ARTICLE IN PRESS YAAMA:1364

Advances in Applied Mathematics ••• (••••) •••–•••

Contents lists available at ScienceDirect

Advances in Applied Mathematics

www.elsevier.com/locate/yaama

Lam's power residue addition sets

Kevin Byard [a], Ron Evans [b,*], Mark Van Veen [c]

[a] Institute of Information and Mathematical Sciences, Massey University, Albany, North Shore, Auckland, New Zealand
[b] Department of Mathematics 0112, University of California at San Diego, La Jolla, CA 92093-0112, United States
[c] Varasco LLC, 2138 Edinburg Avenue, Cardiff by the Sea, CA 92007, United States

ARTICLE INFO

Article history:
Available online xxxx

MSC:
primary 05B10
secondary 11A15, 11T22, 11T24

Keywords:
Qualified residue difference sets
Power residue difference sets
Cyclic difference sets
Power residue addition sets
Cross-correlation function
Cyclotomic numbers
Gauss sums
Jacobi sums

ABSTRACT

Classical n-th power residue difference sets modulo p are known to exist for $n = 2, 4, 8$. During the period 1953–1999, their nonexistence has been proved for all odd n and for $n = 6, 10, 12, 14, 16, 18, 20$. In 1976, Lam showed that *qualified* n-th power residue difference sets modulo p exist for $n = 2, 4, 6$, and he proved their nonexistence for all odd n and for $n = 8, 10, 12$. We further prove their nonexistence for $n = 14, 16, 18, 20$.

1. Introduction

For an integer $n > 1$, let p be a prime of the form $p = nf + 1$. Let H_n denote the set of (nonzero) n-th power residues in $\mathbb{F}_p^*$, where $\mathbb{F}_p$ is the field of p elements. For $\epsilon \in \{0, 1\}$, define $H_{n,\epsilon} = H_n \cup \{1 - \epsilon\}$. Note that $|H_{n,\epsilon}| = f + \epsilon$.

Fix $m \in \mathbb{F}_p^*$. In 1975, Lam [18] introduced *addition sets*, which generalize cyclic difference sets. He called $H_{n,\epsilon}$ an n-th power residue addition set modulo p if there exists an integer $\lambda > 0$ such that the list of differences $s - mt \in \mathbb{F}_p^*$ with $s, t \in H_{n,\epsilon}$ hits each element of $\mathbb{F}_p^*$ exactly λ times. If $m \in H_n$, such an addition set is a *classical* power residue difference set modulo p; see [3, p. 174]. If $m \notin H_n$,

* Corresponding author.
E-mail addresses: k.byard@massey.ac.nz (K. Byard), revans@ucsd.edu (R. Evans), mvanveen@ucsd.edu (M. Van Veen).

0196-8858/$ – see front matter
doi:10.1016/j.aam.2010.09.008

Please cite this article in press as: K. Byard et al., Lam's power residue addition sets, Adv. in Appl. Math. (2010), doi:10.1016/j.aam.2010.09.008

we call such an addition set a *qualified* power residue difference set modulo p with qualifier m; cf. [14,15].

The classical n-th power residue difference sets $H_{n,\epsilon}$ for $n \leqslant 8$ are the following [3, pp. 177–179]:

$$H_{2,\epsilon}, \quad \text{if } p > 3, \quad p \equiv 3 \pmod 4, \tag{1.1}$$

$$H_{4,\epsilon}, \quad \text{if } p > 5, \quad p = (1+8\epsilon) + 4y^2 \text{ for some odd } y, \tag{1.2}$$

$$H_{8,\epsilon}, \quad \text{if } p = (1+48\epsilon) + 8u^2 = (9+432\epsilon) + 64v^2, \text{ with integers } u, v. \tag{1.3}$$

It is known that $H_{n,\epsilon}$ is never a classical power residue difference set when n is odd [3, p. 177], $n = 6$ [3, p. 178], $n = 10$ [26], $n = 12$ [3, p. 179], $n = 14$ [21], $n = 16$ [9,25], $n = 18$ [1,2], and $n = 20$ [10,22]. These nonexistence results were obtained sporadically during the period 1953–1999. The cases with even $n > 20$ are open (see [3, p. 497]), but we conjecture that the list (1.1)–(1.3) is complete.

As was noted above, complete information on the existence of classical n-th power residue difference sets is known for all $n \leqslant 20$. The primary goal of this paper is to similarly obtain complete information on the existence of qualified n-th power residue difference sets for all $n \leqslant 20$.

The qualified n-th power residue difference sets for $n \leqslant 6$ with qualifier m are the following, due to Lam [18,19]:

$$H_{2,\epsilon}, \quad \text{if } p \equiv 1 \pmod 4, \ m \in \mathbb{F}_p^*, \ m \notin H_2, \tag{1.4}$$

$$H_{4,\epsilon}, \quad \text{if } p = (1+8\epsilon) + 16x^2 \text{ for some integer } x, \ m \in H_2, \ m \notin H_4, \tag{1.5}$$

$$H_{6,\epsilon}, \quad \text{if } p = (1+24\epsilon) + 108w^2 \text{ for some integer } w, \ m \in H_3, \ m \notin H_6. \tag{1.6}$$

It is shown in [19] that $H_{n,\epsilon}$ is never a qualified residue difference set when n is odd and when $n = 8$, $n = 10$, and $n = 12$. Lam's results for $n = 2, 4, 6, 8, 10, 12$ have also been obtained in the papers [14,15,4–6], whose authors were at the time unaware of Lam's work. For related addition sets formed by taking unions of index classes for p, see [20, Theorems 3.2–3.5].

In this paper, we accomplish our goal by showing that $H_{n,\epsilon}$ is never a qualified residue difference set when $n = 14, 16, 18, 20$. We also give a new proof of Lam's nonexistence result for odd n, in Section 2. Those looking to find new qualified residue difference sets may thus limit their search to the cases with even $n > 20$. However, we conjecture that the list (1.4)–(1.6) is complete.

It is well known that cyclic difference sets have applications in astronomy [7,12,13,17]. The first author was led to rediscover qualified residue difference sets while working on coded aperture imaging for the European Space Agency's International Gamma-Ray Astrophysical Laboratory (INTEGRAL) [8,27]. Difference sets have also been used in medical imaging [16,24].

Consider a qualified residue difference set $H = H_{n,0}$ modulo $p = nf + 1$ with qualifier m. For integer $t \pmod p$, define a binary array $A(t)$ by setting $A(t) = 1$ if $t \in H$, and $A(t) = 0$ otherwise. Define a post processing array $G(t)$ by setting $G(t) = 1 - n$ if $t \in mH$, and $G(t) = 1$ otherwise. The corresponding cross-correlation function F on the integers is given by

$$F(u) = \sum_{t=0}^{p-1} A(t)G(t+u).$$

Because H is a qualified residue difference set, $F(u) = f$ if $u \equiv 0 \pmod p$, and $F(u) = 0$ otherwise. Periodic two-valued cross-correlation functions such as $F(u)$ are potentially useful in signal processing, aperture synthesis, and image formation techniques.

Please cite this article in press as: K. Byard et al., Lam's power residue addition sets, Adv. in Appl. Math. (2010), doi:10.1016/j.aam.2010.09.008

2. Preliminary theorems

Write $\zeta = \exp 2\pi i/p$, and for any t prime to p, define $\sigma_t \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ by $\sigma_t(\zeta) = \zeta^t$. Let χ be a character (mod p) of order n. Define the Gauss period

$$S(n) = \sum_{r \in H_n} \zeta^r$$

and the Gauss sums

$$g(n) = \sum_{x \in \mathbb{F}_p} \zeta^{x^n}, \qquad G(\chi) = \sum_{x \in \mathbb{F}_p} \chi(x)\zeta^x.$$

These sums are related by [3, pp. 153, 175]

$$g(n) = nS(n) + 1 = \sum_{j=1}^{n-1} G\big(\chi^j\big). \tag{2.1}$$

Whenever $H_{n,\epsilon}$ is a qualified residue difference set with qualifier m, we have

$$\lambda(p-1) = f^2 + 2\epsilon f \tag{2.2}$$

and

$$\big(S(n) + \epsilon\big)\big(\sigma_{-m}S(n) + \epsilon\big) = \epsilon - \lambda, \tag{2.3}$$

and so by combining (2.1)–(2.3), we have

$$\big(g(n) + \nu\big)\big(\sigma_{-m}g(n) + \nu\big) = \nu^2 - p, \tag{2.4}$$

where

$$\nu = n\epsilon - 1.$$

Conversely, it is easily seen that (2.4) implies that $H_{n,\epsilon}$ is a qualified residue difference set with qualifier m. Applying (2.4) with $n = 2$ and using the fact [3, p. 26] that

$$\sigma_{-m}g(2) = \chi(-m)i^{(p-1)^2/4}\sqrt{p},$$

we see that $H_{2,\epsilon}$ is a qualified residue difference set with qualifier m if and only if p and m satisfy the conditions in (1.4).

We now give a new proof of the following result of Lam [19], which shows in particular that qualified n-th power residue difference sets do not exist when n is odd.

Theorem 2.1. *Suppose that $H_{n,\epsilon}$ is a qualified residue difference set modulo p. Then $p \equiv 1 \pmod{2n}$, n is even, and the qualifiers m of $H_{n,\epsilon}$ are precisely those m for which $m \in H_{n/2}$, $m \notin H_n$.*

Please cite this article in press as: K. Byard et al., Lam's power residue addition sets, Adv. in Appl. Math. (2010), doi:10.1016/j.aam.2010.09.008

Proof. The proof for $n = 2$ was given below (2.4), so we may suppose that $n > 2$. Applying σ_{-m} to both sides of (2.4), we see that σ_{m^2} fixes $g(n)$. Hence σ_{m^2} fixes $S(n)$ by (2.1). It follows that $m^2 \in H_n$, so that $m \in H_{n/2}$ and n is even. Finally, f is even by (2.2). □

In the sequel, we prove the nonexistence of qualified n-th power residue difference sets modulo p for $n = 14, 16, 18, 20$. In view of Theorem 2.1, we need only consider those primes $p = nf + 1$ for which f is even. We will need the following theorem of Lam [19, Theorem 3.5] involving the cyclotomic numbers $(i, j) = (i, j)_n$ of order n. Recall that for even f, these numbers satisfy $(j, i) = (i, j) = (-i, j - i)$ [3, p. 69].

Theorem 2.2. *Let $p = nf + 1$ with n and f both even. Then $H_{n,\epsilon}$ is a qualified residue difference set with qualifier m if and only if $m \in H_{n/2}$, $m \notin H_n$,*

$$n^2(0, n/2)_n = p - \nu^2,$$

and

$$n^2(i, n/2)_n = p + 1 + 2\nu, \quad 0 < i < n/2.$$

3. Nonexistence for $n = 14$

In this section, $\nu = 14\epsilon - 1$ and $p = 14f + 1$ with f even.

Theorem 3.1. *$H_{14,\epsilon}$ is never a qualified residue difference set.*

Proof. Assume the contrary. We will obtain a contradiction by using the formulas for the cyclotomic numbers $(i, j) = (i, j)_{14}$ expressed by J.B. Muskat [21] in terms of the integer parameters T, U, and C_i $(1 \leqslant i \leqslant 6)$. These parameters satisfy

$$p = T^2 + 7U^2, \quad T \equiv 1 \pmod 7 \tag{3.1}$$

and [21, p. 265]

$$S := \sum_{i=0}^{6} C_i \zeta_7^i = J(\psi, \psi), \tag{3.2}$$

where ζ_7 is a complex seventh root of unity, $J(\psi, \psi)$ is a Jacobi sum for a character $\psi \pmod p$ of order 7, and

$$\sum_{i=0}^{6} C_i = p - 2. \tag{3.3}$$

Define

$$h_j := \sum_{i=0}^{6} C_i C_{i+j} \quad (0 \leqslant j \leqslant 6), \tag{3.4}$$

where the subscripts are viewed modulo 7. Then by (3.2),

Please cite this article in press as: K. Byard et al., Lam's power residue addition sets, Adv. in Appl. Math. (2010), doi:10.1016/j.aam.2010.09.008

$$p = |S|^2 = \sum_{i=0}^{6} h_i \zeta_7^i, \tag{3.5}$$

so that

$$h_1 = h_2 = h_3 = h_4 = h_5 = h_6 = h_0 - p. \tag{3.6}$$

In view of Theorem 2.2, we have the system of six equations

$$196(i, 7) = p + 1 + 2\nu \quad (1 \leqslant i \leqslant 6). \tag{3.7}$$

First assume $2 \notin H_7$. Solve the system (3.7) to express each C_i $(1 \leqslant i \leqslant 6)$ as a linear combination of p, 1, ν, U, and T. Then $h_2 - h_1 = 20U^2/7$, so $U = 0$, which contradicts (3.1).

It remains to consider the more difficult case where $2 \in H_7$. Write

$$y = (2p - 4 + T - \nu)/7, \qquad C_5 = r, \qquad C_6 = s. \tag{3.8}$$

Solving the system (3.7), we obtain

$$C_1 = y - s, \qquad C_2 = y - r, \qquad C_3 = 3y/2 - U - r - s, \qquad C_4 = -y/2 + U + r + s. \tag{3.9}$$

Then by (3.3),

$$C_0 = p - 2 - 3y. \tag{3.10}$$

Solving the equation

$$3h_1 - h_2 - 2h_3 = 0, \tag{3.11}$$

for s, we obtain

$$s = \bigl(28r^2 + 21y^2 + 8Ur - 56yr + 4yU - 12U^2\bigr)/(28y + 16U - 56r). \tag{3.12}$$

The denominator in (3.12) is nonzero, since substitution of $y/2 + 2U/7$ for r in the left side of (3.11) yields the nonzero value $-13U^2/7$. Thus

$$r = y/2 - Uw \tag{3.13}$$

for some rational number $w \neq -2/7$. Substituting the values of r and s from (3.12)–(3.13) into the equation $h_1 - h_3 = 0$, we deduce that

$$(3w - 1)\bigl(7w^3 - 7w^2 - 7w - 1\bigr) = 0. \tag{3.14}$$

The cubic polynomial in (3.14) clearly has no rational zeros, so we must have $w = 1/3$. By (3.13),

$$r = y/2 - U/3. \tag{3.15}$$

By (3.12) and (3.15), we also have

$$s = y/2 - U/3. \tag{3.16}$$

Please cite this article in press as: K. Byard et al., Lam's power residue addition sets, Adv. in Appl. Math. (2010), doi:10.1016/j.aam.2010.09.008

Use (3.15)–(3.16) to substitute for r and s in the equation

$$h_0 - h_1 - p = 0 \tag{3.17}$$

and then use (3.8) to substitute for y in (3.17). We see that (3.17) reduces to

$$27T^2 + 224U^2 + 18T\nu - 9\nu^2 = 0. \tag{3.18}$$

Solving (3.18) for T, we have

$$9T = -3\nu \pm 2\left(9\nu^2 - 168U^2\right)^{1/2}. \tag{3.19}$$

Since T is an integer, this forces $\nu = 13$ and $U^2 = 9$. Then by (3.19), $T = -5$, which contradicts (3.1). □

4. Nonexistence for *n* = 16

In this section, $\nu = 16\epsilon - 1$ and $p = 16f + 1 = a_4^2 + b_4^2$ with f even and $a_4 \equiv -1 \pmod 4$.

Theorem 4.1. *$H_{16,\epsilon}$ is never a qualified residue difference set.*

Proof. Assume the contrary. First assume that $2 \notin H_4$. We will obtain a contradiction by using the formulas for the cyclotomic numbers $(i, j) = (i, j)_{16}$ found in [11]. By Theorem 2.2,

$$16(1 + a_4) = 256\{(4,8) - (0,8)\} - 128\{(1,8) + (5,8) - (3,8) - (7,8)\} = (\nu + 1)^2.$$

Thus $\nu = a_4$, so $a_4^2 \equiv 1 \pmod{32}$. Since f is even, we also have $p \equiv 1 \pmod{32}$, so that 32 divides b_4^2. Thus 8 divides b_4, contradicting [3, Theorem 7.5.1].

Finally assume that $2 \in H_4$. Let m denote the qualifier for the qualified residue difference set $H_{16,\epsilon}$. By Theorem 2.1, m and $-m$ are octic but not sixteenth power residues (mod p). Thus, by definition of the Gauss sum $g(n)$, $\sigma_{-m}g(16) = 2g(8) - g(16)$. Using this formula in (2.4) with $n = 16$, we obtain

$$g(8)^2 + 2\nu g(8) + p = M^2, \tag{4.1}$$

where as in [9, Eq. (4)], $M^2 = (g(16) - g(8))^2$. Note that if the term p in (4.1) were replaced by $-15p$, then (4.1) would become the equation [9, Eq. (15)]. We can now obtain a contradiction to (4.1) in the same way we obtained a contradiction to [9, Eq. (15)] in [9, pp. 43–44]. We omit the details, instead pointing out the few minor modifications that must be made in the proof in [9]. In [9, Eq. (16)], change the sign of the term $-8p$. In the formula for A below [9, Eq. (17)], change the sign of the term $4a_{16}$. In [9, Eq. (18)], change the sign of the term $-2\alpha\sqrt{p}Y$. Change the sign of the right side of [9, Eq. (19)]. On the left-hand side of the equation above [9, Eq. (21)], change the sign of the term $4a_{16}$. Lastly, in [9, Eq. (23)], 337 should be replaced by 257, which is the first prime for which $p \equiv 1 \pmod{32}$ and $2 \in H_4$. □

5. Nonexistence for *n* = 18

In this section, $\nu = 18\epsilon - 1$ and $p = 18f + 1$ with f even.

Theorem 5.1. *$H_{18,\epsilon}$ is never a qualified residue difference set.*

Please cite this article in press as: K. Byard et al., Lam's power residue addition sets, Adv. in Appl. Math. (2010), doi:10.1016/j.aam.2010.09.008

Proof. Assume the contrary. We will use the formulas for the cyclotomic numbers $(i, j) = (i, j)_{18}$ expressed by Baumert and Fredricksen [1,2] in terms of the integer parameters L, M, and C_i $(0 \leqslant i \leqslant 5)$. These cyclotomic numbers are defined relative to a fixed primitive root $g \pmod p$. Let ind 2, ind 3 denote the indices of 2, 3, respectively, with base g. The parameters L, M satisfy

$$4p = L^2 + 27M^2, \quad L \equiv 7 \pmod 9.$$

Moreover, setting

$$S = \sum_{i=0}^{5} C_i \zeta_9^i, \quad \zeta_9 = \exp 2\pi i/9,$$

we have $|S|^2 = p$, so that

$$p = C_0^2 + C_1^2 + C_2^2 + C_3^2 + C_4^2 + C_5^2 - C_0C_3 - C_1C_4 - C_2C_5, \tag{5.1}$$

$$0 = C_0C_1 + C_1C_2 + C_2C_3 + C_3C_4 + C_4C_5 - C_0C_2 - C_1C_3 - C_2C_4 - C_3C_5, \tag{5.2}$$

$$0 = C_0C_4 + C_1C_5 - C_0C_2 - C_1C_3 - C_2C_4 - C_3C_5 + C_0C_5. \tag{5.3}$$

We will apply Theorem 2.2 in each of the eight cases below.

Case 1. ind $2 \equiv 0 \pmod 9$, ind $3 \equiv 0 \pmod 3$.

We have $648(i, 9) = 2p + 2 + 4\nu$, $1 \leqslant i \leqslant 8$. Adding the three formulas for $i = 1, 2, 4$, we see that $L = 2\nu$. Then from the formulas for $i = 1, 4$, we have $C_1 = C_2 = C_4 + C_5$, and from $i = 3$, we have $C_3 = M$. Thus (5.2) yields

$$C_5^2 + 2C_4C_5 + MC_4 - MC_5 = 0,$$

and (5.3) yields

$$C_5^2 - C_4^2 - MC_4 - 2MC_5 = 0.$$

Eliminating C_4, we obtain

$$C_5^3 - 3C_5M^2 - M^3 = 0.$$

Since $x^3 - 3x - 1$ has no rational solution, we must have $M = C_5 = 0$. This gives the contradiction $4p = L^2$.

Case 2. ind $2 \equiv 0 \pmod 9$, ind $3 \equiv 1 \pmod 3$.

Since $(2, 9) = (2, B)$, we have $C_5 = -2C_4$. Since $(1, 9) = (4, D)$, we have $C_1 + C_2 = 4C_4$. Since $(1, 9) = (1, A)$, we have $C_2 = C_5 + 2C_1$. Combining these three formulas, we see that

$$C_1 = 2C_4, \qquad C_2 = 2C_4, \qquad C_5 = -2C_4.$$

Therefore, since $(2, 9) = (1, A)$, we have

$$C_1 = C_2 = C_4 = C_5 = 0.$$

Please cite this article in press as: K. Byard et al., Lam's power residue addition sets, Adv. in Appl. Math. (2010), doi:10.1016/j.aam.2010.09.008

It then follows from the formula for $(3,9)$ that $M = -C_3$. The formula for $(1,9)$ yields $p+1+L = p+1+2\nu$, so that $L = 2\nu$. The formula for $(3,C)$ then yields

$$p+1+L = p+1-8L+18C_0+9M,$$

so that $M = 2(\nu - C_0)$. Thus by (5.1), $p = C_0^2 + M^2 + MC_0$. Substituting for M, we obtain $p = 3C_0^2 - 6C_0\nu + 4\nu^2$. Since $4p = 4\nu^2 + 27M^2$, we also have $p = 27C_0^2 - 54C_0\nu + 28\nu^2$. The last two equations imply that $\nu = C_0$, so we obtain the contradiction $M = 0$.

Case 3. ind $2 \equiv 1 \pmod 9$, ind $3 \equiv 0 \pmod 3$.

Since $(3,9) = (3,C)$, we have

$$-36C_1 + 54C_2 + 54C_3 + 36C_4 - 72C_5 = 0.$$

Since $(1,9) = (2,B)$, we have

$$90C_1 - 90C_4 + 72C_5 = 0.$$

Since $(2,B) = (4,9)$, we have

$$36C_1 - 36C_4 - 36C_5 = 0.$$

Combining these three formulas, we see that

$$C_5 = 0, \qquad C_1 = C_4, \qquad C_2 = -C_3.$$

Thus by (5.2) and (5.3), $C_0C_1 = C_3^2 = 0$, so that $C_2 = 0$. Then from (5.1), $p = C_0^2 + C_1^2$. This yields the contradiction $p = (C_0 + C_1)^2$.

Case 4. ind $2 \equiv 1 \pmod 9$, ind $3 \equiv 1 \pmod 3$.

Since $(3,9) = (3,C)$, we have

$$-36C_1 + 18C_2 + 54C_3 + 36C_4 = 0.$$

Since $(4,9) = (2,B)$, we have

$$-72C_1 + 36C_2 + 72C_4 = 0.$$

Thus $C_3 = 0$. Since $(1,9) = (2,B)$, we have $C_2 = 90(C_4 - C_1)/36$. Since $(4,9) = (2,B)$, we have $C_2 = -2(C_4 - C_1)$. Thus

$$C_1 = C_4, \qquad C_2 = C_3 = 0.$$

From the formula for $(4,9)$, we have

$$L + 9M + 18C_0 = 2\nu.$$

Since $(1,A) = (4,D)$, we have

$$L + 3M - 2C_0 = 0.$$

Please cite this article in press as: K. Byard et al., Lam's power residue addition sets, Adv. in Appl. Math. (2010), doi:10.1016/j.aam.2010.09.008

These two formulas yield

$$10L + 36M = 2\nu.$$

Summing the formulas for $(2, 9)$, $(1, A)$, and $(4, D)$, we obtain

$$21L + 27M = -12\nu.$$

Eliminating L in the last two formulas, we obtain the contradiction $M = \nu/3$.

Case 5. ind $2 \equiv 1 \pmod 9$, ind $3 \equiv 2 \pmod 3$.

We successively consider the seven formulas for $(1, 9)$, $(1, A)$, $(2, 9)$, $(2, B)$, $(3, 9)$, $(3, C)$, and $(4, D)$. Solve the first for C_0 (in terms of p, ν, L, and M), and then substitute this value into the remaining six formulas. Solve the second for C_1 and then substitute this value into the remaining five formulas. Continue in this way, solving successively for C_2, C_3, C_4, C_5, and M. We thereby obtain the evaluations

$$C_2 = C_3 = C_5 = -C_0 = -(\nu + L)/9, \qquad C_1 = C_4 = (L - 8\nu)/9, \qquad M = (4\nu + L)/9.$$

By (5.2), $0 = (L + \nu)^2$. Thus $L = -\nu$, so that we have the contradiction $M = \nu/3$.

Case 6. ind $2 \equiv 3 \pmod 9$, ind $3 \equiv 0 \pmod 3$.

Since $(1, 9) = (4, D)$, we have $C_1 = C_2$. Thus, since $(1, 9) = (2, B)$, we have $C_1 = C_4 - 2C_5$. Since $(1, A) = (2, 9)$, it follows that

$$C_5 = 3C_4/7, \qquad C_1 = C_4/7.$$

Thus, since $(1, 9) = (1, A)$, we have

$$C_1 = C_2 = C_4 = C_5 = 0.$$

Finally, since $(3, 9) = (4, 9)$, we obtain the contradiction $M = 0$.

Case 7. ind $2 \equiv 3 \pmod 9$, ind $3 \equiv 1 \pmod 3$.

Since $(2, 9) = (4, D)$, we have $C_5 + C_1 = 0$. Since $(1, A) = (4, D)$, we have $C_2 + C_4 = 0$. Since $(1, 9) = (4, 9)$, we have $C_2 = C_4 = 0$. Since $(1, 9) = (2, 9)$, we have $C_1 = C_5 = 0$. From the formula for $(1, 9)$, we have $L = 2\nu$. From the formula for $(3, 9)$, we have $C_3 = \nu - C_0$. From the formula for $(3, C)$, we have $C_0 = -M$. Thus $C_3 = \nu + M$. Then by (5.1), $p = C_3^2 + M^2 + MC_3$. Replacing C_3 by $\nu + M$, we obtain $p = 3M^2 + 3M\nu + \nu^2$. Therefore $4p = 12M^2 + 12M\nu + 4\nu^2$. On the other hand, $4p = 27M^2 + 4\nu^2$, so we obtain the contradiction $15M = 12\nu$.

Case 8. ind $2 \equiv 3 \pmod 9$, ind $3 \equiv 2 \pmod 3$.

Summing the formulas for $(1, 9)$, $(1, A)$, and $(2, 9)$, we obtain

$$6(p + 1 + 2\nu) = 6(p + 1 + L),$$

so that $L = 2\nu$. Thus, from the formula for $(3, 9)$, we obtain the contradiction $M = 0$. □

Please cite this article in press as: K. Byard et al., Lam's power residue addition sets, Adv. in Appl. Math. (2010), doi:10.1016/j.aam.2010.09.008

6. Nonexistence for $n = 20$

In this section, $\nu = 20\epsilon - 1$ and $p = 20f + 1$ with f even.

Theorem 6.1. *$H_{20,\epsilon}$ is never a qualified residue difference set.*

Proof. Assume the contrary. We will use the formulas for the cyclotomic numbers $(i, j) = (i, j)_{20}$ expressed by Muskat and Whiteman [22,23] in terms of the integer parameters c, d, x, u, v, w, d_i $(0 \leqslant i \leqslant 19)$. These cyclotomic numbers are defined relative to a fixed primitive root $g \pmod p$. Let ind 2, ind 5 denote the indices of 2, 5, respectively, with base g. The parameters c, d satisfy [22, p. 197]

$$p = c^2 + 5d^2 \tag{6.1}$$

and the parameters x, u, v, w satisfy [22, Eq. (4.1)]

$$16p = x^2 + 50u^2 + 50v^2 + 125w^2, \tag{6.2}$$

$$x \equiv 1 \pmod 5, \tag{6.3}$$

$$xw = v^2 - 4uv - u^2. \tag{6.4}$$

The parameters d_i satisfy [22, Eq. (2.17)]

$$d_{i+10} = -d_i \quad (0 \leqslant i \leqslant 9) \tag{6.5}$$

and [22, Eq. (2.18)]

$$J\left(\chi, \chi^5\right) = \sum_{j=0}^{9} d_j \zeta_{20}^j, \tag{6.6}$$

where J is a Jacobi sum and χ is a character $\pmod p$ of order 20 such that $\chi(g) = \zeta_{20} := \exp(2\pi i/20)$. Taking absolute values in (6.6), we have

$$p = \left| \sum_{j=0}^{9} d_j \zeta_{20}^j \right|^2. \tag{6.7}$$

By [22, p. 203],

$$h_0 := \sum_{i=0}^{9} d_i^2 = p. \tag{6.8}$$

Expanding (6.7) and using (6.8), we see that for each j with $1 \leqslant j \leqslant 4$,

$$h_j := \sum_{i=0}^{9} d_i d_{i+j} = 0. \tag{6.9}$$

According to the tables [23], there are twenty separate cases to consider. Arguing as in [22, p. 214], we may choose the primitive root g in such a way as to reduce to the eight cases where ind $2 \equiv 0$ or 2 (mod 10). Arguing as in the penultimate paragraph in [22, p. 215], we may reduce further to six cases, by dispensing with the two cases where ind $5 \equiv 2 \pmod 4$, $c \equiv 4 \pmod{10}$. The first four cases below are the simplest; the last two cases are considerably more involved. We used a `Maple` program to perform the lengthy calculations.

Case 1. ind $2 \equiv 0 \pmod{10}$, ind $5 \equiv 0 \pmod 4$, $c \equiv 1 \pmod{10}$.

In view of Theorem 2.2 and the table in [23], we have the matrix equation $AX = B$, where B is the 9×1 column vector $(8\nu, 8\nu, 8\nu, 8\nu, 8\nu, 8\nu, 8\nu, 8\nu, 8\nu)$, X is the 10×1 vector $(c, x, u, v, w, d_0, d_4, d_8, d_{12}, d_{16})$, and A is the 9×10 matrix

$$\begin{pmatrix} 8 & -2 & 120 & 240 & -250 & -24 & 56 & 56 & -24 & -24 \\ 8 & -2 & -120 & -240 & -250 & -24 & -24 & -24 & 56 & 56 \\ -40 & -10 & -120 & 160 & -150 & -8 & -8 & -88 & -8 & 72 \\ -40 & -10 & 120 & -160 & -150 & -8 & 72 & -8 & -88 & -8 \\ 8 & -2 & -240 & 120 & 250 & -24 & 56 & -24 & 56 & -24 \\ 8 & -2 & 240 & -120 & 250 & -24 & -24 & 56 & -24 & 56 \\ -40 & -10 & 160 & 120 & 150 & -8 & -8 & -8 & 72 & -88 \\ -40 & -10 & -160 & -120 & 150 & -8 & -88 & 72 & -8 & -8 \\ 128 & -32 & 0 & 0 & 0 & 136 & -24 & -24 & -24 & -24 \end{pmatrix}$$

whose nine rows correspond to the nine cyclotomic numbers $(1, 10)$, $(1, 11)$, $(2, 10)$, $(2, 12)$, $(3, 10)$, $(3, 13)$, $(4, 10)$, $(4, 14)$, $(5, 10)$ in the table. Solving $AX = B$, we see that every solution X has vanishing third, fourth, and fifth entries, i.e., $u = v = w = 0$. This contradicts (6.2).

Case 2. ind $2 \equiv 0 \pmod{10}$, ind $5 \equiv 0 \pmod 4$, $c \equiv 9 \pmod{10}$.

We proceed as in Case 1, but this time with the 9×10 matrix A defined by

$$\begin{pmatrix} 40 & -10 & 40 & 80 & -50 & 8 & 88 & -72 & 8 & 8 \\ 40 & -10 & -40 & -80 & -50 & 8 & 8 & 8 & -72 & 88 \\ -8 & -2 & 40 & 80 & 50 & 24 & 24 & -56 & 24 & -56 \\ -8 & -2 & -40 & -80 & 50 & 24 & -56 & 24 & -56 & 24 \\ 40 & -10 & -80 & 40 & 50 & 8 & -72 & 8 & 88 & 8 \\ 40 & -10 & 80 & -40 & 50 & 8 & 8 & 88 & 8 & -72 \\ -8 & -2 & 80 & -40 & -50 & 24 & 24 & 24 & -56 & -56 \\ -8 & -2 & -80 & 40 & -50 & 24 & -56 & -56 & 24 & 24 \\ 0 & 0 & 0 & 0 & 0 & 8 & 8 & 8 & 8 & 8 \end{pmatrix}.$$

Solving $AX = B$, we see that every solution X has fifth entry $w = 0$. Thus the integers u and v must be 0 by (6.4), and this contradicts (6.2).

Case 3. ind $2 \equiv 2 \pmod{10}$, ind $5 \equiv 0 \pmod 4$, $c \equiv 1 \pmod{10}$.

We proceed as in Case 1, but this time with the 9×10 matrix A defined by

$$\begin{pmatrix}
88 & -12 & -90 & -130 & -150 & -24 & 56 & 56 & -24 & -24 \\
8 & 23 & 120 & -110 & 175 & -24 & -24 & -24 & 56 & 56 \\
-80 & 10 & -20 & -40 & 150 & -8 & -8 & -88 & -8 & 72 \\
-40 & -10 & -130 & -110 & 100 & -8 & 72 & -8 & -88 & -8 \\
8 & -2 & -50 & 50 & -100 & -24 & 56 & -24 & 56 & -24 \\
48 & -22 & -20 & -40 & -250 & -24 & -24 & 56 & -24 & 56 \\
-40 & 15 & -40 & -30 & -25 & -8 & -8 & -8 & 72 & -88 \\
40 & -20 & 190 & 230 & 250 & -8 & -88 & 72 & -8 & -8 \\
8 & 23 & -60 & 30 & 75 & 136 & -24 & -24 & -24 & -24
\end{pmatrix}.$$

Solving $AX = B$, we see that every solution X has fifth entry $w = \nu/7$, which is impossible since $\nu/7$ is not an integer.

Case 4. ind $2 \equiv 2 \pmod{10}$, ind $5 \equiv 0 \pmod 4$, $c \equiv 9 \pmod{10}$.

We proceed as in Case 1, but this time with the 9×10 matrix A defined by

$$\begin{pmatrix}
-40 & -20 & -10 & 30 & 50 & 8 & 88 & -72 & 8 & 8 \\
40 & 15 & -40 & -30 & -25 & 8 & 8 & 8 & -72 & 88 \\
-48 & -22 & -20 & -40 & 150 & 24 & 24 & -56 & 24 & -56 \\
-8 & -2 & -50 & 50 & -100 & 24 & -56 & 24 & -56 & 24 \\
40 & -10 & -130 & -110 & 100 & 8 & -72 & 8 & 88 & 8 \\
80 & 10 & -20 & -40 & -250 & 8 & 8 & 88 & 8 & -72 \\
-8 & 23 & 120 & -110 & 175 & 24 & 24 & 24 & -56 & -56 \\
-88 & -12 & 110 & 70 & 50 & 24 & -56 & -56 & 24 & 24 \\
40 & 15 & 100 & -50 & -125 & 8 & 8 & 8 & 8 & 8
\end{pmatrix}.$$

Solving $AX = B$, we see that every solution X has fifth entry $w = -2d_4 + \nu/5$, which is impossible since $\nu/5$ is not an integer.

Case 5. ind $2 \equiv 0 \pmod{10}$, ind $5 \equiv 2 \pmod 4$, $c \equiv 6 \pmod{10}$.

Consider the nine linear equations corresponding to the same nine cyclotomic numbers as in Case 1, and solve for d_0, d_4, d_8, d_{12}, d_{16}, d_1, d_5, d_9, d_{13}, to obtain (in view of (6.5)) $d_0 = 3(\nu + x)/5$, $d_1 = (4d_{17} - 2u - 4v - 5w)/4$, $d_2 = (10d - 2\nu - 25u + 25v + 25w - 2x)/20$, $d_3 = (3v - u - 2d_{17})/2$, $d_4 = (10d + 2\nu - 25u - 25v + 25w + 2x)/20$, $d_5 = (-8c + 8d_{17} - 4\nu + 2u - 6v - 5w - 3x)/8$, $d_6 = -(10d + 2\nu + 25u + 25v + 25w + 2x)/20$, $d_7 = -d_{17}$, $d_8 = (-10d + 2\nu - 25u + 25v - 25w + 2x)/20$, $d_9 = (4d_{17} + 4u - 2v - 5w)/4$. We now plug these ten formulas into (6.9) to obtain long expressions for h_1, h_2, h_3, h_4 in terms of the parameters p, ν, c, d, x, u, v, w, d_{17}. In particular,

$$16h_1 = 20d(v - u) + 16\nu v + 8\nu u + (40c + 25w)(u + v) + 3xu + 11xv. \tag{6.10}$$

Since u and v cannot both vanish, we can define the relatively prime pair of integers u_0, v_0 by $u_0 = u/(u, v)$, $v_0 = v/(u, v)$. Since $h_1 = 0$, division by (u, v) in (6.10) yields

$$0 = 20d(v_0 - u_0) + 16\nu v_0 + 8\nu u_0 + (40c + 25w)(u_0 + v_0) + 3xu_0 + 11xv_0. \tag{6.11}$$

By Theorem 2.2, $p \equiv -1 - 2\nu \pmod{25}$, and by (6.2), $16p \equiv x^2 \pmod{25}$. Thus $x^2 \equiv 9 + 18\nu \pmod{25}$, and since ν is either 19 or -1, it follows from (6.3) that $x \equiv 5 + 9\nu \pmod{25}$. If we now substitute $5 + 9\nu$ for x in (6.11), then divide both sides by 5, and finally substitute -1 for ν (mod 5) and 1 for c (mod 5), we obtain the congruence

$$v_0 + du_0 \equiv u_0 + dv_0 \pmod 5. \tag{6.12}$$

Please cite this article in press as: K. Byard et al., Lam's power residue addition sets, Adv. in Appl. Math. (2010), doi:10.1016/j.aam.2010.09.008

Now repeat the argument starting at (6.10) with $h_1 - h_3$ in place of h_1. In place of (6.12), we arrive at the congruence

$$u_0 \equiv -dv_0 \pmod 5. \tag{6.13}$$

From (6.12) and (6.13), it follows that 5 does not divide $u_0 v_0$, and $d^2 \equiv 1 \pmod 5$. Repeat the argument again with $h_2 + h_4$, omitting the division by (u, v). We then obtain the congruence $2w - d + v^2 - 4uv - u^2 \equiv 0 \pmod 5$. In view of (6.4), this simplifies to $2w - d + xw \equiv 0 \pmod 5$. Then by (6.3), $2d \equiv w \pmod 5$. Reducing (6.4) modulo 5 and using (6.13), we have

$$2d \equiv w \equiv xw = v^2 - u^2 - 4uv \equiv v^2 - d^2v^2 + 4dv^2 \equiv 4dv^2 \pmod 5,$$

and so we arrive at the contradiction $v^2 \equiv 3 \pmod 5$.

Case 6. ind $2 \equiv 2 \pmod{10}$, ind $5 \equiv 2 \pmod 4$, $c \equiv 6 \pmod{10}$.

Proceeding as in Case 5, we have $d_0 = (-10d + 12\nu + 5u + 35v - 3x)/20$, $d_1 = (16d_{17} + 12u - 6v + 25w + 5x)/16$, $d_2 = (-20d - 4\nu - 10u - 20v - 25w + x)/40$, $d_3 = (16c - 16d_{17} + 2u + 24v - 5w - 7x)/16$, $d_4 = (20d + 4\nu + 60u + 70v + 75w - x)/40$, $d_5 = (8d_{17} - 4\nu + 2u - 16v + 15w + x)/8$, $d_6 = (20d - 4\nu - 10u - 20v - 25w + x)/40$, $d_7 = -d_{17}$, $d_8 = (4\nu + 10u + 20v + 125w - x)/40$, $d_9 = (16d_{17} + 26u - 8v + 15w + 5x)/16$. Plug these ten formulas into (6.8) and (6.9) to obtain long expressions for h_0, h_1, h_2, h_3, h_4. Write

$$G_0 = -2h_1, \qquad G_1 = p - h_0 - h_2, \qquad G_2 = h_1 - h_3, \qquad G_3 = h_0 - p - h_4,$$

and

$$E = -xw + v^2 - u^2 - 4uv, \qquad F = 16p - x^2 - 50u^2 - 50v^2 - 125w^2.$$

Note that E, F, and the G_i all vanish, by (6.2), (6.4), (6.8), and (6.9).

In the sequel, we will be expressing several parameters in terms of new subscripted parameters, all of which are integers. Since ind $2 \equiv 2 \pmod 5$ in Case 6, it follows from [3, Theorem 3.7.9] that $v = x + u + 2 + 4v_1$, $x = 2x_1 + 1$, and $u = 2u_1 + 1$ (i.e., x, u, and $(v - x - u)/2$ are all odd). Since v is even, it follows easily from (6.4) that $w = 2v - x + 8w_1$. By Theorem 2.2, $p = -1 - 2\nu + 16p_1$. We have $\nu = -1 + 20\nu_1$, where ν_1 is either 0 or 1. Since c is even in Case 6, and $p \equiv 1 \pmod 8$, it follows from (6.1) that $c = 2 + 4c_1$. Thus $d^2 \equiv 6\nu - 1 \pmod{16}$. It follows that $d = \pm(2 - \nu) + 8d_1$. We will consider the two sign possibilities in two separate subcases.

Subcase 1. $d = 2 - \nu + 8d_1$.

The following sequence of integer congruences and their successive implications will ultimately yield the desired contradiction:

$$E/8 - F/16 \equiv 2 + 2w_1 \pmod 4 \quad \text{implies} \quad w_1 = 1 + 2w_2,$$

$$4G_3 \equiv x_1 + v_1 \pmod 2 \quad \text{implies} \quad v_1 = x_1 + 2v_2,$$

$$E/16 - F/32 \equiv 2x_1 + 2w_2 \pmod 4 \quad \text{implies} \quad w_2 = x_1 + 2w_3,$$

$$G_1 - G_2 \equiv u_1 \pmod 2 \quad \text{implies} \quad u_1 = 2u_2,$$

$$G_0/2 \equiv 1 + v_2 \pmod 2 \quad \text{implies} \quad v_2 = 1 + 2v_3,$$

$$E/16 \equiv x_1 \pmod 2 \quad \text{implies} \quad x_1 = 2x_2,$$

Please cite this article in press as: K. Byard et al., Lam's power residue addition sets, Adv. in Appl. Math. (2010), doi:10.1016/j.aam.2010.09.008

$$E/32 \equiv v_3 + w_3 \pmod 2 \quad \text{implies} \quad w_3 = v_3 + 2w_4,$$
$$G_0/4 \equiv v_1 + x_2 \pmod 2 \quad \text{implies} \quad x_2 = v_1 + 2x_3,$$
$$E/64 \equiv 1 + u_2 + w_4 \pmod 2 \quad \text{implies} \quad w_4 = 1 + u_2 + 2w_5,$$
$$G_1/2 \equiv v_1 + u_2 + v_3 \pmod 2 \quad \text{implies} \quad v_3 = v_1 + u_2 + 2v_4,$$
$$E/64 - F/128 \equiv 2 + 2p_1 + 2v_4 \pmod 4 \quad \text{implies} \quad v_4 = 1 + p_1 + 2v_5,$$
$$G_1/4 \equiv d_1 + p_1 \pmod 2 \quad \text{implies} \quad d_1 = p_1 + 2d_2,$$
$$G_2/8 - G_1/8 - G_0/8 \equiv c_1 \pmod 2 \quad \text{implies} \quad c_1 = 2c_2,$$
$$G_0/8 \equiv 1 + p_1 + x_3 \pmod 2 \quad \text{implies} \quad x_3 = 1 + p_1 + 2x_4,$$
$$G_3/4 \equiv 1 + v_1 + u_2 \pmod 2 \quad \text{implies} \quad u_2 = 1 + v_1 + 2u_3,$$
$$G_2/8 \equiv 1 + p_1 + v_5 + d_2 \pmod 2 \quad \text{implies} \quad v_5 = 1 + p_1 + d_2 + 2v_6,$$
$$G_2/16 \equiv 1 + v_6 + d_2 \pmod 2 \quad \text{implies} \quad v_6 = 1 + d_2 + 2v_7,$$
$$G_0/16 - G_1/16 \equiv v_1 + c_2 \pmod 2 \quad \text{implies} \quad c_2 = v_1 + 2c_3,$$
$$E/128 - G_3/8 \equiv 1 \pmod 2 \quad \text{yields the desired contradiction.}$$

Subcase 2. $d = v - 2 + 8d_1$.

The following sequence of integer congruences and their successive implications will ultimately yield the final contradiction:

$$E/8 - F/16 \equiv 2 + 2w_1 \pmod 4 \quad \text{implies} \quad w_1 = 1 + 2w_2,$$
$$4G_3 \equiv x_1 + v_1 \pmod 2 \quad \text{implies} \quad v_1 = x_1 + 2v_2,$$
$$G_1 - G_2 \equiv w_2 + v_2 \pmod 2 \quad \text{implies} \quad w_2 = v_2 + 2w_3,$$
$$E/16 \equiv 1 + u_1 \pmod 2 \quad \text{implies} \quad u_1 = 1 + 2u_2,$$
$$G_0/2 \equiv 1 + v_2x_1 \pmod 2 \quad \text{implies} \quad v_2 = 1 + 2v_3,\ x_1 = 1 + 2x_2,$$
$$G_3/2 \equiv 1 + v_1 + w_3 \pmod 2 \quad \text{implies} \quad w_3 = 1 + v_1 + 2w_4,$$
$$E/32 \equiv v_1 + x_2 \pmod 2 \quad \text{implies} \quad x_2 = v_1 + 2x_3,$$
$$E/64 - F/128 - G_0/4 \equiv 1 \pmod 2 \quad \text{yields the desired contradiction.} \qquad \square$$

Acknowledgment

We are grateful to the referee for pointing out papers [18–20].

References

[1] L.D. Baumert, H. Fredricksen, The cyclotomic numbers of order eighteen with applications to difference sets, Math. Comp. 21 (1967) 204–219.
[2] L.D. Baumert, H. Fredricksen, Table of cyclotomic numbers of order eighteen, http://math.ucsd.edu/~revans/cyclotomic18, 1967.
[3] B.C. Berndt, R.J. Evans, K.S. Williams, Gauss and Jacobi Sums, Wiley, New York, 1998.
[4] K. Byard, On qualified residue difference sets, Int. J. Number Theory 2 (2006) 591–597.
[5] K. Byard, Tenth power qualified residue difference sets, Int. J. Number Theory 5 (2009) 797–803.
[6] K. Byard, Twelfth power qualified residue difference sets, Integers 9 (2009) 401–410.

[7] E. Caroli, J.B. Stephen, G. Di Cocco, L. Natalucci, A. Spizzichino, Coded aperture imaging in X- and gamma-ray astronomy, Space Science Reviews 45 (1987) 349–403.
[8] European Space Agency, INTEGRAL, http://sci.esa.int/science-e/www/object/index.cfm?fobjectid=31149.
[9] R.J. Evans, Bioctic Gauss sums and sixteenth power residue difference sets, Acta Arith. 38 (1980/1981) 37–46.
[10] R.J. Evans, Nonexistence of twentieth power residue difference sets, Acta Arith. 84 (1999) 397–402.
[11] R.J. Evans, J.R. Hill, The cyclotomic numbers of order sixteen, Math. Comp. 33 (1979) 827–835.
[12] J. Gunson, B. Polychronopulos, Optimum design of a coded mask X-ray telescope for rocket applications, Mon. Not. R. Astron. Soc. 177 (1976) 485–497.
[13] J. in 't Zand, Coded aperture camera imaging concept, http://astrophysics.gsfc.nasa.gov/cai/coded_intr.htm.
[14] D. Jennings, K. Byard, An extension for residue difference sets, Discrete Math. 167/168 (1997) 405–410.
[15] D. Jennings, K. Byard, Qualified residue difference sets with zero, Discrete Math. 181 (1998) 283–288.
[16] Y.P. Kazachkov, D.S. Semenov, N.P. Goryacheva, Application of coded apertures in γ-ray cameras, Instrum. Experiment. Tech. 50 (2007) 267–274.
[17] L.E. Kopilovich, Applications of difference sets to the aperture design in multielement systems in radio science and astronomy, in: A. Pott, et al. (Eds.), Difference Sets, Sequences and Their Correlation Properties, Kluwer Acad. Publ., Dordrecht, 1999, pp. 297–330.
[18] C.W.H. Lam, A generalization of cyclic difference sets, I, J. Combin. Theory Ser. A 19 (1975) 51–65.
[19] C.W.H. Lam, Nth power residue addition sets, J. Combin. Theory Ser. A 20 (1976) 20–33.
[20] C.W.H. Lam, Cyclotomy and addition sets, J. Combin. Theory Ser. A 22 (1977) 43–60.
[21] J.B. Muskat, The cyclotomic numbers of order fourteen, Acta Arith. 11 (1965/1966) 263–279.
[22] J.B. Muskat, A.L. Whiteman, The cyclotomic numbers of order twenty, Acta Arith. 17 (1970) 185–216.
[23] J.B. Muskat, A.L. Whiteman, Table of cyclotomic numbers of order twenty, http://math.ucsd.edu/~revans/cyclotomic20, 1970.
[24] W.L. Rogers, K.F. Koral, R. Mayans, P.F. Leonard, J.H. Thrall, T.J. Brady, J.W. Keyes, Coded aperture imaging of the heart, J. Nucl. Med. 21 (1980) 371–378.
[25] A.L. Whiteman, The cyclotomic numbers of order sixteen, Trans. Amer. Math. Soc. 86 (1957) 401–413.
[26] A.L. Whiteman, The cyclotomic numbers of order ten, Proc. Sympos. Appl. Math. 10 (1960) 95–111.
[27] C. Winkler, T.J.-L. Courvoisier, G. Di Cocco, N. Gehrels, A. Gimenez, S. Grebenev, W. Hermsen, J.M. Mas-Hesse, F. Lebrun, N. Lund, G.G.C. Palumbo, J. Paul, J.-P. Roques, H. Schnopper, V. Schonfelder, R. Sunyaev, B. Teegarden, P. Ubertini, G. Vedrenne, A.J. Dean, The INTEGRAL mission, Astron. Astrophys. 411 (2003) L1–L6.

Please cite this article in press as: K. Byard et al., Lam's power residue addition sets, Adv. in Appl. Math. (2010), doi:10.1016/j.aam.2010.09.008