PACIFIC JOURNAL OF MATHEMATICS
Vol 111, No 2, 1984

THE SEXTIC PERIOD POLYNOMIAL

D. H. LEHMER AND EMMA LEHMER

The coefficients of the polynomial whose roots are the six periods of the pth roots of unity are given for every prime $p = 6f + 1$ in terms of L and M in the quadratic partition

$$4p = L^2 + 27M^2.$$

An explicit formula for the discriminant of this polynomial is also given. A complete analysis of the prime factors of the integers represented by the period polynomial and its corresponding form is given.

1. Introduction. In 1893 Carey [**1**] developed a method for obtaining the coefficients of the general period polynomial and gave a table of the sextic polynomial for every prime $p < 500$. His method expresses the coefficients in terms of a sequence $\{\alpha_k\}$, where α_k is the a_{11}-element in the kth power of the matrix (i, j) of cyclotomic numbers. It has recently been shown [**6**] that these α's form a linear recurrence whose scale of relation is the period polynomial and whose initial values are multiple sums of cyclotomic numbers. That Carey's approach to the period polynomial is inefficient is amply demonstrated by the rather long list of errata in Carey's table given in the Appendix to this paper.

It is surprising to note that, until now, no one has given explicit formulas for the coefficients of the sextic period polynomial although there are formulas due to Dickson [**3**] and Whiteman [**10**] for the corresponding cyclotomic numbers. In this paper we give the coefficients and the discriminant of the sextic period polynomial in terms of the fundamental quadratic partitions

$$4p = L^2 + 27M^2 \quad \text{and} \quad p = A^2 + 3B^2.$$

There is also a complete discussion of the prime factors of the numbers represented by the sextic and its associated form.

2. Notation. Let g be a primitive root of the prime

$$p = ef + 1$$

and let

$$\zeta = \exp\{2\pi i/p\}.$$

We define the e periods η_i by

$$\eta_i = \sum_{\nu=0}^{f-1} \zeta^{g^{e\nu+i}} \qquad (i = 0(1)e-1)$$

and the period polynomial by

$$(1) \qquad \psi_6(x) = \prod_{\eta=0}^{e-1} (x - \eta_i) = \sum_{\lambda=0}^{e} a_\lambda x^{e-\lambda}.$$

We will make use of the well-known relation

$$(2) \qquad \eta_k \eta_{k+i} = \sum_{j=0}^{e-1} (i, j)\eta_{k+j} + f\delta_i^\alpha,$$

where (i, j) are the cyclotomic numbers, while $\alpha = 0$ or $e/2$ according as f is even or odd. We will also use the notation

$$y_i = e\eta_i + 1$$

and the reduced period polynomial

$$(3) \qquad F_e(x) = \prod_{i=0}^{e-1} (x - y_i) = \sum_{\lambda=0}^{e} c_\lambda x^{e-\lambda} = e^e \Psi_e((x-1)/e).$$

For $e = 6$ the quantities

$$\theta_i = \eta_i + \eta_{i+3} \qquad (i = 0, 1, 2)$$

are in fact the periods for $e = 3$. We shall use the well-known cubic period polynomial

$$(4) \quad \psi_3(x) = \prod_{i=0}^{2} (x - \theta_i) = x^3 + x^2 - \frac{p-1}{3}x - \frac{p(L+3)-1}{27}$$

whose discriminant $D_3 = p^2 M^2$. The reduced form of $\psi_3(x)$ is

$$(5) \qquad F_3(x) = \prod_{i=0}^{2} \{x - (3\theta_i + 1)\} = \prod_{i=0}^{2} \{x - x_i\}$$
$$= x^3 - 3px - pL.$$

Its discriminant is $(27pM)^2$.

The parameters L and M used above are defined by the quadratic partition

$$4p = L^2 + 27M^2, \qquad L \equiv 1 \pmod 3),$$

which determines M up to a sign. This ambiguity is resolved when necessary, that is, when M is odd its sign is fixed so that

$$L + M \equiv 0 \pmod 4.$$

We use less often the alternative quadratic partition

$$p = A^2 + 3B^2 \qquad (A \equiv 1 \pmod 3).$$

We say that the number k ($1 \leq k \leq p-1$) belongs to class h in case

$$\operatorname{ind}_g k \equiv h \pmod 6.$$

We define the 36 cyclotomic numbers (i, j) as the number of members k in class i for which $k+1$ belongs to class j. These numbers are expressible linearly in terms of p, L and M and also in terms of p, A, B. Dickson **[3]** gave the 36 cyclotomic numbers in terms of p, A, B when $f = (p-1)/6$ is even and Whiteman **[10]** when f is odd. Storer **[8]** gave (i, j) in terms of p, L, M when f is odd. There seem to be no published formulas for (i, j) in terms of p, L, M when f is even. These are given in the appendix of this paper to complete the record. In giving a set of such formulas one is forced to consider four kinds of primes p. Not only need one consider the parity of f, but also whether or not 2 is a cubic residue of p. This fact leaves its mark on what follows. For brevity we write the cubic character of x as $\chi(x)$. When $\chi(x) \neq 1$ we have chosen g so that

$$\operatorname{ind}_g (2) \equiv 2 \pmod 3.$$

In what follows we use a few well-known facts about the numbers A, B, L, M, and two lemmas about quadratic and cubic residues. They are collected here for easy reference.

If M is even, $A = -L/2$, $B = 3M/2$.
If M is odd, $A = (L + 9M)/4$, $B = (L - 3M)/4$.

$$(6)\quad \begin{aligned} &M \text{ even } f \text{ even}, && L \equiv 2 \pmod 4, && M \equiv 0 \pmod 4, && B \equiv 0 \pmod 6.\\ &M \text{ odd } f \text{ even}, && L \equiv 1 \pmod 2, && M \equiv 1 \pmod 2, && B \equiv f \pmod 4.\\ &M \text{ even } f \text{ odd}, && L \equiv 0 \pmod 4, && M \equiv 2 \pmod 4, && B \equiv 3 \pmod 6.\\ &M \text{ odd } f \text{ odd}, && L \equiv 1 \pmod 2, && M \equiv 1 \pmod 2, && B \equiv 1 \pmod 2.\end{aligned}$$

$\chi(2) = 1$ if and only if M is even.
$\chi(2) = 1$ if and only if $B \equiv 0 \pmod 3$.
$\chi(3) = 1$ if and only if $M \equiv 0 \pmod 3$.

LEMMA 1. *If p is a prime $\equiv 1 \pmod 4$ then any odd prime $q \neq p$ dividing $p - u^2$ is a quadratic residue of p. If p is a prime $\equiv 3 \pmod 4$ then any odd prime $q \neq p$ dividing $p + u^2$ is a quadratic residue of p.*

This follows immediately from the law of quadratic reciprocity.

LEMMA 2. *If $p = 6f + 1$ is a prime, then every prime other than p that divides $F_3(x)$ for some integer x is a cubic residue for p, and conversely.*

This lemma follows from cyclotomy for $e = 3$.

COROLLARY 1. *All the prime factors of LM are cubic residues of p.*

Proof. Apply Lemma 2 to $F_3(L) = -27LM^2$.

Tables of A, B, L, M are to be found in Cunningham [2] for all primes $p = 6f + 1 \leq 125683$.

3. The sextic period polynomial. We consider the polynomial (1) whose roots are the six η's. Our problem is to give formulas for the coefficients a_k in terms of p, L, M. We find it much simpler to work with the reduced sextic (3). There are four cases, depending on the parities of f and M.

First we take up the case in which f is even. We arrange the six roots y_i into three sets of two roots each, thus:

$$(y_0, y_3), \qquad (y_1, y_4), \quad (y_2, y_5).$$

Then in view of (5) and (4) we have, in case M is even,

$$y_i + y_{i+3} = 2x_i \qquad (i = 0, 1, 2),$$

and by (2),

$$y_i y_{i+3} = -(p + Lx_i) \qquad (i = 0, 1, 2). \tag{7}$$

Hence our reduced polynomial is

$$F_6(x) = \prod_{i=0}^{2} \{x^2 - 2x_i x - p - Lx_i\}.$$

Multiplying and simplifying we obtain for M and f even:

$$F_6(x) = x^6 - 15px^4 - 20pLx^3 + 15p(p - L^2)x^2 + 6pL(2p - L^2)x - p(p^2 - 3pL^2 + L^4). \tag{8}$$

$$F_6(A) \equiv 0 \pmod M. \tag{8a}$$

In case M is odd, (7) becomes

$$y_i y_{i+3} = -p + \tfrac{1}{2}(L + 9M)x_i + \tfrac{1}{2}(9M - 3L)x_{i+1}.$$

This gives, for M odd, f even,

$$\begin{aligned}(9)\qquad F_6(x) = x^6 &- 15px^4 + p(7L + 27M)x^3 \\ &+9p\{4p - 9M(L - M)/2\}x^2 \\ &-3p\{4p(2L + 9M) - L^2(L + 9M)\}x \\ &+p\{8p^2 + 6pL(9M - L) - L^4\}.\end{aligned}$$

$$(9\text{a})\qquad F_6(L) \equiv 0 \pmod{B}.$$

We next take up the case of odd f. We group the six roots into two sets of three,

$$(y_0, y_2, y_4) \quad \text{and} \quad (y_1, y_3, y_5),$$

so that our sextic becomes the product of two conjugate cubics. If M is even, one of these cubics is

$$(10)\quad x^3 - 3\sqrt{-p}\,x^2 - 3\left(p + L\sqrt{-p}\right)x - pL - (7p - L^2)\sqrt{-p}\,.$$

Multiplying this by its conjugate we get, for M even, f odd,

$$\begin{aligned}(11)\qquad F_6(x) = x^6 &+ 3px^4 + 16pLx^3 + 3p(17p + L^2)x^2 \\ &+6pL(8p - L^2)x + p(49p^2 - 13pL^2 + L^4).\end{aligned}$$

$$(11\text{a})\qquad F_6(A) \equiv 0 \pmod{M}.$$

Finally, if M is odd the cubic (10) becomes

$$\begin{aligned}x^3 - 3\sqrt{-p}\,x^2 &- 3\left(p - \tfrac{1}{2}(L + 9M)\sqrt{-p}\right)x \\ &+p(L - 27M) - (2p + L^2)\sqrt{-p}\,.\end{aligned}$$

Multiplying this by its conjugate we get for M and f odd,

$$\begin{aligned}(12)\qquad F_6(x) = x^6 &+ 3px^4 - p(11L + 27M)x^3 \\ &+9p(12M - L)\{(L + 3M)/2\}x^2 \\ &+3p\{2L^3 + 27M^2(L - 9M)\}x \\ &+p\left[p(L - 27M)^2 + (2p + L^2)^2\right],\end{aligned}$$

$$(12\text{a})\qquad F_6(L) \equiv 0 \pmod{M}.$$

$F_6(x)$ has now been given in all four cases of p.

To get $\psi_6(x)$ we have only to use the identity (3):

$$\psi_6(x) = 6^{-6}F_6(6x+1).$$

For example, in case f is odd and M is even we find

$$\begin{aligned}\psi_6(x) = x^6 + x^5 &+ \frac{1}{12}(p+5)x^4 + \frac{1}{54}\{p(4L+3)+5\}x^3 \\ &+ \frac{1}{432}\{17p^2+16pL+pL^2+6p+5\}x^2 \\ &+ \frac{1}{1296}\{p^2(8L+17)-p(L^3-L^2-8L-2)+1\}x \\ &+ \frac{1}{46656}\{49p^3-p^2(13L^2-48L-51) \\ &\qquad\qquad +p(L^4-6L^3+3L^2+16L+3)+1\}.\end{aligned}$$

4. The discriminant. This important invariant of $\psi_e(x)$ is defined by

$$D_e = \prod_{0\le i<j<e}(\eta_i-\eta_j)^2.$$

Kummer [5] observed that, in general, the discriminant can be decomposed into integral factors. In our case we have

$$|D_6| = P_1^2P_2^2|P_3|, \tag{13}$$

where

$$P_k = \prod_{i=1}^{6}(\eta_i-\eta_{i+k}) \qquad (k=1,2,3). \tag{14}$$

Formulas for P_k will be given in terms of p, L, M, A, B.

The simplest case is the factor P_3. Here we need not separate cases.

THEOREM 1. $P_3 = (-1)^{f+1}pM^4$.

Proof. Using (2) we find that

$$(\eta_i-\eta_{i+3})(\eta_{i+1}-\eta_{i+4}) = M(\theta_i-\theta_{i+1}),$$

where

$$\theta_i = \eta_i+\eta_{i+3}$$

are the roots of the cubic $\Psi_3(x)$. Taking the product over $i = 1, 2$ and 3 we obtain

$$P_3 = \pm M^3\sqrt{D_3},$$

where D_3 is the discriminant of $\Psi_3(x)$, namely p^2M^2. Since $(\eta_i - \eta_{i+3})$ is real or purely imaginary according as f is even or odd, the theorem follows.

Evaluating P_1 and P_2 involves splitting into the usual four parity cases for M and f. There are two approaches via the two formulas

$$\pi_i = (\eta_i - \eta_{i+k})(\eta_{i+3} - \eta_{i+3+k}) = ax_i + bx_{i+1} + c, \tag{15}$$

where $i = 1, 2$ and 3, and a, b, c are integers, and

$$\rho_i = (\eta_i - \eta_{i+k})(\eta_{i+2} - \eta_{i+2+k})(\eta_{i+4} - \eta_{i+4+k}) = \sigma_k \pm \tau_k\sqrt{-p} \tag{16}$$

when f is odd, $i = 1$ and 2, and σ, τ integers. They are obtained using the fundamental identity (2) and are expressible in terms of p, L and M. Taking the product over the three π_i and over the two conjugate ρ_i over i, respectively, we obtain P_1 and P_2 as polynomials in p, L and M. This gives us the following two theorems.

THEOREM 2.

$$P_2 = \begin{cases} 27pM^4/2^6 & (M\ \textit{even}, f\ \textit{even}) \\ pMB^3/2^3 & (M\ \textit{odd}, f\ \textit{even}) \\ pM^2(16p + L^2)/2^6 = L^3F_3(4p/L)/(2^6 \cdot 3^3) & (M\ \textit{even}, f\ \textit{odd}) \\ p\left[p(L+M)^2 + 4(p - LM)^2\right]/2^8 & \\ \qquad = -(A/6)^3F_3(-2p/A) & (M\ \textit{odd}, f\ \textit{odd}). \end{cases}$$

THEOREM 3.

$$P_1 = \begin{cases} pM^4/2^6 & (M\ \textit{even}, f\ \textit{even}) \\ p\left[p(L - 3M)^2 - 4(p - M^2)^2\right]/2^8 & (M\ \textit{odd}, f\ \textit{even}) \\ pM^2(4p + M^2)/2^6 = -pM^2F_3(L/4)/(27L) & (M\ \textit{even}, f\ \textit{odd}) \\ p\left[p(L+M)^2 + 4(p + M^2)^2\right]/2^8 & (M\ \textit{odd}, f\ \textit{odd}). \end{cases}$$

5. Examples.

EXAMPLE 1. $p = 307$, $f = 51$, $L = 16$, $M = 6$, $A = -8$, $B = 9$. The period polynomial is

$$\Psi_6(x) = x^6 + x^5 + 26x^4 + 381x^3 + 4077x^2 + 9666x + 25596.$$

$$P_1 = 307 \cdot 711 = 3^2 \cdot 79 \cdot 307,$$
$$P_2 = 307 \cdot 2907 = 3^2 \cdot 17 \cdot 19 \cdot 307,$$
$$P_3 = 307 \cdot 1296 = 2^4 \cdot 3^4 \cdot 307,$$
$$D_6 = 2^4 \cdot 3^{12} \cdot 17^2 \cdot 19^2 \cdot 79^2 \cdot 307^5.$$

EXAMPLE 2. $p = 331$, $f = 55$, $L = 1$, $M = 7$, $A = 16$, $B = 5$. The period polynomial is

$$\Psi_6(x) = x^6 + x^5 + 28x^4 - 288x^3 + 1950x^2 - 9800x + 84427.$$

$$P_1 = 331 \cdot 2339, \quad P_2 = 331 \cdot 1723, \quad P_3 = 331 \cdot 7^4,$$
$$D_6 = 7^4 \cdot 331^5 \cdot 1723^2 \cdot 2339^2.$$

EXAMPLE 3. $p = 349, f = 58, L = 37, M = -1, A = 7, B = 10.$

$$\Psi_6(x) = x^6 + x^5 - 145x^4 + 278x^3 + 3961x^2 - 5762x - 34459.$$

$$P_1 = 349 \cdot 17^2, \quad P_2 = 349 \cdot 5^3, \quad P_3 = -349, \quad D_6 = -5^6 \cdot 17^4 \cdot 349^5.$$

EXAMPLE 4. $p = 997, f = 166, L = 10, M = 12, A = -5, B = 18.$

$$\Psi_6(x) = x^6 + x^5 - 415x^4 - 1200x^3 + 9820x^2 + 17936x - 12352.$$

$$P_1 = 997 \cdot 2^2 \cdot 3^4, \quad P_2 = 997 \cdot 2^2 \cdot 3^7, \quad P_3 = -997 \cdot 2^8 \cdot 3^4,$$
$$D_6 = -2^{16} \cdot 3^{26} \cdot 997^5.$$

6. The prime factors of $\Psi_6(N)$. The prime factors of the numbers

$$\Psi_6(N) \quad \text{and} \quad S^6\Psi_6(R/S),$$

where N, R, and S are integers, are almost all restricted to the class of sextic residues of p. Such a prime $q \neq p$ is called *exceptional* in case q is not a sextic residue of p. Kummer [**5**] proved in 1846 that the set of exceptional primes is finite for a given p, and every exceptional prime divides the discriminant D_e of $\Psi_e(x)$. Moreover, these primes must divide P_k in case the greatest common factor of k and e exceeds 1. In our case of $e = 6$ the exceptional primes must divide P_2 or P_3. Recently, Evans [**4**] proved a more general theorem.

THEOREM 4 [*Kummer* 5]. *An exceptional prime q satisfies one of the following two conditions. Either*

$q \mid P_2$ *and q is a quadratic, but not a cubic residue of p, or*

$q \mid P_3$ *and q is a cubic, but not a quadratic residue of p.*

We first consider the case of $q = 2$.

THEOREM 5. *If $p = 24n + 1$, then 2 is exceptional if and only if M is odd. If $q = 24n + 13$ or 19, then 2 is exceptional if and only if M is even. If $p = 24n + 7$ then 2 is not exceptional.*

Proof. Let $p = 24n + 1$. Then $(2/p) = 1$. Suppose 2 is exceptional. Then $\chi(2) \neq 1$, for otherwise 2 would be a sextic residue of p. This implies M is odd. Conversely, let M be odd so $\chi(2) \neq 1$. Then $\Psi_6(0)$ or $\Psi_6(1)$ is even according as $A \equiv 1$ or $-1 \pmod 4$. Hence, 2 is exceptional in this case.

Next let $p = 24n + 13$ or 19. Then $(2/p) = -1$. For 2 to be exceptional it is necessary that P_3 be even, that is, that M be even. Conversely, if M is even, then $\Psi_6(0)$ or $\Psi_6(1)$ is even according as $A \equiv 1$ or $-1 \pmod 4$ in case $p = 24n + 13$ and $\Psi_6(0)$ is even in case $p = 24n + 19$.

Finally, let $p = 24n + 7$. Then $(2/p) = 1$ and f is odd. If $\chi(2) = 1$, then 2 is a sextic residue of p. If $\chi(2) \neq 1$, then M is odd and so is P_3. In this case Theorem 2 gives

$$27P_2 = p\left[p^2 - 3p(A/2)^2 + L(A/2)^3\right]$$

which is odd. Hence, 2 is not exceptional in this case.

THEOREM 6. *If $p = 12n + 1$, then 3 is exceptional if and only if M is even and $3 \nmid M$. If $p = 12n + 7$, then 3 is exceptional if and only if $3 \mid M$.*

Proof. First suppose $p = 12n + 7$. Then $(3/p) = -1$. Suppose 3 is exceptional. Then 3 divides P_3. Hence 3 divides M. Conversely, if 3 divides M, then 3 divides $\Psi_6(0)$, $\Psi_6(1)$ or $\Psi_6(-1)$ according as $L \equiv 7$, 4, or $1 \pmod 9$. Hence, 3 is exceptional since $(3/p) = -1$.

Now suppose $p = 12n + 1$. Then $(3/p) = 1$ and f is even. Suppose 3 is exceptional. Then $\chi(3) \neq 1$. Hence by (6), $3 \nmid M$ and $3 \mid P_2$. Since $3 \nmid B$ if M is odd by (6), only the first case of Theorem 2, namely

$$P_2 = 27pM^4/2^6 \qquad (M \text{ even}, f \text{ even}),$$

is divisible by 3, so M is even.

Conversely, if M is even and $3 \nmid M$, so $\chi(3) \neq 1$, then $\Psi_6(0)$, $\Psi_6(1)$ or $\Psi_6(-1)$ is a multiple of 3 according as $L \equiv 7, 4$, or $1 \pmod 9$, so 3 divides $\Psi_6(x)$. Hence, 3 is exceptional.

We finally consider the case $q > 3$. We need two lemmas:

LEMMA 3. *If* $q \mid B$, *then* $(q/p) = 1$ *iff* f *is even.*

This is a consequence of Lemma 1, since $3B^2 = p - A^2$, so $q \mid p - A^2$.

LEMMA 4 [*Sylvester* [9]]. *Every prime of the form* $18n \pm 1$ *divides* $x^3 - 3x - 1$ *for some value of* x *and, conversely, every prime factor* $q > 3$ *of* $x^3 - 3x - 1$ *is of the form* $18n \pm 1$.

THEOREM 7. *The prime* $q > 3$ *is exceptional if and only if either*

$$f \textit{ is odd}, \ q \mid M \textit{ and } \left(\frac{q}{p}\right) = -1,$$

or

$$f \textit{ is even}, \ q \nmid M, \quad M \textit{ is odd}, \ q \mid B \textit{ and } q \neq 18n \pm 1.$$

Proof. First let f be odd. Suppose q is exceptional. if $q \mid P_3$, then $q \mid M$ and, hence, q is a cubic residue of p by Corollary 1. Since q is exceptional we have $(q/p) = -1$. If $q \nmid P_3$, then $q \nmid M$ and $q \mid P_2$. The last two lines of Theorem 2 show that q is both a quadratic and a cubic residue of p, which contradicts the assumption that q is exceptional in case $q \nmid M$.

Conversely, if $q \mid M$ and $(q/p) = -1$, then by (11a) and (3) q divides a value of $\Psi_6(N)$ and, hence, is exceptional.

Next suppose f is even and q is exceptional. If $q \mid M$, then $\chi(q) = 1$ and $4p \equiv L^2 \pmod q$ so $(p/q) = (q/p) = 1$. Therefore q is a sextic residue of p and, hence, not exceptional. Hence, $q \nmid M$, so $q \nmid P_3$. Therefore $q \mid P_2$. Hence, by Theorem 2, M is odd and $q \mid B$. By Lemma 3, $(q/p) = 1$, hence $\chi(q) \neq 1$. By (6) we have $4B = L - 3M$, so $L \equiv 3M \pmod q$ and $p \equiv L^2 \pmod q$. Hence,

$$F_3(Lx)/L^3 = x^3 - 3x(p/L^2) - p/L^2 \equiv x^3 - 3x - 1 \pmod q.$$

Since $\chi(q) \neq 1$, q cannot divide $F_3(N)$ for any value of N. Hence, by Lemma 4, $q \neq 18n \pm 1$.

Conversely, suppose $q \nmid M$, M is odd, $q \mid B$ and $q \neq 18n \pm 1$. Since $q \mid B$, q divides P_2 and $(q/p) = 1$ by Lemma 3. Since $q \neq 18n \pm 1$, q does not divide $F_3(N)$ for any value of N. Hence, by Lemma 2, $\chi(q) \neq 1$. By (9a), $F_6(L) \equiv 0 \pmod q$. Hence q is exceptional.

COROLLARY 2. *All exceptional primes q divide MB.*

To illustrate Theorems 5, 6 and 7 we refer to our examples:

Example 1 illustrates Theorem 6 with $p = 307$, f odd $M = 6$, $q = 3$, $(q/p) = -1$. Hence, 3 is exceptional and 3 divides $\Psi_6(0) = 25596$.

Example 2 illustrates Theorem 7 with $p = 331$, f odd, $M = 7$, $q = 7$, $(q/p) = -1$. Hence, 7 is exceptional and 7 divides $\Psi_6(0) = 84427$.

Example 3 also illustrates Theorem 7 with $p = 349$, f even, $M = -1$, $B = 10$, $q = 5$. Hence, 5 is exceptional and 5 divides $\Psi_6(1) = -36125$.

Example 4 illustrates Theorems 5 and 6 with $p = 997$, f even, $M = 12$, $q = 2, 3$. By Theorem 5, 2 is exceptional and $\Psi_6(0) = -12352$ is even; by Theorem 6, 3 is not exceptional since $3 \mid M$. In fact 3 is a sextic residue of 997 and hence not exceptional.

7. Semi-exceptional primes. An exceptional prime divides a value of $\Psi_e(x)$ and also its discriminant D_e. A prime which is not an eth power residue of p, but divides D_e, has been called *semi-exceptional* by Evans [**4**]. Every exceptional prime is semi-exceptional. Evans [**4**] proved that when $e = 8$ there exist primes p that have semi-exceptional primes q which are *not* exceptional. We prove in what follows that no such phenomenon exists for $e = 6$. Therefore $e = 8$ is the least e for which such primes exist.

For $e = 6$ we call a prime q *special*, with respect to a prime $p = 6f + 1$, in case q is not a sextic residue of p, $q \mid D_6$ and q does *not* divide $\Psi_6(n)$ for any integer n. Hence, a special prime is semi-exceptional but not exceptional.

A special prime q must therefore satisfy either

$$q \mid P_1 \quad (\text{and } q \text{ is not a sextic residue of } p), \tag{17}$$

or

$$q \mid P_2 \quad \text{and} \quad q \text{ is not a quadratic residue of } p, \tag{18}$$

or

$$q \mid P_3 \quad \text{and} \quad q \text{ is not a cubic residue of } p. \tag{19}$$

We first investigate the primes 2 and 3.

THEOREM 8. *The prime 2 is not special.*

Proof. Suppose 2 were special. We separate the four cases of Theorem 5.

Let $p = 24n + 1$. Then $(2/p) = 1$. If M were even, then $\chi(2) = 1$, so 2 is a sextic residue of p. Hence M is odd. But Theorem 5 tells us that 2 is exceptional in this case, so 2 is not special.

Next let $p = 24n + 7$. Since $(2/p) = 1$, M is odd as before. In this case D_6 is odd. In fact in the proof of Theorem 5 we showed that P_3 and P_2 are odd. It remains to show that P_1 is odd.

Since $p \equiv 7 \pmod 8$ and M is odd we can write $p + M^2 = 8m$. Also $L + M = 8s$ by (6), so by the last line of Theorem 3 we have, after dividing by 64, that $4P_1 = p[ps^2 + 4m^2]$, so s is even. Let $s = 2\sigma$ so $L + M = 16\sigma$ and $P_1 = p[p\sigma^2 + m^2]$. Therefore we must show that σ and m are of different parity. This follows from the fact that

$$(L + M)^2 = L^2 + M^2 + 2LM = 4p - 26M^2 + 2ML = 256\sigma^2,$$

while $4p + 4M^2 = 32m$. Subtracting these equations and dividing by 2 gives $15M^2 - LM = 16(m - 8\sigma^2)$, but $M^2 + LM = 16M\sigma$. Finally, adding the last two equations and dividing by 16 gives $M^2 \equiv m + M\sigma \pmod 2$, which makes m and σ of different parity, therefore P_1 is odd.

Therefore 2 is not special if $p = 24n + 7$.

Next let $p = 24n + 13$. In this case D_6 is also odd. In fact, since 2 is not exceptional, Theorem 5 tells us that M is odd. Hence P_3 is odd. By Theorem 2, $P_2 = pMB^3/8$, and by (6) $B \equiv f \equiv 2 \pmod 4$. Hence P_2 is odd. That P_1 is odd is seen from the formula

$$27P_1 = p\{L(a^3 - b^3) + 3ab[(9M + L)a + (9M - L)b]/2\},$$

where $8a = L - 11M$ and $8b = L + 13M$, so a and b are of different parity.

Finally, let $p = 24n + 19$. Then $(2/p) = -1$. By Theorem 5 we have M and, therefore, L odd, and by Theorem 2 we have

$$27P_2 = p\left[p^2 - 3p(A/2)^2 + L(A/2)^3\right],$$

which is odd.

To see that P_1 is odd we note that $p + M^2 = 8m + 4$, while $L + M = 8s$. Using the last line of Theorem 3 we have, in this case,

$$4P_1 = p\left[ps^2 + (2m + 1)^2\right],$$

and hence s is odd. Therefore $4P_1 \equiv p(p + 1) \equiv 4 \pmod 8$ and, hence, P_1 is odd.

THEOREM 9. *The prime $q = 3$ is not special.*

Proof. Let $p = 12n + 1$. Then $(3/p) = 1$. By (18), $3 \mid P_1 P_3$. If $3 \mid P_3$, then $3 \mid M$ and, hence, $\chi(3) = 1$, so 3 is a sextic residue of p and is not special. if $3 \nmid P_3$, but divides P_1, then since $3 \nmid M$, Theorem 3 shows that 3 does not divide P_1.

Let $p = 12n + 7$. Then f is odd. By Theorem 6 we have $3 \nmid M$, so $3 \nmid P_3$. By Theorems 2 and 3 we see that, with f odd, $3 \nmid P_1 P_2$. Hence 3 is not special.

To prove that $q > 3$ is not special we need the following lemma.

LEMMA 5. *Let m and $a \neq b \neq c$ be integers and let $d = (a, b, c)$. Let*

$$m\pi_i = ax_i + bx_{i+1} + c \qquad (i = 0, 1, 2),$$

where x_i are the roots of $F_3(x) = x^3 - 3px - pL$. Next let

$$G_3(x) = (x - \pi_0)(x - \pi_1)(x - \pi_2).$$

Then for all integers N the prime factors of $G_3(N)$ are cubic residues of p, except possibly those that divide, $3pmd$.

Proof. This follows from Theorem 5.4 of [7] with the condition on a, b, c being required for Lemma 5.3 of [7].

THEOREM 10. *Let $q > 3$ be a prime $q \neq p$ dividing P_1 and suppose $q \nmid M$. Then q is a sextic residue of p.*

Proof. Of the four cases of Theorem 3, the first is excluded by $q \nmid M$. The third case shows that q is a sextic residue of p by Lemmas 1 and 2. In the remaining two cases q is seen to be a quadratic residue of p by Lemma 1. It remains to show that in the two remaining cases q is also a cubic residue of p. In these cases (15) becomes

$$24\pi_0 = (L - 11M)x_0 - (L + 13M)x_1 \quad (M \text{ odd}, f \text{ even}),$$

and

$$24\pi_0 = (L + M)x_0 + 8Mx_1 + 8p \qquad (M \text{ odd}, f \text{ odd}).$$

Hence, in both cases, $d = 2^\alpha$, since L and M have no odd factor in common. Applying Lemma 5 and using the fact that $P_1 = \pi_0\pi_1\pi_2 = -G_3(0)/m^3$, we see that all the prime factors $q > 3$ of P_1 are indeed sextic residues of p. Hence the theorem.

THEOREM 11. *No prime $q > 3$ is special.*

Proof. Suppose q is a special prime and $q \mid M$. Then by Corollary 1 we have $\chi(q) = 1$. Since q is not exceptional, $(q/p) = 1$ by Theorem 7. Hence q is a sextic residue of p, so q is not special. Hence $q \nmid M$. By Theorem 10 we have $q \nmid P_1$. Also $q \nmid |P_3| = pM^4$. Hence $q \mid P_2$. If f is even, then $q \mid B$ by Theorem 2. But then

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) = \left(\frac{A^2}{q}\right) = 1,$$

which contradicts (18). Hence f is odd. By the last two cases of Theorem 2, q is a sextic residue of p by Lemmas 1 and 2, so q is not special in all cases.

COROLLARY 3. *All semi-exceptional primes are exceptional for $e = 6$.*

APPENDIX I

Cyclotomic matrix for f even.

00	01	02	03	04	05
01	05	12	13	14	12
02	12	04	14	24	13
03	13	14	03	13	14
04	14	24	13	02	12
05	12	13	14	12	01

$\operatorname{ind} 2 \equiv 0 \pmod 3$	$\operatorname{ind} 2 \equiv 2 \pmod 3$
$36(0,0) = p - 17 + 10L$	$72(0,0) = 2p - 34 - 7L - 27M$
$36(0,1) = p - 5 - 2L + 27M$	$72(0,1) = 2p - 10 + 5L + 9M$
$36(0,2) = p - 5 - 2L + 9M$	$72(0,2) = 2p - 10 - 4L - 36M$
$36(0,3) = p - 5 - 2L$	$72(0,3) = 2p - 10 + 5L + 9M$
$36(0,4) = p - 5 - 2L - 9M$	$72(0,4) = 2P - 10 + 5L + 9M$
$36(0,5) = p - 5 - 2L - 27M$	$72(0,5) = 2p - 10 - 4L + 36M$
$36(1,2) = p + 1 + L$	$72(1,2) = 2p + 2 + 2L - 18M$
$36(1,3) = p + 1 + L$	$72(1,3) = 2p + 2 - 7L + 9M$
$36(1,4) = p + 1 + L$	$72(1,4) = 2p + 2 + 2L - 18M$
$36(2,4) = p + 1 + L$	$72(2,4) = 2p + 2 + 2L + 54M$

APPENDIX II

Errata in F. S. Carey, *Notes on the division of the circle*, Quart. J. Pure Applied Math. **26** (1893), 371.

p	for	read	p	for	read
61	−27	+27	103	1773	1373
109	39	135	127	−977	−972
181	13565	1685	151	6547	6543
193	1936	1744	163	21323	5023
	5182	5184	223	−3276	5644
229	−2103	187		−7122	4592
241	594	580	331	84429	84427
373	381	380			
397	4960	−5040			
433	−130032	−1728			
457	3561	3461			

REFERENCES

[1] F. S. Carey, *Notes on the division of the circle*, Quart. Applied Math., **26** (1893), 322–371.
[2] Allan Cunningham, *Quadratic Partitions*, London, 1904, 266 p, Quadratic and Linear Tables, London, 1927, p. 1–87.
[3] L. E. Dickson, *Cyclotomy, higher congruences and Waring's problem*, Amer. J. Math., **57** (1935), 408–410.
[4] Ronald J. Evans, *Period polynomials for generalized cyclotomic periods*, Manuscripta Math., **40** (1982), 217–243.
[5] E. E. Kummer, *Ueber die Divisoren gewisser Formen der Zahlen, welche aus der Theorie der Kreistheilung enstehen*, J. für Math., **30** (1846), 107–116, Collected Papers, v. 1, pp. 193–202, Springer-Verlag, N.Y., 1975.
[6] D. H. and Emma Lehmer, *Multiple sums of cyclotomic numbers*, Utilitas Mathematica, **23** (1983), 223–239.
[7] ______, *The cyclotomy of hyper-Kloosterman sums*, Acta Arith., **14** (1968), 89–111.
[8] Thomas Storer, *Cyclotomy and Difference Sets*, lectures in Advanced Math. Markham Publ. Co. Chicago, 1967.
[9] J. J. Sylvester, *On certain ternary cubic equations*, Amer. J. Math., **2** (1879), 357–381, Collected papers, v. 3, pp. 325–339, p. 314 Cambridge, 1909.
[10] A. L. Whiteman, *The cyclotomic numbers of order* 12, Acta Arith., **6** (1960), 95–111.

Received August 16, 1982.

UNIVERSITY OF CALIFORNIA
BERKELEY, CA 94720