J. Austral. Math. Soc. **21** (Series A) (1976), 438–446.

# EXISTENCE CRITERIA FOR SUPPLEMENTARY DIFFERENCE SETS

**Dedicated to George Szekeres on his 65th birthday**

EMMA LEHMER

(Received 28 December 1974)

Communicated by Jennifer Seberry Wallis

**Abstract**

Conditions are found for the existence of supplementary difference sets consisting of cosets of $e$-th power residues modulo a prime $p$. For $e = 4, 6$ and 8 all known pairs of sets are listed in the summary.

Some 20 years ago there was a great deal of interest in difference sets from various points of view and it was realized at that time that difference sets composed of cosets of $e$-th power residues modulo a prime $p = ef + 1$ provided the majority of known examples. Criteria for the existence of these residue sets were established and a systematic survey of all possible residue sets for small values of $e$ was undertaken by various writers, see Hall (1956) and Baumert (1971).

About five years ago George Szekeres (1971) introduced pairs and families of supplementary difference sets SDS in which the differences are taken within the sets, but not between the sets. Once again the known examples consisted of combinations of cosets of $e$-th power residues. It seems appropriate at this time to embark on a systematic development of existence criteria for SDS residue sets in general and to apply them to an exhaustive study of small values of the parameters.

In general we can consider a system $\Sigma_m$ of $m$ distinct sets $S_0, S_1, S_1, \cdots, S_{m-1}$, the $n$-th set $S_n$ consisting of a union of $t$ distinct cosets of $e$-th power residues of a prime $p = ef + 1$, so that

$$(1) \qquad S_n = C_{z_0^{(n)}} + C_{z_1^{(n)}} + \cdots + C_{z_{t-1}^{(n)}} \qquad (n = 0, 1, \cdots, m-1).$$

Such a system $\Sigma_m$ is usually denoted by $m - \{p, tf, \lambda\}$, where

$$\lambda = mt(tf-1)/e. \tag{2}$$

We can assume that both $t$ and $m$ do not exceed $e/2$ and that $\Sigma_m$ does not include every coset in order to avoid some trivial cases. The extreme case $t = m = e/2$ was recently considered by the writer (1974). The other extreme case $t = m = 1$ brings us back to ordinary difference sets $C_0$. It is well known that for such sets to exist $e$ must be even and $f$ odd.

The proof of this follows from the condition for the existence of a difference set in terms of the cyclotomic numbers $(i, j)$, which enumerate the number of times that an element of class $C_i$ is followed by an element of class $C_j$. This condition is

$$(0,0) = (1,0) = \cdots = (e-1,0). \tag{3}$$

More generally, since the number of times that an element of class $C_k$ is the difference between elements of class $C_i$ minus $C_j$ is $(z_j - k, z_i - k)$, where $z_i$ is in $C_i$ and $z_j$ is in $C_j$, it follows that if $\lambda_k$ is the number of times that element of $C_k$ is the difference between elements of the system $\Sigma_m$, then

$$\lambda_k = \sum_{n=0}^{m-1} \sum_{i=0}^{t-1} \sum_{j=0}^{t-1} (z_j^{(n)} - k, z_i^{(n)} - k). \tag{4}$$

The condition corresponding to (3) for $\Sigma_m$ to be an SDS becomes

$$\lambda_0 = \lambda_1 = \cdots = \lambda_{e-1}. \tag{5}$$

In order to find conditions for the existence of residue SDS and to find such sets we will need to remember a few simple facts about the cyclotomic numbers $(i, j)$, namely:

$$(i,j) = (e-i, j-i) = \begin{cases} (j,i) & \text{if } f \text{ is even} \\ (j+E, i+E) & \text{if } f \text{ is odd and } e = 2E. \end{cases} \tag{6}$$

and

$$(0,j) \equiv \begin{cases} 1 \pmod 2 & \text{if } 2 \in C_j \\ 0 \pmod 2 & \text{otherwise.} \end{cases} \tag{7}$$

Armed with these facts we can prove the following:

THEOREM 1. *If the SDS $\Sigma_m$ contains a coset $C_n$ an odd number of times and does not contain every coset of $p = ef + 1$, then $e$ is even and $f$ is odd.*

PROOF. Suppose, if possible, that $f$ is even. From (4) we have

$$\lambda_k = 2 \sum_{\nu=0}^{m-1} \sum_{i<j=0}^{t-1} (z_i^{(\nu)} - k, z_j^{(\nu)} - k) + \sum_{\nu=0}^{m-1} \sum_{i=0}^{t-1} (z_i^{(\nu)} - k, z_i^{(\nu)} - k). \tag{8}$$

https://doi.org/10.1017/S1446788700019273 Published online by Cambridge University Press

Using (6) this gives

$$\lambda_k \equiv \sum_{\nu=0}^{m-1} \sum_{i=0}^{t-1} (0, z_i^{(\nu)} - k) \pmod 2 \tag{9}$$

Now let 2 belong to $C_\tau$ and let $k = z_n - \tau$, where $z_n$ is any element of $C_n$. Then the sum in (9) will contain the terms $(0, \tau)$ an odd number of times and hence by (7), $\lambda_k$ will be odd. On the other hand for $k = z_u - \tau$, where $C_u$ is not in $\Sigma_m$, (9) will not contain the term $(0, \tau)$ and therefore $\lambda_k$ will be even. Hence condition (5) is not satisfied and $\Sigma_m$ is not an SDS for $f$ even. Therefore $f$ must be odd and hence $e$ must be even. This proves the theorem.

We note that for $f$ odd and $e = 2E$ it follows from (4) and (6) that $\lambda_k = \lambda_{k+E}$ so that condition (5) becomes

$$\lambda_0 = \lambda_1 = \cdots = \lambda_{E-1} \qquad \text{if} \quad f \quad \text{is odd.} \tag{10}$$

We also note that for $m = 1$ and 2 and any $t$ as well as for $t = 1$ or 2 and any $m$ one coset must come in an odd number of times and the hypothesis of Theorem 1 satisfied, so that in these cases $f$ is odd and $e = 2E$.

We will now consider in detail the case $m = 2$. In the first place if we have an ordinary difference set with $m = 1$, usually normalised to contain $C_0$, then it can be multiplied by an element of $C_i$ to give another difference set, thus giving a system with $m = 2$. We shall call such a system *derived*, and ask if there exist non-derived systems with $m = 2$.

We will start with $m = 2$, $t = 1$, $S_0 = C_0$, $S_1 = C_i$, then $z_0^{(0)} = 0$, and $z_0^{(1)} = i$ and (4) becomes in view of (6)

$$\lambda_k = (k, 0) + (k - i, 0) \qquad (k = 0, 1, \cdots, E-1). \tag{11}$$

We note that by (6) if $i = E$, then

$$\lambda_k = 2(k, 0) \qquad (k = 0, 1, \cdots, E-1). \tag{12}$$

Hence condition (10) is the same as (3) and we have:

THEOREM 2. *There are no non-derived SDS with $S_0 = C_0$ and $S_1 = C_E$ of $e$-th power residues.*

We can now assume that $i \neq E$. If $i$ is prime to $E$ and $E$ is odd, then putting $k = i\nu$ in (11) and using (6) we find that (10) leads to (3).

THEOREM 3. *There are no non-derived SDS of $e$-th power residues if $E$ is odd and $i$ is prime to $E$ of the type $C_0$ and $C_i$.*

COROLLARY. *There are no non-derived SDS $C_0$ and $C_i$ if $E$ is an odd prime.*

If $E$ is even and $i$ is prime to $E$, then condition (11) becomes

https://doi.org/10.1017/S1446788700019273 Published online by Cambridge University Press

$$(13)\qquad \begin{aligned}(i,0) &= (3i,0) = \cdots = ((E-1)i,0)\\ (0,0) &= (2i,0) = \cdots = ((E-2)i,0)\end{aligned}$$

For $e = 4$, condition (13) is trivially satisfied for $i$ odd since $(1,0) = (3,0)$ and $(0,0) = (2,0)$ by (6). Hence we have:

THEOREM 4. *The only non-derived SDS for $e = 4$, $m = 2$ and $t = 1$ are $C_0$ and $C_1$* (or $C_0$ and $C_3$) *for $p = 8n + 5$ given by* $2 - \{p, f, (f-1)/2\}$.

For example $p = 13$, $C_0 = 1, 3, 9$ and $C_1 = 2, 5, 6$, with $\lambda = 1$.

By Theorem 3 there are no non-derived sets for $e = 6$ and $e = 10$. For $e = 8$ conditions (13) are

$$(1,0) = (3,0) \quad \text{and} \quad (0,0) = (2,0) \quad \text{if} \quad i \quad \text{is odd}.$$

Consulting the expressions for the cyclotomic numbers Lehmer (1955) or Storer (1967) in terms of $p = a^2 + 2b^2 = x^2 + 4y^2 \equiv 9 \pmod{16}$ we find that $(1,0) = (3,0)$ if 2 is a quartic residue, but if 2 is not a quartic residue then $(1,0) = (3,0)$ implies $b = 0$ and hence that $p$ is not a prime. In case 2 is a quartic residue the second condition $(0,0) = (2,0)$ implies $a = 1$, or $p = 1 + 2b^2$.

If $i$ is even than by (11) the condition is

$$(0,0) + (2,0) = (1,0) + (3,0)$$

and this implies $1 + x = -2a$. Hence we have:

THEOREM 5. *For $e = 8$, the only SDS with $m = 2, t = 1$ are* $2 - \{p, f, (f-1)/2\}$ *with $S_0 = C_0$ and $S_1 = C_i$ with $i$ odd and 2 a quartic residue of $p = 1 + 2b^2 \equiv 9$* (mod 32); *or with $i$ oddly even and $p = a^2 + 2b^2 = x^2 + 4y^2 \equiv 9$* (mod 32), *and $1 + x = -2a$. These sets are not derived unless 2 is a quartic residue and $a = 1$, $x = -3$, as in $p = 73$.*

For $m = 1, t = 2$, the only known difference set was given by Hayashi (1965) for $e = 10$, $p = 31$, $S_0 = C_0 + C_1$ (or $C_0 + C_9$) based on the primitive root $g = 11$. Hence we have a derived SDS $S_0 = C_0 + C_1$, $S_1 = C_0 + C_9$ for $e = 10$. We next inquire into the possibility of non-derived sets $S_0 = C_0 + C_i$, $S_1 = C_0 + C_j$ $(i \neq j \neq 0)$.

We first note that for $m = t = 2$, $\lambda = 4(2f-1)/e$, $f$ odd and hence there are no such sets if $e$ is divisible by 8, and that $\lambda$ is odd if $e$ is a multiple of 4 and even if $e$ is oddly even. From (4)

$$(14)\qquad \begin{aligned}\lambda_k = {} & 2(k,0) + (k,i) + (k,j) + (k-i,0) + (k-j,0) + (k-i,-i)\\ & + (k-j,-j) = 2(2f-1)/E.\end{aligned}$$

In particular

$$\lambda_0 = 2(0,0) + (0,i) + (0,j) + (-i,0) + (-j,0) + (i,0) + (j,0). \tag{15}$$

$$\lambda_i = 2(i,0) + (-i,0) + (i,j) + (0,0) + (i-j,0) + (0,-i) + (i-j,-j). \tag{16}$$

$$\lambda_j = 2(j,0) + (j,i) + (-j,0) + (j-i,0) + (0,0) + (j-i,-i) + (0,-j). \tag{17}$$

If $j \neq i + E$ these give us two conditions from $\lambda_0 = \lambda_i$ and $\lambda_0 = \lambda_j$,

$$\begin{aligned}(0,0) + (0,i) + (0,j) + (-j,0) + (j,0) &= (i,0) + (i,j) + (i-j,0)\\ &\quad + (0,-i) + (i-j,-j)\end{aligned} \tag{18}$$

and

$$\begin{aligned}(0,0) + (0,i) + (0,j) + (-i,0) + (i,0) &= (j,0) + (j,i) + (j-i,0)\\ &\quad + (0,-j) + (i-j,-j).\end{aligned} \tag{19}$$

If $j = -i$ these simplify to read

$$\begin{aligned}(0,0) + (0,i) + (-i,0) &= (i,-i) + (2i,0) + (2i,i)\\ (0,0) + (0,-i) + (i,0) &= (-i,i) + (-2i,0) + (2i,i).\end{aligned} \tag{20}$$

If $j = i + E$ then (15) and (16) become

$$\begin{aligned}2(0,0) + (0,i) + (0,i+E) + 2(-i,0) + 2(i,0) &= \lambda_0\\ 2(i,0) + 2(-i,0) + (0,E-i) + 2(0,0) + (0,-i) &= \lambda_i\end{aligned} \tag{21}$$

Instead of (17) which is the same as (16) we can use

$$\lambda_{2i} = 2(2i,0) + (2i,i) + (2i,i+E) + 2(i,0) + (i,-i) + (-i,i) \tag{22}$$

to obtain conditions from $\lambda_0 = \lambda_i$ and $\lambda_0 = \lambda_{2i}$ as follows:

$$(0,i) + (0,i+E) = (0,E-i) + (0,-i) \tag{23}$$

and

$$\begin{aligned}2(2i,0) + (2i,i) + (2i,i+E) + (i,-i) + (-i,i) &= 2(0,0) + 2(-i,0)\\ &\quad + (0,E+i) + (0,i).\end{aligned} \tag{24}$$

If $2i = E$ then condition (23) is trivially satisfied. Since for $e = 4$ this is the sole condition we obtain once more the original Szekeres pair of sets $C_0 + C_1$ and

https://doi.org/10.1017/S1446788700019273 Published online by Cambridge University Press

$C_0 + C_3$. If $2i \neq E$, then all the terms of (23) are even, for only one of them can be odd by (7), hence $\lambda_0$ and therefore $\lambda$ must be even, but that implies that $E$ is odd and we have:

THEOREM 6. *For $m = t = 2$ there is no SDS of $e$-th power residues of the type $C_0 + C_i$ and $C_0 + C_{i+E}$ with $E$ even and $i \neq E/2$.*

If $j = E$ we have from (15), (16) and (17)

$$(25) \qquad \lambda_0 = 4(0,0) + (0,i) + (0,E) + (-i,0) + (i,0)$$

$$(26) \qquad \lambda_i = 3(i,0) + (-i,0) + (0,i+E) + (0,0) + (0,-i) + (0,i)$$

Hence $\lambda_0 = \lambda_i$ implies

$$(27) \qquad 3(0,0) + (0,E) = 2(i,0) + (0,-i) + (0,i+E).$$

For $e = 4$ this becomes for $i = 1$, $j = 2$, $p = x^2 + 4y^2$,

$$3(0,0) + (0,2) = 2(1,0) + 2(0,3).$$

But $3(0,0) + (0,2) = (p-5)/4$, while $2(1,0) + 2(0,3) = y + (p-1)/4$. This implies that $y = -1$. If $i = 3$, we get $y = 1$. In either case $p = x^2 + 4$.

These sets $2 - \{p, 2f, 2f-1\}$ consisting of $C_0 + C_1$ and $C_0 + C_2$ were discovered by Wallis (1973).

For $e = 6$, $E = 3$, $\lambda = 2(2f-1)/3$, $p \equiv 31 \pmod{36}$. In case $j = i + 3$, conditions (23) and (24) give for $i = 1$ or $i = 2$

$$(28) \qquad (0,1) + (0,4) = (0,2) + (0,5) = 3(1,2) + (2,1) - 2(0,0).$$

Since only one of $(0,i)$ can be odd by (7) this implies that 2 must be a cubic residue of $p = L^2 + 27M^2$. Looking up the cyclotomic numbers in terms of $L$ and $M$ we find that (27) implies that $L = -2$ and hence that $p = 4 + 27M^2$.

THEOREM 7. *The two sets of sextic residue cosets $C_0 + C_1$ and $C_0 + C_4$ (or $C_0 + C_5$) are SDS $2 - \{p, 2f, 2(2f-1)/3\}$ if and only if $p = 4 + 27M^2 \equiv 31 \pmod{36}$.*

*For $p = 31$,* $S_0 = 1, 2, 3, 4, 6, 8, 12, 16, 17, 24$

$$S_1 = 1, 2, 4, 7, 8, 14, 16, 19, 25, 28$$

*and* $\lambda = 6$. These SDS appear to be new.

If $j = -i$, then conditions (20) become for $e = 6$

$$(0,0) + (0,1) = (1,2) + (2,1) = (0,0) + (0,5) \qquad \text{if} \quad i = 1 \quad \text{or} \quad 5$$

and

$$(0,0) + (0,2) = 2(1,2) = (0,0) + (0,4) \qquad \text{if} \quad i = 2 \quad \text{or} \quad 4.$$

But both $(0,1) = (0,5)$ and $(0,2) = (0,4)$ lead to $y = 0$ in $p = x^2 + 3y^2$ and hence:

THEOREM 8. *There is no SDS of sextic residues of the type $C_0 + C_i$ and $C_0 + C_{-i}$ with $i \neq E$ and $p$ a prime.*

If $i$ or $j$ is $E$ we can inquire about the pair of sets $C_0 + C_i$ and $C_0 + C_E$. Using (27) this implies by (7) that 2 is not a cubic residue and is not in $C_{i+E}$ or $C_{-i}$. Hence for $e = 6$ it is in $C_i$ or in $C_{i-E}$. Noting that

$$\begin{aligned}(i,j)_E &= (i,j) + (i,j+E) + (i+E,j) + (i+E,j+E)\\ &= 2(i,j) + (i,j+E) + (j+E,i)\end{aligned}$$

(27) can be written

$$(0,0)_E - (0,i)_E = (0,-i) - (0,i), \tag{29}$$

while the condition $\lambda_i = \lambda_{2i}$ becomes

$$(0,0)_E - (0,2i)_E = (2i,0) + (2i,i) + (i,-i) - (0,0) - (0,i) - (-i,0). \tag{30}$$

For $i = 1$, this simplifies to

$$\begin{aligned}(0,0)_3 - (0,1)_3 &= (0,5) - (0,1)\\ (0,0)_3 - (0,2)_3 &= (1,2) + (2,1) - (0,0) - (0,1).\end{aligned}$$

Substituting the appropriate expressions for $(i,j)$ when 2 is in $C_1$ in terms of $x, y$ in $p = x^2 + 3y^2$ we obtain $3x - 4y = 4$ and $x - 2y = 6$ which implies $x = -8$, $y = -7$, $p = 211$ and we have a SDS for $C_0 + C_1$ and $C_0 + C_3$ with parameters $2 - \{211, 70, 46\}$ with 2 in $C_1$. If 2 is in $C_2$ the corresponding discussion leads to $x = 10$, $y = 7$, but unfortunately $x^2 + 3y^2 = 247 = 13.19$ is not a prime, hence there is no such set.

If $i = 2$ conaitions (29) and (30) become

$$\begin{aligned}(0,0)_3 - (0,2)_3 &= (0,4) - (0,2)\\ (0,0)_3 - (0,1)_3 &= 2(1,2) - (0,0) - (0,2)\end{aligned}$$

which exclude the case $i = 2$ by (7) as 2 cannot belong to any coset. Hence:

THEOREM 9. *The only SDS of sextic residues of the type $C_0 + C_i$ and $C_0 + C_3$ is $2 - \{211, 70, 46\}$ for $i = 1$ and $2 \in C_1$ (or $i = 5$ and $2 \in C_5$).*

This disposes of all possible sets with $m = t = 2$ and $e = 6$, except the cases $i = 1$, $j = 2$ and $i = 2$, $j = 4$. Using (18) and (19) we have

$$(0,0) + (0,1) + (0,2) = (0,5) + 2(1,2) = (0,4) + (1,2) + (2,1) \quad \text{if } i = 1,\ j = 2$$

$$(0,0) + (0,2) + (0,4) = (0,4) + 2(12) = (0,2) + 2(1,2) \quad \text{if } i = 2,\ j = 4.$$

Hence for $i = 2$ we have $(0,2) = (0,4)$ which leads to $y = 0$ in $p = x^2 + 3y^2$, so there is no set for $p$ a prime. For $i = 1$, however, parity conditions on the $(0, j)$ imply that 2 must be in class $C_3$ or $C_4$. If 2 is a cubic residue, then $(0,4) = (0,5)$ and $(1,2) = (2,1)$ so that we have a single condition $L + 1 = 9M$ in $p = 4L^2 + 27M^2$. For example there is an SDS for $p = 283$, namely, $2 - \{283, 94, 62\}$ composed of sextic cosets $C_0 + C_1$ and $C_0 + C_2$.

When 2 is in $C_4$ relations (31) do not lead to a possible set. Thus we have:

THEOREM 10. *The two sets of sextic residues* $C_0 + C_i$ *and* $C_0 + C_{2i}$ *give an SDS* $2 - \{p, 2f, 2(2f - 1)/3\}$ *if and only if*, $i = 1$, $p = 4L^2 + 27M^2$ *with* $L + 1 = 9M$.

Thus all possible SDS made up of sextic cosets are given by Theorem 7, 9 and 10. (See Summary.)

For $m = 2$, $t = 3$, $e = 6$ we have discovered the sets $2 - \{19, 9, 8\}$ of sextic cosets as the only set of the type $S_0 = C_0 + C_i + C_E$ and $C_0 + C_{-i} + C_E$ with $i = 1$ or $i = 2$. There are no SDS of this type for $e = 8$.

For $m = 2$, $t = 4$, $e = 8$, Szekeres (1971) gave the set $C_0 + C_1 + C_2 + C_3$ and $C_0 + C_1 + C_6 + C_7$ for an even power of a prime, but no sets have been found for $p$ a prime, however an exhaustive search has not been undertaken.

For $m = t = E$ there exist SDS for every $p = 2Ef + 1$ with $f$ odd. These are given in Lehmer (1974).

Summary of known SDS with $m = 2$

| $t$ | $e$ | $S_0$ | $S_1$ | Form of $p$ | least $p$ |
|---|---|---|---|---|---|
| 1 | 4 | $C_0$ | $C_1$ | $p \equiv 5 \pmod 8$ | 13 |
| | 8 | $C_0$ | $C_1$ | $p = 1 + 2b^2 = x^2 + 16y^2$ | 13 |
| | 8 | $C_0$ | $C_2$ | $p = a^2 + 2b^2 = x^2 + 4y^2$ | 41 |
| | | | | $x = -(2a + 1)$ | |
| 2 | 4 | $C_0 + C_1$ | $C_0 + C_2$ | $p = x^2 + 4$ | 13 |
| | 4 | $C_0 + C_1$ | $C_0 + C_3$ | $p \equiv 5 \pmod 8$ | 13 |
| | 6 | $C_0 + C_1$ | $C_0 + C_2$ | $p = 4u^2 + 27v^2$ | 283 |
| | | | | $u = 9v - 1$ | |
| | 6 | $C_0 + C_1$ | $C_0 + C_3$ | $p = 211$ with $2 \in C_1$ | 211 |
| | 6 | $C_0 + C_1$ | $C_0 + C_4$ | $p = 4 + 27y^2$ | 31 |
| | 6 | $C_0 + C_1$ | $C_0 + C_5$ | No Solution | |
| | 6 | $C_0 + C_2$ | $C_0 + C_3$ | No Solution | |
| | 6 | $C_0 + C_2$ | $C_0 + C_4$ | No Solution | |
| | 6 | $C_0 + C_2$ | $C_0 + C_5$ | $p = 4 + 27y^2$ | 31 |
| | 6 | $C_0 + C_3$ | $C_0 + C_4$ | No Solution | |
| | 6 | $C_0 + C_3$ | $C_0 + C_5$ | 211 with $2 \in C_5$ | 211 |
| | 6 | $C_0 + C_4$ | $C_0 + C_5$ | $p = 4u^2 + 27v^2$ | 283 |
| | | | | $u = 9v - 1$ | |
| 3 | 6 | $C_0 + C_1 + C_3$ | $C_0 + C_3 + C_5$ | $p = 19$ | 19 |
| | 6 | $C_0 + C_2 + C_3$ | $C_0 + C_3 + C_4$ | $p = 19$ | 19 |

https://doi.org/10.1017/S1446788700019273 Published online by Cambridge University Press

**References**

L. D. Baumert (1971), *Cyclic Difference Sets*, Lectures Notes in Math., vol. 182, Springer-Verlag.

Marshall Hall (1956), 'A survey of difference sets', *Amer. Math. Soc. Proc.* **7**, 975–986.

Hayashi (1965), 'Computer investigation of difference sets', *Math. Comp.* **19**, 73–78.

Emma Lehmer (1955), 'On the number of solutions of $u^k + D = w^2 \pmod p$', *Pacific J. Math.* **5**, 103–118.

Emma Lehmer (1974), 'A family of supplementary difference sets', *Bull. Austral. Math. Soc.* **10**, 459–462.

T. Storer (1967), *Cyclotomy and Difference Sets*, Lectures in Advanced Math., vol. 2, Markham, Chicago.

George Szekeres (1971), 'Cyclotomy and complementary difference sets', *Acta Arith.* **18**, 349–353.

Jennifer Wallis (1973), 'Some remarks on supplementary difference sets', *Colloquia Mathematica Societatis Janos Bolyai* 10.

1180 Miller Avenue,
Berkeley, California,
U.S.A.

https://doi.org/10.1017/S1446788700019273 Published online by Cambridge University Press