Table des matières du tome XI, fascicule 3

La revue est consacrée à toutes les branches de l'arithmétique et de la théorie des nombres, ainsi qu'aux fonctions ayant de l'importance dans ces domaines.

Prière d'adresser les textes dactylographiés à l'un des redacteurs de la revue ou bien à la Rédaction de

ACTA ARITHMETICA

Warszawa 1 (Pologne), ul. Śniadeckich 8.

La même adresse est valable pour toute correspondance concernant l'échange de Acta Arithmetica.

Les volumes IV et suivants de ACTA ARITHMETICA sont à obtenir chez

Ars Polona, Warszawa 5 (Pologne), Krakowskie Przedmieście 7.

Prix de ce fascicule 3.00 $.

Les volumes I-III (reédits) sont à obtenir chez

Johnson Reprint Corp., 111 Fifth Ave., New York, N. Y.

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XI (1966)

The cyclotomic numbers of order fourteen*

by

J. B. MUSKAT (Pittsburgh, Pa.)

1. Introduction. Let e be an integer greater than 1. A central problem in the theory of cyclotomy is to determine, for each prime $p = ef+1$, the number of solutions $(h, k) = (h, k)_e$ of the congruence

$$g^{es+h}+1 \equiv g^{ei+k} (\mathrm{mod}\, p),$$

$0 \leqslant h, k \leqslant e-1$, $0 \leqslant s, t \leqslant f-1$, where g is a fixed primitive root $(\mathrm{mod}\, p)$. The numbers (h, k) are called *cyclotomic numbers*.

Complete solutions have been given for $e = 2, 3, 4, 5$, and 6 by Dickson [1], for $e = 8$ by Lehmer [4], and for $e = 10$ and 12 by Whiteman [7], [8]. In a complete solution, the cyclotomic numbers are represented as linear combinations of the coefficients

$$B(i, v) = B_e(i, v) = \sum_{j=0}^{e-1} (j, i-vj)_e \tag{1.1}$$

of Jacobi sums of order e. Then the $B(i, v)$, in turn, can be expressed as linear combinations of the coordinates x_n of certain quadratic forms

$$ep = \sum_n a_n x_n^2.$$

If the x_n are known, then the cyclotomic numbers can be computed.

Dickson proved that it is possible to represent the $(h, k)_e$ as linear combinations of the $B_e(i, v)$ if e is an odd prime or twice an odd prime ([2], Theorem 5 and Section 12). Whiteman gave the representations explicitly in both cases ([7], Theorems 1, 3). He went on to obtain a complete solution for $e = 10$ by first expressing the $B_{10}(i, v)$ linearly in terms of the $B_5(i, v)$ ([2], Section 10), and then representing the $B_5(i, v)$ in terms of x, u, v, and w in

$$16p = x^2+50u^2+50v^2+125w^2,$$

* This research was sponsored in part by the National Science Foundation, under Research Grants G 11309 and GP-2091.

where

$$x \equiv 1 (\mathrm{mod}\, 5), \qquad xw = v^2 - 4uv - u^2.$$

In this paper Whiteman's explicit representation of $(h, k)_e$ in terms of the $B_e(i, v)$, where e is twice an odd prime, is transformed into a more compact form (Theorem 2). Dickson's result that, given the septic character of 2, the $B_{14}(i, v)$ can be given as linear combinations of the $B_7(i, v)$ ([2], Section 10) is then employed to express the $(h, k)_{14}$ in terms of the $B_7(i, v)$.

The $B_7(i, v)$ can be represented in terms of the coordinates of

$$p = T^2 + 7U^2 \qquad ([2], (75))$$

and

$$72p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2) \qquad ([2], (33)).$$

The latter was not introduced, as it was not needed in applying the representations obtained to show that the fourteenth power residues (mod p), with or without zero, cannot form a residue difference set.

Finally, these results cannot be extended to $e = 22$, for not all the $B_{22}(i, v)$ are linear combinations of the $B_{11}(i, v)$ ([2], Section 10).

2. Cyclotomy. In this section some information from the theory of cyclotomy is assembled. Proofs in papers of Dickson and Whiteman are cited.

From ([1], p. 394)

$$(h, k) = (e - h, k - h), \tag{2.1}$$

$$(h, k) = \begin{cases} (k, h) & \text{if } f \text{ is even,} \\ (k + \tfrac{1}{2}e, h + \tfrac{1}{2}e) & \text{if } f \text{ is odd,} \end{cases} \tag{2.2}$$

$$\sum_{k=0}^{e-1} (h, k) = \begin{cases} f-1 & \text{if } f \text{ is even and } h \equiv 0 (\mathrm{mod}\, e), \\ f-1 & \text{if } f \text{ is odd and } h \equiv \tfrac{1}{2}e (\mathrm{mod}\, e), \\ f & \text{otherwise.} \end{cases} \tag{2.3}$$

An immediate consequence is

$$\sum_{h=0}^{e-1} (h, k) = \begin{cases} f-1 & \text{if } k \equiv 0 (\mathrm{mod}\, e), \\ f & \text{otherwise.} \end{cases} \tag{2.4}$$

$$\sum_{i=0}^{e-1} B(i, v) = p - 2 \tag{2.5}$$

follows from (1.1) and (2.3). By (1.1) and (2.4),

$$B(i, 0) = \begin{cases} f-1 & \text{if } i \equiv 0 (\mathrm{mod}\, e), \\ f & \text{otherwise.} \end{cases} \tag{2.6}$$

By (2.1), $(j, i - vj) = (e - j, i - vj - j) = \big(e - j, i - (e - j)(e - v - 1)\big)$, so by (1.1),

$$B(i, v) = B(i, e - v - 1). \tag{2.7}$$

Let $\beta = \exp(2\pi i/e)$, $\xi = \exp(2\pi i/p)$. Let χ denote the primitive eth power character (mod p) such that $\chi(g) = \beta$. Define the Jacobi sum

$$\pi(\chi^a, \chi^b) = \sum_{n=2}^{p-1} \chi^a(n) \chi^b(1 - n).$$

It follows from the definition that

$$\pi(\chi^a, \chi^b) = \pi(\chi^b, \chi^a) = (-1)^{bf} \pi(\chi^{-a-b}, \chi^b). \tag{2.8}$$

$$\pi(\chi^{vm}, \chi^n) = (-1)^{vfm} \sum_{i=0}^{e-1} B(i, v) \beta^{ni} \qquad ([5], (2.6)).$$

Define the Gaussian sum (or Lagrange resolvent)

$$\tau(\chi^t) = \sum_{n=1}^{p-1} \chi(n)^t \xi^n.$$

If none of a, b and $a+b$ are divisible by e,

$$\pi(\chi^a, \chi^b) = \tau(\chi^a)\tau(\chi^b)/\tau(\chi^{a+b}),$$

and

$$|\pi(\chi^a, \chi^b)|^2 = p \qquad ([1], \text{p. } 396). \tag{2.9}$$

If $\bar{v}$ satisfies $v\bar{v} \equiv 1 (\mathrm{mod}\, e)$, then

$$B(i, v) = B(\bar{v}i, \bar{v}) \qquad ([7], \text{p. } 97). \tag{2.10}$$

If $e = 2E$, let $D(i, v) = B(i, v) - B(i + E, v)$. If E is odd,

$$\sum_{i=0}^{E-1} D(2i, v) = -1 \qquad ([7], \text{p. } 103). \tag{2.11}$$

3. Cyclotomy where e is twice an odd prime. Let $e = 2E$, E an odd prime. Let $p = ef + 1 = EF + 1$. Define

$$q(n, m) = \begin{cases} 1 & \text{if } m | n, \\ 0 & \text{if } m \nmid n. \end{cases}$$

It is convenient to begin by deriving the representation of $(h, k)_E$ in terms of $B_E(i, v)$. This is equivalent to Theorem 1 of [7].

THEOREM 1.

$$E(h,k)_E = \sum_{v=1}^{E-2} B_E(k+hv,v) - (E-3)F + 1 - q(h,E) - q(k,E) - q(h-k,E).$$

Proof. By (1.1),

$$\sum_{v=1}^{E-2} B_E(k+hv,v)$$

$$= \sum_{v=1}^{E-2}\sum_{j=0}^{E-1} (j, k+hv-vj)_E$$

$$= \sum_{j=0}^{E-1}\left[-(j,k)_E - (j,k-(h-j))_E + \sum_{v=0}^{E-1}(j,k+v(h-j))_E\right]$$

$$= -\sum_{j=0}^{E-1}[(j,k)_E + (E-j,k-h)_E] + \sum_{v=0}^{E-1}(h,k)_E + \sum_{\substack{j=0\\ j\neq h}}^{E-1}\sum_{v=0}^{E-1}(j,k+v(h-j))_E,$$

by (2.1),

$$= -F + q(k,E) - F + q(k-h,E) + E(h,k)_E + (E-1)F + q(h,E) - 1,$$

by (2.3) and (2.4),

$$= E(h,k)_E + (E-3)F + q(h,E) + q(k,E) + q(h-k,E) - 1. \qquad \text{q. e. d.}$$

For $e = 2E$, $(h,k)_e$ can be represented as follows:

THEOREM 2. *Let* $D(i,v) = B_e(i,v) - B_e(i+E,v)$. *Then*

$$4E(h,k)_e = \sum_{v=1}^{E-2} B_E(k+hv,v) - 2f(E-3) + 1 + (-1)^k + (-1)^{h+f} + (-1)^{h-k} +$$
$$+ (-1)^{h-k}D(-h,E) + (-1)^h D(k,E) + (-1)^{h+k+f}D(-k,E) +$$
$$+ \sum_{v=1}^{E-1}\left[D(k+2hv,2v) + (-1)^f D(h+2kv,2v) + D(h-k-2kv,2v)\right] -$$
$$- 2q(k,e) - (1+(-1)^{h+f})q(h,E) - 2q(h-k,e).$$

Proof. Set $s(h,k) = (h,k)_e - (h,k+E)_e$, $t(h,k) = (h,k)_e - (h+E,k)_e$. By rearranging the identity

$$(h,k)_E = (h,k)_e + (h+E,k)_e + (h,k+E)_e + (h+E,k+E)_e,$$

Whiteman showed that

(3.1) $\quad 4(h,k)_e = (h,k)_E + s(h,k) + s(h+E,k) + 2t(h,k)$ ([6], (2.14)).

He proved that

$$E[s(h,k) + s(h+E,k)] = (-1)^k + (-1)^{h+k}D(-h,E) + \sum_{v=0}^{E-1} D(k+2hv,2v),$$

and that

(3.2) $\quad 2Et(h,k)$

$$= \begin{cases} (-1)^h D(k,E) + (-1)^{h+k}D(-k,E) + (-1)^h[1+(-1)^k] + \\ \qquad + \sum_{v=0}^{e-1} D(h+kv,v) & \text{if } f \text{ is even;} \\ (-1)^{h+E}D(k+E,E) + (-1)^{h+k}D(-k+E,E) - (-1)^h[1-(-1)^k] + \\ \qquad + \sum_{v=0}^{e-1} D(h+E+(k+E)v,v) & \text{if } f \text{ is odd} \end{cases}$$

([7], pp. 102-104).

In the summations of (3.2), collect the terms with v even, and group the terms with v odd. Then for f odd or even,

(3.3) $\quad 2Et(h,k) = (-1)^h D(k,E) + (-1)^{h+k+f}D(-k,E) + (-1)^{h+f} +$

$$+ (-1)^{h+k} + (-1)^f \sum_{v=0}^{E-1} D(h+2kv,2v) + \sum_{v=0}^{E-1} D(h+k(2v+1),2v+1).$$

Applying (2.7) to the second summation of (3.3) yields

$$(3.4) \quad \sum_{u=0}^{E-1} D(h+k(2u+1),2u+1) = \sum_{u=0}^{E-1} D(h+k(2u+1),e-2u-2)$$
$$= \sum_{v=0}^{E-1} D(h-k-2kv,2v).$$

Combining Theorem 1 with (3.1)-(3.4) gives

$$4E(h,k)_e = \sum_{v=1}^{E-2} B_E(k+hv,v) - (E-3)2f + 1 -$$
$$- q(h,E) - q(k,E) - q(h-k,E) + (-1)^k + (-1)^{h+f} +$$
$$+ (-1)^{h-k} + (-1)^{h-k}D(-h,E) + (-1)^h D(k,E) + (-1)^{h+k+f}D(-k,E) +$$
$$+ \sum_{v=0}^{E-1}[D(k+2hv,2v) + (-1)^f D(h+2kv,2v) + D(h-k-2kv,2v)].$$

It follows from (2.6) that

$$\sum_{v=0}^{E-1} D(k+2hv, 2v)-q(k, E) = \sum_{v=1}^{E-1} D(k+2hv, 2v)-(-1)^k q(k, E)-q(k, E)$$
$$= \sum_{v=1}^{E-1} D(k+2hv, 2v)-2q(k, e).$$

Similarly,

$$(-1)^f \sum_{v=0}^{E-1} D(h+2kv, 2v)-q(h, E) = \sum_{v=1}^{E-1} D(h+2kv, 2v)-\left(1+(-1)^{h+f}\right)q(h, E),$$

and

$$\sum_{v=0}^{E-1} D(h-k-2kv, 2v)-q(h-k, E) = \sum_{v=1}^{E-1} D(h-k-2kv, 2v)-2q(h-k, e),$$

and the theorem follows.

Let

$$H = \begin{cases} h & \text{if } h \text{ is even,} \\ h+E & \text{if } h \text{ is odd,} \end{cases} \qquad K = \begin{cases} k & \text{if } k \text{ is even,} \\ k+E & \text{if } k \text{ is odd.} \end{cases}$$

Then, by (2.7), Theorem 2 can be expressed in the following form:

(3.5) $$2e(h, k)_e = \sum_{v=1}^{E-2} B_E(k+hv, v)-2f(E-3)+1-$$

$$-2q(k, e)+(-1)^k\left[1+D(-H, E-1)+\sum_{v=1}^{E-1} D(K+2Hv, 2v)\right]-$$

$$-\left(1+(-1)^{h+f}\right)q(h, E)+(-1)^{h+f}\left[1+D(-K, E-1)+\sum_{v=1}^{E-1} D(H+2Kv, 2v)\right]$$

$$-2q(h-k, e)+(-1)^{h-k}\left[1+D(K, E-1)+\sum_{v=1}^{E-1} D(H-K-2Kv, 2v)\right].$$

4. Cyclotomy for $e = 14$. Let $\varphi = \chi^2$. Let $\psi(\varphi^r, \varphi^s)$ denote a Jacobi sum of order 7. Let $\zeta_7 = \exp(2\pi i/7)$. Let $\varphi(2) = \zeta_7^m$.

Because of (3.5), it suffices to show for $e = 14$ that just the $D(i, v)$ having both i and v even can be represented in terms of the $B_7(i, v)$.

THEOREM 3.

$$D(2i, 2) = B_7(i-2m, 1)-2f,$$
$$D(2i, 4) = B_7(4i-2m, 1)-2f,$$
$$D(2i, 6) = B_7(5i-2m, 1)-2f,$$
$$D(2i, 8) = B_7(i-m, 1)-2f,$$
$$D(2i, 10) = B_7(5i-m, 1)-2f,$$
$$D(2i, 12) = B_7(5i-4m, 1)-2f.$$

Proof. Starting from the Gaussian sum identity

$$\tau(\chi^E)\tau(\chi^{2t}) = \chi^{2t}(2)\tau(\chi^t)\tau(\chi^{E+t})$$

(for a proof, see [1], p. 407), Dickson obtained four new relations between Jacobi sums for $e = 14$ ([2], pp. 372, 373):

(4.1) $$\pi(\chi, \chi^6) = (-1)^f\chi^6(2)\pi(\chi, \chi^3),$$

(4.2) $$\pi(\chi, \chi^6) = (-1)^f\chi^2(2)\pi(\chi, \chi),$$

(4.3) $$\pi(\chi^2, \chi^6) = \chi^2(2)\pi(\chi, \chi^6),$$

(4.4) $$\pi(\chi, \chi^2) = \chi^4(2)\pi(\chi^2, \chi^3).$$

By (2.8),

(4.5) $$\pi(\chi^2, \chi^6) = \pi(\chi^6, \chi^6) = \psi(\varphi^3, \varphi^3). \quad \text{Also} \quad \pi(\chi^2, \chi^2) = \psi(\varphi, \varphi).$$

Then, by using (2.8) in conjunction with formulas (4.1) to (4.5), one may express the six Jacobi sums of order 14, $\pi(\chi, \chi^{2t})$, $1 \leqslant t \leqslant 6$, in terms of $\psi(\varphi^r, \varphi^r)$:

(4.6) $$\pi(\chi, \chi^2) = \varphi^2(2)\psi(\varphi, \varphi),$$

(4.7) $$\pi(\chi, \chi^4) = \varphi^4(2)\psi(\varphi^2, \varphi^2),$$

(4.8) $$\pi(\chi, \chi^6) = \varphi^6(2)\psi(\varphi^3, \varphi^3),$$

(4.9) $$\pi(\chi, \chi^8) = \varphi(2)\psi(\varphi, \varphi),$$

(4.10) $$\pi(\chi, \chi^{10}) = \varphi^3(2)\psi(\varphi^3, \varphi^3),$$

(4.11) $$\pi(\chi, \chi^{12}) = \varphi^5(2)\psi(\varphi^3, \varphi^3).$$

Proof of (4.7):

$$\pi(\chi, \chi^4) = (-1)^f\pi(\chi, \chi^9), \qquad \text{by (2.8),}$$
$$= (-1)^f\pi(\chi^{9\cdot 11}, \chi^9) = \pi(\chi^{9\cdot 2}, \chi^9) = \varphi^4(2)\psi(\varphi^2, \varphi^2), \qquad \text{by (4.6).}$$

Now

$$\pi(\chi, \chi^2) = \sum_{i=0}^{6} D(2i, 2)\zeta_7^i = \varphi^2(2)\sum_{i=0}^{6} B_7(i, 1)\zeta_7^i$$
$$= \sum_{i=0}^{6} B_7(i, 1)\zeta_7^{i+2m} = \sum_{i=0}^{6} B_7(i-2m, 1)\zeta_7^i.$$

$$\sum_{i=1}^{6} [D(2i, 2)-D(0, 2)]\zeta_7^i = \sum_{i=1}^{6} [B_7(i-2m, 1)-B_7(-2m, 1)]\zeta_7^i.$$

Equating coefficients yields

(4.12) $$D(2i, 2)-D(0, 2) = B_7(i-2m, 1)-B_7(-2m, 1), \quad 1 \leqslant i \leqslant 6.$$

Sum (4.12) over $i = 0, 1, \ldots, 6$ and apply (2.5) and (2.11):

$$-1-7D(0,2) = p-2-7B_7(-2m,1),$$

$$-D(0,2) = 2f-B_7(-2m,1). \tag{4.13}$$

Subtracting (4.13) from (4.12) yields

$$D(2i,2) = B_7(i-2m,1)-2f.$$

From (4.7),

$$\pi(\chi,\chi^4) = \sum_{i=0}^{6} D(2i,4)\zeta_7^i = \sum_{i=1}^{6}[D(2i,4)-D(0,4)]\zeta_7^i$$

$$= \sum_{i=0}^{6} B_7(i,1)\zeta_7^{2i+4m} = \sum_{i=0}^{6} B_7(4i-2m,1)\zeta_7^i$$

$$= \sum_{i=1}^{6}[B_7(4i-2m,1)-B_7(-2m,1)]\zeta_7^i.$$

Equating coefficients yields

$$D(2i,4)-D(0,4) = B_7(4i-2m,1)-B_7(-2m,1),$$

$$-D(0,4) = 2f-B_7(-2m,1).$$

The proof is similar to that of (4.13). Hence

$$D(2i,4) = B_7(4i-2m,1)-2f.$$

By similar arguments one can prove the other four statements of Theorem 3. q. e. d.

5. Tables of cyclotomic numbers of order 14. One can obtain representations of the cyclotomic numbers $(h,k)_{14}$ in terms of the coefficients of Jacobi sums of order 7 by substituting the formulas of Theorem 3 into (3.5).

By (2.7), $B_7(j,5) = B_7(j,1)$, and $B_7(j,4) = B_7(j,2)$. By (2.10), $B_7(j,3) = B_7(5j,1)$.

If $7|m$, let $M = 1$; if $7\nmid m$, let $M = m$. The $B_7(j,2)$ satisfy

$$B_7(M,2) = B_7(2M,2) = B_7(4M,2) = 2f+\tfrac{1}{7}(T-1)+U,$$

$$B_7(3M,2) = B_7(5M,2) = B_7(6M,2) = 2f+\tfrac{1}{7}(T-1)-U,$$

$$B_7(0,2) = 2f-\tfrac{1}{7}(6T+1),$$

where $T^2+7U^2 = p$, $T \equiv 1 \pmod 7$, and the sign of U is determined by $2U = B_7(M,2)-B_7(3M,2)$. This follows from ([2], (75)) upon verifying that $B_7(1,2)-B_7(3,2)$ is even.

Thus the $(h,k)_{14}$ can be represented as linear combinations of f, 1, T, U, and $B_7(j,1)$, $j = 0, 1, \ldots, 6$. Since

$$\sum_{j=0}^{6} B_7(j,1) = 14f-1,$$

there is one dependent variable; this relation will be used to eliminate $B_7(0,1)$.

There are 196 of the $(h,k)_{14}$, but they may be grouped into forty distinct cases by applying (2.1) and (2.2). The tables will consist of one entry for each of the forty distinct cases. One must also distinguish between f even or odd, and the residue classes (mod 7) of $m = \operatorname{ind} 2$. In order that the tables contain no fractions, the values of 196 $(h,k)_{14}$ will be given.

For $\operatorname{ind} 2 \equiv 0 \pmod 7$, the formulas of Theorem 3 become

$$D(2i,2) = D(2i,8) = B_7(i,1)-2f,$$

$$D(2i,4) = B_7(4i,1)-2f,$$

$$D(2i,6) = D(2i,10) = D(2i,12) = B_7(5i,1)-2f.$$

The formulas for the cyclotomic numbers are given in Tables 1 and 2 (pp. 275 and 276).

For $\operatorname{ind} 2 \not\equiv 0 \pmod 7$, in order to avoid considering six separate cases each for f even and odd, one may take the following approach: Define $M \equiv \operatorname{ind} 2 \pmod{14}$ and M is odd. In equation (3.5) replace h, k, H, and K by hM, kM, HM, and KM, respectively; set $e = 14$. In Theorem 3 replace i by tM, yielding, for example,

$$D(2tM,2) = B_7\big((t-2)M,1\big)-2f,$$

$$D(2tM,4) = B_7\big((4t-2)M,1\big)-2f.$$

The formulas for $(hM,kM)_{14}$, $M \not\equiv 7 \pmod{14}$, are given in Tables 3 and 4 (pp. 277 and 278).

In each table there are, in fact, less than forty distinct cases. This phenomenon has been observed with other even values of e.

If $7|\operatorname{ind} 2$ and f is even, $(1,2) = (2,8)$, $(1,4) = (1,11)$, $(1,6) = (1,9)$, $(2,4) = (4,9)$, $(2,5) = (2,11)$, $(3,6) = (4,8)$.

If $7|\operatorname{ind} 2$ and f is odd, $(1,2) = (1,13)$, $(1,4) = (1,11)$, $(1,6) = (2,1)$, $(2,4) = (2,12)$, $(2,5) = (4,2)$, $(3,4) = (4,1)$.

If $7\nmid\operatorname{ind} 2$ and f is even, $(0,2M) = (0,9M)$, $(0,6M) = (0,13M)$, $(M,3M) = (M,10M)$, $(M,4M) = (4M,8M)$, $(M,9M) = (4M,9M)$, $(M,11M) = (3M,6M)$, $(2M,6M) = (3M,8M)$.

If $7\nmid \mathrm{ind}\,2$ and f is odd, $(0,2M)=(0,9M)$, $(0,3M)=(0,6M)=(0,13M)$, $(M,3M)=(M,10M)$, $(M,4M)=(3M,4M)$, $(M,6M)=(4M,2M)$, $(M,11M)=(4M,M)$, $(M,13M)=(2M,4M)$, $(2M,13M)=(3M,M)$.

By applying (2.1) and (2.2), the first two of the above sets of identities may be summarized as follows:

$$\text{If } 7\mid \mathrm{ind}\,2,\ (h,4h)=(-h,-4h).$$

A partial summary of the last two sets of identities is the following:

$$\text{If } 7\nmid \mathrm{ind}\,2,\ \big(hM,(4h+6)M\big)=\big(-hM,(-4h+6)M\big),$$

provided $h\not\equiv 2,5 \pmod 7$.

6. Application to residue difference sets. A (v,k,λ) *difference set* is a set of k distinct residues $r_1,r_2,\dots,r_k \pmod v$ such that the congruence

$$r_i-r_j\equiv d \pmod v$$

has exactly λ solutions for each $d\not\equiv 0 \pmod v$. A residue difference set is a difference set consisting of the eth power residues, modulo a prime p, without zero. Emma Lehmer proved that no residue difference set exists if f is even; if f is odd, a necessary and sufficient condition for the eth power residues, modulo p, to form a difference set is

$$(6.1)\qquad (i,0)=(f-1)/e,\quad i=0,1,2,\dots,\tfrac{1}{2}e-1 \qquad \text{([3], Theorem III).}$$

A difference set formed by zero and the eth power residues, modulo p, is called a *modified residue difference set*. For such a difference set to exist, f must be odd. Then zero and the eth power residues, modulo p, form a difference set if and only if

$$(6.2)\qquad (f+1)/e=1+(0,0)=(i,0),\quad i=1,2,\dots,\tfrac{1}{2}e-1$$

([3], Theorem III').

The following theorem was suggested by a remark from A. Schinzel:

THEOREM 4. *If $e\equiv 6 \pmod 8$, and 2 is an $\frac{1}{2}e$-th power residue or a quadratic nonresidue, modulo p, then the e-th power residues, modulo p, with or without zero, do not form a residue difference set.*

Proof. $(0,0)$ is odd if and only if 2 is an eth power residue, modulo p ([3], Lemma I). Thus, if 2 satisfies the hypotheses of the theorem (and $(2/p)$ is a Legendre symbol),

$$(6.3)\qquad 2(0,0)\equiv 1+(2/p) \pmod 4.$$

Assume $e\equiv 6 \pmod 8$. Since f must be odd, $p\equiv 3 \pmod 4$. If $(2/p)=1$, $p\equiv 7 \pmod 8$; if $(2/p)=-1$, $p\equiv 3 \pmod 8$. In either case,

$$2(2/p)\equiv p+3 \pmod 8.$$

Substituting into (6.3) gives

$$4(0,0)\equiv p+5 \pmod 8.$$

If the eth power residues, without zero, form a difference set, modulo p, then

$$(0,0)=(p-e-1)/e^2 \qquad \text{([3], Theorem III).}$$

$$4(0,0)=(p-e-1)/(\tfrac{1}{2}e)^2\equiv p-e-1\equiv p+5 \pmod 8.$$

$$e\equiv 2 \pmod 8,\ \text{a contradiction.}$$

If the eth power residues, with zero, form a residue difference set, modulo p, then

$$(0,0)=-1+(p+e-1)/e^2 \qquad \text{([3], Theorem III').}$$

$$4(0,0)=-4+(p+e-1)/(\tfrac{1}{2}e)^2\equiv -4+p+e-1\equiv p+5 \pmod 8.$$

$$e\equiv 2 \pmod 8,\ \text{a contradiction.}$$ q. e. d.

THEOREM 5. *If $p\equiv 1 \pmod{14}$, the fourteenth power residues, modulo p, without zero, do not form a difference set. The fourteenth power residues, modulo p, with zero, do not form a difference set.*

Proof. The case $\mathrm{ind}\,2\equiv 0 \pmod 7$ was eliminated by Theorem 4.

If $\mathrm{ind}\,2\not\equiv 0 \pmod 7$, let $A_i=B_7(iM,1)$. Note that $(4M,0)=(3M,3M)$, $(5M,0)=(2M,2M)$, $(6M,0)=(M,M)$.

Assume that the fourteenth power residues, with or without zero, form a residue difference set. Then for $i=1,2,\dots,6$,

$$(iM,0)-(0,0)=w,$$

where $w=0$ if (6.1) is assumed, while $w=1$ if (6.2) is assumed.

Computing $28[(iM,0)-(0,0)]$, $i=1,\dots,6$, from Table 4 yields the six equations

$$\begin{aligned}
-42f+5+2T+2U+5A_1+3A_2+4A_3+3A_4+A_5+5A_6 &= 28w,\\
56f-2+2T+2U-4A_1-2A_2-4A_3-4A_4-8A_5-6A_6 &= 28w,\\
-42f+5+2T-2U+8A_1+4A_2+4A_3+5A_4-A_5+A_6 &= 28w,\\
-42f+5+2T+2U+5A_1+7A_2+2A_3+6A_4-A_5+2A_6 &= 28w,\\
-42f+5+2T-2U+3A_1+3A_2+6A_3+4A_4+3A_5+2A_6 &= 28w,\\
-42f+5+2T-2U+4A_1+6A_2+2A_3+7A_4-A_5+3A_6 &= 28w.
\end{aligned}$$

For each j, $j=1,2,\dots,6$, solve the six equations simultaneously for A_j, eliminating the other five A_i. The results are

$$\begin{aligned}
168A_1 &= 336f+9+33T-21U-462w,\\
168A_2 &= 336f-61-37T-343U+518w,\\
168A_3 &= 336f-131-107T+7U+1498w,\\
168A_4 &= 336f-5+19T+385U-266w,\\
168A_5 &= 336f+72+96T-1344w,\\
168A_6 &= 336f-47-23T-77U+322w.
\end{aligned} \tag{6.4}$$

Then, by (2.5),

$$168A_0 = 336f-5+19T+49U-266w.$$

Since the product of the Jacobi sum $\psi(\varphi,\varphi)$ with its complex conjugate is the integer p, by (2.9),

$$\sum_{i=0}^{6} A_iA_{i+j} = \sum_{i=0}^{6} A_iA_{i+k}, \quad j,k=1,2,\dots,6. \tag{6.5}$$

Set $j=2$, $k=3$. Replace the terms in (6.5) by their equivalents from (6.4). After factoring out an appropriate constant, one may group terms to obtain

$$(T+U+1-14w)^2+12U^2=0.$$

Hence $U=0$. But this implies that $p=T^2$, which is absurd. This completes the proof.

TABLE 1

ind 2 $\equiv$ 0 (mod 7), if f is even. $C_i = B_7(i,1)$

	f	1	T	U	C_1	C_2	C_3	C_4	C_5	C_6
196(0, 0) =	2030	−184	−12	0	−168	−168	−168	−168	−168	−168
196(0, 1) =	−126	−2	2	14	56	7	14	0	21	−28
196(0, 2) =	−126	−2	2	14	28	28	−7	7	28	−14
196(0, 3) =	−126	−2	2	−14	21	14	56	−28	0	7
196(0, 4) =	−126	−2	2	14	7	28	28	28	−14	−7
196(0, 5) =	−126	−2	2	−14	14	−28	7	21	56	0
196(0, 6) =	−126	−2	2	−14	28	−7	28	−14	7	28
196(0, 7) =	−322	12	−12	0	28	28	28	28	28	28
196(0, 8) =	−126	−2	2	14	28	7	−14	28	−7	28
196(0, 9) =	−126	−2	2	14	0	56	21	7	−28	14
196(0, 10) =	−126	−2	2	−14	−7	−14	28	28	28	7
196(0, 11) =	−126	−2	2	14	7	0	−28	56	14	21
196(0, 12) =	−126	−2	2	−14	−14	28	7	−7	28	28
196(0, 13) =	−126	−2	2	−14	−28	21	0	14	7	56
196(1, 2) =	70	−2	2	0	−7	0	−7	−7	0	−7
196(1, 3) =	−28	5	−5	−7	7	−7	14	21	−14	0
196(1, 4) =	70	−2	2	0	−14	7	−7	−7	7	−14
196(1, 5) =	−28	5	−5	7	14	0	−7	−14	7	21
196(1, 6) =	70	−2	2	0	−7	−14	7	7	−14	−7
196(1, 7) =	70	−2	2	14	−14	−7	0	−14	7	0
196(1, 8) =	70	−2	2	−14	0	7	−14	0	−7	−14
196(1, 9) =	70	−2	2	0	−7	−14	7	7	−14	−7
196(1, 10) =	−28	5	−5	−7	21	7	−14	−7	0	14
196(1, 11) =	70	−2	2	0	−14	7	−7	−7	7	−14
196(1, 12) =	−28	5	−5	7	0	−14	21	14	−7	7
196(2, 4) =	70	−2	2	0	−7	−7	0	0	−7	−7
196(2, 5) =	70	−2	2	0	7	−7	−14	−14	−7	7
196(2, 6) =	−28	5	−5	−7	7	7	0	7	0	0
196(2, 7) =	70	−2	2	14	−14	−14	7	−7	0	0
196(2, 8) =	70	−2	2	0	−7	0	−7	−7	0	−7
196(2, 9) =	70	−2	2	−14	0	0	−7	7	−14	−14
196(2, 10) =	−28	5	−5	7	0	0	7	0	7	7
196(2, 11) =	70	−2	2	0	7	−7	−14	−14	−7	7
196(3, 6) =	70	−2	2	0	0	−7	−7	−7	−7	0
196(3, 7) =	70	−2	2	−14	7	0	−14	0	−14	−7
196(3, 8) =	−28	5	−5	−7	−7	21	0	7	14	−14
196(3, 9) =	−28	5	−5	7	−14	14	7	0	21	−7
196(3, 10) =	70	−2	2	14	−7	−14	0	−14	0	7
196(4, 8) =	70	−2	2	0	0	−7	−7	−7	−7	0
196(4, 9) =	70	−2	2	0	−7	−7	0	0	−7	−7

TABLE 2

ind 2 ≡ 0 (mod 7), if f is odd. $C_i = B_7(i, 1)$

	f	1	T	U	C_1	C_2	C_3	C_4	C_5	C_6
196(0, 0) =	854	−86	−12	0	−70	−70	−70	−70	−70	−70
196(0, 1) =	70	−2	2	14	0	−7	14	−28	21	−28
196(0, 2) =	70	−2	2	14	0	−28	−7	−7	28	−14
196(0, 3) =	70	−2	2	−14	21	14	0	−28	−28	−7
196(0, 4) =	70	−2	2	14	−7	0	28	−28	−14	−7
196(0, 5) =	70	−2	2	−14	14	−28	−7	21	0	−28
196(0, 6) =	70	−2	2	−14	28	−7	0	−14	−7	−28
196(0, 7) =	−1498	110	−12	0	126	126	126	126	126	126
196(0, 8) =	70	−2	2	14	−28	−7	−14	0	−7	28
196(0, 9) =	70	−2	2	14	−28	0	21	−7	−28	14
196(0, 10) =	70	−2	2	−14	−7	−14	−28	28	0	−7
196(0, 11) =	70	−2	2	14	−7	−28	−28	0	14	21
196(0, 12) =	70	−2	2	−14	−14	28	−7	−7	−28	0
196(0, 13) =	70	−2	2	−14	−28	21	−28	14	−7	0
196(1, 0) =	−126	−2	2	14	42	7	0	14	7	0
196(1, 1) =	−126	−2	2	−14	0	7	14	0	7	42
196(1, 2) =	70	−2	2	0	−7	0	−7	−7	0	−7
196(1, 3) =	−28	5	−5	−7	−7	7	14	21	0	−14
196(1, 4) =	70	−2	2	0	0	−7	−7	−7	−7	0
196(1, 5) =	−28	5	−5	7	0	14	−7	−14	21	7
196(1, 6) =	70	−2	2	0	−7	−14	7	7	−14	−7
196(1, 10) =	−28	5	−5	−7	7	21	−14	−7	14	0
196(1, 11) =	70	−2	2	0	0	−7	−7	−7	−7	0
196(1, 12) =	−28	5	−5	7	−14	0	21	14	7	−7
196(1, 13) =	70	−2	2	0	−7	0	−7	−7	0	−7
196(2, 0) =	−126	−2	2	14	14	42	7	7	0	0
196(2, 1) =	70	−2	2	0	−7	−14	7	7	−14	−7
196(2, 2) =	−126	−2	2	−14	0	0	7	7	42	14
196(2, 3) =	−28	5	−5	7	0	0	7	0	7	7
196(2, 4) =	70	−2	2	0	−7	−7	0	0	−7	−7
196(2, 5) =	70	−2	2	0	7	−7	−14	−14	−7	7
196(2, 12) =	70	−2	2	0	−7	−7	0	0	−7	−7
196(2, 13) =	−28	5	−5	−7	7	7	0	7	0	0
196(3, 0) =	−126	−2	2	−14	7	0	42	0	14	7
196(3, 1) =	−28	5	−5	−7	21	−7	0	7	−14	14
196(3, 2) =	−28	5	−5	7	14	−14	7	0	−7	21
196(3, 3) =	−126	−2	2	14	7	14	0	42	0	7
196(3, 4) =	70	−2	2	0	−14	7	−7	−7	7	−14
196(4, 1) =	70	−2	2	0	−14	7	−7	−7	7	−14
196(4, 2) =	70	−2	2	0	7	−7	−14	−14	−7	7

TABLE 3

ind 2 ≢ 0 (mod 7), if f is even. $C_i = B_7(i, 1)$

	f	1	T	U	C_m	C_{2m}	C_{3m}	C_{4m}	C_{5m}	C_{6m}
196(0, 0) =	−28	−37	−12	0	−21	−21	0	−21	63	21
196(0, 1M) =	−126	−2	2	14	28	−14	14	0	0	42
196(0, 2M) =	560	−51	2	14	−49	−35	−42	−49	−49	−49
196(0, 3M) =	−126	−2	2	−14	49	7	0	0	0	14
196(0, 4M) =	−126	−2	2	14	28	28	−14	7	0	21
196(0, 5M) =	−126	−2	2	−14	−14	14	42	7	0	21
196(0, 6M) =	−126	−2	2	−14	7	21	0	28	0	14
196(0, 7) =	364	−37	−12	0	−21	−21	−28	−21	−49	−35
196(0, 8M) =	−126	−2	2	14	0	14	14	0	28	14
196(0, 9M) =	560	−51	2	14	−49	−35	−42	−49	−49	−49
196(0, 10M) =	−126	−2	2	−14	21	7	28	28	0	−14
196(0, 11M) =	−126	−2	2	14	0	28	14	35	0	−7
196(0, 12M) =	−126	−2	2	−14	14	−14	14	7	56	−7
196(0, 13M) =	−126	−2	2	−14	7	21	0	28	0	14
196(1M, 2M) =	70	−2	2	0	−7	−7	14	0	0	−28
196(1M, 3M) =	−28	5	−5	−7	−7	14	−7	14	0	7
196(1M, 4M) =	70	−2	2	0	0	0	−14	−14	0	0
196(1M, 5M) =	−28	5	−5	7	0	−21	7	21	0	14
196(1M, 6M) =	70	−2	2	0	−21	7	−14	0	0	0
196(1M, 7) =	70	−2	2	14	14	0	−14	0	0	−28
196(1M, 8M) =	70	−2	2	−14	−7	−7	0	−28	0	14
196(1M, 9M) =	70	−2	2	0	7	−7	0	−14	0	−14
196(1M, 10M) =	−28	5	−5	−7	−7	14	−7	14	0	7
196(1M, 11M) =	70	−2	2	0	−14	0	0	0	0	−14
196(1M, 12M) =	−28	5	−5	7	14	7	7	−21	0	14
196(2M, 4M) =	70	−2	2	0	−7	7	14	−14	−28	0
196(2M, 5M) =	70	−2	2	0	7	−35	−14	14	0	0
196(2M, 6M) =	−28	5	−5	−7	21	0	7	0	0	−7
196(2M, 7) =	−616	47	2	14	49	63	56	49	49	49
196(2M, 8M) =	70	−2	2	0	−7	−21	0	14	−28	14
196(2M, 9M) =	70	−2	2	−14	0	0	−28	7	0	−7
196(2M, 10M) =	−28	5	−5	7	−14	7	−7	7	28	0
196(2M, 11M) =	70	−2	2	0	−7	7	−28	−14	0	14
196(3M, 6M) =	70	−2	2	0	−14	0	0	0	0	−14
196(3M, 7) =	70	−2	2	−14	−21	−7	14	−14	0	0
196(3M, 8M) =	−28	5	−5	−7	21	0	7	0	0	−7
196(3M, 9M) =	−28	5	−5	7	0	7	21	−7	0	0
196(3M, 10M) =	70	−2	2	14	−14	−28	0	7	0	7
196(4M, 8M) =	70	−2	2	0	0	0	−14	−14	0	0
196(4M, 9M) =	70	−2	2	0	7	−7	0	−14	0	−14

TABLE 4

ind 2 $\not\equiv$ 0 (mod 7), if f is odd. $C_i = B_7(i, 1)$

	f	1	T	U	C_m	C_{2m}	C_{3m}	C_{4m}	C_{5m}	C_{6m}
196(0, 0) =	168	−37	−12	0	−21	−21	−14	−21	7	−7
196(0, 1M) =	70	−2	2	14	28	−14	−14	0	−14	−14
196(0, 2M) =	−616	47	2	14	49	63	56	49	49	49
196(0, 3M) =	70	−2	2	−14	−7	−7	0	−28	0	14
196(0, 4M) =	70	−2	2	14	0	−28	−14	−7	0	21
196(0, 5M) =	70	−2	2	−14	−14	14	−14	7	−28	7
196(0, 6M) =	70	−2	2	−14	−7	−7	0	−28	0	14
196(0, 7) =	560	−37	−12	0	−21	−21	−42	−21	−105	−63
196(0, 8M) =	70	−2	2	14	0	14	−14	0	14	−42
196(0, 9M) =	−616	47	2	14	49	63	56	49	49	49
196(0, 10M) =	70	−2	2	−14	−35	−7	28	0	0	−14
196(0, 11M) =	70	−2	2	14	−28	−28	14	21	0	−7
196(0, 12M) =	70	−2	2	−14	14	−14	−42	7	28	−21
196(0, 13M) =	70	−2	2	−14	−7	−7	0	−28	0	14
196(1M, 0) =	−126	−2	2	14	14	0	14	0	14	28
196(1M, 1M) =	−126	−2	2	−14	7	21	0	28	0	14
196(1M, 2M) =	70	−2	2	0	−21	−7	0	14	−14	0
196(1M, 3M) =	−28	5	−5	−7	21	0	7	0	0	−7
196(1M, 4M) =	70	−2	2	0	0	0	−14	−14	0	0
196(1M, 5M) =	−28	5	−5	7	−14	−7	7	21	14	0
196(1M, 6M) =	70	−2	2	0	−7	−7	−14	0	−14	14
196(1M, 10M) =	−28	5	−5	−7	21	0	7	0	0	−7
196(1M, 11M) =	70	−2	2	0	−14	0	0	0	0	−14
196(1M, 12M) =	−28	5	−5	7	0	21	7	−21	14	0
196(1M, 13M) =	70	−2	2	0	7	−21	14	0	−14	−14
196(2M, 0) =	560	−51	2	14	−49	−35	−42	−49	−49	−49
196(2M, 1M) =	70	−2	2	0	−7	7	0	−14	14	−28
196(2M, 2M) =	−126	−2	2	−14	0	0	28	7	28	7
196(2M, 3M) =	−28	5	−5	7	14	−7	21	−7	−14	14
196(2M, 4M) =	70	−2	2	0	7	−21	14	0	−14	−14
196(2M, 5M) =	70	−2	2	0	7	−21	−28	0	14	0
196(2M, 12M) =	70	−2	2	0	−7	21	0	−28	−14	0
196(2M, 13M) =	−28	5	−5	−7	−7	14	−7	14	0	7
196(3M, 0) =	−126	−2	2	−14	35	7	14	14	0	0
196(3M, 1M) =	−28	5	−5	−7	−7	14	−7	14	0	7
196(3M, 2M) =	−28	5	−5	7	0	−7	−7	7	14	14
196(3M, 3M) =	−126	−2	2	14	14	28	0	21	0	7
196(3M, 4M) =	70	−2	2	0	0	0	−14	−14	0	0
196(4M, 1M) =	70	−2	2	0	−14	0	0	0	0	−14
196(4M, 2M) =	70	−2	2	0	−7	−7	−14	0	−14	14

References

[1] L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. 57 (1935), pp. 391-424.

[2] — *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc. 37 (1935), pp. 363-380.

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

[4] — *On the number of solutions of* $u^k + D \equiv w^2 \pmod{p}$, Pacif. J. Math. 5 (1955), pp. 103-118.

[5] A. L. Whiteman, *The sixteenth power residue character of* 2, Canad. J. Math. 6 (1954), pp. 364-373.

[6] — *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc. 86 (1957), pp. 401-413.

[7] — *The cyclotomic numbers of order ten*, Proceedings of the Symposia in Applied Mathematics 10, pp. 95-111, American Mathematical Society, Providence, Rhode Island, 1960.

[8] — *The cyclotomic numbers of order twelve*, Acta Arith. 6 (1960), pp. 53-76.

Reçu par la Rédaction le 31. 8. 1964