manuscripta math. 40, 217 - 243 (1982)

manuscripta
mathematica

PERIOD POLYNOMIALS FOR GENERALIZED CYCLOTOMIC PERIODS

Ronald J. Evans*

The theory of cyclotomic period polynomials is developed for general periods of an arbitrary modulus, extending known results for the Gauss periods of prime modulus. Primes dividing the discriminant of the period polynomial are investigated, as are those primes dividing values of the period polynomial.

1. Introduction and notation

Let n and s be relatively prime positive integers. Write $\zeta_n = \exp(2\pi i/n)$. Let $G = G_n$ be the group of $\varphi(n)$ reduced residues (mod n) and let H be an arbitrary subgroup of index e in G. For $c \in G$, define $\sigma_c \in \mathrm{Gal}(\mathbb{Q}(\zeta_{ns})/\mathbb{Q}(\zeta_s))$ by $\sigma_c(\zeta_n) = \zeta_n^c$, $\sigma_c(\zeta_s) = \zeta_s$.

Let r denote the product of the distinct prime factors of n, or twice that, according as $8 \nmid n$ or $8 \mid n$. Choose $a \in \mathbb{Z}[\zeta_{sn}^r]$, $a \neq 0$. We can now define the generalized period

$$\eta = \sum_{h \in H} \sigma_h(a\zeta_n) \tag{1.1}$$

If $a = 1$ and H is cyclic, then η is the cyclotomic period studied for prime n by Gauss in 1801 and for general n by Kummer [12] in 1856.

*Author has NSF grant MCS-8101860

0025-2611/82/0040/0217/$05.40

In the case $a = 1$, Diamond, Gerth, and Vaaler [4] have proved the beautiful result that $\eta \neq 0$ iff

(1.2) no nontrivial element of H is $\equiv 1 \pmod{r}$.

(For example, (1.2) holds if n is squarefree. An example for prime power n is given in Corollary 10.) In Theorem 5, this result is proved for general nonzero $a \in \mathbb{Z}[\zeta_{ns}^{r}]$.

In [5], it was proved for cyclic H that if $\eta \neq 0$, then η has degree $e = |G/H|$ over $\mathbb{Q}(\zeta_s)$. This now follows for general H by Theorem 6. Consequently for $\eta \neq 0$ and $s = 1$, the minimal polynomial of η over $\mathbb{Q}$ has the form

$$\psi(z) = \prod_{i=1}^{e} (z - \tau_i(\eta)), \tag{1.3}$$

where the $\tau_i(\eta)$ are the distinct conjugates of η.

We call $\psi(z)$ the period polynomial of η. Its discriminant is denoted by $D(\psi)$.

For prime n, the period polynomial of η has been explicitly computed for all values of $e \leq 5$ (see [3]), for $e = 6$ [18A], and for $e = 8$ [6]. Gurak [7], [8] and the Lehmers [17], [18] have recently studied the beginning coefficients of the period polynomial in the case that n is large in comparison to $f = |H|$. In order to apply their results for general periods, Theorem 6 is needed.

Theorem 4 shows that if (1.2) holds and $t \nmid a_n$ (in the ring of algebraic integers) for a given rational prime t, then $\eta \not\equiv \sigma_c(\eta) \pmod{t}$ for all $c \in G - H$. This result is needed in our subsequent investigations in Theorem 8 of prime factors of the discriminant $D(\psi)$.

Note that Theorem 4 is easy to prove when n is prime, since then $a \in \mathbb{Z}(\zeta_s)$ and the set $\zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}$ is a relative integral basis for $\mathbb{Q}(\zeta_{sn})$ over $\mathbb{Q}(\zeta_s)$. The argument for general n is considerably more complicated, as the proof of Theorem 4 shows.

In the sequel, q denotes any (rational) prime not dividing na. We often view q as an element of G; e.g., $q \in H$ means $q \equiv h \pmod{n}$ for some $h \in H$.

Suppose that (1.2) holds and $s = 1$. The prime q is said to be exceptional if $q \notin H$ and $\psi(z)$ has a zero (mod q). If $q \notin H$ and $q \mid D(\psi)$, then q is said to be semiexceptional. Theorem 7, (3.8) shows that exceptional primes are semiexceptional. In particular, there are only finitely many exceptional primes for each fixed pair a, n. On the other hand, semiexceptional primes needn't be exceptional. For example, with $a = 1$, $n = 73$, $e = |G/H| = 8$, $q = 3$, we have $D(\psi) = 3^4 2^{54} 73^7$ [20, p. 442] and $3 \notin H$, since 3 is not octic (mod 73); thus 3 is semiexceptional. However, 3 is not exceptional because $\psi(z)$ has no zero (mod 3) [20, (33)].

In §4 and §5, the exceptional and semiexceptional primes are explicitly determined for prime n in the cases $e = 4$ and $e = 8$. The case $e = 6$ is discussed in [18A]. For all other values of $e \leq 8$, no such primes exist, by Corollary 9. The determination of exceptional and semiexceptional primes for $e = 4$ was first accomplished by Sylvester [24], [26], but his proof (see [25]) uses the erroneous assumption that, for general e, semiexceptional primes are exceptional.

The primary purpose of this paper is to prove Theorems 7 and 8. In the case that n is prime, much of Theorem 7 was proved by Kummer [11, p. 197]. (Note Weil's remarks about Kummer's paper in [13, pp. 4, 955].) I. Schur [23] anticipated part of (3.8) for general n. In the case that n is prime, Sylvester [24], [26] stated (3.6) without proof. Also for

prime n, E. Lehmer [21, p. 22] gave (3.7) and applied it to give residuacity criteria for $e = 3, 4$. As is indicated in the examples at the end of §3, special cases of Corollaries 9 and 10 have been proved by E. Lehmer [22] in 1968 and more recently by D. H. and E. Lehmer [16] in 1981.

In §6, we list a few corrections to literature quoted in this paper.

2. Periods

In the sequel, if $n > 1$, let p be the largest prime factor of n, and write

$$n = p^{\alpha}m, \quad \text{with} \quad p \nmid m, \ \alpha \geq 1. \tag{2.1}$$

Write

$$r = r_0 p_0, \tag{2.2}$$

where $p_0 = 4$ if $n = 2^{\alpha} \geq 8$, and $p_0 = p$ otherwise. Note that r_0 is the product of the distinct prime factors of m, or twice that, according as $8 \nmid m$ or $8 \mid m$.

Lemma 1. Suppose that $x, k \in \mathbb{Z}$ with $p \nmid k$, and that $p^B \| (x - 1)$ where $B \geq 1$, but $B > 1$ when $p = 2$. Then

$$p^{A+B} \| (x^{kp^A} - 1) \quad \text{for each integer} \quad A \geq 0.$$

Proof. The proof follows easily by induction on A.

Lemma 2. Let $x \in \mathbb{Z}$, $x \equiv 1 \pmod{r}$, and $x \not\equiv 1 \pmod{n}$. Then for some $d > 0$ and some prime t such that $t^2 | n$,

(2.3) $$x^d \equiv 1 \pmod{n/t} \text{ and } x^d \not\equiv 1 \pmod{n}.$$

Proof. The result is true for $n \leq 4$, so suppose that $n > 4$. We proceed by induction on the number of distinct prime factors of n.

Case 1. $$p^\alpha | (x - 1).$$

Since $x \equiv 1 \pmod{r_0}$ and $x \not\equiv 1 \pmod{m}$, the induction hypothesis yields some $d > 0$ and some prime t such that $t^2 | m$, $x^d \equiv 1 \pmod{m/t}$, and $x^d \not\equiv 1 \pmod{m}$. Thus (2.3) holds for this pair d,t.

Case 2. $$p^\alpha \nmid (x - 1).$$

Since $x \equiv 1 \pmod{r}$, we have $p^B \| (x - 1)$, where $\alpha > B \geq 1$ and $B > 1$ when $p = 2$. Since p is the largest prime factor of n, $p \nmid \varphi(m)$. Define $d = \varphi(m)p^A$, where $A = \alpha - B - 1$. Note that $A \geq 0$. By Lemma 1, $p^{\alpha-1} \| (x^d - 1)$. Also $x^d \equiv 1 \pmod{m}$ since $\varphi(m) | d$. Therefore (2.3) holds with $t = p$. Finally note that $p^2 | n$ since $\alpha > B \geq 1$.

Lemma 3. Suppose that (1.2) holds and $G = H$. Then $\eta = \pm a$.

Proof. Since (1.2) holds and $G = H$, reduction (mod r) maps $G = G_n$ isomorphically onto G_r. Thus $\varphi(r) = \varphi(n)$, so $r = n$. In particular, n is squarefree and $a \in \mathbb{Z}[\zeta_s]$. Therefore, from (1.1),

$$\eta = \sum_{x \in G} \sigma_x(a\zeta_n) = a \sum_{x \in G} \zeta_n^x .$$

The Ramanujan sum $\sum_{x \in G} \zeta_n^x$ equals $\mu(n)$ [1, Theorem 8.6], where μ is the Moebius function. As n is squarefree, $\mu(n) = \pm 1$, so $\eta = \pm a$.

Theorem 4. Suppose that no nontrivial element of H is $\equiv 1 \pmod r$. Let t be a prime with $t \nmid na$. Then

$$\eta \not\equiv \sigma_c(\eta) \pmod t \quad \text{for all} \quad c \in G - H. \tag{2.4}$$

Proof. The theorem is true for $n \leq 4$, so let $n > 4$. We proceed by induction on the number of distinct prime factors of n. Consider the subgroup $I \subset H$ defined by

$$I = \{x \in H : x \equiv 1 \pmod{p^\alpha}\}. \tag{2.5}$$

Reduction (mod m) maps I isomorphically onto a subgroup $J \subset G_m$. Write

$$H = \bigcup_{i=1}^{k} x_i I, \tag{2.6}$$

a disjoint union of cosets with $x_1 = 1$. Then

$$\begin{aligned} R := \sigma_{m+p^\alpha}(\eta) &= \sum_{h \in H} \sigma_{h(m+p^\alpha)}(a)\zeta_m^h \zeta_{p^\alpha}^h \\ &= \sum_{i=1}^{k} \sigma_{x_i}\left\{\zeta_{p^\alpha} \sum_{x \in I} \sigma_x\left(\sigma_{m+p^\alpha}(a)\zeta_m\right)\right\} = \sum_{i=1}^{k} \sigma_{x_i}\left(\delta\zeta_{p^\alpha}\right), \end{aligned} \tag{2.7}$$

where

$$\delta = \sum_{x \in I} \sigma_x\left(\sigma_{m+p^\alpha}(a)\zeta_m\right). \tag{2.8}$$

For $w \in G_m$, define $\tau_w \in \mathrm{Gal}\left(\mathbb{Q}\left(\zeta_{ns}\right)/\mathbb{Q}\left(\zeta_{sp^\alpha}\right)\right)$

by

$$\tau_w(\zeta_m) = \zeta_m^w\ ,\ \tau_w\left(\zeta_{sp^\alpha}\right) = \zeta_{sp^\alpha}. \tag{2.9}$$

Then

$$\delta = \sum_{x \in J} \tau_x\left(\sigma_{m+p^\alpha}(a)\zeta_m\right) \tag{2.10}$$

Thus δ is a generalized period of the type in (1.1), with the roles of η, n, G, H, a, s, r played by δ, m, G_m, J, $\sigma_{m+p^\alpha}(a)$, sp^α, r_0, respectively. Furthermore, it follows from (1.2) that no nontrivial element of the subgroup $J \subset G_m$ is $\equiv 1 \pmod{r_0}$. Therefore, by induction hypothesis,

$$\tau_w(\delta) \not\equiv \delta \pmod{t} \text{ for all } w \in G_m - J. \tag{2.11}$$

If $J \neq G_m$, it follows from (2.11) that

$$\delta \not\equiv 0 \pmod{t}. \tag{2.12}$$

In fact, since $t \nmid a$, Lemma 3 shows that (2.12) also holds when $J = G_m$.

For $1 \le i \le k$, write

$$x_i = p_0 s_i + r_i,\ cx_i = p_0 s_i' + r_i' \quad (0 < r_i, r_i' < p_0). \tag{2.13}$$

We proceed to show that

(2.14) $r_1,\ldots,r_k$ are distinct and $r_1',\ldots,r_k'$ are distinct.

Assume for the purpose of contradiction that $x_i \equiv x_j \pmod{p_0}$ for some i, j with $i \neq j$. Then $x := x_i x_j^{-1} \equiv 1 \pmod{p_0}$. On the other hand, $x \not\equiv 1 \pmod{p^\alpha}$, since the cosets in (2.6) are distinct. Thus

$$p^B \| (x - 1) \quad \text{with} \quad 1 \leq B < \alpha, \quad \text{and} \quad B > 1 \quad \text{when} \quad p = 2.$$

By Lemma 1,

$$x^{p^{\alpha-B}} \equiv 1 \pmod{p^\alpha}. \tag{2.15}$$

Since $x^{\varphi(r)} \equiv 1 \pmod{r}$ and $x \in H$, (1.2) yields

$$x^{\varphi(r)} \equiv 1 \pmod{p^\alpha}. \tag{2.16}$$

Since p is the largest prime factor of n, the exponents $p^{\alpha-B}$ and $\varphi(r)$ in (2.15) and (2.16) are relatively prime. This yields the contradiction $x \equiv 1 \pmod{p^\alpha}$. Therefore, the assumption $x_i \equiv x_j \pmod{p_0}$ is false, and consequently (2.14) holds.

Suppose that $\eta \equiv \sigma_c(\eta) \pmod{t}$ for some $c \in G$. To prove (2.4), it must be shown that $c \in H$. By (2.7),

$$\sum_{i=1}^{k} \sigma_{x_i}(\delta)\zeta_{p^\alpha}^{x_i} = R \equiv \sigma_c(R) = \sum_{i=1}^{k} \sigma_{cx_i}(\delta)\zeta_{p^\alpha}^{cx_i} \pmod{t}. \tag{2.17}$$

By (2.17) and (2.13),

$$(2.18)\qquad \sum_{i=1}^{k}\left(\zeta_{p^\alpha}^{p_0 s_i}\sigma_{x_i}(\delta)\right)\zeta_{p^\alpha}^{r_i} \equiv \sum_{i=1}^{k}\left(\zeta_{p^\alpha}^{p_0 s_i'}\sigma_{cx_i}(\delta)\right)\zeta_{p^\alpha}^{r_i'} \pmod{t}.$$

The elements $\zeta_{p^\alpha}, \zeta_{p^\alpha}^2, \ldots, \zeta_{p^\alpha}^{p_0-1}$ comprise all or part of a relative integral basis for $\mathbb{Q}\left(\zeta_{sn}\right)$ over $\mathbb{Q}\left(\zeta_{sn}^{p_0}\right)$. Thus, in view of (2.14) and (2.18), there is a fixed value of i such that $r_i' = r_1$ and

$$(2.19)\qquad \zeta_{p^\alpha}^{p_0 s_1}\sigma_{x_1}(\delta) \equiv \zeta_{p^\alpha}^{p_0 s_i'}\sigma_{cx_i}(\delta) \pmod{t}.$$

Note that $x_1 = 1$, $r_1 = 1$, and $s_1 = 0$. Thus the left side of (2.19) equals δ. Define

$$(2.20)\qquad d := cx_i = p_0 s_i' + 1.$$

Then since $r_i' = r_1 = 1$, (2.19) yields $\delta \equiv \zeta_{p^\alpha}^{d-1}\sigma_d(\delta) \pmod{t}$, so

$$(2.21)\qquad \sigma_d(\delta) \equiv \zeta_{p^\alpha}^{1-d}\delta \pmod{t}.$$

Assume for the purpose of contradiction that $d \not\equiv 1 \pmod{p^\alpha}$. Then by (2.20), $p^B \| (1-d)$ for some B with $1 \le B < \alpha$, and $B > 1$ when $p = 2$. Define

$$(2.22)\qquad d_A = d^{\varphi(m)p^A} \qquad (A \ge 0).$$

Fix $A = \alpha - B - 1$. By Lemma 1,

$$(2.23)\qquad p^{\alpha-1} \| (d_A - 1);$$

consequently

$$mp^{\alpha-1} \mid (d_A - 1). \tag{2.24}$$

Applying σ_d successively $\varphi(m)p^A - 1$ times to the members of (2.21), we obtain

$$\sigma_{d^A}(\delta) \equiv \delta\zeta_{p^\alpha}^{1-d_A} \pmod{t}. \tag{2.25}$$

By (2.8), $\delta \in \mathbb{Q}(\zeta_{ns}^p)$, so by (2.24), $\sigma_{d^A}(\delta) = \delta$. Therefore (2.25) becom

$$\delta \equiv \delta\zeta_{p^\alpha}^{1-d_A} \pmod{t}. \tag{2.26}$$

By (2.26) and (2.23), $t \mid \delta(1 - \zeta_p)$, so $t \mid \delta p$. This is impossible since $t \neq p$ and $t \nmid \delta$ by (2.12). Therefore

$$d \equiv 1 \pmod{p^\alpha}. \tag{2.27}$$

By (2.27) and (2.21),

$$\sigma_d(\delta) \equiv \delta \pmod{t}. \tag{2.28}$$

Reduction (mod m) maps d to an element $y \in G_m$. By (2.27) and (2.9),

$$\tau_y(\delta) = \sigma_d(\delta). \tag{2.29}$$

From (2.28) and (2.29),

$$\tau_y(\delta) \equiv \delta \pmod{t}. \tag{2.30}$$

In view of (2.11) and (2.30), $y \in J$. Thus, by the definitions of J and y, $d \equiv h \pmod{m}$ for some $h \in I$. Since also $d \equiv 1 \equiv h \pmod{p^{\alpha}}$, it follows that $d \equiv h \pmod{n}$. Therefore $d \in H$, so by (2.20) and (2.6), $c \in H$, as desired.

Theorem 5. No nontrivial element of H is $\equiv 1 \pmod{r}$ iff $\eta \neq 0$.

Proof. Suppose that (1.2) holds. If $G = H$, then $\eta \neq 0$ by Lemma 3. If $G \neq H$, then $\eta \neq 0$ by Theorem 4.

Conversely, suppose that (1.2) fails to hold. By Lemma 2, (2.3) holds for some $x \in H$ and integers d, t with t prime such that $t^2 | n$. Define $u = n/t$ and $K = \{h \in H : h \equiv 1 \pmod{u}\}$. Write

$$H = \bigcup_{\nu} x_{\nu} K \tag{2.31}$$

a union of disjoint cosets. By (2.3), K contains the nontrivial element $h = x^d$. Since $h \equiv 1 \pmod{u}$ and $t | u$, we have $h^t \equiv 1 \pmod{n}$. Thus $h, h^2, \ldots, h^t$ are t distinct elements of K. Moreover, K contains no other elements; for if K had more than t elements, then two such elements k_1 and k_2 would satisfy $(k_1 - 1)/u \equiv (k_2 - 1)/u \pmod{t}$, whence $k_1 \equiv k_2 \pmod{n}$. Thus $K = \{h^i : 1 \leq i \leq t\}$. Write $h^i = 1 + w_i u$. The w_i run through a complete residue system (mod t) as i runs from 1 to t, so

$$\sum_{i=1}^{t} \zeta_t^{w_i} = 0.$$

Consequently, from (2.31),

$$(2.32)\qquad \eta = \sum_{\nu} \sum_{i=1}^{t} \sigma_{x_\nu}\, \sigma_{h^i}\left(a\zeta_n\right) = \sum_{\nu} \sum_{i=1}^{t} \sigma_{x_\nu}\left(a\zeta_n^{h^i}\right)$$

$$= \sum_{\nu} \sigma_{x_\nu}\left(a\zeta_n \sum_{i=1}^{t} \zeta_t^{w_i}\right) = 0,$$

where the second equality of (2.32) holds because $h^i \equiv 1 \pmod{u}$.

Theorem 6. If $\eta \neq 0$, then η has degree $e = |G/H|$ over $\mathbb{Q}(\zeta_s)$.

Proof. Suppose that $\eta \neq 0$. Then (1.2) holds by Theorem 5. Therefore Theorem 4 can be applied to show that $\eta \neq \sigma_c(\eta)$ for each $c \in G - H$. It is clear from (1.1) that $\eta = \sigma_c(\eta)$ for $c \in H$. Thus η is fixed by exactly $|H|$ automorphisms σ_c in $\mathrm{Gal}(\mathbb{Q}(\zeta_{ns})/\mathbb{Q}(\zeta_s))$, so η has degree e over $\mathbb{Q}(\zeta_s)$.

3. Exceptional and semiexceptional primes

Throughout the sequel, q is a prime with $q \nmid na$; H is chosen such that (1.2) holds, so $\eta \neq 0$; $s = 1$; and $M = \langle H, q \rangle$ is the subgroup of G generated by H and q.

We identify the elements $c \in G$ with the elements $\sigma_c \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$, and similarly the elements of G/H with those in the corresponding Galois group. When an element of G or G/H is to be viewed as an automorphism, it will be denoted by either σ or τ. Thus the period polynomial $\psi(z)$ in (1.3) can be written as

$$(3.1)\qquad \psi(z) = \prod_{\tau \in G/H} \left(z - \tau(\eta)\right).$$

For each $\tau \in G$, define

(3.2) $$P_\tau = N\big(\eta - \tau(\eta)\big),$$

where N denotes the norm from $\mathbb{Q}(\eta)$ to $\mathbb{Q}$. The discriminant $D(\psi)$ of the period polynomial $\psi(z)$ equals

(3.3) $$D(\psi) = \prod_{1 \neq \tau \in G/H} P_\tau$$

For prime n, explicit formulas for $D(\psi)$ are known for small e. See [14] for $e \leq 4$; [22] for $e = 5$; [18A] for $e = 6$; and [6] for $e = 8$.

Let $\mathfrak{O}$ denote the ring of integers in $\mathbb{Q}(\eta)$. The symbol Q will be reserved for a prime ideal of $\mathfrak{O}$ dividing $q\mathfrak{O}$.

Theorem 7. The prime q has the following properties.

(3.4) If $q \mid D(\psi)$, e.g., if q is semiexceptional, then $q \mid \prod_{\sigma \in G/M} \sigma\big(\eta - \tau(\eta)\big)$ and $q^{|M/H|} \Big| P_\tau$ for each $\tau \in G$ such that $q \mid P_\tau$.

(3.5) If $\psi(z)$ has a zero (mod q), e.g., if q is exceptional, then $q \mid \prod_{\sigma \in G/M} \sigma\big(\eta - \tau(\eta)\big)$ and $q^{|M/H|} \Big| P_\tau$, for each $\tau \in M$. Conversely, if $q \mid P_\tau$ for $\tau = \sigma_q$, then $\psi(z)$ has a zero (mod q).

(3.6) If $q \in H$, then $\psi(z)$ has a zero (mod q^k) for any $k > 0$.

(3.7) If $q \nmid D(\psi)$, then $q \in H$ iff $\psi(z)$ has a zero (mod q).

(3.8) If q is exceptional, then $q \mid D(\psi)$ and q is semiexceptional.

Proof. From (3.3), we see that (3.5) implies (3.8). Together (3.6) and (3.8) imply (3.7). It remains to prove (3. 4) - (3.6). This will

be done in Cases 1 - 3, respectively.

By Theorem 6,

$$H = \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/\mathbb{Q}(\eta)\right) \tag{3.9}$$

and

$$G/H = \mathrm{Gal}(\mathbb{Q}(\eta)/\mathbb{Q}). \tag{3.10}$$

For any field K with $\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta_n)$, let $D_q(K)$ denote the decomposition group for q in K, and let $f_q(K)$ denote its order. We have [10, p. 104]

$$D_q\left(\mathbb{Q}(\zeta_n)\right) = \langle \sigma_q \rangle = \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/Z\right) \tag{3.11}$$

for the decomposition field Z. By (3.9) - (3.11), we have

$$M = \langle H, q \rangle = \mathrm{Gal}\left(\mathbb{Q}(\zeta_n)/Z \cap \mathbb{Q}(\eta)\right) \tag{3.12}$$

and

$$D_q\left(\mathbb{Q}(\eta)\right) = \mathrm{Gal}\left(\mathbb{Q}(\eta)/Z \cap \mathbb{Q}(\eta)\right) = M/H. \tag{3.13}$$

Case 1. $q \mid D(\psi)$.

By (3.3), $q \mid P_\tau$ for some $\tau \in G - H$. By (3.2),

$$Q \mid \left(\eta - \tau(\eta)\right) \tag{3.14}$$

for some choice of Q. By (3.10) and (3.13),

(3.15) $$\mathfrak{O}q = \prod_{\sigma \in G/M} \sigma(Q).$$

By (3.14) and (3.15),

(3.16) $$q \prod_{\sigma \in G/M} \sigma\big(\eta - \tau(\eta)\big).$$

Since $f_q\big(Q(\eta)\big) = |M/H|$ by (3.13), it follows by taking norms in (3.14) that

(3.17) $$q^{|M/H|} \Big| P_\tau.$$

Now (3.4) follows by (3.16) and (3.17).

Case 2A. $\psi(z)$ has a zero (mod q).

Here q divides $\psi(u) = N(u - \eta)$ for some $u \in \mathbb{Z}$, so

(3.18) $$Q \Big| (u - \eta)$$

for some choice of Q. By (3.13), $\tau(Q) = Q$ for all $\tau \in M$. Thus, application of τ in (3.18) shows that (3.14) holds for all $\tau \in M$. The proof of Case 1 now shows that (3.16) and (3.17) hold for all $\tau \in M$. This proves the first part of (3.5).

Case 2B. $q \Big| P_\tau$ for $\tau = \sigma_q$.

We have

$$\eta^q \equiv \sum_{h \in H} \sigma_h(a\gamma_n)^q \equiv \tau(\eta) \pmod{q}. \tag{3.19}$$

Since $q \mid P_\tau$, we have $Q \mid \left(\eta - \tau(\eta)\right)$ for some choice of Q. Together with (3.19), this yields

$$Q \mid (\eta^q - \eta). \tag{3.20}$$

Now,

$$\eta^q - \eta \equiv \prod_{k=0}^{q-1} (\eta - k) \pmod{q}, \tag{3.21}$$

so by (3.20), $Q \mid (\eta - k)$ for some integer k. Thus q divides $N(k - \eta) = \psi(k)$. This proves the second part of (3.5).

Case 3. $q \in H$.

Since $q \in H$, the group in (3.9) contains that in (3.11), so $Z \supset \mathbb{Q}(\eta)$. Thus q splits completely in $\mathbb{Q}(\eta)$. For any choice of Q, it follows that Q is a first degree prime, that is, $N(Q) = q$. Thus, for any $k > 0$, the ring $\mathcal{O}/Q^k$ has $N(Q^k) = q^k$ elements, and there is a ring isomorphism

$$\mathcal{O}/Q^k \approx \mathbb{Z}/q^k\mathbb{Z}. \tag{3.22}$$

By (3.22), $\eta \equiv u \pmod{Q^k}$ for some $u \in \mathbb{Z}$, so $q^k = N(Q^k)$ divides $\psi(u) = N(u - \eta)$. This proves (3.6).

Theorem 8. If q is semiexceptional, then $G \neq M$.

Proof. Suppose that q is semiexceptional and $G = M$. Then by (3.4),

$$\eta \equiv \tau(\eta) \pmod{q} \text{ for some } \tau \in G - H.$$

This contradicts Theorem 4.

Corollary 9. If $e = |G/H|$ is prime, then there are no semiexceptional (or exceptional) primes.

Proof. Suppose that q is semiexceptional and e is prime. Then $H < \langle H,q \rangle = M = G$, which contradicts Theorem 8. Thus, if e is prime, no primes are semiexceptional (or exceptional, by (3.8)).

Corollary 10. Let $n = p^{\alpha}$ for any odd prime p, with $\alpha \geq 1$, and let $d|(p - 1)$. Let H be the group of $p^{\alpha-1}d$-th powers (mod n). (Note that (1.2) holds.) If $q|D(\psi)$, then $(\text{ind } q, p^{\alpha-1}d) > 1$, where ind q denotes the index of q with respect to any primitive root (mod n).

Proof. Suppose that $q|D(\psi)$ and $(\text{ind } q, p^{\alpha-1}d) = 1$. Then q is semiexceptional and $G = \langle H,q \rangle = M$, which contradicts Theorem 8.

Examples.

In the three examples below, $n = p^{\alpha}$ for an odd prime p, with $\alpha \geq 1$.

1. Let $n = p^2$ and let H be the group of p-th powers (mod n). Then there are no semiexceptional or exceptional primes, by Corollary 10. This was proved for $a = 1$ by the Lehmers [16, Theorems 14 and 15].

2. Let $n = p^{\alpha}$ with $\alpha > 1$, and let H be the group of $p^{\alpha-1}$-th powers (mod n). Then all semiexceptional primes, if any, are p-th powers (mod n), by Corollary 10; c.f. [16, p. 297].

3. Let $n = p = ef + 1$ and let H be the group of (nonzero) e-th power residues (mod p), with e prime. Then there are no semiexceptional or exceptional primes. This special case of Corollary 9 was proved for $a = 1$ by E. Lehmer [22, p. 375]. A generalization involving Kloosterman sums is given in [15, p. 108].

4. Exceptional and semiexceptional primes for $e = 4$

In this section, $a = 1$; $n = p = 4f + 1 = X^2 + Y^2$ with $X \equiv 1$ (mod 4); and H is the group of quartic residues (mod p). We will explicitly characterize the sets of exceptional and semiexceptional primes q. The cases $q = 2$ and $q > 2$ are considered in Theorems 11 and 12, respectively. For the most part, the results in these theorems were stated without proof by Sylvester [24], [25], [26].

From (1.1), η is the quartic period

$$\eta = \sum_{v=1}^{f} \zeta_p^{g^{4v}}, \tag{4.1}$$

where g is a primitive root (mod p). For $\tau = \sigma_g^i$, write $\eta_i = \tau(\eta)$ and $P_i = P_\tau$. By [2, Theorem 3.11], the four conjugates of η, namely η_0, η_1, η_2, and η_3, have the form

$$\left\{\sqrt{p} - 1 \pm \left(2\left(\frac{2}{p}\right)p - 2X\sqrt{p}\right)^{1/2}\right\}/4, \left\{-\sqrt{p} - 1 \pm \left(2\left(\frac{2}{p}\right)p + 2X\sqrt{p}\right)^{1/2}\right\}/4. \tag{4.2}$$

The following well known formulae for the quartic period polynomial $\psi(z)$ and its discriminant $D(\psi)$ can be obtained directly from (4.2):

$$(4.3)\quad \psi(z) = z^4 + z^3 + z^2\left(-2p + (-1)^f(3-p)\right)/8 + z\left(1 + 2pX - p - 2p(-1)^f\right)/16 + \left(1 + 8pX - 4pX^2 - 2p + 5p^2 - 4(-1)^f(p + p^2)\right)/256,$$

and

$$(4.4)\quad D(\psi) = P_1^2P_2 \text{ with } P_2 = pY^2/4 \text{ and } P_1 = -pY^2/16 + p^2\left(1 - (-1)^f\right)/8.$$

Theorem 11. We have

(4.5) f is even iff $D(\psi)$ is even,

and

(4.6) f is even iff $\psi(z)$ has a zero (mod 2).

Moreover, the following are equivalent:

(4.7) 2 is exceptional;

(4.8) 2 is semiexceptional;

(4.9) 2 is quadratic but not quartic (mod p);

(4.10) $4 \| Y$.

Proof. Suppose that f is odd. Than $\left(\frac{2}{p}\right) = -1$, so $M = G$. Thus $D(\psi)$ is odd by Theorem 8. Then (3.5) implies that $\psi(z)$ has no zero (mod 2).

Suppose now that f is even. Then $\left(\frac{2}{p}\right) = 1$ and $4|Y$ by [2, Theorem 3.17]. Since $P_2 = pY^2/4$ by (4.4), P_2 is even. Therefore, $2|D(\psi)$.

Moreover, by (3.5), $\psi(z)$ has a zero (mod 2). This completes the proof of (4.5) and (4.6).

By (3.8), (4.7) implies (4.8). Assume (4.8). Then $2|D(\psi)$, so $2|f$ by (4.5). Since moreover 2 is not quartic (mod p) by (4.8), it follows that (4.9) holds. The equivalence of (4.9) and (4.10) can be seen from [2, Theorem 3.17]. Finally, assume (4.9). Then $2|f$, so $\psi(z)$ has a zero (mod 2) by (4.6). This gives (4.7).

Theorem 12. Let $q > 2$. There are no odd semiexceptional primes if f is even. If f is odd, then the following are equivalent:

(4.11) q is semiexceptional;

(4.12) q is exceptional;

(4.13) $q \equiv 3 \pmod 4$ and $q|Y$.

Proof. In [6, Appendix], it was proved that there are no odd semiexceptional primes when f is even, and it was also proved that (4.12) and (4.13) are equivalent. By (3.8), (4.12) implies (4.11). Finally, suppose (4.11) holds, with $2 \nmid f$. We will deduce (4.13). Since $q|D(\psi)$, q divides P_1 or P_2. If $q|P_1$, then $q|(4p - Y^2)/16$ by (4.4). In this event, E. Lehmer [20, Theorem III] proved that q is quartic (mod p), which contradicts (4.11). Thus $q|P_2$, so by (4.4), $q|Y$. If $q \equiv 1 \pmod 4$, then q would be quartic by the biquadratic reciprocity law [9], so $q \equiv 3 \pmod 4$.

5. Exceptional and semiexceptional primes for $e = 8$

In this section, $a = 1$; $n = p = 8f + 1 = X^2 + Y^2 = C^2 + 2D^2$ with $X \equiv C \equiv 1 \pmod 4$; and H is the group of octic residues (mod p). We will explicitly characterize the sets of semiexceptional and exceptional primes q. The cases $q = 2$ and $q > 2$ are considered in Theorems 13 and 14, respectively.

From (1.1), η is the octic period

$$\eta = \sum_{v=1}^{f} \zeta_p^{g^{8v}} , \tag{5.1}$$

where g is a primitive root (mod p). For $\tau = \sigma_{g^i}$, define $\eta_i = \tau(\eta)$ and $P_i = P_\tau$. The octic period polynomial $\psi(z)$, the η_i and P_i, and the discriminant $D(\psi) = P_1^2P_2^2P_3^2P_4$ are explicitly computed in [6]. From these computations, we have

$$P_4 = p2^8Y^2D^4, \tag{5.2}$$

$$16(\eta_0 + \eta_4 - \eta_1 - \eta_5)(\eta_0 + \eta_4 - \eta_3 - \eta_7) \tag{5.3}$$

$$= p + X\sqrt{p} + (2p^2 + 2pX\sqrt{p})^{1/2},$$

$$\eta_0 + \eta_2 + \eta_4 + \eta_6 - \eta_1 - \eta_3 - \eta_5 - \eta_7 = \sqrt{p} ; \tag{5.4}$$

and

$$2(\eta_0 + \eta_4 - \eta_2 - \eta_6)^2 = p + X\sqrt{p} . \tag{5.5}$$

Let $\mathfrak{O}$ denote the ring of integers in $\mathbb{Q}(\eta)$. The symbol Q will again be used for a prime ideal in $\mathfrak{O}$ dividing $q\mathfrak{O}$. Define

(5.6) $$N = \begin{cases} 1, & \text{if } q \text{ is quartic (mod } p), \\ -1, & \text{otherwise.} \end{cases}$$

Theorem 13. For $q = 2$,

(5.7) $D(\psi)$ is odd iff $2|f$ and $N = -1$;

(5.8) $\psi(z)$ has a zero (mod 2) iff $N = 1$.

(5.9) 2 is exceptional iff 2 is quartic but not octic (mod p).

(5.10) 2 is semiexceptional iff either 2 is quartic but not octic (mod p) or $2 \nmid f$, $N = -1$.

Proof. In Cases 1, 2, and 3 below, we will prove, respectively, that

(5.11) if $2|f$, $N = -1$, then $2 \nmid D(\psi)$;

(5.12) if $2 \nmid f$, $N = -1$, then $2|D(\psi)$ but $\psi(z)$ has no zero (mod 2);

and

(5.13) if $N = 1$, then $\psi(z)$ has a zero (mod 2).

Theorem 13 follows from (5.11) - (5.13), with the aid of (3.5) and (3.8).

Case 1. $2|f$, $N = -1$.

Assume that $2|D(\psi)$. Then $2|P_i$ for some i, $1 \le i \le 4$. For some

choice of Q, $Q|(\eta_0 - \eta_i)$. Since $\sigma_q \in M$, it follows from (3.13) that $\sigma_q(Q) = Q$. Therefore, since $N = -1$, $Q|(\eta_j - \eta_{i+j})$ for every even j. In particular, this yields $Q|(\eta_0 - \eta_4)$ if i is even. Thus $2|P_4$ if $2|i$. However, by [2, Theorems 3.15 and 3.17], $2\|D$ and $4\|Y$. Therefore P_4 is odd by (5.2), so i is odd. Consequently $Q|(\eta_0 - \eta_1 + \eta_2 - \eta_3 + \eta_4 - \eta_5 + \eta_6 - \eta_7)$, which contradicts (5.4).

Case 2. $2\nmid f$, $N = -1$.

By [2, Theorems 3.15 and 3.17], $4|Y$ and $4|D$. Thus P_4 is even by (5.2), so $2|D(\psi)$.

Now suppose that $\psi(z)$ has a zero (mod 2). Since $N = -1$, it follows from (3.5) that $2|P_2$. Then by (3.4),

$$2|(\eta_0 - \eta_2)(\eta_1 - \eta_3). \tag{5.14}$$

It is well known [20,(3)] that

$$\eta_m\eta_{m+u} = \sum_{k=0}^{7} (u, k - m)_8 \eta_k, \quad \text{if } 4\nmid u, \tag{5.15}$$

where $(x,y)_8$ denotes a cyclotomic number (mod p) of order 8. By (5.14) and (5.15),

$$0 \equiv (\eta_0 - \eta_2)(\eta_1 - \eta_3) = \sum_{k=0}^{7} C_k\eta_k \pmod 2, \tag{5.16}$$

where

$$C_k = (1,k)_8 + (1,k-2)_8 - (3,k)_8 - (1,k-1)_8 . \tag{5.17}$$

By (5.16), C_k is even for each k, so $2|C_4$. However, the table of values of $(x,y)_8$ given in [19, pp. 116-117] shows that $C_4 = (X - C)/8$, which is odd by [2, Theorems 3.14 and 3.16]. This contradiction proves that $\psi(z)$ has no zero (mod 2).

Case 3. $N = 1$

By [2, Theorem 3.17], $8|Y$, so P_4 is even by (5.2). Consequently $\psi(z)$ has a zero (mod 2) by (3.5).

Theorem 14. Let $q > 2$. Then

(5.18) q is exceptional iff $q|DY$ and q is quartic but not octic (mod p),

and

(5.19) q is semiexceptional iff $q|DY$ and q is not octic (mod p).

Proof. We proved (5.18) in [6, Theorem 3]. To prove (5.19), first suppose that $q|DY$. Then by (5.2), $q|P_4$, so $q|D(\psi)$. Conversely, suppose that q is semiexceptional. It remains to prove that $q|DY$. If $q|P_4$, then $q|DY$. Thus suppose that $q|P_i$ for some i, $1 \le i \le 3$. We know that q is quadratic, otherwise $G = M$, which contradicts Theorem 8. If $N = -1$, then the proof of Theorem 13, Case 1, shows that $q|P_4$, so $q|DY$. Finally, assume that $N = 1$. First assume that $q|P_2$, so $Q|(\eta_0 - \eta_2)$ for some choice of Q. Since $\sigma_q(Q) = Q$ and $N = 1$, it follows that $Q|(\eta_0 - \eta_2 + \eta_4 - \eta_6)$. Then by (5.5), q divides $(p + X\sqrt{p})(p - X\sqrt{p}) = pY^2$, so $q|Y$. Finally, assume that $q|P_1P_3$. Then $Q|(\eta_0 - \eta_1)(\eta_0 - \eta_3)$ for some choice of Q, so

$Q|(\eta_0 - \eta_1 + \eta_4 - \eta_5)(\eta_0 - \eta_3 + \eta_4 - \eta_7)$. Thus by (5.3), Q divides $(p + X\sqrt{p})^2 - (2p^2 + 2pX\sqrt{p}) = pX^2 - p^2 = -pY^2$, so $q|Y$.

6. Some corrections to the literature

In [5], the argument after (20) should be applied with $e = p^A\varphi(m)$ instead of $e = p^A$. In [3], the right side of the congruence in (4.9) should be multiplied by (2/p). In [19, p. 117], the cyclotomic numbers (1,5), (1,6), (7,5), and (7,6) equal (0,3), (1,3), (1,3), and (1,7), respectively, not (1,3), (0,3), (1,6), and (1,3), as given in the table. In [21, (12)], replace +a by -a. On line 12 of [16, p. 297], replace $p^{\alpha-1}$ by p; also, lines 17 - 18 should be replaced by an assertion equivalent to Corollary 10 of this paper. In the formulas for $Q_0(y)$ and $Q_1(y)$ in [14, p. 404], insert -15 before the bracket]; also, in the formula for $Q_1(y)$, the coefficient of p^2 in braces should be $8X(3)+8X(-3)-8X(-1)-3$.

References

1. T. M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, N. Y., 1976

2. B. C. Berndt and R. J. Evans, Sums of Gauss, Jacobi, and Jacobsthal, J. Number Theory 11 (1979), 349-398

3. B. C. Berndt and R. J. Evans, The determination of Gauss sums, Bull. Amer. Math. Soc. 5 (1981), 107-129

4. H. G. Diamond, F. Gerth III, and J. D. Vaaler, Gauss sums and Fourier analysis on multiplicative subgroups of $\mathbb{Z}_q$, (to appear)

5. R. J. Evans, Generalized cyclotomic periods, Proc. Amer. Math. Soc. 81 (1981), 207-212

6. R. J. Evans, The octic period polynomial, (to appear)

7. S. Gurak, Minimal polynomials for Gauss circulants and cyclotomic units, Pac. J. Math. (to appear)

8. S. Gurak, Minimal polynomials for circular numbers, (to appear)

9. K. Ireland and M. Rosen, A classical introduction to modern number theory, Springer-Verlag, N. Y., 1982

10. G. J. Janusz, Algebraic number fields, Academic Press, N. Y., 1973

11. E. E. Kummer, Ueber die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung enstehen, J. Mathematik 30 (1846), 107-116; Collected Papers, v. 1, pp. 193-202, A. Weil, ed., Springer-Verlag, N. Y., 1975

12. E. E. Kummer, Theorie der idealen Primfaktoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $\omega^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist, Math. Abh. Akad. Wiss. Berlin (1856), 1-47; Collected Papers, v. 1, pp. 583-629, A. Weil, ed., Springer-Verlag, N. Y., 1975

13. E. E. Kummer, Collected Papers, v. 1., A. Weil, ed., Springer-Verlag, N. Y., 1975

14. D. H. and E. Lehmer, The cyclotomy of Kloosterman sums, Acta. Arith. 12 (1967), 385-407

15. D. H. and E. Lehmer, The cyclotomy of hyper-Kloosterman sums, Acta Arith. 14 (1968), 89-111

16. D. H. and E. Lehmer, Cyclotomy for nonsquarefree moduli, Lecture notes in Math., v. 899, pp. 276-300, Springer-Verlag, N. Y., 1981

17. D. H. and E. Lehmer, Cyclotomy with short periods, (to appear)

18. D. H. and E. Lehmer, Multiple sums of cyclotomic numbers, Utilitas Math. (to appear)

18A. D. H. and E. Lehmer, The sextic period polynomial,(to appear)

19. E. Lehmer, On the number of solutions of $u^k + D \equiv w^2 \pmod{p}$, Pac. J. Math. 5 (1955), 103- 118

20. E. Lehmer, Period equations applied to difference sets, Proc. Amer. Math. Soc. 6 (1955), 433-442

21. E. Lehmer, Criteria for cubic and quartic residuacity, Mathematika 5 (1958), 20-29

22. E. Lehmer, On the divisors of the discriminant of the period equation, Amer. J. Math. 90 (1968), 375-379

23. I. Schur,
Sitzungs. Berlin Math. Ges. 11 (1912), 40-50

24. J. J. Sylvester, Instantaneous proof of a theorem of Lagrange on the divisors of the form $Ax^2 + By^2 + Cz^2$ with a postscript on the divisors of the functions which multisect the primitive roots of unity, Amer. J. Math. 3 (1880), 390-392; Mathematical Papers, v. 3, pp. 446-448, Chelsea, N. Y., 1973

25. J. J. Sylvester, On the multisection of the roots of unity, Johns Hopkins University Circulars 1 (1881), 150-151; Mathematical Papers, v. 3, pp. 477-478, Chelsea, N. Y., 1973

26. J. J. Sylvester, Sur les diviseurs des fonctions des périodes des racines primitives de 1' unité, Comptes Rendus 92 (1881), 1084-1086; Mathematical Papers, v. 3, pp. 479-480, Chelsea, N. Y., 1973

Department of Mathematics
University of California, San Diego
La Jolla, CA 92093

(Received September 22, 1982)