

**6[12C20].**—J. B. MUSKAT & K. S. WILLIAMS, *Cyclotomy of Order Twelve Over*  $\text{GF}(p^2)$ ,  $p^2 \equiv 1 \pmod{12}$ , One page of text and nine pages of tables, deposited in the UMT file, 1986.

Let  $e \geq 2$  and  $l \geq 1$  be integers and let  $p$  be an odd prime such that  $e$  divides  $p^l - 1$ . We set  $q = p^l$  and define the positive integer  $f$  by  $q = ef + 1$ . The finite field with  $q$  elements is denoted by  $\text{GF}(q)$ . We fix once and for all a generator  $\gamma$  of the multiplicative group  $\text{GF}(q)^* = \text{GF}(q) - \{0\}$ . Further we set  $g = \gamma^{1+p+\dots+p^{l-1}}$ , so that  $g$  is a primitive root modulo  $p$ . For  $\alpha \in \text{GF}(q)^*$  the index of  $\alpha$  with respect to  $\gamma$  is the unique integer  $n$  such that  $\alpha = \gamma^n$  ( $0 \leq n \leq q - 2$ ) and is denoted by  $\text{ind}_\gamma \alpha$ .

The number of solutions  $\alpha \in \text{GF}(q)^+ = \text{GF}(q)^* - \{1\}$  of the pair of congruences

$$(1.1) \quad \begin{cases} \text{ind}_\gamma(\alpha - 1) \equiv h \pmod{e}, \\ \text{ind}_\gamma \alpha \equiv k \pmod{e}, \end{cases}$$

is denoted by  $(h, k)_e$ , where  $h$  and  $k$  are integers such that  $0 \leq h \leq e - 1$ ,  $0 \leq k \leq e - 1$ . The numbers  $(h, k)_e$  are called the cyclotomic numbers of order  $e$  over  $\text{GF}(q)$  and they depend on  $p, l, e$ , and  $\gamma$ . The cyclotomic numbers have the following properties:

$$(1.2) \quad (h, k)_e = (e - h, k - h)_e,$$

$$(1.3) \quad (h, k)_e = \begin{cases} (k, h)_e & \text{if } f \text{ is even,} \\ (k + \frac{1}{2}e, h + \frac{1}{2}e)_e & \text{if } f \text{ is odd,} \end{cases}$$

$$(1.4) \quad (h, k)_e = (ph, pk)_e.$$

It is a central problem in the theory of cyclotomy to obtain explicit formulae for these numbers. This has been done for a number of values of  $e \leq 24$  and  $l \geq 1$ . The determination of the cyclotomic numbers of order twelve over  $\text{GF}(p)$ , where  $p \equiv 1 \pmod{12}$ , was carried out by Whiteman in [5] (the case  $e = 12, l = 1$ ). Whiteman gives the cyclotomic numbers of order twelve over  $\text{GF}(p)$  as linear combinations of  $p, 1, a, b, x$ , and  $y$ , where

$$(1.5) \quad p = a^2 + b^2 = x^2 + 3y^2, \quad a \equiv 1 \pmod{4}, \quad x \equiv 1 \pmod{6}.$$

Using the method described in [3] and the evaluation of the Eisenstein sums

$$(1.6) \quad E_e(\beta^m) = \sum_{c=0}^{p-1} \beta^{m \text{ind}_\gamma(1 + c\gamma^{(p+1)/2})} \quad (\beta = \exp(2\pi i/e))$$

of order  $e$  over  $\text{GF}(p^2)$ , when  $e = 12$ , given by Berndt and Evans [2], the authors have determined the cyclotomic numbers of order twelve over  $\text{GF}(p^2)$ . Analogous to the results of Whiteman, we found that the cyclotomic numbers of order twelve over  $\text{GF}(p^2)$  can be expressed as linear combinations of  $p^2, p, 1, a^2 - b^2, 2ab, x^2 - 3y^2, 2xy$ , where

$$(1.7) \quad p^2 = (a^2 - b^2)^2 + (2ab)^2 = (x^2 - 3y^2)^2 + 3(2xy)^2.$$

The complete set of tables is given in the UMT file as well as in [4].

A summary of the results is as follows.

Since  $p^2 \equiv 1 \pmod{12}$  we have  $p \equiv 1, 5, 7, \text{ or } 11 \pmod{12}$ . In the case  $p \equiv 11 \pmod{12}$  the phenomenon of uniform cyclotomy occurs (see [1, Definition 1]) and there are just three different cyclotomic numbers [1, Theorem 1], namely

$$(2.1) \quad \begin{cases} 144(0, 0)_{12} = p^2 + 110p - 35, \\ 144(0, i)_{12} = 144(i, 0)_{12} = 144(i, i)_{12} = p^2 - 10p - 11, & i \neq 0, \\ 144(i, j)_{12} = p^2 + 2p + 1, & 0 \neq i \neq j \neq 0. \end{cases}$$

Here  $i$  and  $j$  denote integers with  $0 \leq i, j \leq 11$ .

For  $p \equiv 1 \pmod{12}$  it is only necessary to evaluate thirty-one of the  $e^2 = 144$  cyclotomic numbers, as the others can be deduced from them using (1.2) and (1.3). It is shown [4] that the thirty-one cyclotomic numbers  $144(i, j)_{12}$  are integral linear combinations of  $p^2, 1, a^2 - b^2, 2ab, x^2 - 3y^2, 2xy$ , where the integers  $a, b, x, y$  are defined by

$$(2.2) \quad E_{12}(\beta^3) = a + bi, \quad E_{12}(\beta^2) = x + yi\sqrt{3}, \quad \beta = \exp(2\pi i/12),$$

and satisfy

$$(2.3) \quad p = a^2 + b^2, \quad a \equiv (-1)^k \pmod{4}, \quad p = 12k + 1,$$

$$(2.4) \quad p = x^2 + 3y^2, \quad x \equiv 1 \pmod{3}.$$

There are six sets of formulae depending upon  $\text{ind}_g 2 \pmod{3}$  and which of  $a$  or  $b$  is divisible by 3.

For  $p \equiv 5 \pmod{12}$  it is only necessary to evaluate twenty of the  $e^2 = 144$  cyclotomic numbers, as the others can be deduced from them using (1.2), (1.3), and (1.4). It is shown [4] that each of the twenty numbers  $144(i, j)_{12}$  can be expressed as an integral linear combination of  $p^2, p, 1, a^2 - b^2, 2ab$ , where the integers  $a, b$  are defined by

$$(2.5) \quad E_{12}(\beta^3) = a + bi, \quad \beta = \exp(2\pi i/12),$$

and satisfy

$$(2.6) \quad p = a^2 + b^2, \quad a \equiv (-1)^{k+1} \pmod{4}, \quad p = 12k + 5.$$

There are two sets of formulae depending on whether  $a \equiv b \pmod{3}$  or  $a \equiv -b \pmod{3}$ .

For  $p \equiv 7 \pmod{12}$  it is only necessary to evaluate twenty-two of the  $e^2 = 144$  cyclotomic numbers as the others can be deduced from them using (1.2), (1.3), and (1.4). It is shown [4] that each of the twenty-two numbers  $144(i, j)_{12}$  can be expressed as a linear combination of  $p^2, p, 1, x^2 - 3y^2, 2xy$ , where the integers  $x, y$  are defined by

$$(2.7) \quad E_{12}(\beta^2) = x + yi\sqrt{3}$$

and satisfy

$$(2.8) \quad p = x^2 + 3y^2, \quad x \equiv -1 \pmod{3}.$$

There are three sets of formulae depending upon the value of  $\text{ind}_g 2 \pmod{3}$ .

These formulae can be used to obtain new residuacity criteria. For example, the following theorem is proved in [4].

**THEOREM.** *Let  $p \equiv 5 \pmod{12}$  be a prime. Let  $\gamma$  be a generator of  $\text{GF}(p^2)^*$ . Set  $g = \gamma^{1+p}$  so that  $g$  is a primitive root  $\pmod{p}$ . Then, with  $a$  and  $b$  as defined in (2.5), we have*

$$(2.9) \quad \text{ind}_g(-3) \equiv \begin{cases} 1 \pmod{4} & \text{if } a \equiv -b \pmod{3}, \\ 3 \pmod{4} & \text{if } a \equiv b \pmod{3}. \end{cases}$$

#### AUTHORS' SUMMARY

Department of Mathematics and Computer Sciences  
Bar-Ilan University  
Ramat-Gan, Israel

Department of Mathematics and Statistics  
Carleton University  
Ottawa, Ontario, Canada K1S 5B6

1. L. D. BAUMERT, W. H. MILLS & R. L. WARD, "Uniform cyclotomy," *J. Number Theory*, v. 14, 1982, pp. 67–82.
2. B. C. BERNDT & R. J. EVANS, "Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer," *Illinois J. Math.*, v. 23, 1979, pp. 374–437.
3. C. FRIESEN, J. B. MUSKAT, B. K. SPEARMAN & K. S. WILLIAMS, "Cyclotomy of order 15 over  $\text{GF}(p^2)$ ,  $p \equiv 4, 11 \pmod{15}$ ," *Internat. J. Math. Math. Sci.* (To appear.)
4. J. B. MUSKAT & K. S. WILLIAMS, *Cyclotomy of Order Twelve Over  $\text{GF}(p^2)$ ,  $p^2 \equiv 1 \pmod{12}$* , Carleton Mathematical Series No. 217, January 1986, 73 pp.
5. A. L. WHITEMAN, "The cyclotomic numbers of order twelve," *Acta Arith.*, v. 6, 1960, pp. 53–76.