ACTA ARITHMETICA
LXXXIX.4 (1999)

Nonexistence of twentieth power residue difference sets

by

Ronald Evans (La Jolla, Cal.)

1. Introduction. Let $\mathbb{F}_p$ denote the field of p elements, where p is prime. A subset $H \subset \mathbb{F}_p$ is a *difference set* $(\mathrm{mod}\, p)$ if there is a fixed integer $\lambda > 0$ such that every element of $\mathbb{F}_p^*$ can be written as a difference of two elements of H in exactly λ ways.

Let $H_k = H_{k,p}$ denote the set of (nonzero) kth power residues $(\mathrm{mod}\, p)$, where $k > 1$ and p is a prime of the form $p = kf + 1$. If H_k is a difference set $(\mathrm{mod}\, p)$, it is called a kth *power residue difference set*. If $H_k \cup \{0\}$ is a difference set $(\mathrm{mod}\, p)$, it is called a *modified* kth *power residue difference set*.

By 1953, the kth power residue and modified kth power residue difference sets had been found for $k = 2$, 4, and 8 (see [3], [2, Chapter 5]). In the period 1953–1967, the combined work of seven authors showed the *non*existence of such difference sets for all other $k < 20$; see the book [1] or [2, Chapter 5] for references.

In 1970, Muskat and Whiteman [4] obtained partial results for the case $k = 20$ by showing that H_{20} and $H_{20} \cup \{0\}$ are never difference sets $(\mathrm{mod}\, p)$ when 5 is a quartic residue $(\mathrm{mod}\, p)$. Regarding the remaining case where 5 is a quartic nonresidue $(\mathrm{mod}\, p)$, they wrote: "Efforts to prove that there are no residue difference sets or modified residue difference sets... were unsuccessful." (See [4, p. 215].)

The purpose of this note is to complete the proof that H_{20} and $H_{20} \cup \{0\}$ are never difference sets $(\mathrm{mod}\, p)$. This solves Research Problem 11 in [2, p. 497]. (Research Problem 12, the analogous problem for $k = 24$, is still open.)

2. Strategy and notation. Let (i, j), $0 \le i, j \le 19$, denote the cyclotomic numbers of order 20 with respect to a fixed primitive root g $(\mathrm{mod}\, p)$, where $p = 20f + 1$. Assume for the purpose of contradiction that H_{20} or $H_{20} \cup \{0\}$ is a difference set $(\mathrm{mod}\, p)$. Then ([3], [4, p. 214]) f is odd, 5 is a

1991 *Mathematics Subject Classification*: Primary 05B10.

quartic nonresidue $(\mathrm{mod}\, p)$, and

$$1600(0,0) = 4p - 80 - 4\nu^2, \tag{1}$$

$$1600(i,0) = 4p - 76 + 8\nu, \quad 1 \le i \le 9, \tag{2}$$

where

$$\nu = \begin{cases} -1 & \text{if } H_{20} \text{ is a difference set,} \\ 19 & \text{if } H_{20} \cup \{0\} \text{ is a difference set.} \end{cases} \tag{3}$$

The cyclotomic numbers in (1) and (2) are expressed in the tables of [4] as linear combinations of $p, 1, c, d, x, u, v, w$, and d_j $(0 \le j \le 19)$, where these integral parameters are as defined in [4]. In particular (see [4, eqs. (4.14), (4.1), (2.18), (2.17)]),

$$p = c^2 + 5d^2, \tag{4}$$

$$16p = x^2 + 125w^2 + 50u^2 + 50v^2, \tag{5}$$

$$x \equiv 1 \ (\mathrm{mod}\, 5), \tag{6}$$

$$xw = v^2 - u^2 - 4uv, \tag{7}$$

$$p = \Big| \sum_{j=0}^{9} d_j \zeta^j \Big|^2, \quad \text{where } \zeta = \exp(2\pi i/20), \tag{8}$$

and

$$d_j = -d_{j-10} \quad \text{for } 10 \le j \le 19. \tag{9}$$

If we formally expand

$$\sum_{j=0}^{9} d_j \zeta^j \sum_{j=0}^{9} d_{9-j} \zeta^j \ - \ p\zeta^9, \tag{10}$$

and then make the substitutions

$$\zeta^k = -\zeta^{k-10} \quad (10 \le k \le 18),$$
$$\zeta^9 = \zeta^7 - \zeta^5 + \zeta^3 - \zeta, \quad \zeta^8 = \zeta^6 - \zeta^4 + \zeta^2 - 1,$$

we obtain the sum

$$\sum_{r=0}^{7} G_r \zeta^r, \tag{11}$$

where

$$G_0 = -2 \sum_{j=0}^{9} d_j d_{j+1}, \tag{12}$$

$$G_1 = p - \sum_{j=0}^{9} d_j^2 - \sum_{j=0}^{9} d_j d_{j+2}, \tag{13}$$

$$G_2 = \sum_{j=0}^{9} d_j d_{j+1} - \sum_{j=0}^{9} d_j d_{j+3}, \tag{14}$$

$$G_3 = \sum_{j=0}^{9} d_j^2 - p - \sum_{j=0}^{9} d_j d_{j+4}, \tag{15}$$

$G_4 = G_0/2$, $G_5 = -G_3$, $G_6 = -G_2 - G_0$, and $G_7 = -G_1$. By (8), the sums in (10) and (11) vanish, and thus

$$G_0 = G_1 = G_2 = G_3 = 0, \tag{16}$$

since $\{1, \zeta, \zeta^2, \ldots, \zeta^7\}$ is a basis for $\mathbb{Q}(\zeta)$ over $\mathbb{Q}$.

Our strategy is to obtain the desired contradiction by showing that (2) is inconsistent with (4)–(7) and (16). As was pointed out in [4, p. 215], we need to consider just two cases. The first case is

$$\mathrm{ind}_g 2 \equiv 5 \pmod{10}, \quad c \equiv 6 \pmod{10} \tag{17}$$

and the second case is

$$\mathrm{ind}_g 2 \equiv 1 \pmod{10}, \quad c \equiv 6 \pmod{10}. \tag{18}$$

These cases are discussed in Sections 3 and 4, respectively.

3. The case $\mathrm{ind}_g 2 \equiv 5 \pmod{10}$**,** $c \equiv 6 \pmod{10}$**.** View the last nine rows of Table 4 in [4, pp. 212–213] as a system of nine linear equations in the nine variables $d_0, d_4, d_8, d_{12}, d_{16}, d_1, d_5, d_9$, and d_{13}. Replace each $1600(i, 0)$ in this system by $4p - 76 + 8\nu$ (see (2)). Using *Maple* to solve this system, we obtain expressions for the nine variables as linear combinations of $\nu, c, d, x, w, u, v, d_{17}$ over $\mathbb{Q}$. For example, $d_0 = -3(x + \nu)/5$. Then from (12)–(15), each of G_0, G_1, G_2, and G_3 can be written as a quadratic polynomial in p, ν, c, d, x, w, u, v over $\mathbb{Q}$ (d_{17} does not appear). These polynomials are rather cumbersome (e.g., G_1 and G_3 each have 18 terms) and so we do not write them explicitly here. A *Maple* program which produces these polynomials is currently available upon request.

Reducing (2) and (5) (mod 25), and using (6), we deduce that

$$x \equiv 5 - \nu \pmod{25}. \tag{19}$$

Also, by (3) and (17),

$$5\nu \equiv -5 \pmod{25}, \quad 5c \equiv 5 \pmod{25}. \tag{20}$$

We cannot have $u = v = 0$, in view of (5) and (7). Hence one can define

$$u_0 = u/\gcd(u, v), \quad v_0 = v/\gcd(u, v). \tag{21}$$

Dividing the equality $0 = G_0 - G_2$ by $\gcd(u, v)$ and then reducing mod 25, we obtain

$$0 \equiv 18xu_0 + xv_0 + 5cu_0 + 10cv_0 + 3\nu u_0 + 21\nu v_0 \pmod{25}.$$

Substituting in the value of x given by (19), and then making the substitutions for 5ν and $5c$ given by (20), we obtain

$$0 \equiv 10u_0 - 5v_0 \pmod{25}. \tag{22}$$

Reduction of the equality $0 = G_1 + G_3$ modulo 25 yields, after the substitution of x from (19),

$$0 \equiv 20\nu w + 10cw + 5d + 20uv + 20v^2 + 5u^2 \pmod{25}.$$

After substitutions from (20) and (22), this becomes

$$0 \equiv 5d - 10w \pmod{25}. \tag{23}$$

From (7) and (22), we see that $5 \mid xw$, so that by (6), $5 \mid w$. Thus by (23),

$$d \equiv w \equiv 0 \pmod{5}. \tag{24}$$

Dividing the equality $0 = G_0 + G_2$ by $\gcd(u, v)$ and then reducing mod 25, we obtain, after the substitution of x from (19),

$$0 \equiv 20u_0 + 10\nu u_0 + 5cu_0 + 20du_0 + 15dv_0 + 15v_0 \pmod{25}.$$

After substitutions from (20), (22), and (24), this becomes

$$0 \equiv 20u_0 \pmod{25}.$$

Then $5 \mid u_0$, which contradicts (22), because $\gcd(u_0, v_0) = 1$ by (21). This completes the proof that H_{20} and $H_{20} \cup \{0\}$ are never difference sets in the case (17).

4. The case $\operatorname{ind}_g 2 \equiv 1 \pmod{10}$**,** $c \equiv 6 \pmod{10}$**.** We express G_0, G_1, G_2 and G_3 as quadratic polynomials just as in Section 3, except that instead of using the last nine rows of Table 4, we use rows 21, 22, 38, 40, 52, 55, 63, 67, 71 of Table 1 in [4, pp. 204–207]. The polynomials are more complicated than those in Section 3; for example, G_3 has 28 terms instead of 18.

Since f is odd, $p \equiv 5 \pmod{8}$. Since c is even by (18), and $p = c^2 + 5d^2$ by (4), it follows that $4 \mid c$. Write

$$c = 4c_2, \tag{25}$$

where c_2, as well as each parameter introduced below, is integral. Since ν is -1 or 19 by (3), write

$$\nu = -1 + 4\nu_2. \tag{26}$$

By (2),

$$p = 19 - 2\nu + 16p_4. \tag{27}$$

From [2, Theorem 3.7.9, p. 135], we can write

$$x = 1 + 2x_1, \tag{28}$$

$$u = 2u_1, \tag{29}$$

$$v = x + u + 4s_2. \tag{30}$$

Further, from [2, eq. (3.7.46), p. 135],

$$w = x - 2u + 8t_3. \tag{31}$$

Write

$$E := -xw + v^2 - u^2 - 4uv, \tag{32}$$

so that $E = 0$ by (7).

From $E/8 \equiv 0 \pmod 2$, we see that $t_3 + s_2$ is even. From $4G_1 \equiv 0 \pmod 2$, we see that $1 + u_1 + s_2$ is even. Thus

$$s_2 = 1 + u_1 + 2s_3, \tag{33}$$

$$t_3 = 1 + u_1 + 2t_4. \tag{34}$$

We now consider separately the two cases $d \equiv \pm 1 \pmod 4$.

Case 1: $d \equiv -1 \pmod 4$. In this case, write

$$d = -1 + 4d_2. \tag{35}$$

From $E/16 \equiv 0 \pmod 2$, we see that $1 + s_3 + t_4$ is even. From $G_0/2 \equiv 0 \pmod 2$, we see that $x_1 s_3 + u_1 + t_4$ is even. From $G_1 \equiv 0 \pmod 2$, $x_1 s_3 + u_1$ is even, so that t_4 is even and s_3 is odd. From $G_2 \equiv 0 \pmod 2$, $x_1 u_1 + x_1$ is even. From $G_3 \equiv 0 \pmod 2$, $x_1 u_1 + x_1 + u_1$ is even. Combining these five results, we can write

$$t_4 = 2t_5, \tag{36}$$

$$s_3 = 1 + 2s_4, \tag{37}$$

$$u_1 = 2u_2, \tag{38}$$

$$x_1 = 2x_2. \tag{39}$$

From these formulas we arrive at

$$G_1/2 + G_2/2 + E/32 \equiv 1 \pmod 2, \tag{40}$$

which is a contradiction, since $G_1 = G_2 = E = 0$.

Case 2: $d \equiv 1 \pmod 4$. In this case, $d \equiv -\nu \pmod 8$, since by (7), (25), and (27), $19 - 2\nu \equiv p \equiv 5d^2 \pmod{16}$. Thus write

$$d = -\nu + 8d_3. \tag{41}$$

From $E/16 \equiv 0 \pmod 2$, we see that $1 + s_3 + t_4$ is even. From $G_0/2 \equiv 0 \pmod 2$, $x_1 s_3$ is even. From $G_1 \equiv 0 \pmod 2$, u_1 is even. From $G_2 \equiv 0 \pmod 2$, $1 + x_1 t_4$ is even. From $G_3 \equiv 0 \pmod 2$, $x_1 + x_1 t_4$ is even. Combining these five results, we can write

$$t_4 = 1 + 2t_5, \tag{42}$$

$$s_3 = 2s_4, \tag{43}$$

$$u_1 = 2u_2, \tag{44}$$

$$x_1 = 2x_2 + 1. \tag{45}$$

From $E/32 \equiv 0 \pmod 2$, $1+u_2+t_5+s_4$ is even. From $G_0/4 \equiv 0 \pmod 2$, $s_4 + \nu_2$ is even. From $G_1/2 \equiv 0 \pmod 2$, $\nu_2 + u_2 + x_2 + t_5 + s_4$ is even. Combining these three results, we can write

$$s_4 = -\nu_2 + 2s_5, \tag{46}$$

$$x_2 = 1 - \nu_2 + 2x_3, \tag{47}$$

$$t_5 = 1 - \nu_2 + u_2 + 2t_6. \tag{48}$$

From these formulas, we arrive at

$$G_0/8 + G_1/4 + G_3/4 \equiv 1 \pmod 2, \tag{49}$$

which is a contradiction, since $G_0 = G_1 = G_3 = 0$.

The contradictions obtained in Cases 1 and 2 complete the proof that H_{20} and $H_{20} \cup \{0\}$ are never difference sets in the case (18).

References

[1] L. D. Baumert, *Cyclic Difference Sets*, Lecture Notes in Math. 182, Springer, Berlin, 1971.

[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, New York, 1998.

[3] E. Lehmer, *On residue difference sets*, Canad. J. Math. 5 (1953), 425–432.

[4] J. B. Muskat and A. L. Whiteman, *The cyclotomic numbers of order twenty*, Acta Arith. 17 (1970), 185–216.

Department of Mathematics
University of California, San Diego
La Jolla, California 92093-0112
U.S.A.
E-mail: revans@ucsd.edu

Received on 20.11.1998 (3521)