MATHEMATICS OF COMPUTATION
VOLUME 40, NUMBER 162
APRIL 1983, PAGES 677-683

Twenty-Fourth Power Residue Difference Sets

By Ronald J. Evans*

Abstract. It is proved that if p is a prime $\equiv 1 \pmod{24}$ such that either 2 is a cubic residue or 3 is a quartic residue (mod p), then the twenty-fourth powers (mod p) do not form a difference set or a modified difference set.

1. Introduction. Let $p = ef + 1$ be a prime with fixed primitive root g. Let H denote the set of (nonzero) eth power residues (mod p). For integers i, j (mod p), define the cyclotomic number (i, j) of order e to be the number of integers n (mod p) for which n/g^i and $(1 + n)/g^j$ are both in H. If there exists $\alpha \geqslant 1$ such that every nonzero integer (mod p) can be expressed as a difference (mod p) of elements of H (resp., $H \cup \{0\}$) in exactly α ways, one calls H a *difference set* (resp. *modified difference set*).

E. Lehmer [7] has shown that

(1) H is a difference set if and only if $2 \mid e$, $2 \nmid f$, and
$$(i,0) = (f-1)/e \text{ for all } i = 0, 1, 2, \ldots, (e-2)/2,$$

and

(1′) H is a modified difference set if and only if $2 \mid e$, $2 \nmid f$, and
$$1 + (0,0) = (i,0) = (f+1)/e \text{ for all } i = 1, 2, \ldots, (e-2)/2.$$

In Section 5 of this paper, we use Lehmer's result, a table of cyclotomic numbers of order twenty-four [6], and a formula for Gauss sums of order twenty-four [3, Theorem 3.32] to prove the following theorem.

THEOREM. *Suppose that* $p = 24f + 1$ *is a prime such that either* 2 *is a cubic residue or* 3 *is a quartic residue* (mod p). *Then the twenty-fourth powers* (mod p) *do not form a difference set or a modified difference set.*

2. History. Chowla [4] and Lehmer [7] have constructed eth power residue difference sets and modified difference sets in the cases $e = 2, 4, 8$. The eth power residue difference sets and modified difference sets have been proved nonexistent for all other values of $e \leqslant 24$, except in the following unsolved cases:

(A) $e = 20$, $p \equiv 21 \pmod{40}$, 5 nonquartic (mod p),
(B) $e = 22$, $p \equiv 23 \pmod{88}$, 2 not an eleventh power (mod p),

---

Received March 10, 1982.
1980 *Mathematics Subject Classification.* Primary 05B10, 12C20; Secondary 10G05.
Key words and phrases. Power residue difference sets, cyclotomic numbers, Gauss and Jacobi sums.
*Author has NSF grant MCS8101860.

and

(C) $e = 24$, $p \equiv 25 \pmod{48}$, 2 noncubic and 3 nonquartic $\pmod{p}$.

See [7] for $e = 6$; [13], [14] for $e = 10, 12$; [9, Theorems 4 and 5] for $e = 14, 22$; [12], [5] for $e = 16$; [2] for $e = 18$; and [10] for $e = 20$. See also the paper of Berndt and Evans [3, §5] and the books of Baumert [1], Mann [8], and Storer [11].

3. The Tables of Cyclotomic Numbers of Order Twenty-Four. In the sequel we use the notation of Section 1 with $e = 24$. Let $\zeta = \exp(2\pi i/24)$ and fix a character χ $\pmod{p}$ of order twenty-four such that $\chi(g) = \zeta$. For characters $\lambda, \Psi \pmod{p}$, define the Jacobi sums

$$J(\lambda, \Psi) = \sum_{n \pmod{p}} \lambda(n)\Psi(1-n), \qquad K(\lambda) = \lambda(4)J(\lambda, \lambda).$$

It is known [3, §3] that there exist integers X, Y, A, B, C, D, U, V such that

$$K(\chi^6) = -X + 2Yi \qquad (p = X^2 + 4Y^2, X \equiv 1 \pmod{4}),$$
$$K(\chi^4) = -A + Bi\sqrt{3} \qquad (p = A^2 + 3B^2, A \equiv 1 \pmod{6}),$$
$$K(\chi^3) = -C + Di\sqrt{2} \qquad (p = C^2 + 2D^2, C \equiv 1 \pmod{4}),$$

and

$$K(\chi) = U + 2Vi\sqrt{6} \qquad (p = U^2 + 24V^2, U \equiv -C \pmod{3}).$$

Since $J(\chi, \chi^2) \in \mathbf{Z}[\zeta]$, there exist integers $D_0, D_1, \ldots, D_7$ such that

$$J(\chi, \chi^2) = \sum_{i=0}^{7} D_i \zeta^i.$$

In the 48 tables [6], each number $576(i, j)$ has been expressed as a linear combination of p, 1, X, Y, A, B, C, D, U, V, $D_0, \ldots, D_7$ over $\mathbf{Z}$.

4. Gauss Sums of Order Twenty-Four. Consider the Gauss sum

$$G_e = \sum_{n=0}^{p-1} \exp(2\pi i n^e/p).$$

Define, for real γ,

$$F_e(\gamma) = |G_e + \gamma|^2 - (p(e-1) + \gamma^2). \tag{2}$$

It is known [3, p. 391] that, for $e = 24$,

(3) H is a difference set (resp., modified difference set) if and only if $F_{24}(-1) = 0$ (resp., $F_{24}(23) = 0$).

5. Proof of Theorem. By (1) and (1′), we may assume that f is odd. Define $V' \in \{0, 1\}$ by $V' \equiv V \pmod{2}$. Let $Z = \operatorname{ind} 2 \pmod{12}$ and $T = \operatorname{ind} 3 \pmod{8}$, where the indices are taken with respect to the primitive root $g \pmod{p}$. We may assume without loss of generality that $Z \in \{0, 2, 4, 6\}$ and $T \in \{0, 2, 4\}$ (otherwise replace g by an appropriate power of g such as g^{-1}, g^5, or g^7).

Assume that H is a difference set or a modified difference set. In particular, then, by (1) and (1′), the numbers

$$\alpha(i) = 576(i, 0)$$

are equal for $1 \leqslant i \leqslant 11$. We will produce a contradiction in each of the nine cases below. The last case is considerably more complicated than the others since it incorporates the results on Gauss sums from Section 4 and [3, Theorem 3.32].

Case 1. $V' = Z = 0$.

From Tables 25–27 in [6],

$$0 = \alpha(1) + \alpha(5) - \alpha(7) - \alpha(11) = 192Y, \quad \text{if } T = 0,$$
$$0 = \alpha(1) + \alpha(7) - \alpha(5) - \alpha(11) = 48B, \quad \text{if } T = 2,$$

and

$$0 = \alpha(10) - \alpha(2) = 48B, \quad \text{if } T = 4.$$

Since clearly Y and B are nonzero, this is a contradiction.

Case 2. $V' = 0$, $Z = 2$.

From Tables 28 and 30,

$$0 = \alpha(11) - \alpha(5) = 96Y, \quad \text{if } T = 0,$$

and

$$0 = \alpha(5) + \alpha(9) + \alpha(1) - \alpha(3) - \alpha(7) - \alpha(11) = 288Y, \quad \text{if } T = 4.$$

(Note that $T \neq 2$ in this case, since 3 is quartic by hypothesis.)

Case 3. $V' = 0$, $Z = 4$.

From Tables 31 and 33,

$$0 = \alpha(1) - \alpha(7) = 96Y, \quad \text{if } T = 0,$$

and

$$0 = \alpha(3) + \alpha(7) + \alpha(11) - \alpha(1) - \alpha(5) - \alpha(9) = 192Y, \quad \text{if } T = 4.$$

Case 4. $V' = 0$, $Z = 6$.

From Tables 34–36,

$$0 = \alpha(3) - \alpha(9) = 96Y, \quad \text{if } T = 0,$$
$$0 = \alpha(1) + \alpha(8) - \alpha(4) - \alpha(5) = 48B, \quad \text{if } T = 2,$$

and

$$0 = \alpha(2) + \alpha(8) - \alpha(4) - \alpha(10) = 96B, \quad \text{if } T = 4.$$

Case 5. $V' = 1$, $Z = 2$.

From Tables 40 and 42,

$$0 = \alpha(1) - \alpha(7) = 96Y, \quad \text{if } T = 0,$$

and

$$0 = \alpha(1) + \alpha(5) + \alpha(9) - \alpha(3) - \alpha(7) - \alpha(11) = 96Y, \quad \text{if } T = 4.$$

Case 6. $V' = 1$, $Z = 6$.

From Tables 46–48,

$$0 = \alpha(1) - \alpha(5) = 48B, \quad \text{if } T = 0,$$
$$0 = \alpha(1) + \alpha(7) - \alpha(5) - \alpha(11) = 48B, \quad \text{if } T = 2,$$

and

$$0 = \alpha(4) - \alpha(8) = 48B, \quad \text{if } T = 4.$$

Case 7. $V' = 1, Z = 4$.

First suppose that $T = 4$. Then from Table 45, $14(\alpha(4) + \alpha(8)) + 5\alpha(0) = 33p - 879 - 306A$. By (1) or (1′), the left side above equals $33p - 825$ or $33p - 2121$, respectively. This yields a contradiction in either case.

Finally, suppose that $T = 0$. Then from Table 43, $0 = 2\alpha(7) + 2\alpha(5) + \alpha(2) + 5\alpha(8) - 5\alpha(4) - \alpha(10) - 4\alpha(3) = 288A + 72B$, so $B = -4A$ and $p = A^2 + 3B^2 = 49A^2$, which is absurd.

Case 8. $V' = 1, Z = 0, T \neq 0$.

From Tables 38 and 39,

$$0 = \alpha(2) + \alpha(7) - \alpha(10) - \alpha(11) = 144B, \quad \text{if } T = 2,$$

and

$$0 = \alpha(2) + \alpha(8) - \alpha(4) - \alpha(10) = 96B, \quad \text{if } T = 4.$$

Case 9. $V' = 1, Z = 0, T = 0$.

Assume for the moment that H is a difference set rather than a modified difference set. Then by (1),

$$p - 25 = \alpha(0) = \alpha(1) = \alpha(3). \tag{4}$$

From Table 37,

$$0 = \alpha(1) - \alpha(5) = 48B + 48D_4, \tag{5}$$

$$0 = \alpha(0) - \alpha(6) = 16A + 8C - 24, \tag{6}$$

and

$$0 = \alpha(2) - \alpha(4) = -16A - 8C - 24U. \tag{7}$$

By (12)–(14), we have

$$B = -D_4 \tag{8}$$

and

$$U = -1. \tag{9}$$

From (11), (13), (15), (16), and the formula for $\alpha(1)$ (in Table 37), we obtain

$$A = 13 \tag{10}$$

and

$$C = -23. \tag{11}$$

From (11), (18), and the formula for $\alpha(3)$,

$$X = 5. \tag{12}$$

From (11), (16), (17), (19), and the formula for $\alpha(0)$,

$$2D_0 + D_4 = 16. \tag{13}$$

Conversely, if equalities (8)–(13) hold, then H is a difference set; this follows easily from (1) and Table 37. We will see shortly that (8)–(13) cannot all hold. It is interesting to note, however, that (9)–(13) all hold for $p = 601$.

By arguing as above, we can show that H is a modified difference set if and only if the following equalities (8′)–(13′) all hold:

$$B = -D_4, \tag{8′}$$

$$U = 23, \tag{9′}$$

$$(10') \qquad A = -299,$$

$$(11') \qquad C = 529,$$

$$(12') \qquad X = -115,$$

$$(13') \qquad 2D_0 + D_4 = -368.$$

Unfortunately we do not see how to obtain contradictions from (8)–(13) or (8′)–(13′) directly from the properties of the Jacobi sums in Section 3. Instead, we obtain contradictions using the results of Section 4 and [3, Theorem 3.32], via the following technical lemma.

LEMMA. *Suppose that* $F_{24}(\gamma) = 0$. *Then for some* $\tau = \pm 1$ *and* $\nu = \pm 1$,

$$(14) \qquad 16(U + \sigma)(\sigma - C)(p + X\sigma) = s^2 - 4Apqr,$$

where

$$\sigma = \sqrt{p}, \quad R = \nu(2p - 2X\sigma)^{1/2}, \quad q = 2 + (\gamma - X)/\sigma + R(1 + \tau)/\sigma,$$

$$r = 2U - A + \gamma - 2\tau X + R(1 + \tau) + 2\sigma(2 + \tau) + (\gamma - U)R\tau/\sigma,$$

and

$$s = -4p + R(\gamma - 2\tau A + C + 2U) - \sigma(\gamma + 2A + X + 2C - 4U).$$

Proof. For brevity, write $G = G_3$. Define T as in [3, (3.37)]. By [3, Theorems 3.8 and 3.20], there exists a value of $\nu = \pm 1$ (specifying R) such that

$$(15) \qquad G_{12} = G + G^2/\sigma - \sigma + R + T.$$

In view of [3, Theorem 3.19], there exists a value of $\tau = \pm 1$ such that

$$(16) \qquad T = \tau GR/\sigma,$$

since $3 \nmid X$ by (12), (12′). Since f is odd by hypothesis, the expression $W = \pm(R_1 + R_5 + R_7 + R_{11})$ given in [3, p. 379] is purely imaginary. Thus, by (15), (16), and [3, Theorem 3.32], we have

$$(17) \qquad G_{24} = G + G^2/\sigma - \sigma + R + \tau GR/\sigma \pm i((2\sigma - 2C)(2\sigma - R))^{1/2} \pm i((2U + 2\sigma)(4\sigma + 2G + 2R - \tau GR/\sigma))^{1/2},$$

where the first five terms on the right of (17) are real and the last two terms are purely imaginary. By (2) and (17), we have, for real γ,

$$F_{24}(\gamma) = |G_{24} + \gamma|^2 - \gamma^2 - 23p,$$

so

$$(18) \qquad F_{24}(\gamma) = -23p - \gamma^2 + \left(G + G^2/\sigma - \sigma + R + \tau GR/\sigma + \gamma\right)^2 + (2\sigma - 2C)(2\sigma - R) + (2U + 2\sigma)(4\sigma + 2G + 2R - \tau RG/\sigma) \pm 4L,$$

where

$$(19) \qquad L^2 = (U + \sigma)(\sigma - C)(2\sigma - R)(4\sigma + 2G + 2R - \tau RG/\sigma).$$

From [3, Theorem 3.6], since 2 is cubic (mod p),

$$(20) \qquad G^3 = 3pG - 2Ap.$$

Expanding the right side of (18) and then using (20) to express G^3 and G^4 in terms of smaller powers of G, we see that

$$\begin{aligned}F_{24}(\gamma) \mp 4L = {} & -23p - \gamma^2 + G^2 + (3G^2 - 2AG) + p + (2p - 2X\sigma) \\ & + (2G^2 - 2G^2X/\sigma) + \gamma^2 + (6\sigma G - 4A\sigma) - 2\sigma G \\ & + 2GR + 2\tau G^2R/\sigma + 2G\gamma - 2G^2 + 2RG^2/\sigma \\ & + (6\tau RG - 4\tau AR) + 2\gamma G^2/\sigma - 2\sigma R - 2\tau RG \\ & - 2\sigma\gamma + (4\tau\sigma G - 4\tau XG) + 2\gamma R + 2\gamma\tau RG/\sigma \\ & + 4p - 4C\sigma - 2\sigma R + 2CR + 8U\sigma + 4UG + 4UR \\ & - 2\tau URG/\sigma + 8p + 4\sigma G + 4\sigma R - 2\tau RG.\end{aligned}$$

Since $F_{24}(\gamma) = 0$ by the hypothesis of the Lemma, it follows that

$$\pm 2L = qG^2 + rG + s. \tag{21}$$

Squaring the right side of (21) and then using (20) to simplify as before, we find that

$$4L^2 = G^2(r^2 + 2qs + 3pq^2) + G(6pqr + 2rs - 2Apq^2) + (s^2 - 4Apqr). \tag{22}$$

Now, the degrees of G and R over $\mathbf{Q}$ are 3 and 4, respectively, and it is consequently easy to see that G has degree 3 over $\mathbf{Q}(R)$. From (19), we can express the left side of (22) as a linear polynomial in G over $\mathbf{Q}(R)$ with constant term

$$16(U + \sigma)(\sigma - C)(p + X\sigma).$$

Since the constant term on the right side of (22) is $s^2 - 4Apqr$, the Lemma is proved.

Assume that H is a difference set, so that (8)–(13) hold. Then by (3), $F_{24}(-1) = 0$, so by the Lemma, (14) holds with $\gamma = -1$. Thus,

$$16(p^2 + 27p^{3/2} + 87p - 115p^{1/2}) = s^2 - 52pqr, \tag{23}$$

where q, r, s are given in the following table:

τ	q	r	s
-1	$2 - 6/\sigma$	$2\sigma - 6$	$12\sigma - 4p$
1	$2 - 6/\sigma + 2R/\sigma$	$-26 + 6\sigma + 2R$	$12\sigma - 4p - 52R$

If $\tau = -1$, the right side of (23) equals $16(p^2 - 19p^{3/2} + 87p - 117p^{1/2})$, which yields a contradiction. If $\tau = 1$, we can express the right side of (23) as a linear polynomial in R over $\mathbf{Q}(\sigma)$ and then compare coefficients of R in (23) to obtain the contradiction $0 = 416(5p^{1/2} - p)$.

Finally, assume that H is a modified difference set, so that (8′)–(13′) hold. Then by (3), $F_{24}(23) = 0$, so by the Lemma, (14) holds with $\gamma = 23$. Thus

$$16(p^2 - 621p^{3/2} + 46023p + 1399205p^{1/2}) = s^2 + 1196pqr, \tag{23'}$$

where q, r, s are given in the following table:

τ	q	r	s
-1	$2 + 138/\sigma$	$138 + \sigma$	$-4p - 276\sigma$
1	$2 + 138/\sigma + 2R/\sigma$	$598 + 6\sigma + 2R$	$-4p - 276\sigma + 1196R$

If $\tau = -1$, the right side of (23′) equals $16(p^2 + 437p^{3/2} + 46023p + 1423539p^{1/2})$, which yields a contradiction. If $\tau = 1$, comparison of coefficients of R in (23′) yields the contradiction $0 = 9568(p + 115p^{1/2})$.

Department of Mathematics
University of California at San Diego
La Jolla, California 92093

1. L. D. BAUMERT, *Cyclic Difference Sets*, Lecture Notes in Math., vol. 182, Springer-Verlag, Berlin, 1971.

2. L. D. BAUMERT & H. FREDERICKSEN, "The cyclotomic numbers of order eighteen with applications to difference sets," *Math. Comp.*, v. 21, 1967, pp. 204–219.

3. B. C. BERNDT & R. J. EVANS, "Sums of Gauss, Jacobi, and Jacobsthal," *J. Number Theory*, v. 11, 1979, pp. 349–398.

4. S. CHOWLA, "A property of biquadratic residues," *Proc. Nat. Acad. Sci. India Sect. A*, v. 14, 1944, pp. 45–46.

5. R. J. EVANS, "Bioctic Gauss sums and sixteenth power residue difference sets," *Acta Arith.*, v. 38, 1980, pp. 37–46.

6. R. J. EVANS, "Table of cyclotomic numbers of order twenty-four," *Math. Comp.*, v. 35, 1980, pp. 1036–1038; UMT file **12[9.10]**, 98 pp.

7. E. LEHMER, "On residue difference sets," *Canad. J. Math.*, v. 5, 1953, pp. 425–432.

8. H. B. MANN, *Addition Theorems*, Wiley, New York, 1965.

9. J. B. MUSKAT, "The cyclotomic numbers of order fourteen," *Acta Arith.*, v. 11, 1966, pp. 263–279.

10. J. B. MUSKAT & A. L. WHITEMAN, "The cyclotomic numbers of order twenty," *Acta Arith.*, v. 17, 1970, pp. 185–216.

11. T. STORER, *Cyclotomy and Difference Sets*, Markham, Chicago, Ill., 1967.

12. A. L. WHITEMAN, "The cyclotomic numbers of order sixteen," *Trans. Amer. Math. Soc.*, v. 86, 1957, pp. 401–413.

13. A. L. WHITEMAN, *The Cyclotomic Numbers of Order Ten*, Proc. Sympos. Appl. Math., vol. 10, Amer. Math. Soc., Providence, R.I., 1960, pp. 95–111.

14. A. L. WHITEMAN, "The cyclotomic numbers of order twelve," *Acta Arith.*, v. 6, 1960, pp. 53–76.