ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 2, Spring 1985

CYCLOTOMY OF ORDER TWICE A PRIME

EMMA LEHMER

Dedicated to the memory of E. G. Straus

Gauss defined f-nomial periods for a prime $p = ef + 1$ as

(1) $$\eta_j = \sum_{r_i \in C_j} \zeta_p^{r_i} \text{ where } \zeta_p = \exp(2\pi_\delta i/p)$$

and C_j is the residue class with index j with respect to some primitive root g. These periods satisfy an irreducible monic period equation of degree e with integer coefficients

(2) $$f_e(x) = \prod_{j=0}^{e-1} (x - \eta_j) = 0.$$

Kummer proved that if p is replaced by a general n then all the prime factors of the integers represented by $f_e(N)$, where N is any integer, are e-th power residues of p, except possibly when they divide P_k with $(e, k) = r \neq 1$, where

(3) $$P_k = \prod_{i=0}^{e-1} (\eta_i - \eta_{i+k})$$

in which case they may be only r-th power residues of p. Kummer [**3**] called such primes exceptional.

Recently Evans [**2**, p.13] proved Kummer's theorem for a generalized cyclotomy in which

(4) $$\eta_j = \sum_{r \in C_j} \alpha_i \zeta_n^r \text{ with } \alpha_i \in \mathbf{Z}(\zeta_s),\ (s, n) = 1.$$

He also defined semiexceptional divisors as those divisors of the discriminant $D_e = \prod_{k=1}^{e-1} P_k$ that are not e-th powers residues and found for $e = 8$ some semiexceptional divisors which are not exceptional [**2**, p.22–24].

In a recent paper [**5**] we considered in great detail the special case of $e = 6$ and p a prime and found that all semiexceptional divisors are exceptional in this case. In doing this it became necessary to use a lemma derived from Theorem 5.2 of our paper [**4**] on Kloosterman sums

Received by the editors August 1, 1983.

$$S(h) = \sum_{x=1}^{p-1} \zeta_p^{x+h\bar{x}} \, (x\bar{x} \equiv 1 (\mathrm{mod}\ p)).$$

If we define the generalized periods by $\theta_j = \sum_{h \in C_j} S(h)$ then it turned out that for e even

$$(5) \qquad e\,\theta_j = \sum_{i=0}^{e-1} \psi_e(-4g^{j-2i})\,\eta_i + (-1)^{j+(p-1)/2}(p-1),$$

where

$$\psi_e(\kappa) = \sum_{x=1}^{p-1} \left(\frac{x^e + \kappa}{p}\right)$$

are the Jacobsthal sums, and therefore rational integers.

Theorem 5.2 showed that for e a prime all the odd prime factors $q \neq p$ of the numbers represented by $G_e(N)$, where

$$(6) \qquad G_e(X) = \prod_{j=0}^{e-1} (x - \theta_j)$$

are e-th power residues of p. The only property of the θ's used in the proof was that the θ's are distinct modulo q. This can be ensured by requiring in (5) that $\delta = (a_0, a_1, \ldots, a_{e-1}) = 1$ and that not all the a_i are equal. Therefore we can restate our Theorem 5.2 as follows:

LEMMA 1. *Let $p = ef + 1$, where p and e are primes and let*

$$H_e(x) = \prod_{i=0}^{e-1} (x - \pi_i),\ \pi_i = \sum_{\nu=0}^{e-1} a_i \eta_{i+\nu}$$

Let $\delta = (a_0, a_1, \ldots, a_{e-1})$ and suppose that not all the a_i are equal, then for any integer N all the odd prime factors $q \neq p$ are e-th power residues of p with the possible exception of the divisors of δ.

In what follows we will make use of this lemma in order to relate the ordinary Gaussian cyclotomy for $p = 2ef + 1$ with e and p both prime to the generalized cyclotomy of order e in which the periods are linear combinations of Gaussian periods.

Let $p = 2ef + 1$ and let

$$(7) \qquad \eta'_j = \sum_{r \in C_j} \zeta_p^r \; (j = 0, 1, \ldots, 2e-1),$$

satisfy the period equation

$$(8) \qquad f_{2e}(x) = \prod_{j=0}^{2e-1} (x - \eta'_j) = 0.$$

Then obviously

$$(9) \qquad \eta'_j + \eta'_{j+e} = \eta_j$$

where η_j is an η of order e in (1).

Let $(i, j) = (i, j)_{2e}$ be the cyclotomic numbers of order $2e$, i.e., the number of times that an element of class C_i is followed by an element of class C_j. It is well known that [8]

$$\eta'_j \eta'_{j+k} = \sum_{i=0}^{e-1} (k, i)\, \eta'_{i+j} + f\varepsilon \tag{10}$$

where $\varepsilon = 0$, except when $k = 0$ and f is even, or when $k = e$ and f is odd, when $\varepsilon = 1$.

$$P_k = \prod_{i=0}^{2e-1} (\eta'_i - \eta'_{i+k}) = N(\pi_k)$$

where

$$\pi_k = (\eta'_0 - \eta'_k)(\eta'_e - \eta'_{e+k}) = \eta'_0\eta'_e - \eta'_0\eta'_{k+e} - \eta'_k\eta'_e + \eta'_k\eta'_{e+k}.$$

By (10) we have

$$\pi_k = \sum_{\nu=0}^{2e-1} [(e, \nu) - (k + e, \nu) - (e - k, \nu - k) + (e, \nu - k)]\eta'_\nu + \begin{cases} 2f(-1)^{f-1}, & k = e \\ 2f, & f \text{ odd} \\ 0 & \text{otherwise.} \end{cases} \tag{11}$$

Using the well known relation [8]

$$(i, j) = (2e - i, j - i) \tag{12}$$

we see that the coefficient of $\eta'_{\nu+e}$ in (11) is the same as the coefficient of η'_ν so that by (9) we can write

$$\pi_k = \sum_{\nu=0}^{e-1} a_\nu \eta_{\kappa+\nu} \tag{13}$$

where, since $\sum_{\nu=0}^{e-1} \eta_\nu = -1$, the coefficients a_ν by (11) are given by

$$a_\nu = (e, \nu) - (k + e, \nu) - (e - k, \nu - k) + (e, \nu - k) + \begin{cases} 2f(-1)^f, & \text{if } k = e \\ -2f, & \text{if } f \text{ odd} \\ 0 & \text{otherwise.} \end{cases} \tag{14}$$

We will now examine when the conditions on the a_i in Lemma 1 are satisfied.

Using the well known sum [8]

$$\sum_{j=0}^{2e-1} (i, j) = \begin{cases} f - 1 & \text{if } i = 0 \text{ and } f \text{ is even} \\ f - 1 & \text{if } i = e \text{ and } f \text{ is odd} \\ f & \text{otherwise} \end{cases} \tag{15}$$

we find from (14), using the fact that $a_{e+\nu} = a_\nu$, that

$$\sum_{\nu=0}^{e-1} a_\nu = \begin{cases} [f-(f-1)-(f-1)+f+4ef]/2 = 2ef+1 = p, & \text{if } k = e \text{ and } f \text{ even} \\ [f-1-f-f+(f-1)-4ef]/2 = -2ef-1 = -p, & \text{if f odd} \\ [f-f-f+f]/2 = 0 & \text{otherwise.} \end{cases} \tag{16}$$

Therefore conditions on the a's in Lemma 1 are satisfied if f is odd. For f even they are satisfied if $k = e$. For $k \neq e$ the a's cannot all be equal, but divisors of δ_k may not be e-th power residues. Therefore, Lemma 1 leads to the following.

THEOREM 1. *Let $p = 2ef + 1$ and let q be an odd prime $\neq p$ dividing $H_e(x)$ for some integer N, then q is an e-th power residue if f is odd. Let f be even; q is an e-th power residue if $q \mid P_e$, but if $q \mid P_k$ for $k \neq e$, then it is an e-th power residue provided that $q \nmid \delta_k$.*

A part of Evans' general theorem about exceptional primes for the case of $p = 2ef + 1$, e a prime, can be stated as follows:

THEOREM 2. Evans [**2**]. *The odd prime $q \neq p$ is exceptional if and only if either*
$q \mid P_{2k}$ and is a quadratic, but not an e-th power residue of p. or $q \mid P_e$ and is e-th power, but not a quadratic residue of p. Moreover if the exceptional prime $q \mid P_e$ then $q^2 \mid P_e$, and if $q \mid P_{2k}$ then $q^e \mid P_{2k}$.

We can now sharpen. Evans' theorem for the case of $p = 2ef + 1$ as follows:

THEOREM 3. *Let $p = 2ef + 1$, e and $q \neq p$ be odd primes, then q is exceptional for f odd if and only if*

$$q \mid P_e \text{ and } \left(\frac{q}{p}\right) = -1. \tag{17}$$

If f is even, then q is exceptional if and only if either (17) *holds or*

$$q \mid P_{2\nu},\ q \mid \delta_{2\nu} \text{ and } q \text{ is not an e-th power residue.} \tag{18}$$

PROOF. This is an immediate consequence of Theorems 1 and 2.

In [**5**] we introduced a notion of a special prime. Such a prime q is not exceptional, but it divides the discriminant and is not an *e-th* power residue.

Using the previous theorems we can state the following theorem.

THEOREM 4. *Let q be special, then q must satisfy the following conditions*

(19) $$q \nmid P_e;\ \textit{if}\ q \mid P_k\ \textit{for}\ k \neq e\ \textit{then} \left(\frac{q}{p}\right) = -1.$$

If f is even then there is another condition, namely, q is not a $2e$-th power,

(20) $$k\ \textit{odd},\ q \mid P_k\ \textit{for}\ k \neq e,\ q \mid \delta_k,$$

Conversely if q satisfies these conditions then it is special.

PROOF. By Theorem 1 all the divisors of P_e are *e-th* power residues. If $(q/p) = 1$, they are $2e$-*th* power residues and if $(q/p) = -1$ then they are exceptional by Theorem 3, therefore in either case they are not special. Similarly if f is odd or if f is even and $q \nmid \delta_k$, then q is an e-th power residue and hence $(q/p) = -1$. If $q \mid \delta_k$, then q need not be an e-th power residue in general and therefore (20) is necessary if k is odd. If k were even then such a prime would be exceptional and not special.

We will now illustrate the use of these theorems in case $2e = 10$. We make use of Dickson's quadratic form [**1**]

(21) $$16p = x^2 + 50u^2 + 50v^2 + 125w^2$$

with the side conditions

(22) $$xw = v^2 - u^2 - 4uv, \qquad x \equiv 1 \pmod 5)$$

which has four solutions

(23) $$(x, u, v, w), (x, -u, -v, w), (x, v, -u, -w), (x, -v, u-w)$$

together with a table of cyclotomic numbers $(i,j)_{10}$ found in Whiteman [**9**] and a computer printout of Muskat's table of (x, u, v, w) for $p < 50000$. There also exists a table for $p < 10000$ by K. S. Williams [**10**].

For f even and 2 a quintic residue of p one finds by (11) using Whiteman's table that

$$4\pi_2 = (-w - 2u + v)\eta_0 + 4w\eta_1 + (-w + 2u + v)\eta_2 - w\eta_3 - w\eta_4$$
$$4\pi_4 = (w + u + 2v)\eta_0 + w\eta_1 - 4w\eta_2 + w\eta_3 + (w - u - 2v)\eta_4$$

so that if $q \mid \delta_2$, then q must divide u, v and w, but that implies that $q \mid D_5$ given in [7], namely

(24) $$256\ D_5 = p^4[w^2(4v - 3u) - u(u - v)^2]^2[w^2(3v + 4u) + v(v + u)^2]^2$$

and so q is a quintic residue in this case. Moreover by (21) we have $16p \equiv x^2 \pmod q$ so that since f is even $(q/p) = 1$ and hence q is a 10-th power residue and therefore is neither exceptional nor special, if it divides P_2. The same conclusion will be reached for divisors of P_6 and P_8. In fact $P_2 = P_8$ and $P_4 = P_6$.

In case 2 is not a quintic residue we find from Whiteman's table that

$$16\pi_2 = (x-4u-2v+w)\eta_0 + 2(v-u+3w)\eta_1 + 4(u+v-w)\eta_2 + 2(v-u+3w)\eta_3 + (-x+4u-6v-9w)\eta_4,$$

This implies that if $q|\delta_2$, then the following conditions hold:

$$u \equiv 2w,\ v \equiv -w,\ x \equiv 5w \text{ and } p \equiv 25w^2 \pmod q, \tag{25}$$

or else $u \equiv v \equiv w \equiv 0 \pmod q$, but in the latter case $q|D_5$ as before and is a tenth power residue, so we are left with (25).
Similarly

$$16\pi_4 = (x+2u+8v-w)\eta_0 - (x+2u-9w)\eta_1 + (-x+4u+2v-w)\eta_2 - 4(u+v-w)\eta_3 + (x-v-11w)\eta_4.$$

If $q|\delta_4$, then argueing as before we find that condition (25) must hold. Hence for cyclotomy with $2e = 10$ Theorem 3 becomes:

THEOREM 5. *The odd prime $q \neq p$ is exceptional if and only if*

$$p = 10n + 1,\ q|P_5 \text{ and } \left(\frac{q}{p}\right) = -1.$$

$$p = 20n + 1,\ q \nmid P_5, \text{ but } q|P_{2k},\ \chi_5(q) \neq 1 \text{ and (25) holds.}$$

Our table for $p < 500$ provides many examples of exceptional primes, marked with an asterisk, which divide P_5 and appear to the second power, but none that divide P_{2k}. To show that such primes exist we point to the following examples:

$$p = 1801,\ x = -29,\ u = 16,\ v = 1,\ w = 11 \text{ and } q = 3$$

$$p = 7001,\ x = -29,\ u = -5,\ v = -36,\ w = -19 \text{ and } q = 11.$$

There is no example for $q = 5$ because (25) cannot hold or for $q = 7$ because (25) implies $u \equiv -2v \pmod q$ which in turn implies that 7 is a quintic residue and therefore not exceptional. K. S. Williams [**11**] gives conditions for quintic residuacity for $q < 20$ which show that $q = 11$, 13, 17, and 19 are quintic non-residues if $u \equiv -2v \pmod q$. This can also be checked by substituting the conditions (25) into the reduced quintic period polynomial given in [**6**]

$$F_5(z) = z^5 - 10pz^3 - 5pxz^2 - 5p[(x^2 - 125w^2)/4 - p]z + p^2x - p[x^3 + 625(u^2 - v^2)w]/8. \tag{26}$$

Letting $z \equiv 5wt$ we obtain

$$F_5(5wt)/(5w)^5 \equiv t^5 - 10t^3 - 5t^2 + 10t - 1 \pmod q$$

which is irreducible modulo q for $11 \leqq q \leqq 41$, so that all these primes are quintic non-residues of p. To find other examples the following special case may be of interest:

THEOREM 6. *Let* $p = 20n + 11$ *and let* $u \equiv v \equiv w \pmod q$. *Then* q *is exceptional if and only if* $q \equiv -1 \pmod 4$.

PROOF. Since $u \equiv v \pmod q$ it follows that q is a quintic residue of p. By (21) we have $16p \equiv x^2 \pmod q$, so that $(p/q) = 1$. By Theorem 5 we must have $(q/p) = -1$ so that $p \equiv q \equiv -1 \pmod 4$ and f is odd. It remains to show that in this case q divides P_5. Letting $x \equiv 4a \pmod q$ we find that under the above conditions

$$\pi_5 = \begin{cases} a(\eta_0 + (a+1)/5) \pmod q \text{ if } \chi_5(2) = 1 \\ a(\eta_2 + (a+1)/5) \pmod q \text{ if } \chi_5(2) \neq 1. \end{cases}$$

Therefore in either case

$$P_5 = a^5 f_5(-(a+1)/5)) = F_5(-a) \equiv 0 \pmod q,$$

since with $u \equiv v \equiv w \equiv 0 \pmod q$ and $x \equiv 4a \pmod q$ we have by (26)

$$F_5(z) \equiv (z+a)^4(z-4a) \pmod q.$$

This proves the theorem.

It is interesting to note that if $\chi_5(2) \neq 1$, then q also divides P_1 since $16\pi_1 = (4a-1)/5 - \eta_4$ and hence $2^{20}P_1 \equiv F_5(4a) \equiv 0 \pmod q$. Examples of Theorem 6 are given below:

q	p	x	u	v	w
3	1051	-29	9	6	9
3	1471	-19	6	15	9
3	2131	11	6	21	-9
3	2791	41	-24	9	9
7	38791	-209	-56	49	-49
7	44851	-229	-49	-70	49

No example for $q = 11$ has been found for $p < 100000$.

Finally we have to look at π_1 and π_3 to see if condition (25) of Theorem 5 can hold for the case $2e = 10$. Again there are two cases. If $\chi_5(2) = 1$, then

$$4\pi_1 = (u-w)\eta_0 - (u+w)\eta_1 + w\eta_2 + w\eta_4$$
$$4\pi_3 = (v+w)\eta_0 - w\eta_1 - w\eta_2 + (w-v)\eta_3$$

and hence if $q|\delta$, then q divides w and u or v and hence by (22) it divides u, v, and w in both cases and is a quintic residue of p. But by (21) we have

$16p \equiv x^2 \pmod{q}$ so that q is a 10-th power residue of p since f is even. Hence q is not special.

If $\chi_5(2) \neq 1$, then

$$16\pi_1 = (x-6v+5w)\eta_0 + (x+2u+8v-w)\eta_1 + (-x+6u+8v+w)\eta_2 - (x+4u+6v+9w)\eta_3 + 4(-u-v+w)\eta_4.$$

$$16\pi_3 = 4(3u-v+w)\eta_0 + 2(-u+v-5w)\eta_1 + (-x-4u+2v-w)\eta_2 + (x-4u-2v+w)\eta_3 + 2(-u+v+3w)\eta_4.$$

In both cases $\delta = 1$ so that condition (25) of Theorem 5 does not hold. Since $P_7 = P_3$ and $P_9 = P_1$ we can now restate Theorem 4 in the case of $2e = 10$ as follows:

THEOREM 7. *If $p = 10f + 1$ then a prime $q \neq p$ is special if and only if $q \nmid P_5$, but $q | P_k$ for $k \neq 5$, and $(q/p) = -1$.*

It is an open question whether special primes exist in this case or in general for cyclotomy of order twice a prime. We have shown in [5] that there are none for cyclotomy of order 6 by giving explicit formulas for all P_k. Theoretically it could be done in the present case but it would involve a prodigious amount of algebra and should be automated.

p	P_1/p	P_2/p	P_3/p	P_4/p	P_5/p
31	67	5^3	5^2	5^2	1
41	83	-3^2	-1	1	-3^{2*}
61	1	47	13	-13	11^{2*}
71	971	4079	37^2	1663	1
101	3637	17	-17	701	-1
131	70061	10957	307	28297	71^{2*}
151	$2^2 \cdot 19 \cdot 491$	2^{13}	2^{15}	$2^8 \cdot 227$	2^{16}
181	3571	3917	73	773	$-7^{2*} \cdot 17^{2*}$
191	$5 \cdot 37633$	5^4	$5 \cdot 383$	$5^2 \cdot 4423$	1
211	152081	1933	3591069	116657	601^2
241	-2^{10}	$-2^7 \cdot 181$	-2^8	$-2^7 \cdot 211$	$-2^8 \cdot 19^{2*}$
251	75017	$2^4 \cdot 5^3 \cdot 271$	$2^4 \cdot 5 \cdot 6173$	5^8	2^{16}
271	$5^2 \cdot 41621$	$5^5 \cdot 83$	7013	$5^2 \cdot 83 \cdot 211$	239^{2*}
281	-1607	53 79	21859	-59 727	661^{2*}
311	$7^2 \cdot 13 \cdot 571$	$13 \cdot 65323$	$7^3 \cdot 13 \cdot 89$	$7^2 \cdot 89^2$	$11^{2*} \cdot 13^2$
331	$79 \cdot 7883$	$31 \cdot 1607$	68879	$89 \cdot 10009$	23^{2*}
401	9203	$-2^{5*} \cdot 29^2$	24439	$-2^{5*} \cdot 2971$	-503^2
421	-64013	149	-185291	$-401 \cdot 457$	-541^{2*}
431	$2^{13} \cdot 3^4$	$2^4 \cdot 3^6 \cdot 503$	$2^2 \cdot 3^6 \cdot 433$	$2^{11} \cdot 3^5$	$2^{14} \cdot 3^2$
461	445157	-1811	69379	113 5531	$-13^{2*}37^{2*}$
491	$3^6 \cdot 37 \cdot 571$	$3^6 \cdot 43^2$	$3^7 \cdot 37$	$3 \cdot 37 \cdot 97 \cdot 643$	$3^2 \cdot 373^{2*}$

REFERENCES

1. L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. Jn. Math. **57** (1935) 408–410.

2. Ronald J. Evans, *Period polynomials for generalized cyclotomic periods*, Manuscripta Math. **40** (1982) 217–243.

3. E. E. Kummer, *Uber die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung enstehen*, Jn. für Math. **30** (1846), 107–116, Collected Papers. v.1, 193–202. Springer-Verlag, N.Y. 1975.

4. D. H. and Emma Lehmer, *The cyclotomy of hyper-Kloosterman sums*, Acta Arith. **14** (1968) 89–111.

5. D. H. and Emma Lehmer, *The sextic period polynomial*, Pacific Jn. of Math. **111** (1984) 341–355.

6. Emma Lehmer, *The quintic character of* 2 *and* 3, Duke Math. Jn. **18** (1951)11–18. [The factor p is omitted before the last square bracket in (10) on p. 16.]

7. Emma Lehmer, *On the divisors of the discriminant of the period equation*, Amer. Jn. of Math. **90** (1968) 375–379.

8. Thomas Storer, *Cyclotomy and Difference Sets*, Lectures in Advanced Math. v.2, Markham Publ. Co., Chicago, 1967.

9. A. L. Whiteman, *Cyclotomic Numbers of order* 10, Proc. Tenth Symp. Applied Math. A.M.S. 1958, v. 10. (1960) 95–111.

10. K. S. Williams, *Table of Solutions* (x, u, v, w) *of the Diophantine System* $16p = x^2 + 50u^2 + 50v^2 + 125w^2$, $xw = v^2 - u^2 - 4uv$, $x \equiv 1 \pmod 5$ *for primes* $p < 10000$, $p \equiv 1 \pmod 5$, Carleton Univ. Ottawa, Manuscript of 13 pages deposited in the UMT file of Math. Comp.

11. K. S. Williams, *Explicit criteria for quintic residuacity*, Math. Comp. **30** (1976) 847–853.

1180 MILLER AVE BERKELY, CA 94708