PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 51, Number 2, September 1975

THE CYCLOTOMIC NUMBERS OF ORDER SEVEN[1]

PHILIP A. LEONARD AND KENNETH S. WILLIAMS

ABSTRACT. The cyclotomic numbers of order seven are given in terms of the solutions of a certain system of three quadratic diophantine equations. This is analogous to L. E. Dickson's evaluation of the cyclotomic numbers of order five, and is a convenient approach for applications to the theory of power residues.

1. **Introduction.** Let g be a primitive root of an odd prime p. Let $e > 1$ be a divisior of $p - 1$ and write $p - 1 = ef$. The cyclotomic number $(h, k) = (h, k)_e$ is defined to be the number of solutions s, t of the trinomial congruence

$$g^{es+h} + 1 \equiv g^{et+k} \pmod p, \qquad 0 \le s, t \le f - 1. \tag{1.1}$$

A central problem in the theory of cyclotomy is to obtain formulae for the numbers (h, k). The cases $e = 2, 3, 4, 5, 6, 8, 9, 10, 12, 14, 15, 16, 18$ and 20 have been treated by several authors, beginning with L. E. Dickson [2]–[4], with fuller treatments due to Emma Lehmer ([6], $e = 8$), A. L. Whiteman ([13]–[15], $e = 10, 12, 16$), J. B. Muskat ([9], $e = 14$), L. Baumert and H. Fredricksen ([1], $e = 9, 18$), and Muskat and Whiteman ([10], $e = 20$).

When $e = 7$ the cyclotomic numbers can be given in terms of certain Dickson-Hurwitz sums using the work of Muskat [9, Theorem 1] or a theorem of Whiteman [15, Theorem 1]. In this paper we obtain these cyclotomic numbers in terms of the solutions of a certain triple of diophantine equations, analogous to the expressions for the cyclotomic numbers of order 5 in terms of the solutions of a pair of diophantine equations (see for example [15, p. 101]). This formulation is often useful in applications (see §3). We make use of the following recent result of the authors [7, Theorems 2 and 3]. If $p \equiv 1 \pmod 7$ then there are exactly six integral simultaneous solutions of

Received by the editors July 15, 1973 and, in revised form, May 6, 1974.

AMS (MOS) subject classifications (1970). Primary 12C20; Secondary 10A15, 10B05, 10G05.

Key words and phrases. Cyclotomic numbers, Jacobi sums, Dickson-Hurwitz sums.

[1] This research was supported by a grant (no. A7233) from the National Research Council of Canada.

Copyright © 1975, American Mathematical Society

the triple of diophantine equations

$$72p = 2x_1^2 + 42(x_2^2 + x_3^2 + x_4^2) + 343(x_5^2 + 3x_6^2), \tag{1.2}$$

$$\begin{aligned} &12x_2^2 - 12x_4^2 + 147x_5^2 - 441x_6^2 + 56x_1x_6 \\ &\quad + 24x_2x_3 - 24x_2x_4 + 48x_3x_4 + 98x_5x_6 = 0, \end{aligned} \tag{1.3}$$

$$\begin{aligned} &12x_3^2 - 12x_4^2 + 49x_5^2 - 147x_6^2 + 28x_1x_5 \\ &\quad + 28x_1x_6 + 48x_2x_3 + 24x_2x_4 + 24x_3x_4 + 490x_5x_6 = 0, \end{aligned} \tag{1.4}$$

satisfying $x_1 \equiv 1 \pmod 7$, distinct from the two "trivial" solutions $(-6t, \pm 2u, \pm 2u, \mp 2u, 0, 0)$, where t is given uniquely and u is given ambiguously by

$$p = t^2 + 7u^2, \qquad t \equiv 1 \pmod 7. \tag{1.5}$$

If $(x_1, x_2, x_3, x_4, x_5, x_6)$ is a nontrivial solution with $x_1 \equiv 1 \pmod 7$ then two others are given by $(x_1, -x_3, x_4, x_2, \frac{1}{2}(-x_5 - 3x_6), \frac{1}{2}(x_5 - x_6))$ and $(x_1, -x_4, x_2, -x_3, \frac{1}{2}(-x_5 + 3x_6), \frac{1}{2}(-x_5 - x_6))$. Each of the other three can be obtained from one given above by changing the signs of x_2, x_3, x_4. It is surprising to us that this result, which parallels a similar result (see for example [2, I, Theorem 8]) for $p \equiv 1 \pmod 5$, and which is implicit in the work of Dickson [2], [3], does not appear in the literature. See [5] and [11, p. 128] for comments related to $p \equiv 1 \pmod 7$.

2. Calculation of the cyclotomic numbers of order 7. The numbers (h, k) satisfy the following well-known relations [11, p. 25]:

$$(h, k) = (h + ae, k + be) \quad \text{for any integers } a \text{ and } b, \tag{2.1}$$

$$(h, k) = (k, h) \quad \text{if } f \text{ is even}, \tag{2.2}$$

$$(h, k) = (e - h, k - h). \tag{2.3}$$

With $e = 7$ the formulae (2.1), (2.2), (2.3) yield the matrix

$$\begin{bmatrix} A & B & C & D & E & F & G \\ B & G & H & I & J & K & H \\ C & H & F & K & L & L & I \\ D & I & K & E & J & L & J \\ E & J & L & J & D & I & K \\ F & K & L & L & I & C & H \\ G & H & I & J & K & H & B \end{bmatrix} \tag{2.4}$$

in which the letter in the hth row and kth column, $h, k = 0, 1, 2, \cdots, 6$, represents the value of (h, k). Thus the evaluation of the $e^2 = 49$ cyclotomic numbers of order 7 reduces to the determination of the 12 quantities $A, B, C, D, E, F, G, H, I, J, K, L$. (2.4) has been given by Whiteman [12, p. 63].

Let g be any primitive root of the prime $p \equiv 1 \pmod 7$ and set $\zeta = \exp(2\pi i/7)$. For any integers m and n we define the Jacobi sum $J(m, n)$ by

$$J(m, n) = \sum_{x, y=1; x+y\equiv 1 \pmod p}^{p-1} \zeta^{m \operatorname{ind}_g x + n \operatorname{ind}_g y},$$

where $\operatorname{ind}_g x$ denotes the unique integer k such that $x \equiv g^k \pmod p$, $0 \le k \le p-2$. It was shown in [7] that

$$J(1, 1) = \sum_{i=1}^{6} c_i \zeta^i, \tag{2.5}$$

the integers $c_1, \cdots, c_6$ being given by

$$\begin{aligned} 12c_1 &= -2x_1 + 6x_2 + 7x_5 + 21x_6, & 12c_4 &= -2x_1 - 6x_4 - 14x_5, \\ 12c_2 &= -2x_1 + 6x_3 + 7x_5 - 21x_6, & 12c_5 &= -2x_1 - 6x_3 + 7x_5 - 21x_6, \\ 12c_3 &= -2x_1 + 6x_4 - 14x_5, & 12c_6 &= -2x_1 - 6x_2 + 7x_5 + 21x_6, \end{aligned} \tag{2.6}$$

where $(x_1, x_2, x_3, x_4, x_5, x_6)$ is a nontrivial solution of (1.1)–(1.3) satisfying $x_1 \equiv 1 \pmod 7$, and

$$J(1, 2) = -t + u\sqrt{-7}, \tag{2.7}$$

where the integers t and u satisfy $p = t^2 + 7u^2$, $t \equiv 1 \pmod 7$.

The Dickson-Hurwitz sums of order 7 are defined by

$$J(1, j) = \sum_{i=0}^{6} B(i, j)\zeta^i \qquad (j = 0, 1, \cdots, 6), \tag{2.8}$$

and

$$\sum_{i=0}^{6} B(i, j) = p - 2. \tag{2.9}$$

They have the following properties (see for example [15, p. 97]):

$$B(i, j) = B(i, 6-j), \tag{2.10}$$

$$B(i, 0) = \begin{cases} f-1 & \text{if } i = 0, \\ f & \text{if } 1 \le i \le 6, \end{cases} \tag{2.11}$$

(2.12) $$B(i, j) = B(i\bar{j}, \bar{j}) \quad \text{if } j \neq 0 \text{ and } j\bar{j} \equiv 1 \pmod 7.$$

Since $\sum_{i=1}^{6} c_i = -x_1$ by (2.6), (2.8) and (2.9) we obtain for $i = 1, 2, \cdots, 6$,

(2.13) $$B(i, 1) = c_i + B(0, 1) = c_i + (p - 2 + x_1)/7.$$

Also as $-1 = \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5 + \zeta^6$ and $\sqrt{-7} = \zeta + \zeta^2 - \zeta^3 + \zeta^4 - \zeta^5 - \zeta^6$, we obtain from (1.5), (2.7), (2.8), (2.9)

$$7B(0, 2) = -6t + p - 2,$$

(2.14) $$7B(1, 2) = 7B(2, 2) = 7B(4, 2) = t + 7u + p - 2,$$

$$7B(3, 2) = 7B(5, 2) = 7B(6, 2) = t - 7u + p - 2.$$

Equation (2.14) is due to Muskat [9, p. 270]. Whiteman [15, Theorem 1] has shown that

$$7(h, k) = \sum_{v=0}^{6} B(vh + k, v) - 6f + \begin{cases} 1 & \text{if } 7 \nmid h, \\ 0 & \text{if } 7 \mid h. \end{cases}$$

Using this together with (2.6), (2.10), (2.11), (2.12), (2.13) and (2.14) we obtain the cyclotomic numbers in terms of t, u, $x_1, \cdots, x_6$. In applying these expressions given in the Theorem below we must indicate how the sign of u is to be chosen given a nontrivial solution $(x_1, \cdots, x_6)$ of (1.2)–(1.4) satisfying $x_1 \equiv 1 \pmod 7$. If $7 \nmid u$ this is easy as we see from the Theorem that $7(B - G) = 4u + 2x_2 - x_3$, so we need only choose u such that

(2.15) $$u \equiv 3x_2 + 2x_3 \pmod 7.$$

If however $7 \mid u$ it appears to be necessary to use (2.5), (2.6), (2.7) and the identity

(2.16) $$pJ(1, 2) = J(1, 1)J(2, 2)J(4, 4).$$

Thus, for example, when $p = 379$ a nontrivial solution of (1.2)–(1.4) with $x_1 \equiv 1 \pmod 7$ is given by

$$x_1 = -13, \quad x_2 = 10, \quad x_3 = 13, \quad x_4 = -12, \quad x_5 = -5, \quad x_6 = 1,$$

and so by (2.6) we have

$$c_1 = 6, \quad c_2 = 4, \quad c_3 = 2, \quad c_4 = 14, \quad c_5 = -9, \quad c_6 = -4.$$

Using these values in (2.5) and computing $J(1, 1)\,J(2, 2)\,J(4, 4)$ we obtain from (2.7) and (2.16) that $t = -6$, $u = -7$.

Theorem. *Let p be a prime* $\equiv 1 \pmod 7$. *If* $(x_1, \cdots, x_6)$ *is any non-trivial solution of* (1.2)–(1.4) *with* $x_1 \equiv 1 \pmod 7$ *and* (t, u) *is the solution of* (1.5) *with* $t \equiv 1 \pmod 7$ *and* u *given by* (2.15) *or by* (2.16) *as indicated above, then for some primitive root* $g \pmod p$ *the cyclotomic numbers of order* 7 *are given by* (2.4) *and*

$$49A = p - 20 - 12t + 3x_1,$$

$$588B = 12p - 72 + 24t + 168u - 6x_1 + 84x_2 - 42x_3 + 147x_4 + 147x_6,$$

$$588C = 12p - 72 + 24t + 168u - 6x_1 + 84x_3 + 42x_4 - 294x_6,$$

$$588D = 12p - 72 + 24t - 168u - 6x_1 + 42x_2 + 84x_4 - 147x_5 + 147x_6,$$

$$588E = 12p - 72 + 24t + 168u - 6x_1 - 42x_2 - 84x_4 - 147x_5 + 147x_6,$$

$$588F = 12p - 72 + 24t - 168u - 6x_1 - 84x_3 - 42x_4 - 294x_6,$$

$$588G = 12p - 72 + 24t - 168u - 6x_1 - 84x_2 + 42x_3 + 147x_5 + 147x_6,$$

$$588H = 12p + 12 + 24t + 8x_1 - 196x_5,$$

$$588I = 12p + 12 - 60t - 84u - 6x_1 + 42x_2 + 42x_3 - 42x_4,$$

$$588J = 12p + 12 + 24t + 8x_1 + 98x_5 - 294x_6,$$

$$588K = 12p + 12 - 60t + 84u - 6x_1 - 42x_2 - 42x_3 + 42x_4,$$

$$588L = 12p + 12 + 24t + 8x_1 + 98x_5 + 294x_6.$$

3. **An application.** It is well known (see for example [11, p. 26]) that 2 is a seventh power (mod p) if and only if $(0, 0) \equiv 1 \pmod 2$, that is by the Theorem if and only if $x_1 \equiv 0 \pmod 2$. Note that $x_1 \equiv 1 \pmod 7$ is given uniquely by the system (1.2)–(1.4). For further results of this kind see [8].

REFERENCES

1. L. D. Baumert and H. Fredricksen, *The cyclotomic numbers of order eighteen with applications to difference sets*, Math. Comp. 21 (1967), 204–219. MR 36 #6370.

2. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem.* I, II, Amer. J. Math. 57 (1935), 391–424, 463–474.

3. ———, *Cyclotomy and trinomial congruences*, Trans. Amer. Math. Soc. 37 (1935), 363–380.

4. ———, *Cyclotomy when e is composite*, Trans. Amer. Math. Soc. 38 (1935), 187–200.

5. E. Lehmer, *On the quintic character of* 2, Bull. Amer. Math. Soc. 55 (1949), 62–63. Abstract #72.

6. E. Lehmer, *On the number of solutions of* $u^k + D \equiv w^2 \pmod{p}$, Pacific J. Math. 5 (1955), 103–118. MR 16, 798.

7. P. A. Leonard and K. S. Williams, *A diophantine system of Dickson*, Rend. Accad. Naz. Lincei 56 (1974), 145–150.

8. ———, *The septic character of* 2, 3, 5, *and* 7, Pacific J. Math. 52 (1974), 143–147.

9. J. B. Muskat, *The cyclotomic numbers of order fourteen*, Acta Arith. 11 (1965/66), 263–279. MR 33 #1302.

10. J. B. Muskat and A. L. Whiteman, *The cyclotomic numbers of order twenty*, Acta Arith. 17 (1970), 185–216. MR 42 #3050.

11. T. Storer, *Cyclotomy and difference sets*, Lectures on Advanced Math., No. 2, Markham, Chicago, Ill., 1967. MR 36 #128.

12. A. L. Whiteman, *Theorems on quadratic partitions*, Proc. Nat. Acad. Sci. U.S.A. 36 (1950), 60–65. MR 11, 332.

13. ———, *The cyclotomic numbers of order sixteen*, Trans. Amer. Math. Soc. 86 (1957), 401–413. MR 19, 1160.

14. ———, *The cyclotomic numbers of order twelve*, Acta Arith. 6 (1960), 53–76. MR 22 #9480.

15. ———, *The cyclotomic numbers of order ten*, Proc. Sympos. Appl. Math., vol. 10, Amer. Math. Soc., Providence, R.I., 1960, pp. 95–111. MR 22 #4682.

DEPARTMENT OF MATHEMATICS, ARIZONA STATE UNIVERSITY, TEMPE, ARIZONA 85281

DEPARTMENT OF MATHEMATICS, CARLETON UNIVERSITY, OTTAWA, ONTARIO, K1S 5B6, CANADA (Current address of both authors)