PACIFIC JOURNAL OF MATHEMATICS
Vol. 118, No. 2, 1985

ON SPECIAL PRIMES

EMMA LEHMER

In fond memory of Ernst Straus

A special prime q is a prime which divides the discriminant of a general period polynomial of degree e associated with the prime $p = ef + 1$, but q is neither an eth power residue of p nor a divisor of any value of this polynomial.

These primes are very rare. Evans found some for the classical cyclotomic octic. There are none for lower degree cyclotomic polynomials. This paper finds special primes for the two quartics arising from the cyclotomy of Kloosterman sums for $e = 8$ and shows that there are none for $e < 8$.

Introduction. In two earlier papers on the cyclotomy of Kloosterman Sums [**3**, **4**] we proved that for e a prime and $p = ef + 1$ the Kloosterman equation is irreducible and represents numbers all of whose prime factors are eth power residues of p. However, when e is even the equation splits into two irreducible equations of degree $e/2$. The question arises as to whether these two equations can have factors which are not $e/2$th power residues. Such factors are called *exceptional* and they have to divide the discriminant of the equations. Evans [**2**] raised the question of whether all the divisors of the discriminant of the cyclotomic period polynomials are eth power residues. He called the divisors of he discriminant which are not eth power residues *semiexceptional* and showed that for $e = 8$ there exist semiexceptional divisors which are not exceptional. We studied the problem for $e = 6$ in [**5**], where we called such semiexceptional divisors *special*, and showed that they do not exist for $e = 6$. In [**8**] I studied a wider range of period equations of degree $2e$, where e is a prime without finding any special primes. In what follows such primes will be found for the two Kloosterman quartics for $e = 8$ together with the exceptional primes for the two cubics for $e = 6$, as well as for the two quadratics found in [**3**] for $e = 4$.

1. **Kloosterman sums.** The Kloosterman sum $S(h)$ is defined by

$$S(h) = \sum_{x=1}^{p-1} \epsilon(x + h\bar{x}), \qquad x\bar{x} \equiv 1 \pmod{p}$$

where

$$\epsilon(\nu) = \exp(2\pi i\nu/p), \qquad p \text{ a prime.}$$

We write $p = ef + 1$ and put the integers $h = 1, 2, \ldots, p-1$ into cosets C_j with respect to some primitive root g, where every h in C_j is such that $\operatorname{ind}_g h \equiv j \pmod{e}$. In [3] we defined

$$\theta_j = \sum_{h \in C_j} S(h) \qquad (j = 0, 1, \ldots, e-1).$$

We showed that if e is a prime then the θ_j satisfy an irreducible equation of degree e, while for even e the θ_{2j} satisfy an irreducible equation of degree $e/2$, while the θ_{2j+1} satisfy a companion equation of the same degree. For $e = 4$ we let $p = a^2 + b^2$, $a \equiv 1 \pmod 4$, $y_i = 4\theta_{2i} - 1$ and $z_i = 4\theta_{2i+1} - 1$ and obtained the two equations

$$F_2(y) = y^2 - 2py + p^2 - 4pa^2 \quad \text{and} \quad G_2(z) = z^2 - 2pz + p^2 - 4b^2p$$

with discriminants $D(F_2) = 4pa^2$ and $D(G_2) = 4pb^2$.

We now let q be an odd prime. Obviously if $q|a$ then $F_2(y) \equiv (y-p)^2 \pmod q$, and if $q|b$ then $G_2(z) \equiv (z-p)^2 \pmod q$ so that both equations have solutions modulo q.

The following facts are well known: (see [7] for example)

LEMMA 1. *All the divisors of b are quartic residues of p. If $q|a$, then q is a quartic residue of p if and only if $q = 8n \pm 1$.*

This leads at once to the following:

THEOREM 1. *If $q|a$ then q is exceptional for $F_2(y)$ if and only if $q = 8n \pm 3$. There are no exceptional divisors for $G_2(z)$ and neither equation has special divisors.*

It was shown in [3], formula (6.7) that the Kloosterman periods are linear combinations of the cyclotomic periods

$$\eta_i = \sum_{\nu \in C_i} \epsilon(\nu).$$

For e even the formula reads

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

where the coefficients Ψ_e are the Jacobstal sums

$$(2) \qquad \psi_e(h) = \sum_{x=1}^{p-1} \chi(x^e + h).$$

For $e = 6$ [5] formula (48) gives for $p = A^2 + 3B^2$, $4p = L^2 + 27M^2$, $L \equiv A \equiv 1 \pmod 3$

$$\Psi_6(g^r) = \begin{cases} -2(2A+1) & \text{if } r \equiv 0 \pmod 6 \\ 2(A-1) & \text{if } r \equiv \pm 2 \pmod 6 \\ 0 & \text{if } r \equiv 3 \pmod 6 \\ \pm B & \text{if } r \equiv \pm \pmod 6 \end{cases} \tag{3}$$

where by a suitable choice of the primitive roots g we can match the signs of B and r.

For $e = 8$ Theorem 4.7 of [1] can be restated in our notation to read with $p = a^2 + b^2 = c^2 + 2d^2$, $a \equiv c \equiv 1 \pmod 4$, f even

$$\psi_8(g^r) = \begin{cases} -2(2c+a+1) & \text{if } r \equiv 0 \pmod 8 \\ 2(2c-a-1) & \text{if } r \equiv 4 \pmod 8 \\ 2(a-1) & \text{if } r \equiv \pm 2 \pmod 8 \\ 2(b \pm d) & \text{otherwise.} \end{cases} \tag{4}$$

We will also need to know that

$$\Psi(g) = -\Psi(\bar{g}). \tag{5}$$

We are now ready to take up the special cases of $e = 6$ and $e = 8$.

2. The sextic case. We note that the coefficients of η_i and of η_{i+3} are equal in (1) and that $\eta_i + \eta_{i+3} = \eta_i'$ is of order 3, so that if we let $x_i = 3\eta_i' + 1$ then the x_i satisfy the reduced cubic

$$f_3(x) = x^3 - 3px - pL \quad \text{with } D(f_3) = (27pM)^2.$$

Substituting the values of ψ_6 given in (3) into (1) we find that for f even and 2 a cubic residue

$$3\theta_{2i} = -Ax_i + (p+1)/2.$$

Similarly if we let $\delta_i = \eta_i' - \eta_{i+1}'$ then

$$3\theta_{2i+1} = B\delta_i - (p-1)/2$$

where the δ_i are the roots of the less familiar cubic

$$g_3(x) = x^3 - px - pM \quad \text{with } D(g_3) = (pL)^2.$$

Therefore letting

$$y_i = 3\theta_{2i} - (p+1)/2 \quad \text{and} \quad z_i = 3\theta_{2i+1} + (p-1)/2$$

we see that the y_i and the z_i satisfy respectively

$$F_3(x) = A^3 f_3(-x/A) \quad \text{and} \quad G_3(x) = B^3 g_3(x/B)$$

with discriminants

$$D(F_3) = (27pMA^3)^2 \quad \text{and} \quad D(G_3) = (pLB^3)^2.$$

If 2 is not a cubic residue then the roots simply permute and the equations remain unaltered. However if f is odd then the y_i satisfy G_3, while the x_i satisfy F_3 so we obtain nothing new. In order to assertain whether F_3 and G_3 have any exceptional or special divisors we must examine the divisors of AM for F_3 and of LB for G_3. We first recall some well known facts [see **5**].

LEMMA 2. *All the divisors of L and M are cubic residues. If 2 is a cubic residue then all the divisors of A and B are also cubic residues. If 2 is not a cubic residue and if $q \nmid 3$ divides B then q is a cubic residue if and only if $q = 18n \pm 1$.*

The last part of the lemma was obtained in [**5**] by using f_3 together with the fact that all the divisors $q \nmid 3$ of $x^3 - 3x - 1$ are $q = 18n \pm 1$. Similarly we can use g_3, all of whose divisors $q \nmid 3$ are cubic residues, to prove

LEMMA 3. *If 2 is not a cubic residue of p and if $q|A$, then q is a cubic residue of p if and only if $q = 18n \pm 1$.*

Proof. If 2 is not a cubie residue then $4A = L + 9M$, so that since $q|A$, then $L \equiv -9M \pmod{q}$. Putting this into

$$g_3(3Mx) \equiv 27M^3(x^3 - 3x - 1) \pmod{q}$$

we see that since $q \nmid 3M$, $q = 18n \pm 1$. Conversely if $q = 18n \pm 1$, then it is a cubic residue and hence a divisor of $g_3(x)$.

This leads to the following theorem.

THEOREM 2. *If 2 is a cubic residue then neither F_3 nor G_3 have any exceptional or special primes. If 2 is not a cubic residue then 2 is exceptional for F_3 if $p = 12n + 7$ and for G_3 if $p = 12n + 1$. The primes $q = 18n \pm 5$ or $q = 18n \pm 7$ are exceptional for F_3 if $q|A$ and for G_3 if $q|B$.*

Proof. Since $F_3(0) \equiv 0 \pmod{A}$ and $G_3(0) \equiv 0 \pmod{B}$ there are no special primes. If 2 is a cubic residue, then all the divisors of AB are cubic residues. If 2 is not a cubie residue it is exceptional for F_3 if it divides A in which case $p = 12n + 7$, and for G_3 if it divides B so that $p = 12n + 1$. If

$q = 3$ then q does not divide A and is a cubic residue if it divides B, so it is not exceptional. By Lemmas 2 and 3 the primes $q = 18n \pm 1$ are the only cubic residues that divide A or B. The remaining primes $q = 18n \pm 5$ and $q = 18n \pm 7$ are exceptional for F_3 if they divide A and for G_3 if they divide B. This completes the proof of the theorem.

2. The octic case. Let $p = 8f + 1 = a^2 + b^2 = c^2 + 2d^2$, $a \equiv c \equiv 1 \pmod 4$. As in the sextic case we make the transformation

$$y_i = 4\theta_{2i} - (p+1)/2 \quad \text{and} \quad z_i = 4\theta_{2i+1} + (p-1)/2$$

and calculate the θ_{2i} and the θ_{2i+1} by substituting the Jacobsthal sums (4) into (1). Taking (5) into account, we obtain

$$\begin{aligned} y_i &= -(a+2c)\eta_i + a\eta_{i+1} + (2c-a)\eta_{i+2} + a\eta_{i+3} \\ &= -a\sqrt{p} - 2c(\eta_i - \eta_{i+2}) \end{aligned} \tag{6}$$

so that

$$y_i + y_{i+2} = -2a\sqrt{p} \quad \text{and} \quad y_i y_{i+2} = (a^2 - 2c^2)p + (-1)^i 2ac^2\sqrt{p}.$$

This gives

$$F_4(y) = [y^2 + p(a^2 - 2c^2)]^2 - 4a^2p(y + c^2)^2. \tag{7}$$

The discriminant $D(F_4) = P_1^2(F_4)P_2(F_4)$ where

$$P_k(F_4) = \prod_{i=0}^{3}(y_i - y_{i+k}).$$

We see from (6) that

$$y_0 - y_2 = -4c(\eta_0 - \eta_2) \quad \text{and} \quad y_1 - y_3 = -4c(\eta_1 - \eta_3)$$

so that

$$P_2(F_4) = [16c^2(\eta_0 - \eta_2)(\eta_1 - \eta_3)]^2 = 64b^2c^4p.$$

Similarly

$$\begin{aligned} y_0 - y_1 &= -2\sqrt{p}\,a - 2c(\eta_0 - \eta_1 - \eta_2 + \eta_3) \\ y_2 - y_3 &= -2pa + 2c(\eta_0 - \eta_1 - \eta_2 + \eta_3) \end{aligned}$$

so that

$$\begin{aligned} (y_0 - y_1)(y_2 - y_3) &= 4pa^2 - 4c^2(\eta_0 - \eta_1 - \eta_2 + \eta_3)^2 \\ &= 4p(a^2 - c^2) - 4c^2b\sqrt{p}, \end{aligned}$$

while

$$(y_1 - y_2)(y_3 - y_4) = 4p(a^2 - c^2) + 4c^2 b\sqrt{p}\,.$$

Therefore

$$(8) \qquad P_1(F_4) = 16p\left[p(a^2 - c^2)^2 - b^2c^4\right] = 16pa^2(4d^4 - pb^2)$$
$$= 16pa^2\left[p(a^2 - 2c^2) + c^4\right].$$

Therefore

$$D(F_4) = 2^{14}a^4b^2c^4(4d^4 - pb^2)^2.$$

Similarly we find that

$$z_i = (b + 2d)\eta_0 - (b + 2d)\eta_1 + (b - 2d)\eta_2 - (b - 2d)\eta_3$$

so that

$$z_{2i} = b\sqrt{p} \pm 2d(\eta_0 - \eta_1 - \eta_2 + \eta_3)$$

while

$$z_{2i+1} = -b\sqrt{p} \pm 2d(\eta_0 + \eta_1 - \eta_2 - \eta_3).$$

This gives

$$z_i + z_{i+2} = \pm 2b \quad \text{and} \quad z_i z_{i+2} = p(b^2 - 4d^2) \pm 4bd^2\sqrt{p}$$

so that

$$(9) \qquad G_4(z) = \left[z^2 + p(b^2 - 4d^2)\right]^2 - 4b^2p(z + 2d^2)^2.$$

To get the discriminant we note that

$$P_2(G_4) = 256d^4\left[(\eta_0 - \eta_1 - \eta_2 + \eta_3)(\eta_0 + \eta_1 - \eta_2 - \eta_3)\right]^2 = 256a^2d^4p$$

while

$$P_1 = \left[4pa^2 - 16d^2(\eta_0 - \eta_2)^2\right]\left[4pa^2 - 16d^2(\eta_1 - \eta_3)^2\right]$$
$$= \left[4pa^2 - 8d^2\left(p + \sqrt{p}\,a\right)\right]\left[4pa^2 - 8d^2\left(p - \sqrt{p}\,a\right)\right]$$
$$= 16p\left[p(b^2 - 2d^2)^2 - 4a^2d^4\right] = 16pb^2\left[(b^2 - 4d^2)p + 4d^4\right]$$
$$= 16pb^2(c^4 - pa^2).$$

Therefore

$$D(G_4) = 2^{16}a^2b^2d^4p^3(c^4 - pa^2)^2.$$

It is interesting to note that G_4 can be obtained from F_4 by interchanging a with b and c^2 with $2d^2$. This is of course also true of the discriminants, but this duality is not apparent from the roots of the equations.

We now turn our attention to the prime factors of the numbers represented by the two equations which divide the corresponding discriminants. The classical cyclotomic quartic for $p = 8f + 1$ is

$$f_4(x) = (x^2 - p)^2 - 4p(x - a)^2 \quad \text{with } D(f_4) = p^3 b^6/4$$

has no exceptional or special divisors. This is no longer true for our two quartics. In fact we have the following 2 theorems.

THEOREM 3. *Let q be an odd prime. If q divides both a and c it is exceptional for F_4 if and only if $q = 8n \pm 3$. If $q|a$, but $q \nmid c$, then q is special for F_4 if and only if $q = 8n \pm 3$.*

Proof. If $q|a$, then $q|D(F_4)$ and $p \equiv b^2 \pmod q$ so that

$$F_4(y) \equiv y^2 - 2b^2c^2 \pmod q.$$

By Lemma 1 we see that q is not a quartic residue of p if and only if $q = 8n \pm 3$ so in this case it is exceptional if $F_4(y) \equiv 0 \pmod q$, but this is the case if and only if $c \equiv 0 \pmod q$, since q cannot divide both a and b. If $c \not\equiv 0 \pmod q$, then q is special. This proves the theorem.

THEOREM 4. *If q divides a it is exceptional for G_4 if and only if $q = 8n \pm 3$; it is never special.*

Proof. As before, q is not a quartic residue by Lemma 1 and

$$G_4(-b^2) = [b^4 + b^2(b^2 - 4d^2)]^2 - 4b^4(-b^2 + 2d^2)^2 \equiv 0 \pmod q.$$

THEOREM 5. *If $q|c$, but $q \nmid a$, then q is exceptional with respect to F_4 if and only if $q = 8n \pm 1$ is not a quartic residue of p. It is special for F_4 if and only if $q = 8n \pm 3$.*

Proof. Since $q|c$, we have $p \equiv 2d^2 \pmod q$ and $(p/q) = (q/p) = (2/q)$.

$$F_4(y) \equiv (y^2 - 2a^2d^2) \pmod q.$$

This congruence has a solution if and only if $q = 8n \pm 1$, in which case q is exceptional if q is not a quartic residue of p. If $q = 8n \pm 3$ then q is a quadratic non-residue of p and the congruence has no solution so that q is special.

THEOREM 6. *If $q|d$, then q is exceptional for G_4 if and only if q is not a quartic residue of p. It is never special.*

Proof. In this case $p \equiv c^2 \pmod{q}$ and

$$G_4(z) \equiv (z^2 - c^2b^2)^2 \equiv 0 \pmod{q}$$

for $z = bc$. Since q divides the discriminant of $G_4(z)$ it is exceptional if it is not a quartic residue of p.

We will now suppose that $q \nmid ac$ for F_4 and that $q \nmid ad$ for G_4, therefore $q \nmid P_2(F_4)$ or $P_2(G_4)$. Moreover all the y_i, as well as all the z_i are incongruent modulo q in this case. Therefore the proof of Theorem 5.2 in [**4**] is valid so that all the divisors of $P_1(F_4)$, except possibly those of ac, and all the divisors of $P_1(G_4)$, except possibly those of ad are quartic residues of p and hence are neither exceptional nor special. This gives us the following

THEOREM 7. *All the prime divisors of $c^4 - pa^2$ and of $4d^4 - pb^2$ are quartic residues of p.*

It would be of interest to find a direct proof of Theorem 7 and to characterize the divisors of c and d which are quartic residues of $p = c^2 + 2d^2$.

REFERENCES

[1] Bruce C. Berndt and Ronald J. Evans, *Sums of Gauss, Jacobi and Jacobsthal*, J. Number Theory, **11** (1979), 385.

[2] Ronald J. Evans, *Period polynomials for generalized cyclotomic periods*, Manuscripta Math., **40** (1982), 217–283.

[3] D. H. and Emma Lehmer, *The cyclotomy of Kloosterman sums*, Acta Arithmetica, **12** (1967), 25–407.

[4] ______, *The cyclotomy of hyper-Kloosterman sums*, Acta Arithmetica, **14** (1968), 89–111.

[5] ______, *The sextic period polynomial*, Pacific J. Math., **111** (1984), 341–355.

[6] Emma Lehmer, *On the number of solutions of $u^k + D = w^2 \pmod{p}$*, Pacific J. Math., **5** (1955), 103–118.

[7] ______, *Criteria for cubic and quartic residuacity*, Mathematica, **5** (1958), 20–29.

[8] ______, *Cyclotomies with degree twice a prime*, to appear in the Rocky Mountain J.

Received June 6, 1984.

1180 MILLER AVE.
BERKELEY, CA 94708