ is odd,} \\ g^{\nu} x^{e/2} \pmod{pq} & \text{if } ff'\eta \text{ is even.} \end{cases}$$

For the fixed elements g and x, we now define the *cyclotomic classes* C_i $(i = 0, 1, \cdots, e - 1)$ by the rule

$$C_i = \{g^s x^i \pmod{pq}: s = 0, 1, \cdots, d - 1\}.$$

For fixed i and j, the *cyclotomic number* (i, j) is the number of solutions modulo pq in s and t $(s, t = 0, 1, \cdots, d - 1)$ of the trinomial congruence

$$g^s x^i + 1 \equiv g^t x^j \pmod{pq}.$$

LEMMA 2. *The cyclotomic numbers satisfy the following relations.*

(i) $(i, j) = (i \pm ae, j \pm be)$ *for all integers* a *and* b;

(ii) $(i, j) = (e - i, j - i)$;

(iii)
$$(i, j) = \begin{cases} (j, i) & \text{if } ff'\eta \text{ is odd,} \\ \left(j + \frac{e}{2}, i + \frac{e}{2}\right) & \text{if } ff'\eta \text{ is even;} \end{cases}$$

(iv) *if* $-1 \in C_I$, *then*

$$\sum_{j=0}^{e-1} (i, j) = \frac{(p - 2)(q - 1)}{e} - \eta \frac{p - 1}{e} \gamma_i + \delta_i,$$

where $\gamma_i = \begin{cases} 1 & \text{if } I + i \equiv 0 \pmod{\eta}, \\ 0 & \text{otherwise} \end{cases}$ *and* $\delta_i = \begin{cases} 1 & \text{if } i = I, \\ 0 & \text{otherwise.} \end{cases}$

LEMMA 3. $\eta \mid e$.

Proof. g belongs to the exponent $\frac{(p - 1)(q - 1)}{\varepsilon\eta} = \frac{(p - 1)(q - 1)}{e} = d$ modulo pq. ∎

When $\eta = 1$, the discussion reduces to the case where g is a primitive root of pq [5].

LEMMA 4. (i) *Let* g^* *be a primitive root of* q *other than* g', *and use Lemma* 1 *with* g^* *in place of* g' *to define an integer* $x^* \equiv g^u x^k \pmod{pq}$. *Then* g.c.d. $(k, e) = 1$, *and if* $(i, j)^*$ *are the cyclotomic numbers corresponding to* g *and* x^*, *then*

$$(i, j)^* = (ki, kj).$$

(ii) *For each* η *there are* $\phi(\varepsilon)$ *disjoint classes* G_i $(i = 0, 1, \cdots, \phi(\varepsilon) - 1)$ *of generators* g *of* pq *characterized by the following: If* $g \in G_i$ *and* g.c.d. $(r, d) = 1$, *then* $g^r \in G_i$.

Proof of (ii). $\phi(p-1)\phi\left(\frac{q-1}{\eta}\right) = \phi(\varepsilon)\phi(d)$. ■

We remark that for fixed x, the elements g and g^r generate the same cyclotomy modulo pq.

3. DIFFERENCE SETS MODULO pq

We define several subsets of the integers modulo pq:

$$P = \{ap: a \in \text{RRS (mod q)}\},$$

$$Q = \{aq: a \in \text{RRS (mod p)}\},$$

$$Q^* = \{aq: a \in \text{CRS (mod p)}\},$$

$$P^1 = \{ap: (a/q) = -1\},$$

$$P^2 = \{ap: (a/q) = +1\}.$$

For each pair g and x, we define the sets

$$D_1 = C_0 + Q^*, \qquad D_2 = C_0 + P^1 + Q,$$

and we shall discuss conditions under which D_i constitutes a difference set modulo pq in terms of η.

The following lemma is independent of η.

LEMMA 5. (i) *If α is an element of P^1, then the number of solutions of the congruence* $\beta - \gamma \equiv \alpha$ (mod pq) $(\beta, \gamma \in P^1)$ *is*

$$\frac{q-5}{4} \text{ if } q \equiv 1 \pmod 4, \qquad \frac{q-3}{4} \text{ if } q \equiv 3 \pmod 4.$$

(ii) *If α is an element of P^2, then the number of solutions of the above congruence is*

$$\frac{q-1}{4} \text{ if } q \equiv 1 \pmod 4, \qquad \frac{q-3}{4} \text{ if } q \equiv 3 \pmod 4.$$

Proof. The number of solutions in (i), for example, of our congruence is precisely the number of times that the difference of two nonsquares is again a nonsquare modulo q. ■

4. THE CASE $\eta = 1$

It was shown in [5] that D_1 forms a difference set modulo pq if and only if

A(i) $$q = (e-1)p + 2,$$

A(ii) $$(i, 0) = (e-1)\left(\frac{p-1}{e}\right)^2 \qquad (i = 0, 1, \cdots, e-1).$$

Quite similarly, it can be shown that D_2 forms a difference set modulo pq if and only if

B(i) $$q = 4(e - 1)\left(\frac{p - 1}{e}\right) - 1,$$

B(ii) $$(0, 0) = (i, 0) + 3 = \frac{(p - 1 - e)(q + e^2 - 2e - 1)}{e^2} + (e - 1) \quad (i = 1, 2, \cdots, e - 1).$$

LEMMA 6. *If* $\eta = 1$, *then for no primes* p *and* q *does* D_2 *form a difference set* modulo pq.

Proof. Let

$$M = (i, 0) = \frac{(p - 1 - e)(q + e^2 - 2e - 1)}{e^2} + (e - 4) \quad (i = 1, 2, \cdots, e - 1).$$

Then

$$\sum_{i=0}^{e-1} (i, 0) = (e - 1)M + (M + 3) = \frac{(p - 2)(q - 2) - 1}{e} + 1,$$

so that $e^2 M = (p - 2)(q - 2) - 2e - 1$. Substituting the value of M into this equation and simplifying, we find that

$$q = (e - 1)(p - 3) - 1,$$

which, together with condition B(i), implies that $\frac{p - 1}{e} = \frac{p - 3}{4}$, whence $e = 6$ and $p = 7$. Then B(i) gives $q = 19$; but both inequivalent cyclotomies modulo $7 \cdot 19 = 133$ have $(0, 0) = 0$ for $\eta = 1$, in violation of B(ii). ■

5. THE CASE $\eta = 2$

LEMMA 7. *A necessary condition that* D_i $(i = 1, 2)$ *be a difference set* modulo pq *is that* $q \equiv 3 \pmod 4$.

Proof. Suppose $q \equiv 1 \pmod 4$. Exactly one of the elements $1 - nq$ $(n = 0, 1, \cdots, p - 1)$ is congruent to mp modulo pq. If $(m/p) = 1$ (or $(m/p) = -1$), then

$$g^s(1 - nq) = m'p \quad \text{and} \quad \left(\frac{m'}{p}\right) = 1 \quad \left(\text{or } \left(\frac{m'}{p}\right) = -1\right).$$

Hence only P^2 (only P^1) occurs among the C_0-Q-differences. Further, since $(-1/q) = 1$,

$$\left(\frac{g^s(1 - nq)}{p}\right) = \left(\frac{g^s(nq - 1)}{p}\right).$$

But P occurs among the C_0-C_0-differences $\left(\frac{p - 1 - e}{e}\right)\left(\frac{q - 1}{e}\right)$ times.

Now consider D_2. Arguing as above, we can show that, exclusive of the P^1-P^1-differences, P^1 and P^2 each occur an even number of times. But P^1 and P^2 occur $\frac{q-5}{4}$ and $\frac{q-1}{4}$ times, respectively, among the P^1-P^1-differences. ∎

We now examine the ways in which elements of P and Q (or P and Q^*) can arise among the D_i-D_i-differences (i = 1, 2) for $q \equiv 3 \pmod 4$.

LEMMA 8. *The number of solutions of the congruence* $x - y \equiv z \pmod{pq}$ *is*

(i) $\frac{(p-1)(q-1-e)}{e^2}$ $\quad (x, y \in C_0,\ z \in P)$,

(ii) $\eta\,\frac{(p-1-\varepsilon)(q-1)}{e^2}$ $\quad (x, y \in C_0,\ z \in Q$ *or* $z \in Q^*)$,

(iii) $\frac{q-3}{4}$ $\quad (x, y \in P^1,\ z \in P)$,

(iv) p $\quad (x, y, z \in Q^*)$,

(v) $p - 2$ $\quad (x, y, z \in Q)$,

(vi) $\eta\,\frac{p-1}{e}$ $\quad (x \in C_0,\ y \in Q$ *or* $y \in Q^*,\ z \in P)$,

(vii) $\left[1 - \left(\frac{p}{q}\right)\right]\frac{q-1}{e}$ $\quad (x \in C_0,\ y \in P^1,\ z \in Q)$.

Proof. (ii) Consider the differences

$$g^{i+m(q-1)/\eta} - g^i \quad \left(m = 1, \cdots, \frac{p-1-\varepsilon}{\varepsilon};\ i = 0, \cdots, d-1\right).$$

There are $\frac{p-1-\varepsilon}{\varepsilon}$ classes of differences, each class containing $p - 1$ distinct elements, and each element occurring $\frac{q-1}{e}$ times.

(vi) The proof is contained in the proof of Lemma 7.

(vii) If $(\alpha/q) = -1$ and the congruence $1 - \alpha p \equiv nq \pmod{pq}$ has solutions, then it has exactly one, and in this case

$$Q = \{g^i(1 - ap) \pmod{pq}: i = 0, 1, \cdots, p-2\}.$$

(Whether such an α exists clearly depends upon the quadratic character of p with respect to q.) Hence each element $z \in Q$ occurs $\frac{q-1}{e}$ times among the C_0-P^1-differences; similarly, it occurs $\frac{q-1}{e}$ times as a P^1-C_0-difference. Otherwise, the element z does not occur. ∎

From Lemmas 7 and 8 we get immediately the following necessary conditions for D_i (i = 1, 2) to be a difference set modulo pq when $\eta = 2$:

(1) When $\eta = 2$, D_1 is a difference set modulo pq only if

$$q \equiv 3 \pmod 4 \qquad \text{and} \qquad q = -\frac{(e^2 - e - 1)p + (2e + 1)}{p - (e + 1)}.$$

(2) When $\eta = 2$, D_2 is a difference set modulo pq only if

$$q \equiv 3 \pmod 4 \qquad \text{and} \qquad q = \frac{(1 + 2\varepsilon - 4\varepsilon^2)p - [1 + 2(\varepsilon \pm \varepsilon) - 5\varepsilon^2]}{p - (1 \pm \varepsilon)^2},$$

where the + or - sign is chosen, throughout, according as $(p/q) = +1$ or $(p/q) = -1$.

It is clear from the second condition in (1) that when $\eta = 2$, D_1 cannot form a difference set modulo pq for any primes p and q, since $e + 1 \leq p$. We now examine the case for D_2 with $\eta = 2$ for the first few values of $\varepsilon = e/2$ (note that $p < (1 \pm \varepsilon)^2$):

If $\varepsilon = 1$, then $p = 3$ and $q = 1$ or $q = \frac{1}{3}$.

The case $\varepsilon \equiv 0 \pmod 2$ cannot occur, since $q \equiv 1 \pmod e \equiv 3 \pmod 4$.

If $\varepsilon = 3$, then $p = 7$, $q = 19$ or $p = 13$, $q = 115$.

If $\varepsilon = 5$, then $p = 11$ and $q = 35$ or $q = 171$; or $p = 31$, $q = 531$.

If $\varepsilon = 7$, then $p = 29$ and $q = \frac{719}{5}$ or $q = 715$; or $p = 43$, $q = \frac{1081}{3}$.

If $\varepsilon = 9$, then $p = 19$ and $q = 67$ or $q = \frac{599}{5}$; or $p = 37$ and $q = \frac{1213}{7}$ or $q = 403$; or $p = 73$, $q = 811$.

Hence, for $e \leq 20$, $\eta = 2$, there are two possibilities:

$$\left.\begin{array}{l} e = 6;\ \ p = 7,\ \ q = 19 \\ e = 18:\ p = 73,\ q = 811 \end{array}\right\} (p/q) = 1,$$

whence $\lambda = \frac{(p - 1)(q - 1 - e)}{e^2} + \frac{q - 3}{4} + \eta\,\frac{p - 1}{e} = 8, 386$; respectively.

Proceeding as in Lemma 8, we find that for $\eta = 2$, D_2 forms a difference set modulo pq if and only if

(i) $q \equiv 3 \pmod 4$,

(ii) $q = \frac{(1 + 2\varepsilon - 4\varepsilon^2)p - [1 + 2(\varepsilon \pm \varepsilon) - 5\varepsilon^2]}{p - (1 \pm \varepsilon)^2}$,

(iii) $\lambda = \frac{(p - 1)(q - 1 - e)}{e^2} + \frac{q - 3}{4} + \frac{p - 1}{\varepsilon} = (0, 0) + \eta\,\frac{p - 1}{e} + N_0 + N_\varepsilon$, and

$$(i, 0) = (0, 0) - 1 + N_0 + N_\varepsilon - N_i - N_{\varepsilon+i} \qquad (i = 1, 2, \cdots, e - 1),$$

where N_i is the number of solutions of the congruence

$$y + 1 \equiv z \pmod{pq} \qquad (y \in C_i,\ z \in P^1).$$

We remark that it is not necessary to construct C_i $(i = 1, 2, \cdots, e - 1)$ in order to evaluate N_i, since N_i is also the number of solutions of the congruence

$$y + x^{e-1} \equiv z \pmod{pq} \qquad \left(y \in C_0,\ z \in \begin{cases} P^1 & \text{if } i \text{ is even,} \\ P^2 & \text{if } i \text{ is odd} \end{cases}\right).$$

We now examine the set D_2 for the cases where $p = 7$, $q = 19$ or $p = 73$, $q = 811$.

Case 1. $p = 7$, $q = 19$; $e = 6$: $v = 133$, $k = 32$, $\lambda = 8$.

There are $\phi(\varepsilon) = 2$ distinct classes of generators modulo 133 for $\eta = 2$:

$$G_0 = \{5, 54, 66, 80, 101, 131\}, \qquad G_1 = \{17, 24, 47, 61, 73, 82\}.$$

Let us choose $x = 15$.

If we let 5 and 17 represent G_0 and G_1, respectively, then

$$D_2 = \{1, 5, 125, 93, 66, 64, 54, 4, 20, 100, 101, 106, 131, 123, 16, 80;$$
$$14, 21, 56, 70, 84, 91, 98, 105, 126; 19, 38, 57, 76, 95, 114\} \text{ modulo } 133,$$
$$D_2^* = \{1, 17, 23, 125, 130, 82, 64, 24, 9, 20, 74, 61, 106, 73, 44, 83, 81, 47;$$
$$14, 21, 56, 70, 84, 91, 98, 105, 126; 19, 38, 57, 76, 95, 114\} \text{ modulo } 133.$$

For D_2, we find directly that

$$N_0 = 1, \quad N_1 = 1, \quad N_2 = 2, \quad N_3 = 3, \quad N_4 = 1, \quad N_5 = 1$$

and $(0, 0) = 2$, $(1, 0) = 3$, $(2, 0) = 2$. Hence

$$(i, 0) = (0, 0) - 1 + N_0 + N_\varepsilon - N_i - N_{i+\varepsilon} \qquad (i = 1, 2, \cdots, 5)$$

and

$$\lambda = \frac{(p-1)(q-1-e)}{e^2} + \frac{q-3}{4} + \eta\,\frac{p-1}{e} = 8.$$

Therefore D_2 forms a difference set modulo 133 with $v = 133$, $k = 32$, $\lambda = 8$ [4, page 986].

For D_2^*, we find that

$$N_0 = 3, \quad N_1 = 1, \quad N_2 = 1, \quad N_3 = 1, \quad N_4 = 2, \quad N_5 = 1$$

and $(0, 0) = 4$, $(1, 0) = 1$, $(2, 0) = 2$. Now

$$1 = (1, 0) \neq (0, 0) - 1 + N_0 + N_\varepsilon - N_i - N_{i+\varepsilon} = (0, 0) = 4;$$

hence D_2^* does not form a difference set modulo 133.

Case 2. $p = 73$, $q = 811$; $e = 18$: $v = 59203$, $k = 3717$, $\lambda = 386$.

It would be tedious indeed to verify the sufficient condition (iii) that D_2 be a difference set modulo 59203; instead, we employ the elementary necessary condition $k(k - 1) = \lambda(v - 1)$. In this case, we find that

$$k(k - 1) < 16000 < \lambda(v - 1).$$

Hence no difference set occurs in this case.

6. A RELATED CYCLOTOMY; $\eta = 2$, $\varepsilon = e$

When $\eta = 2$ and $\varepsilon = \text{g.c.d.}\left(p - 1, \frac{q-1}{\eta}\right) = e$, then $f = \frac{p-1}{e}$, $f' = \frac{q-1}{2e}$, and $d' = eff'$. Hence g is not a generator of pq. In this case we define x as in the following lemma.

LEMMA 9. *Let* g' *and* g'' *be primitive roots of* p *and* q, *respectively, and define* x (modulo pq) *by the conditions*

$$x \equiv g' \pmod p, \qquad x \equiv g'' \pmod q.$$

Then, when $\eta = 2$, $\varepsilon = e$, *the* 2ed *integers*

$$g^s x^i \qquad (s = 0, 1, \cdots, d - 1;\ i = 0, 1, \cdots, 2e - 1)$$

constitute a reduced residue system modulo pq.

We again define $C_i = \{g^s x^i : s = 0, 1, \cdots, d - 1\}$ for $i = 0, 1, \cdots, 2e - 1$, and we easily derive results for this system corresponding to the Lemmas 2, 3, and 4.

7. DIFFERENCE SETS MODULO pq; $\eta = 2$, $\varepsilon = e$

Using the above methods we can prove the following theorem.

THEOREM 1. *If* $\eta = 2$, $\varepsilon = e$, *and* f' *is even, then the set* $C_0 + C_1 + Q^*$ *forms a difference set* modulo pq *if and only if*

(1) $$3q = 2(e+1)p + 1,$$

(2) $$(i, 0) + (i - 1, 0) + (i, 1) + (i + e, 1) = (e+1)\left(\frac{p-1}{e}\right)^2 - 2\left(\frac{p-1}{e}\right)$$

$$(i = 0, 1, \cdots, 2e - 1).$$

COROLLARY. *If* $C_0 + C_1 + Q^*$ *forms a difference set* modulo pq, *then* $\lambda = (e+1)\left(\frac{p-1}{e}\right)^2$.

Clearly there is no difference set of the above type for $e = 2$, for then $0 \equiv 3q \not\equiv 6p + 1 \equiv 1 \pmod 3$ by the necessary condition (1) of the theorem.

When $e = 4$, the form of the cyclotomic matrix is

i \ j	0	1	2	3	4	5	6	7
0	A	B	C	D	E	F	G	H
1	I	J	K	L	F	D	L	M
2	N	O	N	M	G	L	C	K
3	J	O	O	I	H	M	K	B
4	A	I	N	J	A	I	N	J
5	I	H	M	K	B	J	O	O
6	N	M	G	L	C	K	N	O
7	J	K	L	F	D	L	M	I

Array 1.

(by Lemma 2, (i), (ii), and (iii)); therefore condition (2) of the theorem becomes

$$\left.\begin{array}{c} A+B+I+J \\ A+H+I+J \\ I+M+N+O \\ J+K+N+O \end{array}\right\} = (e+1)\left(\frac{p-1}{e}\right)^2 - 2\left(\frac{p-1}{e}\right).$$

Then, a modification of the techniques developed in [2], [3], and [5] can be used to prove the following result.

LEMMA 10. *If* $\eta = 2$, $e = \varepsilon = 4$, *and* f' *is even, then the inequivalent cyclotomic numbers can be given in the form*

$$32A = 4M_0 + 7 + 2a + 3x + 2S + 2X,$$

$$32B = 4M_1 - 1 + 4b + 2c - x + 2y + 2T + 2X + 4Y,$$

$$32C = 4M_0 - 1 + 2a + 4c - x + 2S - 4T - 2X,$$

$$32D = 4M_1 - 1 - 2c + 4d - x - 2y - 2T + 2X + 4Y,$$

$$32E = 4M_0 - 1 - 6a + 3x - 6S - 6X,$$

$$32F = 4M_1 - 1 - 4b + 2c - x + 2y + 2T + 2X - 4Y,$$

$$32G = 4M_0 - 1 + 2a - 4c - x + 2S + 4T - 2X,$$

$$32H = 4M_1 - 1 - 2c - 4d - x - 2y - 2T + 2X - 4Y,$$

$$32I = 4M_1 + 3 - 2c - x + 2y - 2T - 2X,$$

$$32J = 4M_1 + 3 + 2c - x - 2y + 2T - 2X,$$

$$32K = 4M_1 - 1 + 2a + 2b + 2d + x - 2S - 4Y,$$

$$32L = 4M_1 - 1 - 2a + 2b - 2d + x + 2S,$$

$$32M = 4M_1 - 1 + 2a - 2b - 2d + x - 2S + 4Y,$$

$$32N = 4M_0 + 3 - 2a - x - 2S + 2X,$$

$$32O = 4M_1 - 1 - 2a - 2b + 2d + x + 2S,$$

where $2eM_1 = (p - 2)(q - 1)$, $eM_0 = eM_1 - 2(p - 1)$, and

$$pq = a^2 + b^2 + c^2 + d^2,$$

$$q = x^2 + y^2, \qquad x \equiv 1 \pmod 4,$$

$$pq = S^2 + T^2, \qquad S \equiv 1 \pmod 4,$$

$$q = X^2 + 2Y^2, \qquad X \equiv 1 \pmod 4,$$

the signs of y, T, and Y being ambiguously determined.

Hence by Lemma 10, Theorem 1 for $e = 4$ can be restated as follows.

THEOREM 2. *If $\eta = 2$, $e = \varepsilon = 4$, and f' is even, then necessary conditions for the existence of a difference set of the type described in Theorem 1 are*

(1) $$y + 2Y = 0, \quad b + c + d + T = 0, \quad 2 + a + b - d + S = 0;$$

(2) $$M_0 + 3M_1 + 2 = 8\left[5\left(\frac{p-1}{4}\right)^2 - 2\left(\frac{p-1}{4}\right)\right].$$

Condition (2) reduces to $(p - 5)(5p - 4) = 0$, and condition (1) of Theorem 1 with $p = 5$ yields $q = 17$. Hence there are at most $\phi(\varepsilon) = 2$ difference sets of the above type, that is, modulo 85.

Inspection of the decompositions of $pq = 85$ and $q = 17$ show that there is at most one difference set modulo 85 (by condition (2) of Theorem 2), when

$$a = -3, \ b = -2, \ c = -6, \ d = 6;$$

$$x = 1, \quad y = -4;$$

$$S = 9, \quad T = 2;$$

$$X = -3, \ Y = 2.$$

Substitution of these constants into Lemma 10 yields the set of values

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	0	0	2	0	0	2	0	1	1	0	1	0	0	2

which, by Array 1, determines all the cyclotomic numbers corresponding to this case.

This cyclotomy is afforded, for example, by the choice $g = 2$, $x = 7$. The difference set arising from Theorem 1 is then the set

$$C_0 + C_1 + Q^* = \{1, 2, 4, 8, 16, 32, 64, 43;\ 7, 14, 28, 56, 27, 54, 23, 46;\ 0, 17, 34, 51, 68\} \text{ modulo } 85,$$

which corresponds (see [4, p. 98]) to a plane in 3-space.

REFERENCES

1. J. W. Bergquist, *Difference sets and congruences modulo a product of primes*, Dissertation, University of Southern California (1963).

2. L. Carlitz and A. L. Whiteman, *The number of solutions of some congruences modulo a product of primes*, Trans. Amer. Math. Soc. 112 (1964), 536-552.

3. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. 57 (1935), 391-424.

4. M. Hall, Jr., *A survey of difference sets*, Proc. Amer. Math. Soc. 7 (1956), 975-986.

5. A. L. Whiteman, *A family of difference sets*, Illinois J. Math. 6 (1962), 107-121.

The University of Michigan