# A FAMILY OF DIFFERENCE SETS[1]

To my revered teacher Hans Rademacher
on his seventieth birthday

BY
ALBERT LEON WHITEMAN

## 1. Introduction

A set of $k$ distinct residues $r_1, r_2, \cdots, r_k$ modulo $v$ is called a difference set if all nonzero residues modulo $v$ occur $\lambda$ times among the differences $r_i - r_j$ $(i \neq j)$. The integers $v, k, \lambda$ are called the parameters of the set and satisfy the relation $k(k-1) = \lambda(v-1)$. Difference sets arise in a natural way in many combinatorial and statistical problems and have been extensively studied. There is given in [8] a survey of all difference sets with parameters $v, k, \lambda$ for which $k$ is in the range $3 \leqq k \leqq 50$.

The problem studied in this paper was suggested to the author by the following theorem of Stanton and Sprott [10].

THEOREM. *Let $g$ be a primitive root of both $p$ and $p+2$, where $p$ and $p+2$ are a pair of twin primes. Then the numbers*

$$1, g, g^2, \cdots, g^{(p^2-3)/2}; \quad 0, p+2, 2(p+2), \cdots, (p-1)(p+2)$$

*form a difference set with parameters $v = p(p+2)$, $k = (v-1)/2$, $\lambda = (v-3)/4$.*

In the light of this theorem our problem may now be described as follows. Let $g$ denote a common primitive root of two distinct primes $p$ and $q$. Let $e$ denote the greatest common divisor of $p-1$ and $q-1$, and let $d$ be defined by means of the equation $(p-1)(q-1) = de$. We shall investigate the conditions under which the set of numbers

$$1, g, g^2, \cdots, g^{d-1}; \quad 0, q, 2q, \cdots, (p-1)q \tag{1.1}$$

constitutes a difference set with the parameters

$$v = pq, \qquad k = (v-1)/e, \qquad \lambda = (v-1-e)/e^2. \tag{1.2}$$

Necessary and sufficient conditions for the existence of such difference sets are given in Theorem 1 of §3. Since $k = d + p$, we have at once the necessary condition: $q = (e-1)p + 2$. That this condition is also sufficient when $e = 2$ is a consequence of the Stanton-Sprott theorem. Indeed, we show in §4 that Theorem 1 with $e = 2$ actually reduces to the Stanton-Sprott theorem.

In §5 we consider the case $e = 4$. We prove in Theorem 4 that if $g$ is suitably selected, then the set of numbers (1.1) forms a difference set with the

Received March 3, 1961.
[1] This research was sponsored in part by the National Science Foundation.

parameters (1.2) if and only if $q = 3p + 2$ and $(v - 1)/4$ is an odd square. This result resembles a theorem of Chowla [5] which states that the biquadratic residues modulo a prime $p = 4f + 1$ form a difference set if and only if $(p - 1)/4$ is an odd square. Theorem 4 exhibits a family of difference sets not previously known. The simplest example in this family has the parameters $v = 901, k = 225, \lambda = 56$ and consists of the numbers

$$1, 5, 5^2, \cdots, 5^{207}; \quad 0, 53, 106, \cdots, 848.$$

It is of interest to digress and point out that the Stanton-Sprott theorem has an important application in the theory of Hadamard matrices.[2] These are the square matrices with entries $\pm 1$ and of order $N$ such that $HH^T = NI$. Here $H^T$ is the transpose of $H$, and $I$ is the identity matrix of order $N$. By a theorem of Todd [11] the existence of a difference set with parameters $v = 4t - 1, k = 2t - 1, \lambda = t - 1$ implies the existence of a Hadamard matrix of order $4t$. Hence the Stanton-Sprott theorem implies the following theorem of Gruner [7]:[3] If $p$ and $p + 2$ are twin primes, then there exist Hadamard matrices of order $p(p + 2) + 1$.

The method of this paper is based on cyclotomy. Since the modulus $v$ in (1.2) is composite, a modified approach is necessary. The usual formulation of cyclotomic theory is based on the fact that if $g$ is a primitive root of a prime $p$, then the $p - 1$ numbers $g^s$ $(s = 0, 1, \cdots, p - 2)$ constitute a reduced residue system modulo $p$. However, if $p$ and $q$ are distinct primes, the modulus $v = pq$ does not possess a primitive root. In §2 we get around this difficulty by employing a common primitive root $g$ of $p$ and $q$ and establishing the existence of a number $x$ such that the $(p - 1)(q - 1)$ numbers $g^s x^i$ $(s = 0, \cdots, d - 1; i = 0, \cdots, e - 1)$ constitute a reduced residue system modulo $v$.

In summary, we repeat that this paper is concerned with the cases $e = 2$ and $e = 4$; we plan in a later paper to discuss the cases $e = 6$ and $e = 8$.

## 2. Cyclotomy modulo $v$

Let $v = pq$, where $p$ and $q$ are distinct primes. In this section we develop the rudiments of a theory of cyclotomy modulo $v$. Lemma 1 overcomes the difficulty that arises because $v$ does not possess a primitive root. Although our method is rather different, we follow the pattern of the modulo $p$ case as presented by Bachmann [1].

The main tool may be stated as follows.

LEMMA 1.[4] *Let $g$ be a fixed primitive root of both $p$ and $q$; let $e$ denote the greatest common divisor of $p - 1$ and $q - 1$, and put $(p - 1)(q - 1) = de$.*

[2] A summary of the literature concerning the existence problem for Hadamard matrices is available in [2].

[3] The author is indebted to Alfred Brauer for this reference. Gruner's theorem was rediscovered by Brauer in [3].

[4] The author wishes to thank Professor N. J. Fine for kindly suggesting the proof of Lemma 1.

*Then there exists an integer $x$ such that the de integers $g^s x^i$ ($s = 0, \cdots, d-1$; $i = 0, \cdots, e-1$) constitute a reduced residue system modulo $v$.*

*Proof.* The existence of a common primitive root $g$ of $p$ and $q$ is assured by the Chinese remainder theorem. Let $x$, $y$ be a pair of integers satisfying the simultaneous congruences

$$\begin{aligned} x &\equiv g \pmod{p}, \qquad y \equiv 1 \pmod{p}, \\ x &\equiv 1 \pmod{q}, \qquad y \equiv g \pmod{q}. \end{aligned} \tag{2.1}$$

That unique values of $x$ and $y$ exist modulo $v$ is also assured by the Chinese remainder theorem. Clearly we have $xy \equiv g \pmod{v}$. By [9, p. 54] a common primitive root of $p$ and $q$ is at the same time a primitive $\lambda$-root of $pq$. Therefore the exponent to which $g$ belongs modulo $v$ is $\lambda(v)$, the least common multiple of $p-1$ and $q-1$. It follows that

$$\lambda(v) = (p-1)(q-1)/e = d.$$

We shall prove that the integer $x$ defined by (2.1) satisfies the assertion of the lemma. For this purpose we first show that no power $g^s$ ($s = 0, \cdots, d-1$) of $g$ is congruent modulo $v$ to a power $x^i$ ($i = 0, \cdots, e-1$) of $x$ except when $s = i = 0$. This is true because the congruence $x^s y^s \equiv x^i \pmod{v}$ in conjunction with (2.1) implies the divisibility relations $(p-1) \mid (s-i)$ and $(q-1) \mid s$. Consequently $e \mid i$, and so $i \geqq e$ unless $i = 0$. It follows that the congruence

$$g^s x^i \equiv g^t x^j \pmod{v} \qquad (s, t = 0, \cdots, d-1; \quad i, j = 0, \cdots, e-1)$$

is not possible unless $s = t$ and $i = j$. The proof of Lemma 1 is thus complete.

We remark that the integer $x$ of Lemma 1 is not unique. Thus the integer $y$ defined by (2.1) could serve equally well in the same role. We also point out that a primitive $\lambda$-root of $v$ is not necessarily a primitive root of both $p$ and $q$. For example, 2 is a primitive $\lambda$-root of 21 and a primitive root of 3. But 2 is not a primitive root of 7.

It is an immediate consequence of Lemma 1 and its proof that $x^e$ is congruent modulo $v$ to a power of $g$. That is, the congruence

$$x^e \equiv g^\mu \pmod{v} \tag{2.2}$$

prevails for some fixed integer $\mu$ such that $0 \leqq \mu \leqq d-1$. We note that $\mu \neq 1$ because $x$ cannot belong to the exponent $\phi(v)$ modulo $v$.

Let us now put $p-1 = ef$, $q-1 = ef'$, $d = eff'$. Since $(f, f') = 1$, $f$ and $f'$ cannot both be even. If $ff'$ is odd, then $-1 \equiv g^{d/2} \pmod{v}$. But if $ff'$ is even, then there is no value of $s$ ($s = 0, \cdots, d-1$) such that the congruence $-1 \equiv g^s \pmod{v}$ is satisfied. We therefore put $-1 \equiv g^s x^i \pmod{v}$ with $0 < i < e$. Squaring both members of this congruence and using (2.2), we find that the two assumptions $0 < i < \frac{1}{2}e$ and $\frac{1}{2}e < i < e$ both lead to contradictions. The only remaining possibility is

$i = \frac{1}{2}e$. We have thus proved that

$$-1 \equiv \begin{cases} g^{\nu}x^{e/2} \pmod{v} & (ff' \text{ even}), \\ g^{d/2} \pmod{v} & (ff' \text{ odd}), \end{cases} \tag{2.3}$$

where $\nu$ is some fixed integer such that $0 \leqq \nu \leqq d - 1$.

Lemma 1 provides the basis for our definition of the cyclotomic number $(i, j) = (i, j)_e$. By means of this lemma the $(p - 1)(q - 1)$ positive integers less than $v$ and prime to $v$ are separated into $e$ classes $C_0, \cdots, C_{e-1}$ each containing $d$ numbers in the following manner. The integer $a \in C_i$ provided that

$$a \equiv g^s x^i \pmod{v} \tag{2.4}$$

for some $s$ ($s = 0, \cdots, d - 1$). For fixed integers $i, j$ the cyclotomic constant $(i, j)$ denotes the number of members of the class $C_i$ that are followed by a member of $C_j$. In other words, $(i, j)$ is the number of solutions $s, t$ of the trinomial congruence

$$g^s x^i + 1 \equiv g^t x^j \pmod{v}, \tag{2.5}$$

where the values of $s$ and $t$ are each selected from the integers $0, 1, \cdots, d - 1$. It is clear from (2.2) that the value of $(i, j)$ is unaltered if either $i$ or $j$ is augmented (or diminished) by a multiple of $e$.

We should keep in mind that the number $(i, j)$ is a function of $g$ and $x$ as well as $v$. Let $g$ and $x$ be given by Lemma 1. Keep $g$ fixed, and let $x'$ be another integer with the property of $x$. Then $x' \equiv g^u x^k \pmod{v}$ for some pair of integers $u, k$ ($u = 0, \cdots, d - 1$; $k = 0, \cdots, e - 1$). It follows from (2.2) that $k$ is relatively prime to $e$. Indeed, if $(k, e) = \delta > 1$, $e = e_1 \delta$, $k = k_1 \delta$, then $x'^{e_1} \equiv g^{ue_1 + \mu k_1} \pmod{v}$. The proof of Lemma 1 shows that the last congruence is impossible. The correspondence between the numbers $(i, j)'$ for $g$ and $x'$ and the numbers $(i, j)$ for $g$ and $x$ is now given by the equation $(i, j)' = (ki, kj)$. Next, keep $x$ fixed in Lemma 1, and replace $g$ by $g^r$, where $r$ is any integer prime to $d$. Then $g^r$ is also a common primitive root of $p$ and $q$. The set of powers of $g^r$ modulo $v$ is in some order the same as the set of powers of $g$. Hence the correspondence between the numbers $(i, j)^{(r)}$ for $g^r$ and $x$ and the numbers $(i, j)$ for $g$ and $x$ is given by the equation $(i, j)^{(r)} = (i, j)$. It is, however, not necessarily the case that all common primitive roots $g$ of $p$ and $q$ are powers of a single one. Thus, if $(0, 0)$ and $(0, 0)'$ correspond to two roots $g$ and $g'$ respectively, then the value of $(0, 0)$ does not necessarily equal the value of $(0, 0)'$. In this connection see Lemma 6 in §5.

Let us suppose in the rest of this section that the choice of $g$ and $x$ in Lemma 1 is kept fixed. We proceed to develop two basic properties ((2.6) and (2.7)) of the symbol $(i, j)$.

Multiplying both members of (2.5) by the reciprocal of its first term, we get

$$g^{-\mu - s} x^{e-i} + 1 \equiv g^{t-s} x^{j-i} \pmod{v},$$

with $\mu$ fixed by (2.2). The exponents $-\mu - s$ and $t - s$ uniquely determine $s$ and $t$ modulo $d$. Hence we obtain the formula

$$(i, j) = (e - i, j - i). \tag{2.6}$$

When $ff'$ is even, the congruence (2.5) may be written as

$$g^{t+\nu}x^{j+(e/2)} + 1 \equiv g^{s+\nu}x^{i+(e/2)} \pmod{v},$$

where $\nu$ is fixed by (2.3). On the other hand, when $ff'$ is odd, (2.5) may be written as

$$g^{t+(d/2)}x^{j} + 1 \equiv g^{s+(d/2)}x^{i} \pmod{v}.$$

We have therefore established the formula

$$(i, j) = \begin{cases} (j + \tfrac{1}{2}e, i + \tfrac{1}{2}e) & (ff' \text{ even}), \\ (j, i) & (ff' \text{ odd}). \end{cases} \tag{2.7}$$

The following linear relation will be useful in later sections:

$$\sum_{j=0}^{e-1} (i, j) = \frac{(p - 2)(q - 2) - 1}{e} + \delta_i, \tag{2.8}$$

where we have made the definition

(2.9) $\delta_i = 1$ if $ff'$ is even and $i = \frac{1}{2}e$, or if $ff'$ is odd and $i = 0$; $\delta_i = 0$ in all other cases.

In order to prove (2.8) it is convenient to put $N = N(s) = 1 + g^s x^i$ for a fixed value of $i$. Let $N_v$ denote the number of values of $s$ ($s = 0, \cdots, d - 1$) for which $N$ is divisible by $v$. Then (2.3) and (2.9) are summarized in the formula $N_v = \delta_i$. Also let $N_p$ denote the number of values of $s$ for which $N$ is divisible by $p$ but not by $v$. As $s$ ranges from 0 to $d - 1$, the least positive remainders of $g^s x^i$ modulo $p$ range $(q - 1)/e$ times over each of the integers between 1 and $p - 1$. Hence $N_p = f' - \delta_i$. Similarly, let $N_q$ denote the number of values of $s$ for which $N$ is divisible by $q$ but not by $v$. We now obtain $N_q = f - \delta_i$. The left member of (2.8) may be interpreted as the number of values of $N$ that are relatively prime to $v$. This number is clearly equal to $d - N_v - N_p - N_q$, which reduces to the right member of (2.8).

Formula (2.8) may be expressed alternatively as follows.

$$\sum_{j=0}^{e-1} (j, i) = \frac{(p - 2)(q - 2) - 1}{e} + \varepsilon_i, \tag{2.10}$$

where $\varepsilon_i = 1$ if $i = 0$ and $\varepsilon_i = 0$ if $1 \leqq i \leqq e - 1$. Whether $ff'$ is even or odd, (2.10) follows from (2.8) upon applying (2.7).

Finally, we return to the notation of (2.4); for fixed $i$ ($i = 0, \cdots, e - 1$) the class $C_i$ consists of the numbers $g^s x^i$ ($s = 0, \cdots, d - 1$) modulo $v$. We shall need the following lemma in §§3 and 5.

LEMMA 2. *Let $r$ be a fixed integer divisible by $p$ or $q$ but not by $v$. Then the number of solutions of the congruence*

$$y - z \equiv r \pmod{v} \tag{2.11}$$

*with $y$ in class $C_1$ and $z$ in class $C_0$ is given by $(p-1)(q-1)/e^2$.*

*Proof.* Because of symmetry we may assume without loss of generality that $r$ is divisible by $p$. Let $g$ be a primitive root of $p$ and $q$, and let $x$ be defined as in Lemma 1. Then $x \not\equiv 1 \pmod{v}$, and $g^u x \equiv 1 \pmod{p}$ for some fixed integer $u$ such that $0 \leqq u \leqq p-2$. In order for the congruence $g^t x - g^s \equiv r \pmod{v}$ $(s, t = 0, \cdots, d-1)$ to be solvable, it is necessary that $t \equiv s + u \pmod{p-1}$. Let $s$ range over the set of integers $\{0, 1, \cdots, d-1\}$. We divide this set into $(p-1)/e$ disjoint subsets each of which contains $q-1$ consecutive integers. Thus the $j$th $(j = 0, \cdots, (p-1-e)/e)$ subset consists of the integers

$$j(q-1),\ j(q-1)+1,\ \cdots,\ j(q-1)+q-2. \tag{2.12}$$

For a fixed value of $m$ $(m = 0, \cdots, (q-1-e)/e)$ consider the $q-1$ differences $g^{m(p-1)+s+u}x - g^s$ as $s$ ranges over the integers in (2.12). Each of these differences is divisible by $p$, but no two of them are congruent modulo $v$. Otherwise we would have the congruence $x \equiv g^{d-u-m(p-1)} \pmod{v}$ in violation of the proof of Lemma 1. It follows that the $q-1$ differences are congruent modulo $v$ in some order to the integers $p, 2p, \cdots, (q-1)p$. Consequently, as $m$ ranges from 0 to $(q-1-e)/e$ and $s$ ranges from 0 to $d-1$, the fixed value of $r$ occurs exactly $(p-1)(q-1)/e^2$ times amongst the differences under consideration. This completes the proof of Lemma 2.

The theory of cyclotomy modulo $v$ initiated in this section is interesting in its own right. The author is preparing a further development of the subject for publication elsewhere.

## 3. Difference sets modulo $v$

The object of this section is to establish a connection between the cyclotomic numbers $(i, j)$ and difference sets of the type described by means of (1.1) and (1.2). Our principal result may be stated as follows.

THEOREM 1. *Let $e$ denote the greatest common divisor of $p-1$ and $q-1$ where $p$ and $q$ are distinct primes, and put $(p-1)(q-1) = de$. Let $g$ be a primitive root of both $p$ and $q$. Then the numbers*

$$1,\ g,\ g^2,\ \cdots,\ g^{d-1};\ \ 0,\ q,\ 2q,\ \cdots,\ (p-1)q \tag{3.1}$$

*form a difference set with parameters $v = pq, k = (v-1)/e, \lambda = (v-1-e)/e^2$ if and only if the following two conditions are satisfied:*

$$q = (e-1)p + 2, \tag{3.2}$$

$$(i, 0) = (e-1)((p-1)/e)^2 \qquad (i = 0, 1, \cdots, e-1). \tag{3.3}$$

It should be noted that the number $(i, 0)$ is a function of $g$ and $x$ in Lemma 1. However, when condition (3.3) is satisfied, all the $(i, 0)$ are equal. The value of $(i, 0)$ is then no longer a function of $x$.

The statement that the numbers in (3.1) form a difference set of multiplicity $\lambda$ is equivalent to the statement that for every fixed integer $r$ not divisible by $v$ there are $\lambda$ solutions of the congruence

$$y - z \equiv r \pmod{v} \qquad (r \not\equiv 0 \pmod{v}) \tag{3.4}$$

with $y$ and $z$ selected from (3.1). For the sake of brevity we shall say that each of the numbers $1, g, g^2, \cdots, g^{d-1}$ is in class $C_0$, and that each of the numbers $0, q, 2q, \cdots, (p-1)q$ is in class $D$. This is consistent with the notation of (2.4). The proof of Theorem 1 will be expedited with the aid of the next two lemmas.

LEMMA 3. *Let $r$ be a fixed integer not divisible by $q$. Then the number of solutions of the congruence* (3.4) *with $y$ in class $C_0$ and $z$ in class $D$ is equal to $(p-1)/e$.*

*Proof.* As in the proof of Lemma 2 we divide the set of integers $\{0, 1, \cdots, d-1\}$ into $(p-1)/e$ disjoint subsets each of which contains $q-1$ consecutive integers. For values of $s$ in the $j$th subset (2.12), exactly one of the numbers $g^s - r$ is divisible by $q$. Lemma 3 is thus established.

LEMMA 4. *Let $r$ be a fixed integer divisible by $p$ but not by $q$. Then the number of solutions of the congruence* (3.4) *with $y$ and $z$ both in class $C_0$ is given by $(p-1)(q-1-e)/e^2$.*

*Proof.* Since the following proof is a slight modification of the proof of Lemma 2, we shall not present it in complete detail. A necessary condition for the solvability of $g^t - g^s \equiv r \pmod{v}$ $(s, t = 0, \cdots, d-1)$ is $t \equiv s \pmod{p-1}$. The exponent to which $g$ belongs modulo $v$ is $d$. Therefore, for each integer $m = 1, \cdots, (q-1-e)/e$ the difference $g^{m(p-1)} - 1$ is divisible by $p$ but not by $v$. But if $m = 0$, this difference also equals zero and hence is divisible by $v$. It follows that for a fixed $m$ $(m = 1, \cdots, (q-1-e)/e)$ no two of the $q-1$ differences $g^{m(p-1)+s} - g^s$ with $s$ in (2.12) are congruent modulo $v$. As a result, these $q-1$ differences are congruent modulo $v$ in some order to the integers $p, 2p, \cdots, (q-1)p$. Consequently, as $m$ ranges from 1 to $(q-1-e)/e$ and $s$ ranges from 0 to $d-1$, the fixed value of $r$ occurs $(p-1)(q-1-e)/e^2$ times amongst the differences under consideration. This completes the proof of Lemma 4.

*Proof of Theorem* 1. We first establish the necessity of conditions (3.2) and (3.3). Let us suppose that the numbers in (3.1) form a difference set with the prescribed parameters. Then (3.2) is an immediate consequence of the relation $k = d + p$. To establish (3.3) it suffices to restrict our attention to any fixed value of $r$ relatively prime to $v$. The number of solutions of (3.4)

with $y$ and $z$ both in class $C_0$ is the same as the number of solutions of $\bar{z}r + 1 \equiv \bar{z}y \pmod{v}$, with $z\bar{z} \equiv 1 \pmod{v}$. From the definition of the cyclotomic number in (2.5) it follows that if $r$ is in class $C_i$ $(i = 0, \cdots, e-1)$, then this number is also equal to $(i, 0)$. Moreover, by Lemma 3 the number of solutions of (3.4) with $y$ in class $C_0$ and $z$ in class $D$ is $(p-1)/e$. Again, by Lemma 3 the number of solutions of (3.4) with $y$ in class $D$ and $z$ in class $C_0$ is $(p-1)/e$. The multiplicity $\lambda$ of the difference set under consideration is therefore equal to $(i, 0) + 2(p-1)/e$. Making use of (3.2) we now deduce (3.3). This completes the proof of necessity.

To prove the sufficiency of conditions (3.2) and (3.3), let us henceforth suppose that (3.2) is satisfied and that all the numbers $(i, 0)$ $(i = 0, \cdots, e-1)$ are equal. Then (2.10) yields

$$e(i, 0) = \sum_{j=0}^{e-1} (j, 0) = (e-1)(p-1)^2/e$$

for each integer $i = 0, \cdots, e-1$. Hence the common value of the numbers $(i, 0)$ is in fact the right member of (3.3). Let us also note that (3.2) in conjunction with the relation $k = d + p$ implies that $k = (v-1)/e$.

To complete the proof we have to show that the numbers in (3.1) form a difference set of multiplicity $\lambda = (v - 1 - e)/e^2$. There are three cases to consider.

(i) The integer $r$ in (3.4) is divisible by $p$. By Lemma 3 the number of solutions of (3.4) with $y$ in class $C_0$ and $z$ in class $D$ is $(p-1)/e$. Again, by Lemma 3 the number of solutions of (3.4) with $y$ in class $D$ and $z$ in class $C_0$ is also $(p-1)/e$. By Lemma 4 the number of solutions of (3.4) with $y$ and $z$ both in class $C_0$ is $(p-1)(q-1-e)/e^2$. Employing (3.2) we derive the result that the number of solutions of (3.4) with $y$ and $z$ each selected from (3.1) is $\lambda = (pq - 1 - e)/e^2$.

(ii) The integer $r$ in (3.4) is divisible by $q$. By Lemma 4 (with $p$ and $q$ interchanged) the number of solutions of (3.4) with $y$ and $z$ both in class $C_0$ is $(p-1-e)(q-1)/e^2$. It is also clear that the number of solutions of (3.4) with $y$ and $z$ both in class $D$ is equal to $p$. For if $z$ takes on any one of the $p$ values in class $D$, then $y$ is in class $D$ and is uniquely determined. The total number of solutions in this case again turns out to equal $\lambda$.

(iii) The integer $r$ in (3.4) is relatively prime to $v$. We have already demonstrated (in the necessity portion of the proof) that if $r$ is in class $C_i$ $(i = 0, \cdots, e-1)$, then the number of solutions of (3.4) with $y$ and $z$ selected from (3.1) is equal to $(i, 0) + 2(p-1)/e$. Replacing $(i, 0)$ by its value in (3.3) we find again that the number in question reduces to $\lambda = (pq - 1 - e)/e^2$. Thus the proof of Theorem 1 is in all cases complete.

The purpose of the next theorem is to show that Theorem 1 cannot be invoked to produce a difference set when $(p-1)(q-1)/e^2$ is odd. Specifically, we shall prove the following result.

THEOREM 2. *Let the hypotheses in the first two sentences of Theorem* 1 *be satisfied. Furthermore, put* $p - 1 = ef$, $q - 1 = ef'$. *Then the numbers* (3.1) *cannot form a difference set of the type prescribed in Theorem* 1 *if* $ff'$ *is odd.*

*Proof.* Throughout the proof of Theorem 2 we shall assume that $ff'$ is odd. The symbol $(i, 0)$ takes on $e$ values as $i$ ranges from 0 to $e - 1$. We shall show that exactly one of these values is odd, and the remaining $e - 1$ are even. As a result, condition (3.3) of Theorem 1 fails to be satisfied.

By (2.6) we have $(i, i) = (e - i, 0)$. Hence it suffices to show that exactly one of the values $(i, i)$ $(i = 0, \cdots, e - 1)$ is odd, and that the remaining $e - 1$ are even. Let $r$ be an integer in class $C_i$ $(i = 0, \cdots, e - 1)$. Since $ff'$ is odd, it follows from (2.3) that $v - r$ is also in class $C_i$. The symbol $(i, i)$ counts the number of pairs $r, r + 1$ $(r = 0, \cdots, v - 1)$ such that $r$ and $r + 1$ are both in class $C_i$. For every such pair there corresponds a pair $v - r - 1, v - r$ $(v - r - 1 = 0, \cdots, v - 1)$ of the same type. Therefore the contribution to the cyclotomic number $(i, i)$ is even unless there is an $r$ such that $r = v - r - 1$. In other words, the cyclotomic number $(i, i)$ is odd or even according as $(v - 1)/2$ belongs to the class $C_i$ or not. Theorem 2 is thus established.

## 4. The case $e = 2$

In this section we first obtain exact formulas for the cyclotomic numbers $(i, j)$ in the case $e = 2$. We then show that the Stanton-Sprott theorem in §1 is an immediate consequence of Theorem 1 in §3.

The number of common primitive roots modulo $v$ of $p$ and $q$ is $\phi(p - 1)\,\phi(q - 1)$. Now let $e = 2$ so that $d = (p - 1)(q - 1)/2$, and let $g$ be one such root. Then the other common primitive roots of $p$ and $q$ are those powers $g^r$ for which $r$ is relatively prime to $d$. The set of powers of $g^r$ modulo $v$ is in some order the same as the set of powers of $g$. Consequently the value of $(0, 0)$ does not depend upon the selection of $g$. Indeed, it turns out that the values of the four constants $(i, j)$ with $i, j = 0, 1$ are all independent of $g$ and $x$ in Lemma 1.

We now evaluate the $(i, j)$ explicitly. There are two sets of cyclotomic formulas according as $ff'$ is even or odd.

*Case* 1. Let $ff'$ be even. By (2.6) and (2.7) we have $(0, 0) = (1, 0) = (1, 1)$. Applying (2.8) with $i = 0$ and $i = 1$ we obtain at once

$$(4.1) \qquad (0, 0) = \frac{(p - 2)(q - 2) + 1}{4}, \qquad (0, 1) = \frac{(p - 2)(q - 2) - 3}{4}.$$

*Case* 2. Let $ff'$ be odd. In this case we derive from (2.6) and (2.7) the relations $(0, 1) = (1, 0) = (1, 1)$. Applying (2.8) again with $i = 0$ and $i = 1$ we get

$$(4.2) \qquad (0, 0) = \frac{(p - 2)(q - 2) + 3}{4}, \qquad (0, 1) = \frac{(p - 2)(q - 2) - 1}{4}$$

We now have on hand the necessary formulas for the application of Theorem 1 with $e = 2$. We shall prove the following formulation of the theorem of Stanton and Sprott.

THEOREM 3. *Let $g$ be a common primitive root of the primes $p$ and $q$; let $(p - 1, q - 1) = 2$ and $d = (p - 1)(q - 1)/2$. Then the set of numbers*

$$1, g, g^2, \cdots, g^{d-1}; \quad 0, q, 2q, \cdots, (p - 1)q$$

*is a difference set with parameters $v = pq$, $k = (v - 1)/2$, $\lambda = (v - 3)/4$ if and only if $q = p + 2$.*

*Proof.* For the deduction of Theorem 3 from Theorem 1 with $e = 2$ we need consider only Case 1 in view of Theorem 2. Actually in Case 2, (4.2) implies that $(0, 0) \neq (1, 0)$. Therefore condition (3.3) of Theorem 1 fails to be satisfied. Turning to Case 1 we see that (3.2) states that $q = p + 2$. When this condition is satisfied, (4.1) yields $(0, 0) = (1, 0) = ((p - 1)/2)^2$ so that condition (3.3) is also satisfied. Conversely, the validity of (3.3) implies the validity of (3.2). We note as well that $d - 1 = (p^2 - 3)/2$ when $q = p + 2$. The proof of Theorem 3 is thus complete.

Stanton and Sprott [10] have generalized Theorem 3. Their result establishes the existence of the abelian difference set (see [10] for the definition) with parameters $v = p^n(p^n + 2)$, $k = (v - 1)/2$, $\lambda = (v - 3)/4$, where $p^n$ and $q^m = p^n + 2$ are both prime powers.

## 5. The case $e = 4$

The purpose of this section is to produce a family of difference sets conforming to Theorem 1 with $e = 4$. We shall require precise formulas for the cyclotomic numbers $(i, j) = (i, j)_4$. When $e = 4$, both primes $p$ and $q$ in the product $v = pq$ are of the form $4n + 1$. By a well-known theorem [9, p. 128] there are exactly two representations of $v$ in the form $v = a^2 + 4b^2$ with $a \equiv 1 \pmod 4$ and the sign of $b$ indeterminate. Let

$$(5.1) \qquad v = a^2 + 4b^2, \qquad v = a'^2 + 4b'^2 \qquad (a \equiv a' \equiv 1 \pmod 4)$$

denote these two representations. Let $g$ be a common primitive root of $p$ and $q$, and let $x$ be selected as in Lemma 1; let $(i, j)$ be the cyclotomic number defined by means of (2.5). We now prove

LEMMA 5. *When $e = 4$ the sixteen cyclotomic constants $(i, j)$ $(i, j = 0, 1, 2, 3)$ depend solely upon one of the two decompositions in* (5.1).

*Proof.* With the aid of (2.6) and (2.7) the sixteen constants $(i, j)_4$ can be expressed in terms of just five of these numbers. These relations are exhibited schematically in the following two tables. In each table the entry in row $i$ and column $j$ is equal to $(i, j)_4$.

(5.2)

$ff'$ even

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | $A$ | $B$ | $C$ | $D$ |
| 1 | $E$ | $E$ | $D$ | $B$ |
| 2 | $A$ | $E$ | $A$ | $E$ |
| 3 | $E$ | $D$ | $B$ | $E$ |

$ff'$ odd

| | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | $A$ | $B$ | $C$ | $D$ |
| 1 | $B$ | $D$ | $E$ | $E$ |
| 2 | $C$ | $E$ | $C$ | $E$ |
| 3 | $D$ | $E$ | $E$ | $B$ |

At this point it is convenient to divide the discussion into two cases according as $ff'$ is even or odd.

*Case* 1. Let $ff'$ be even. By means of (2.4) the $(p-1)(q-1)$ integers in a reduced residue system modulo $v$ are separated into four classes $C_0$, $C_1$, $C_2$, $C_3$ each containing $d = (p-1)(q-1)/4$ numbers. Exploiting a cyclotomic device due to Gauss [6, p. 81] we consider the number $N$ of solutions of the congruence

$$1 + \alpha + \beta + \gamma \equiv 0 \pmod{v}, \tag{5.3}$$

where $\alpha \in C_0$, $\beta \in C_1$, $\gamma \in C_2$. We proceed to calculate the number $N$ in two ways.

In the first place, let $\alpha$ run over the $d$ integers in $C_0$. Then $-\alpha$ runs over the $d$ integers in $C_2$ in view of (2.3). By the first table in (5.2) the number of times that $1 + \alpha \in C_i$ is $A$, $B$, $C$, or $D$ according as $i = 0, 1, 2$, or 3. For a fixed $\alpha$ such that $1 + \alpha \in C_i$, the corresponding number of solutions in $\beta$, $\gamma$ of (5.3) is $E$, $D$, $B$, or $E$ according as $i = 0, 1, 2$, or 3. By (2.3) there is no value of $\alpha$ for which $1 + \alpha$ is divisible by $v$. There are $(q-1)/4$ values of $\alpha$ for which $1 + \alpha$ is divisible by $p$, and $(p-1)/4$ values of $\alpha$ for which $1 + \alpha$ is divisible by $q$. Consider now a fixed value of $\alpha$ for which $1 + \alpha$ is divisible by either $p$ or $q$. The corresponding number of solutions in $\beta$, $\gamma$ of (5.3) is then the same as the number of solutions of (2.11) in Lemma 2 with $e = 4$. Applying Lemma 2 we see that this number is $(p-1)(q-1)/16$. Collecting the results in this paragraph we now get

$$\begin{aligned} N = {} & (p-1)(q-1)^2/64 \\ & + (p-1)^2(q-1)/64 + AE + BD + BC + DE. \end{aligned} \tag{5.4}$$

In the second place, let $\beta$ in (5.3) run over the $d$ integers in $C_1$. By the first table in (5.2) the number of times that $1 + \beta \in C_i$ is $E$, $E$, $D$, or $B$ according as $i = 0, 1, 2$, or 3. For a fixed $\beta$ such that $1 + \beta \in C_i$, the corresponding number of solutions in $\alpha$, $\gamma$ of (5.3) is $A$, $E$, $A$, or $E$ according as $i = 0, 1, 2$, or 3. By (2.3) there is no value of $\beta$ for which $1 + \beta$ is divisible by $v$. There are $(q-1)/4$ values of $\beta$ for which $1 + \beta$ is divisible by $p$, and $(p-1)/4$ values of $\beta$ for which $1 + \beta$ is divisible by $q$. Consider first a fixed value of $\beta$ for which $1 + \beta$ is divisible by $p$. The corresponding number

of solutions in $\alpha, \gamma$ of (5.3) is then the same as the number of solutions of (3.4) in Lemma 4 with $e = 4$. Applying Lemma 4 we see that this number is $(p-1)(q-5)/16$. Similarly, for a fixed $\beta$ such that $1+\beta$ is divisible by $q$ this number is $(p-5)(q-1)/16$. The combined results in this paragraph now yield

$$N = (p-1)(q-1)^2/64 + (p-1)^2(q-1)/64 - (p-1)(q-1)/8 + AE + E^2 + AD + BE. \tag{5.5}$$

Equating the values of $N$ in (5.4) and (5.5) we get at once

$$(p-1)(q-1)/8 = E^2 + AD + BE - BD - BC - DE. \tag{5.6}$$

Next we simplify (5.6). For this purpose we employ the equations

$$\begin{aligned} A + B + C + D &= M, \\ B + D + 2\mathrm{E} &= M, \\ A + E &= \tfrac{1}{2}(M+1), \end{aligned} \tag{5.7}$$

which follow from (2.8) and the first table in (5.2). Here we have put $M = ((p-2)(q-2) - 1)/4$. Using the relations in (5.7) we may transform (5.6) as follows.

$$\begin{aligned} 2(p-1)(q-1) &= 16(E^2 + AD - BE - BD + AB - DE) \\ &= 4(4E^2 + 4E - 1 - 8AE + 4A^2 + (D-B)^2) \\ &= (4(E-A)+1)^2 + 4(D-B)^2 + 4M - 1. \end{aligned} \tag{5.8}$$

Substituting the value of $M$ in (5.7) we find that the last equation in (5.8) reduces to

$$v = pq = (4(E-A)+1)^2 + 4(D-B)^2. \tag{5.9}$$

The quadratic partition in (5.9) is clearly one of the two decompositions in (5.1), say the first. Accordingly we put

$$a = 4(E-A) + 1, \qquad b = D - B. \tag{5.10}$$

The values of the cyclotomic numbers in the first table of (5.2) are now determined by (5.7), (5.9), and (5.10). We deduce the following formulas immediately.

$$\begin{aligned} &8(0,0) = -a + 2M + 3, \qquad 8(0,1) = -a - 4b + 2M - 1, \\ &8(0,2) = 3a + 2M - 1, \qquad 8(0,3) = -a + 4b + 2M - 1, \\ &8(1,0) = a + 2M + 1. \end{aligned} \tag{5.11}$$

*Case* 2. Let $ff'$ be odd. The analysis in this case is completely similar to that in Case 1. We omit the details and give only the formulas for the $(i, j)$.

$$
\begin{aligned}
&8(0,0) = 3a + 2M + 5, \qquad 8(0,1) = -a + 4b + 2M + 1,\\
&8(0,2) = -a + 2M + 1, \qquad 8(0,3) = -a - 4b + 2M + 1,\\
&8(1,2) = a + 2M - 1.
\end{aligned} \tag{5.12}
$$

Lemma 5 is thus established. We recognize, moreover, the following possibility. A change in the choice of $g$ may lead to the replacement of $a$ and $b$ in formulas (5.11) and (5.12) by $a'$ and $b'$ respectively. We shall next discuss the question of distinguishing between these two alternatives.

When $e = 4$, the common primitive roots of $p$ and $q$ can be separated into two classes $G$, $G'$. If $g \in G$, $g' \in G'$, then every root in $G$ is a power of $g$, while every root in $G'$ is a power of $g'$. The cyclotomic number $(0, 0)$ may be defined as the number of solutions of the congruence

$$g^s + 1 \equiv g^t \pmod{v} \qquad (0 \leqq s, t \leqq d - 1). \tag{5.13}$$

Correspondingly, $(0, 0)'$ may be defined as the number of solutions of (5.13) with $g$ replaced by $g'$. It is clear that the value of $(0, 0)$ does not depend upon the choice of $g$ in $G$. The natural supposition that $(0, 0)$ differs in value from $(0, 0)'$ is correct but rather difficult to prove. Indeed the following result, which we formulate as a lemma, has been demonstrated in another paper [4].

LEMMA 6. *If* $(0, 0)$ *and* $(0, 0)'$ *are the cyclotomic numbers corresponding to* $g \in G$ *and* $g' \in G'$ *respectively, then the following inequality holds*:

$$(0, 0) \neq (0, 0)'. \tag{5.14}$$

Lemma 6 has the following interpretation. The first and last formulas in (5.11) state that $8(0, 0) = -a + 2M + 3$ and $8(1, 0) = a + 2M + 1$, where $a$ appears in the first decomposition of (5.1). The lemma now asserts that $8(0, 0)' = -a' + 2M + 3$ and $8(1, 0)' = a' + 2M + 1$, where $a'$ appears in the second decomposition of (5.1). Essential use of this interpretation will be made in the proof of the next theorem. We are now in the position to state our main result as follows.

THEOREM 4. *Let* $p$ *and* $q$ *be two primes such that* $(p - 1, q - 1) = 4$, *and let* $d = (p - 1)(q - 1)/4$. *In the notation of Lemma* 6 *let* $g \in G$ *and* $g' \in G'$. *Then one* (*but not both*) *of the sets*

$$1, g, g^2, \cdots, g^{d-1}; \quad 0, q, 2q, \cdots, (p - 1)q, \tag{5.15a}$$

$$1, g', g'^2, \cdots, g'^{d-1}; \quad 0, q, 2q, \cdots, (p - 1)q, \tag{5.15b}$$

*is a difference set with parameters* $v = pq$, $k = (v - 1)/4$, $\lambda = (v - 5)/16$ *if and only if* $q = 3p + 2$ *and* $(v - 1)/4$ *is an odd square.*

*Proof.* Theorem 4 is a consequence of Theorem 1 with $e = 4$ and Lemma 5. In view of Theorem 2 we need consider only Case 1 of Lemma 5. Actually

in Case 2 we may deduce immediately from (5.12) that condition (3.3) of Theorem 1 cannot be satisfied. For the relation $(0, 0) = (2, 0)$ implies $a = -1$. But $a = 4((1, 2) - (0, 2)) + 1$, and hence $a \equiv 1 \pmod 4$. This contraction disposes of Case 2.

We now turn to Case 1. When $e = 4$, condition (3.2) of Theorem 1 states that $q = 3p + 2$. Suppose, to begin with, that $g$ is a root for which condition (3.3) is satisfied. In view of the first table in (5.2) this condition is equivalent to the relation $(0, 0) = (1, 0) = 3((p - 1)/4)^2$. Equating the values of $(0, 0)$ and $(1, 0)$ in (5.11) we find at once that $a = 1$ or $v = 1 + 4b^2$. Since $k = d + p$ and $d$ is even, it follows that $(v - 1)/4$ is an odd square. Furthermore, the common value of $(0, 0)$ and $(1, 0)$ is $(M + 1)/4$, which reduces to $3((p - 1)/4)^2$ when $q = 3p + 2$. Conversely, suppose that $(v - 1)/4$ is an odd square. Then we may write $v = 1 + 4b^2$, where $b$ is odd. Hence in (5.1) either $a = 1$ or $a' = 1$. We now appeal to the first and last formulas of (5.11) in conjunction with Lemma 6. The lemma clearly implies that either $(0, 0) = (1, 0) = (M + 1)/4$ or $(0, 0)' = (1, 0)' = (M + 1)/4$. Hence condition (3.3) of Theorem 1 is satisfied for one of the two sets (5.15a), (5.15b) when $q = 3p + 2$. The proof of Theorem 4 is thus complete.

Let us now seek examples to illustrate Theorem 4. It is convenient to put $c = 2(3f + 1)$, where $p = 4f + 1$. Then the conditions $q = 3p + 2$, $(v - 1)/4 = b^2$ ($b$ odd) lead to the Pell equation

$$c^2 - 3b^2 = 1. \tag{5.16}$$

The fundamental solution of (5.16) is given by $c_1 = 2$, $b_1 = 1$. The general positive solution of (5.16) is given by $c_n$, $b_n$, where for $n \geqq 2$ the numbers $c_n$ and $b_n$ satisfy the recurrence relations

$$\begin{aligned} c_n &= 4c_{n-1} - c_{n-2} && (c_1 = 2, c_2 = 7), \\ b_n &= 4b_{n-1} - b_{n-2} && (b_1 = 1, b_2 = 4). \end{aligned} \tag{5.17}$$

Values of $c_n$ and $b_n$ have been computed for $n = 1(1)\ 15$. In this range the values for $n = 3$ and $n = 9$ are the only two such that $p = 4f + 1$ and $q = 3p + 2$ are both primes.

The solution $c_3 = 26$, $b_3 = 15$ yields $p = 17$, $q = 53$, $d = 208$, $v = 901$, $k = 15^2$, $\lambda = 56$. Selecting $g = 5$ as the common primitive root of 17 and 53 we find that $(0, 0) = (1, 0) = 48$. Condition (3.3) of Theorem 1 is now satisfied, and the validity of the example given in the introduction is thereby confirmed.

The solution $c_9 = 70226$, $b_9 = 40545$ leads to the pair of primes $p = 46817$, $q = 140453$; hence $d = 1643850208$. By condition (3.3) of Theorem 1 there is a common primitive root $g$ of $p$ and $q$ for which $(0, 0) = (1, 0) = 410950848$. For this $g$ the numbers in (5.15a) form a difference set with parameters $v = 6575588101$, $k = 40545^2$, $\lambda = 410974256$. The actual calculation of $g$ in

this example has not yet been carried out; the author intends to accomplish this task with the aid of a computing machine.

We conclude with the remark that there are no further difference sets with $v < 10^{18}$ coming under the scope of Theorem 4.

## References


1. P. Bachmann, *Die Lehre von der Kreisteilung*, 2nd ed., Leipzig and Berlin, B. G. Teubner, 1921.
2. R. C. Bose and S. S. Shrikhande, *A note on a result in the theory of code construction*, Information and Control, vol. 2 (1959), pp. 183–194.
3. A. Brauer, *On a new class of Hadamard determinants*, Math. Zeitschrift, vol. 58 (1953), pp. 219–225.
4. L. Carlitz and A. L. Whiteman, *Congruences modulo a product of primes*, in course of preparation.
5. S. Chowla, *A property of biquadratic residues*, Proc. Nat. Acad. Sci. India, Sect. A, vol. 14 (1944), pp. 45–46.
6. C. F. Gauss, *Werke, Bd. II*, Königlichen Gesellschaft der Wissenschaften, Göttingen, 1876.
7. W. Gruner, *Einlagerung des regulären n-Simplex in den n-dimensionalen Würfel*, Comment. Math. Helv., vol. 12 (1939–1940), pp. 149–152.
8. M. Hall, Jr., *A survey of difference sets*, Proc. Amer. Math. Soc., vol. 7 (1956), pp. 975–986.
9. W. J. LeVeque, *Topics in number theory, vol. 1*, Reading, Massachusetts, Addison-Wesley, 1956.
10. R. G. Stanton and D. A. Sprott, *A family of difference sets*, Canadian J. Math., vol. 10 (1958), pp. 73–77.
11. J. A. Todd, *A combinatorial problem*, J. Math. Phys., vol. 12 (1933), pp. 321–333.



The Institute for Advanced Study
Princeton, New Jersey
Institute for Defense Analyses
Princeton, New Jersey
University of Southern California
Los Angeles, California