MATHEMATICS OF COMPUTATION
VOLUME 41, NUMBER 164
OCTOBER 1983, PAGES 743-758

Cyclotomy With Short Periods

By D. H. Lehmer and Emma Lehmer

Abstract. This paper develops cyclotomy for periods of lengths 2, 3 and 4 for moduli which are primes and products of two primes.

1. Introduction. Cyclotomy for a prime modulus $p = ef + 1$ goes back to Gauss who defined f-nomial periods η_j in terms of a primitive root g as follows:

$$\eta_j = \sum_{i=0}^{f-1} \zeta_p^{g^{ei+j}}, \quad \text{where } \zeta_p = \exp(2\pi i/p).$$

Although the ordering of the η's depends on the primitive root g, the equation $\psi_p(x) = 0$ of degree e satisfied by the η's is independent of g. In the last half century cyclotomies have been developed for small values of $e \leqslant 30$.

Kummer [4] considered cyclotomy for a composite modulus n in which case ef is Euler's $\varphi(n)$. In general, n will not possess a primitive root g, and a suitable generator must be chosen. In case n is squarefree such a cyclotomy always exists although not uniquely. For references see [7].

This paper is concerned with small values of f rather than e. One of the three possible cyclotomies for $f = 2$ was considered by Sylvester [9] in 1879.

Our interest in the problem for $f = 3$ was rekindled by Daniel Shanks, who was interested in sums of kth powers of the trinomial

$$\eta = \zeta + \zeta^a + \zeta^{a^2}, \quad \text{where } \zeta = \exp(2\pi i/n),\ a^3 \equiv 1 \pmod{n}$$

and its conjugates in connection with some third order recurring sequences used in tests for primality [1]. We noted and proved that $S_k = \Sigma\eta^k$ is independent of the choice of a for $n = pq$, where $p \leqslant q$ are primes and $k < \sqrt{n}$.

This result was presented at the 1981 West Coast Number Theory Conference, where we learned that Gurak [2] has recently considered the period equation $\psi_p(x) = 0$ and the corresponding S_k for p a prime and $f = 2$. Since then he generalized his results to other polynomials and to $n = pq$ in [3].

In this paper we will consider in detail the cases of $f = 2, 3$ and 4 for p and pq and for all values of a for which $a^f \equiv 1 \pmod{pq}$. We will give formulas for the coefficients and for the sums of powers of the roots of the cyclotomic polynomials and for their discriminants.

The several illustrative examples in this paper were computed by an exact technique explained in the final section.

Received February 11, 1982.
1980 *Mathematics Subject Classification*. Primary 10A40.

2. The case $f = 2$. Sylvester [9] took for the periods the real number

$$\theta = \zeta_n + \zeta_n^{-1} = 2\cos(2\pi/n)$$

and its conjugates.

Here we take for the periods the complex number

$$\eta = \zeta_n + \zeta_n^a, \quad \text{where } a^2 \equiv 1 (\operatorname{mod} n)$$

and its conjugates, mentioned briefly in [9, pp. 336–338]. For $n = pq$ the two values of $a \neq -1$ can be characterized by

$$a_1 \equiv \begin{cases} -1 & (\operatorname{mod} p) \\ 1 & (\operatorname{mod} q) \end{cases} \quad \text{and} \quad a_2 \equiv \begin{cases} 1 & (\operatorname{mod} p) \\ -1 & (\operatorname{mod} q). \end{cases}$$

We first look at the sum of the kth powers of the periods. This we denote by $S_k(p)$ in case $n = p$ and $a = -1$. For $n = pq$ we have $S_k(pq, -1)$, $S_k(pq, a_1)$ and $S_k(pq, a_2)$.

THEOREM 1. *If $n = p$, so that $a = -1$ and $f = 2$, we have*

$$S_k(p) = -2^{k-1} + \frac{p}{2} \sum_{\nu \equiv k/2 \,(\operatorname{mod} p)} \binom{k}{\nu}.$$

Proof.

$$2S_k(p) = \sum_{j=1}^{p-1} \left(\zeta_p^j + \zeta_p^{-j}\right)^k = \sum_{\nu=0}^{k} \binom{k}{\nu} \sum_{j=1}^{p-1} \zeta_p^{j(2\nu-k)} = \sum_{\nu=0}^{k} \binom{k}{\nu} [-1 + p\delta_k^{2\nu}],$$

where

$$\delta_k^{2\nu} = \begin{cases} 1 & \text{if } k \equiv 2\nu \,(\operatorname{mod} p), \\ 0 & \text{otherwise.} \end{cases}$$

Hence the theorem follows.

The polynomial whose roots are the periods can be written

$$\psi_p(x) = \prod_{\nu=1}^{e} \left(x - (\zeta_p^\nu + \zeta_p^{-\nu})\right) = x^e + a_1 x^{e-1} + \cdots + a_e. \tag{1}$$

The coefficients a_r are determined from Newton's formulas. Gauss (see [9]) found them explicitly as follows:

$$a_r = (-1)^{[r/2]} \binom{e - [(r+1)/2]}{[r/2]}, \tag{2}$$

where $[y]$ is the greatest integer $\leqslant y$.

The discriminant of $\psi_p(x)$ is $p^{(p-3)/2}$ (Lehmer [5]).

3. The Case $n = pq$. The analogue of Theorem 1 is

THEOREM 2. *If $f = 2$, then*

$$S_k(pq, -1) = 2^{k-1} - \frac{p}{2} \sum_{\mu \equiv k/2 \,(\operatorname{mod} p)} \binom{k}{\mu} - \frac{q}{2} \sum_{\mu \equiv k/2 \,(\operatorname{mod} q)} \binom{k}{\mu} + \frac{pq}{2} \binom{k}{k/2},$$

where $\binom{k}{k/2} = 0$ if k is odd.

Proof. As in Theorem 1 we have

$$2S_k(pq,-1) = \sum_{\nu=0}^{k}\binom{k}{\nu}\sum_{(j,n)=1}\zeta_n^{j(2\nu-k)} = \sum_{\nu=0}^{k}\binom{k}{\nu}A_\nu,$$

where

$$\begin{array}{ll} A_\nu = \mu(n) = \mu(pq) = 1 & \text{if } (2\nu-k,n)=1, \\ A_\nu = -(p-1) & \text{if } p \mid (2\nu-k), q \nmid (2\nu-k), \\ A_\nu = -(q-1) & \text{if } q \mid (2\nu-k), p \nmid (2\nu-k), \\ A_\nu = (p-1)(q-1) & \text{if } pq \mid (2\nu-k). \end{array}$$

Substituting this into $\Sigma_{\nu=0}^{k}\binom{k}{\nu}A_\nu$ gives the theorem.

We next take up the case $S_k(pq,a)$. We may suppose that

$$a \equiv -1 \pmod p \quad \text{and} \quad a \equiv 1 \pmod q,$$

since the second cyclotomy can be obtained by an interchange of p and q.

If a is even, we can replace a by $pq+a$, and therefore we can assume that

$$a+1 = 2\lambda p \quad \text{and} \quad a-1 = 2\mu q.$$

Hence

$$\zeta_{pq} + \zeta_{pq}^{a} = \zeta_{pq}(1+\zeta_p^{2\mu}) = \zeta_{pq}^{1+q\mu}(\zeta_p^{\mu}+\zeta_p^{-\mu}) = \zeta_q^{\lambda}(\zeta_p^{\mu}+\zeta_p^{-\mu}) = \zeta_q^{\lambda}\theta_\mu,$$

since $1+q\mu = 1+(a-1)/2 = (a+1)/2 = \lambda p$. Therefore, with $p' = (p-1)/2$,

$$S_k(pq,a) = \sum_{\lambda=1}^{q-1}\zeta_q^{\lambda k}\sum_{\mu\neq 1}^{p'}\theta_\mu^k = S_k(p)\sum_{\lambda=1}^{q-1}\zeta_q^{\lambda k} = \begin{cases} -S_k(p) & \text{if } q \nmid k, \\ (q-1)S_k(p) & \text{if } q \mid k. \end{cases}$$

By Theorem 1 this gives

THEOREM 3.

$$S_k(pq,a) = \left(2^{k-1} - \frac{p}{2}\sum_{\nu\equiv k/2 \,(\mathrm{mod}\, p)}\binom{k}{v}\right)(1-q\Delta_k^0)$$

where

$$\Delta_k^0 = \begin{cases} 1 & \textit{if } q \mid k, \\ 0 & \textit{otherwise}. \end{cases}$$

COROLLARY. *The first $q-1$ values of $S_k(pq,a)$ and the first $q-1$ coefficients of $\psi_{pq}(a,x)$ do not depend on q so that*

$$S_k(pq_1,a) = S_k(pq_2,a) \quad \textit{for } k < q_1 < q_2,$$

and

$$c_\nu(pq_1) = c_\nu(pq_2) \quad \textit{for } \nu < q_1 < q_2,$$

where $c_\nu(pq)$ are the coefficients of $\psi_{pq}(a,x)$.

THEOREM 4. *Let $\psi_p^{(m)}(y)$ be the polynomial whose roots are the mth powers of the roots of $\psi_p(x)$. Then*

$$(3) \qquad \psi_{pq}(a,x) = \psi_p^{(q)}(x^q)/\psi_p(x).$$

Proof. The roots of $\psi_p(x)\psi_{pq}(a, x)$ are $\theta_\tau\zeta_q^\nu$, $\nu = 0, 1, \ldots, q-1$; $\tau = 1, 2, \ldots, p'$.

The roots of $\psi_p^{(q)}(y)$ are $y = \theta_1^q, \theta_2^q, \ldots, \theta_{p'}^q$.

The roots of $\psi_p^{(q)}(x^q)$ are therefore $x = \theta_\tau\zeta_q^\nu$, $\nu = 0, 1, \ldots, q-1$; $\tau = 1, 2, \ldots, p'$. Hence the theorem follows.

Regarding the coefficients of $\psi_{pq}(a, x)$ we have

THEOREM 5. *Let*

$$(4) \qquad \psi_{pq}(a, x) = \sum_{k=0}^{d} c_k x^{d-k}, \qquad d = \varphi(pq)/2 = p'(q-1),$$

$$\psi_p^{(m)}(x) = \sum_{s=0}^{p'} a_s^{(m)} x^{p'-s}.$$

Then the coefficients c_r *satisfy the recurrence*

$$(5) \qquad c_r = \sum_{s=1}^{p'} (-1)^{1+[s/2]} \binom{p'+1-s}{[s/2]} c_{r-s} + a_{r/q}^{(q)},$$

where $a_t^{(q)} = 0$ *if* t *is not an integer.*

Proof. By Theorem 4 we can write

$$\psi_p(x)\psi_{pq}(a, x) = \psi_p^{(q)}(x^q).$$

Identifying the coefficients of $x^{p'q-r}$ on both sides and using (2),we obtain (5).

Another expression for c_r coming out of Theorem 4 is

THEOREM 6. *Let*

$$\left[x^{p'}\psi_p(1/x)\right]^{-1} = \sum_{n=0}^{\infty} b_n x^n.$$

Then

$$c_r = b_r + a_1^{(q)} b_{r-q} + a_2^{(q)} b_{r-2q} + \cdots.$$

Proof. This follows from (3) and (4). Thus Theorem 6 gives an easy way to get the coefficients of $\psi_{pq}(a, x)$ once the coefficients b_n have been computed.

THEOREM 7. *If* $n_1 = pq_1$ *and* $n_2 = pq_2$ *for two primes* $q_1 < q_2$, *then the two polynomials* $\psi_{pq_1}(a, x)$ *and* $\psi_{pq_2}(a, x)$ *have the same* q_1 *first and last coefficients and moreover*

$$(6) \qquad S_k(pq_1, a) = S_k(pq_2, a) = S_k(p) \quad \textit{for } 0 < k < q_1.$$

Proof. By (5) with $k < q_1$, c_r does not depend on q, so the first q_1 coefficients are the same for $\psi_{pq_1}(a, x)$ and $\psi_{pq_2}(a, x)$. If we replace x by $1/x$ in (3) and multiply both sides by $x^{p'(q-1)}$, this has the effect of reversing the order of the coefficients in all three polynomials in (6). The first q coefficients of $x^{p'(q_1-1)}\psi_{pq_1}(a, x^{-1})$ and of $x^{p'(q_2-1)}\psi_{pq_2}(a, x^{-1})$ are now the last q coefficients of $\psi_{pq_1}(a, x)$ and $\psi_{pq_2}(a, x)$, and the theorem follows from Theorem 3.

We note that Eq. (6) is an example of a solution of the multigrade Terry-Escott problem [6] in cyclotomic integers.

In the special case of $p = 3$, $\psi_3(x) = x + 1$ and by (3)

$$\psi_{3q}(a, x) = (x^q + 1)/(x + 1) = Q_q(-x)$$

whose roots are $-\zeta_q^\nu$.

In case $p = 5$, $p' = 2$ and $\psi_5(x) = x^2 + x - 1$,

$$\psi_5^{(q)}(x^q) = x^{2q} + L_q x^q - 1, \quad \text{where } L_q = \left(\left(1 + \sqrt{5}\right)/2\right)^q + \left(\left(1 - \sqrt{5}\right)/2\right)^q$$

and (5) becomes

$$c_r = -c_{r-1} + c_{r-2} + \begin{cases} L_q & \text{if } k = q, \\ 0 & \text{otherwise.} \end{cases}$$

Thus the coefficients of $\psi_{5q}(a, x)$ are

$$1, -1, 2, -3, 5, \ldots, F_{q-1}, F_q, F_{q-1}, F_{q-2}, \ldots, 3, 2, 1, 1,$$

where F_n is the nth Fibonacci number. This was done for a general q in Lehmer [8].

In case $p = 7$, $p' = 3$,

$$\psi_7(x) = x^3 + x^2 - 2x - 1, \quad \text{and} \quad \psi_7^{(q)}(x^q) = x^{3q} + a_1^{(q)}x^{2q} + a_2^{(q)}x^q - 1,$$

where

$$a_1^{(q)} = -S_q(7) = 2^{q-1} - \frac{7}{2} \sum_{\nu \equiv q/2 (\mathrm{mod}\ 7)} \binom{q}{\nu}.$$

$$2a_2^{(q)} = \left(a_1^{(q)}\right)^2 - S_{2q}(7).$$

By (5)

$$c_r = -c_{r-1} + 2c_{r-2} + c_{r-3} + \begin{cases} a_1(q) & \text{if } k = q, \\ a_2^{(q)} & \text{if } k = 2q. \end{cases}$$

For small values of q the $a_1^{(q)}$ and $a_2^{(q)}$ are tabulated below together with a few of the polynomials $\psi_{pq}(a, x)$. It will be noticed that the constant term is equal to one. This follows from (2) and the fact that the product of the roots of $\psi_{pq}(a, x)$ is the same as the product of the roots of $\psi_p(x)$.

q	$a_1^{(q)}$	$a_2^{(q)}$
3	4	-11
5	16	-57
11	639	-7372
13	2094	-37221
17	22220	-948823
19	72220	-4790529

$$\psi_{15}(4, x) = x^4 - x^3 + 2x^2 + x + 1,$$

$$\psi_{21}(13, x) = x^6 - x^5 + 3x^4 + 5x^2 - 2x + 1,$$

$$\psi_{35}(6, x) = x^{12} - x^{11} + 3x^{10} - 4x^9 + 9x^8 + 2x^7 + 12x^6 + x^5 + 25x^4 - 11x^3 + 5x^2 - 2x + 1,$$

$$\psi_{77}(34, x) = x^{30} - x^{29} + 3x^{28} - 4x^{27} + 9x^{26} - 14x^{25} + 28x^{24} - 47x^{23} + 89x^{22}$$
$$-155x^{21} + 286x^{20} + 132x^{19} + 285x^{18} + 265x^{17} + 437x^{16} + 378x^{15}$$
$$+761x^{14} + 432x^{13} + 1468x^{12} + 157x^{11} + 3211x^{10} - 1429x^{9} + 636x^{8}$$
$$-283x^{7} + 126x^{6} - 56x^{5} + 25x^{4} - 11x^{3} + 5x^{2} - 2x + 1,$$

$$\psi_{91}(27, x) = x^{36} - x^{35} + 3x^{34} - 4x^{33} + 9x^{32} - 14x^{31} + 28x^{30} - 47x^{29} + 89x^{28}$$
$$-155x^{27} + 286x^{26} - 507x^{25} + 924x^{24} + 442x^{23} + 899x^{22} + 909x^{21}$$
$$+1331x^{20} + 1386x^{19} + 2185x^{18} + 1918x^{17} + 3838x^{16} + 2183x^{15}$$
$$+7411x^{14} + 793x^{13} + 16212x^{12} - 7215x^{11} + 3211x^{10} - 1429x^{9}$$
$$+636x^{8} - 283x^{7} + 126x^{6} - 56x^{5} + 25x^{4} - 11x^{3} + 5x^{2} - 2x + 1.$$

The discriminant of Sylvester's $\psi_{pq}(x)$ is known to be $p^{(p-2)(q-1)/2}q^{(p-1)(q-2)/2}$ (Lehmer [5]). The discriminant of $\psi_{pq}(a, x)$ cannot be given explicitly since it may contain other factors besides p and q. However, we have the following theorem.

THEOREM 8. *The discriminant* Δ *of* $\psi_{pq}(a, x)$ *is divisible by* $p^{(p-3)(q-1)/2}q^{(q-2)(p-1)/2}$.

Proof. Among the differences of the roots in

$$\prod\left(\theta_{\nu_1}\zeta^{j_1} - \theta_{\nu_2}\zeta^{j_2}\right), \qquad \begin{cases} j = 1,2,\ldots,q-1, \\ \nu = 1,2,\ldots,p', \end{cases}$$

there are two special cases:

Case I. If $\nu_1 = \nu_2$, the product $\prod\theta_\nu(\zeta^{j_1} - \zeta^{j_2})$ is the discriminant of $Q_q(x)$ raised to the power p', since $|\prod\theta_\nu| = 1$. Hence $q^{(q-1)p'}$ divides Δ.

Case II. If $j_1 = j_2$, then the product is the discriminant of $\psi_p(x)$ raised to the power $q - 1$, since the product $\prod\zeta^i = 1$. Therefore Δ is also divisible by $p^{(p-3)(q-1)/2}$. Hence the theorem.

The following table gives the discriminants of $\psi_{pq}(a, x)$ and the factors supplied by the theorem.

Polynomial	| Discriminant |	Theorem 8
$\psi_{15}(4, x)$	$2^2 3^2 5^2$	$3^2 5^2$
$\psi_{15}(11, x)$	5^3	5^3
$\psi_{21}(8, x)$	7^5	7^5
$\psi_{21}(13, x)$	$3^3 7^4 13^2$	$3^3 7^4$
$\psi_{35}(6, x)$	$5^9 7^8 181^6$	$5^9 7^8$
$\psi_{35}(29, x)$	$5^6 7^{10} 13^{10}$	$5^6 7^{10}$

We note that the constant term of these polynomials is always 1. This follows from the fact that e is even and, since

$$\eta = \zeta_{pq} + \zeta_{pq}^{a} = -\zeta_{pq}\left(-1 - \zeta_{pq}^{a-1}\right),$$

the product over all conjugates gives

$$N\left(\zeta_{pq} + \zeta_{pq}^{a}\right) = Q_{pq}(-1) = \left.\frac{(x^{pq} - 1)(x - 1)}{(x^{p} - 1)(x^{q} - 1)}\right|_{x=-1} = 1.$$

3. The Case $f = 3$. For this section we will need the following simple lemma.

LEMMA. *Let $f(x, y) = (k - 3(x+y)/2)^2 + 3(x-y)^2/4$. Then inside and on the boundary of the triangle formed by the vertices $(0, k)$, $(0,0)$, and $(k,0)$ we have*

$$\max f(x, y) = k^2.$$

Proof. It is easily seen that

$$f(0,k) = f(0,0) = f(k,0) = k^2.$$

Next we see that

$$\frac{\partial^2 f}{\partial x^2} = \frac{\partial^2 f}{\partial y^2} = 6. \tag{7}$$

Therefore, inside the triangle, $f(x, y)$ does not attain a maximum. On the interior of the sides (7) still holds, so that $f(x, y)$ has no maximum there either. Hence $f(x, y)$ attains its maximum k^2 at the vertices of the triangle. Hence the Lemma.

We begin our discussion with the case of $n = p = 3e + 1$. The periods are in this case

$$\eta = \zeta_p + \zeta_p^a + \zeta_p^{a^2}$$

and its conjugates. Here a is either one of the two solutions of

$$a^2 + a + 1 \equiv 0 \pmod{p}.$$

We first look at the sum $S_k(p)$ of the kth powers of the periods.

THEOREM 9. *If $k < \sqrt{p}$, then*

$$S_k(p) = \begin{cases} -3^{k-1} + \frac{p}{3}\binom{3m}{m}\binom{2m}{m} & \text{if } k = 3m, \\ -3^{k-1} & \text{otherwise.} \end{cases}$$

Proof. We have

$$\eta^k = \left(\zeta_p + \left(\zeta_p^a + \zeta_p^{a^2}\right)\right)^k = \sum_{\nu=0}^{k} \zeta_p^\nu \binom{k}{\nu}\left(\zeta_p^a + \zeta_p^{a^2}\right)^{k-\nu}$$

$$= \sum_{\nu=0}^{k}\binom{k}{\nu}\sum_{\lambda=0}^{k-\nu}\binom{k-\nu}{\lambda}\zeta_p^{\nu + a\lambda + a^2(k-\lambda-\nu)}.$$

Replacing ζ by ζ^j ($j = 1, 2, \ldots, p-1$) and summing over j, we get

$$3S_k = \sum_{\nu=0}^{k}\binom{k}{\nu}\sum_{\lambda=0}^{k-\nu}\binom{k-\nu}{\lambda}\sum_{j=1}^{p-1}\zeta_p^{j(\nu + a\lambda + a^2(k-\lambda-\nu))}. \tag{8}$$

The value of the inner sum over j is

$$\begin{cases} p - 1 & \text{if } p \mid \nu + a\lambda + a^2(k-\lambda-\nu), \\ -1 & \text{otherwise.} \end{cases}$$

Since

$$\sum_{\nu=0}^{k}\binom{k}{\nu}\sum_{\lambda=0}^{k-\nu}\binom{k-\nu}{\lambda} = \sum_{\nu=0}^{k}\binom{k}{\nu}2^{k-\nu} = 3^k,$$

we have

$$3S_k(p) = -3^k + pT_k, \tag{9}$$

where

$$T_k = \sum_{\nu=0}^{k} \binom{k}{\nu} \sum_{\lambda=0}^{k-\nu} \binom{k-\nu}{\lambda}, \qquad \nu + a\lambda + a^2(k-\nu-\lambda) \equiv 0 \pmod{p}.$$

The condition under the summation, using the fact that $a^3 = 1 \pmod{p}$ and $a^2 + a + 1 \equiv 0 \pmod{p}$, can be replaced by

$$\begin{aligned} \lambda &\equiv a(\nu + k/(a-1)) \quad &(\text{mod } p) \\ &\equiv a\nu - (a-1)k/3 \quad &(\text{mod } p) \end{aligned}$$

or

$$a(3\nu - k) \equiv (3\lambda - k) \quad (\text{mod } p).$$

Cubing both sides, we have

$$(3\nu - k)^3 - (3\lambda - k)^3 \equiv 0 \pmod{p}.$$

That is

$$p \mid (\nu - \lambda) \quad \text{or} \quad f(\nu, \lambda) \equiv 0 \pmod{p},$$

where $f(\nu, \lambda)$ is the function defined in the lemma. Using the lemma and the fact that $\nu < k$, $\lambda < k$ and the assumption that $k < \sqrt{p}$, it follows that p cannot divide either $\nu - \lambda$ or $f(\nu, \lambda)$ except when $\nu = \lambda$ or $f(\nu, \lambda) = 0$. The vanishing of $f(\nu, \lambda)$ implies $\nu = \lambda$ and $k = 3\nu$. Therefore T_k consists of a single term and in fact is

$$T_k = \binom{k}{k/3}\binom{k-k/3}{k/3} = \begin{cases} \binom{3m}{m}\binom{2m}{m} & \text{if } k = 3m, \\ 0 & \text{otherwise.} \end{cases}$$

The theorem now follows from (9).

Theorem 9 now allows us to calculate the first $\sqrt{p}$ coefficients c_k of

$$\psi_p(a, x) = \sum_{k=0}^{e} c_k x^{e-k}$$

by means of Newton's formula

$$kc_k = \sum_{\nu=1}^{k} S_\nu(p) c_{k-\nu}. \tag{10}$$

The first nine coefficients which are valid for all primes $p = 3e + 1 > L_k$ are tabulated below:

k	c_k	L_k
0	1	
1	1	
2	2	
3	$-(2p - 14)/3$	
4	$-(2p - 35)/3$	7
5	$-(4p - 91)/3$	13
6	$(2p^2 - 73p + 728)/9$	13
7	$(2p^2 - 115p + 1976)/9$	31
8	$(4p^2 - 272p + 5434)/9$	43
9	$-(4p^3 - 354p^2 + 11298p - 135850)/81$	43

The coefficients c_k for $k = 0$ to 5 were given by Gurak [2]. He also proved that c_k is a polynomial in p of degree $[k/3]$. We can sharpen this result by giving

THEOREM 10. *If* $k < \sqrt{n}$ *then*

$$c_k = b_k p^{[k/3]} + O(p^{[k/3]-1}),$$

where $b_{3m} = b_{3m+1} = b_{3m+2}/2 = (-2/3)^m/m!$.

The proof is by triple induction using (9). The first few polynomials and their discriminants are as follows:

p	a	$\psi_p(x)$
7	2	$x^2 + x + 2$
13	3	$x^4 + x^3 + 2x^2 - 4x + 3$
19	7	$x^6 + x^5 + 2x^4 - 8x^3 - x^2 + 5x + 7$
31	5	$x^{10} + x^9 + 2x^8 - 16x^7 - 9x^6 - 11x^5 + 43x^4 + 6x^3 + 63x^2 + 20x + 25$
37	10	$x^{12} + x^{11} + 2x^{10} - 20x^9 - 13x^8 - 19x^7 + 85x^6 + 51x^5 + 94x^4 - 2x^3 - 13x^2 - 77x + 47$
43	6	$x^{14} + x^{13} + 2x^{12} - 24x^{11} - 17x^{10} - 27x^9 + 143x^8 + 81x^7 + 83x^6 - 209x^5 + 163x^4 + 88x^3 + 235x^2 - 168x + 79$

p	$\lvert\Delta_p\rvert$
7	7
13	$3^2 13^3$
19	$7^2 11^2 19^5$
31	$5^{14} 31^9 67^2$
37	$37^{11} 47^2 149^2 211^2 223^2 433^2$
43	$43^{13} 79^2 251^2 307^2 337^2 823^2 1033^2$

For $n = pq$, where p and q are primes of the form $6m + 1$ the periods are

$$\eta = \zeta_{pq} + \zeta_{pq}^{a} + \zeta_{pq}^{a^2} \tag{11}$$

and its conjugates. Here a is a solution of $a^3 \equiv 1 \pmod{pq}$. There are four solutions with $a \not\equiv 1 \pmod{p}$. If a is replaced by $a^2 \pmod{pq}$ then (11) remains unaltered. Hence there are just two values of a available, a_1 and a_2 such that $a_1^2 \not\equiv a_2 \pmod{pq}$. For example if $pq = 91$, the four solutions are 9, 16, 74 and 81 (mod 91). We can take $a_1 = 9$ and $a_2 = 16$. Without loss of generality we can choose p to be that prime for which

$$a_1 \equiv a_2 \pmod{p} \quad \text{and} \quad a_1 \equiv a_2^2 \pmod{q}. \tag{12}$$

We begin by considering the sum $S_k(pq, a)$ of the kth powers of the periods for $a = a_1$ and $a = a_2$. If we examine the proof of Theorem 9 and replace p by pq, we find that (8) becomes

$$3S_k(pq, a) = \sum_{\substack{\nu=0 \\ \lambda=0}}^{\infty} \binom{k}{\nu}\binom{k-\nu}{\lambda} \sum_{(j,pq)=1} \zeta_{pq}^{j\tau(a,\nu,\lambda)}, \tag{13}$$

where

$$\tau(a, \nu, \lambda) = \nu + a\lambda + a^2(k - \nu - \lambda) \equiv 2\nu + \lambda - k + a(2\lambda + \nu - k) \pmod{pq}.$$

Now take $a = a_1$ and $a = a_2$. It is easily verified from (12) that

$$\tau(a_1, \nu, \lambda) \equiv \tau(a_2, \nu, \lambda) \pmod{p},$$
$$a_1\tau(a_1, \nu, \lambda) \equiv a_2\tau(a_2, \lambda, \nu) \pmod{q},$$

and

$$\binom{k}{\nu}\binom{k-\nu}{\lambda} = \binom{k}{\lambda}\binom{k-\lambda}{\nu};$$

hence we have by (13)

THEOREM 11.

$$S_k(pq, a_1) \equiv S_k(pq, a_2) \pmod{pq}.$$

We can strengthen this theorem for $k < \sqrt{pq}$ as follows:

THEOREM 12. *If $k < \sqrt{pq}$, then $S_k(pq, a_1) = S_k(pq, a_2)$.*

Proof. The actual difference between $S_k(pq, a_1)$ and $S_k(pq, a_2)$ can arise only in the cases in which

$$\tau(a, \nu, \lambda) \equiv 0 \pmod{pq}.$$

Replacing p by pq in the last part of the proof of Theorem 9, we find that if $k < \sqrt{pq}$, the only contribution occurs when $k = 3m$ and $\nu = \lambda = m$, and that this contribution is

$$\binom{3m}{m}\binom{2m}{m}$$

which does not depend on the value of a_1 and a_2. The theorem follows.

COROLLARY. *The first $\sqrt{pq}$ coefficients of $\psi_{pq}(a_1, x)$ are the same as those of $\psi_{pq}(a_2, x)$. These two polynomials are congruent modulo pq by Theorem* 11.

Proof. This follows from Newton's formula (10).

We next give an example of Theorem 12 for $pq = 91$. We let

$$9 \mid D_k = S_k(91, 9) - S_k(91, 16) \quad \text{and} \quad 9 \mid d_k = c_k(91, 9) - c_k(91, 16)$$

k	$S_k(91,9)$	D_k	$c_k(91,16)$	d_k
1	1	0	-1	0
2	3	0	-1	0
3	151	0	-49	0
4	-1	0	51	0
5	-54	0	60	0
6	2331	0	800	0
7	-468	0	-855	0
8	-2153	0	-1148	0
9	43207	0	-5098	0
10	-17022	0	5795	0
11	-59135	11	8093	1
12	864911	0	12180	-1

13	-505842	0	-16002	-1
14	-1515336	1092	-18667	29
15	18108456	0	-14901	-27
16	-14114393	-4368	30577	-291
17	-37682369	49504	1760	163
18	390775617	-18	-13345	483
19	-376953425	-260338	-13354	296
20	-918400306	1705440	28188	-334
21	8616559263	-3990	19047	-474
22	9736808331	10147137	8804	-54
23	-22043146317	51482970	-4089	129
24	192976186783	-425040	2367	2

4. The Case $f = 4$. If p is a prime, then the solutions of

$$a^4 \equiv 1 \pmod{p} \quad \text{with } a \not\equiv \pm 1 \pmod{p}$$

are $\pm a$, where $a^2 \equiv -1 \pmod{p}$. Therefore the periods are

$$\eta = \zeta_p + \bar{\zeta}_p + \zeta_p^a + \bar{\zeta}_p^a \tag{14}$$

and their conjugates. Now

$$\begin{aligned} \eta^k &= \sum_{\nu=0}^{k} (\zeta_p + \bar{\zeta}_p)^\nu \binom{k}{\nu} (\zeta_p^a + \bar{\zeta}_p^a)^{k-\nu} \\ &= \sum_{\nu=0}^{k} \binom{k}{\nu} \sum_{r=0}^{\nu} \binom{\nu}{r} \zeta_r^{2r-\nu} \sum_{s=0}^{k-\nu} \binom{k-\nu}{s} \zeta_p^{a(2s-k+\nu)} \\ &= \sum_{\nu=0}^{k} \sum_{r=0}^{\nu} \sum_{s=0}^{k-\nu} \binom{k}{\nu} \binom{\nu}{r} \binom{k-\nu}{s} \zeta_p^{2r-\nu+a(2s-k+\nu)}. \end{aligned} \tag{15}$$

Summing η^k over its conjugates, we get

$$4S_k(p, a) = \sum_{\nu=0}^{k} \sum_{r=0}^{\nu} \sum_{s=0}^{k-\nu} \binom{k}{\nu} \binom{\nu}{r} \binom{k-\nu}{s} \left[-1 + p\delta_{2r-\nu}^{a(k-\nu-2s)}\right],$$

where

$$\delta_i^j = \begin{cases} 1 & \text{if } i \equiv j \pmod{p}, \\ 0 & \text{otherwise.} \end{cases}$$

Since

$$\sum_{\nu=0}^{k} \sum_{r=0}^{\nu} \sum_{s=0}^{k-\nu} \binom{k}{\nu} \binom{\nu}{r} \binom{k-\nu}{s} = 4^k,$$

we have

THEOREM 13. *If* $f = 4$ *and* p *is a prime, then*

$$4S_k(p, a) = -4^k + pV_k,$$

where

$$V_k = \sum_{\nu=0}^{k} \sum_{r=0}^{\nu} \sum_{s=0}^{k-\nu} \binom{k}{\nu} \binom{\nu}{r} \binom{k-\nu}{s}, \qquad 2r - \nu \equiv a(k - \nu - 2s) \pmod{p}.$$

It remains to evaluate V_k. Although we cannot do this in general we have the following theorem.

THEOREM 14. *If* $k < \sqrt{p}$, *then*

$$S_k = -4^{k-1} + \begin{cases} \frac{p}{4}\binom{k}{k/2}^2 & \text{if } k \text{ is even}, \\ 0 & \text{otherwise}. \end{cases}$$

Proof. The condition under the sum defining V_k when squared becomes

$$(\nu - 2r)^2 + (k - \nu - 2s)^2 \equiv 0 \pmod{p}. \tag{16}$$

Since $0 \leqslant r \leqslant \nu$ and $0 \leqslant s \leqslant k - \nu$, the largest value of $(\nu - 2r)^2 + (k - \nu - 2s)^2$ with ν fixed is obtained with $r = 0$ and $s = 0$. The largest value of $\nu^2 + (k - \nu)^2$ is obtained for $\nu = 0$ or k and is in fact k^2. But $p > k^2$. Hence the only way to meet condition (16) is to have $\nu = 2r$ and $k - \nu = 2s$. If k is odd, then ν is odd, but $\nu = 2r$. Hence the condition is contradictory and so

$$V_k = 0 \quad \text{if } k \text{ is odd}.$$

When k is even and $\nu = 2r$ we have

$$V_k = \sum_{r=0}^{k/2} \binom{k}{2r}\binom{2r}{r}\binom{k-2r}{k/2-r} = \binom{k}{k/2} \sum_{r=0}^{k/2} \binom{k/2}{r}^2 = \binom{k}{k/2}^2.$$

Hence the theorem.

The coefficients can now be obtained from Newton's formulas and as in the case of $f = 3$ can be expressed as polynomials in p of degree $[k/2]$. The first few coefficients are

k	c_k	
1	1	
2	$-(p - 5)/2$	
3	$-(p - 15)/2$	
4	$(p^2 - 28p + 195)/8$	
5	$(p^2 - 48p + 663)/8$	$(p > 13)$
6	$-(p^3 - 69p^2 + 1655p - 13923)/48$	$(p > 13)$
7	$-(p^3 - 99p^2 + 3599p - 49725)/48$	$(p > 37)$

The first few polynomials for $f = 4$ are given below:

p	$\psi_p(x)$
5	$x + 1$
13	$x^3 + x^2 - 4x + 1$
17	$x^4 + x^3 - 6x^2 - x + 1$
29	$x^7 + x^6 - 12x^5 - 7x^4 + 28x^3 + 14x^2 - 9x + 1$
37	$x^9 + x^8 - 16x^7 - 11x^6 + 66x^5 + 32x^4 - 73x^3 - 7x^2 + 7x + 1$
41	$x^{10} + x^9 - 18x^8 - 13x^7 + 91x^6 + 47x^5 - 143x^4 - 7x^3 + 72x^2 - 23x + 1$
53	$x^{13} + x^{12} - 24x^{11} - 19x^{10} + 190x^9 + 116x^8 - 681x^7 - 246x^6 + 738x^5$ $+215x^4 - 291x^3 - 68x^2 + 10x + 1$

61 $x^{15} + x^{14} - 28x^{13} - 23x^{12} + 276x^{11} + 182x^{10} - 1193x^9 - 592x^8$
$+2307x^7 + 956x^6 - 1721x^5 - 908x^4 + 316x^3 + 262x^2 + 42x + 1$
73 $x^{18} + x^{17} - 34x^{16} - 29x^{15} + 435x^{14} + 311x^{13} - 2671x^{12} - 1551x^{11}$
$+8348x^{10} + 3867x^9 - 13106x^8 - 4608x^7 + 9365x^6 + 1994x^5 - 2859x^4$
$-250x^3 + 224x^2 + 32x + 1$

The corresponding discriminants are as follows:

p	Δ_p
13	13^2
17	$2^2 17^3$
29	$17^2 29^6$
37	$31^2 37^8 43^2$
41	$-3^6 41^9 83^2$
53	$23^4 53^{12} 83^2 317^2 719^2$
61	$11^{10} 61^{14} 599^2$
73	$-3^6 73^{17} 557^2 1459^2 3797^2 5693^2 9463^2$

Just as in the case of $f = 2$, these polynomials for $f = 4$ all have constant term 1. This follows from

$$\eta = \zeta_{pq} + \zeta_{pq}^{a} + \zeta_{pq}^{-1} + \zeta_{pq}^{-a} = \zeta^{-a}(-1 - \zeta^{a-1})(-1 - \zeta^{a+1})$$

so that $N(\eta) = Q_{pq}^2(-1) = 1$.

We next take up the case of $n = pq$, where $p \equiv q \equiv 1 \pmod 4$ are distinct primes. We now have two values of a, say a_1 and a_2, with $a_1 \not\equiv -a_2$ for which

$$a^2 \equiv -1 \pmod{pq}, \quad \text{with } a \not\equiv \pm 1 \pmod{pq}.$$

We can choose p to be that prime for which

$$(17) \qquad a_1 - a_2 \equiv 0 \pmod p \quad \text{and} \quad a_1 + a_2 \equiv 0 \pmod q.$$

For example, if $pq = 65$, we can choose $a_1 = 8$ and $a_2 = 18$, $p = 5$, $q = 13$.

THEOREM 15. *For all values of k*

$$S_k(pq, a_1) \equiv S_k(pq, a_2) \pmod{pq}.$$

Proof. If we examine the proof of Theorem 13, we see that (15) holds when p is replaced by pq, that is

$$(18) \qquad 4S_k(pq, a) = \sum_{\nu, r, s} \binom{k}{\nu}\binom{\nu}{r}\binom{k-\nu}{s} \sum_{(j, pq)=1} \zeta^{j\tau(a,\nu,r,s)},$$

where $\tau(a, \nu, r, s) = 2r - \nu + a(2s + \nu - k)$.

Letting $a = a_1$ and a_2, we find from (17) that

$$(19) \qquad \begin{aligned} \tau(a_1, \nu, r, s) &\equiv \tau(a_2, \nu, r, s) && \pmod p, \\ a_1\tau(a_1, \nu, r, s) &\equiv -\tau(a_2, k - \nu, s, r) && \pmod q \end{aligned}$$

and that

$$\binom{k}{\nu}\binom{\nu}{r}\binom{k-\nu}{s}$$

is unaltered by the substitution

$$\begin{pmatrix} \nu, r, s \\ k - \nu, s, r \end{pmatrix}.$$

Hence $S_k(pq, a_1) \equiv S_k(pq, a_2)$ modulo p and modulo q.

THEOREM 16. *If $k < \sqrt{pq}$, then*

$$S_k(pq, a_1) = S_k(pq, a_2).$$

Proof. Since the inner sum in (18) depends only on whether $\tau(a, \nu, r, s)$ is prime to pq, divisible by p or q or pq, most of the terms in (18) are not changed when a_1 is replaced by a_2. In fact by (19) it is only when

$$\tau(a, \nu, r, s) \equiv 0 \pmod{pq}$$

for a_1 or a_2 that any change occurs. By (16) we have

$$(\nu - 2r)^2 + (k - \nu - 2s)^2 \equiv 0 \pmod{pq}.$$

But since

$$(\nu - 2r)^2 + (k - \nu - 2s)^2 < k^2,$$

it follows that since $k^2 < pq$

$$\nu = 2r \quad \text{and} \quad k - \nu = 2s. \tag{20}$$

If we assume that

$$\tau(a_1, \nu, r, s) \equiv 0 \pmod{pq} \quad \text{and} \quad \tau(a_2, \nu, r, s) \not\equiv 0 \pmod{pq},$$

then $\nu - 2r \not\equiv 0 \pmod{p}$. But this contradicts (20). Hence in (18) $\tau(a, \nu, r, s)$ makes the same contribution in (18) for $a = a_1$ and $a = a_2$.

Theorem 16 implies that the leading $\sqrt{pq}$ coefficients of the two polynomials $\psi_{pq}(a_1, x)$ and $\psi_{pq}(a_2, x)$ are the same. Moreover, the two polynomials are congruent modulo pq by Theorem 15. We illustrate this by giving $\psi_{65}(8, x)$ and $\psi_{85}(13, x)$ and the differences between the polynomials for the two values of a.

$$\begin{aligned} \psi_{65}(8, x) = x^{12} - x^{11} - 25x^{10} + 25x^9 + 196x^8 - 170x^7 - 571x^6 \\ +350x^5 + 586x^4 - 170x^8 - 90x^2 - x + 1, \\ \psi_{65}(18, x) - \psi_{65}(8, x) = 65x^2(x - 1), \\ \psi_{85}(13, x) = x^{16} - x^{15} - 33x^{14} + 33x^{13} + 392x^{12} - 375x^{11} - 2107x^{10} \\ +1886x^9 + 5305x^8 - 4506x^7 - 5677x^6 + 5235x^5 + 1412x^4 \\ -2398x^3 + 732x^2 - 69x + 1, \\ \psi_{85}(38, x) - \psi_{85}(13, x) = -85x(5x^4 - 5x^3 - 11x^2 + 10x - 1). \end{aligned}$$

The discriminants of these polynomials are

$$\begin{aligned} \Delta_{65}(8) &= 2^{18}5^{13}13^{11}577^2853^2, \\ \Delta_{65}(18) &= 5^9 13^{11}47^4 827^2 863^2, \\ \Delta_{85}(13) &= 5^{12}13^{16}17^{15}157^4 1871^2, \\ \Delta_{85}(38) &= 5^{12}13^2 17^{15}47^2 293^2 463^4 557^2 7603^2. \end{aligned}$$

5. Computational Methods. The routines employed in the calculation of S_k, $\psi_n(x)$ and Δ_n are based on the representation of the cyclotomic integer

$$A_1\zeta_n + A_2\zeta_n^2 + \cdots + A_n\zeta_n^n$$

by the vector

$$(A_1, A_2, \ldots, A_n).$$

This vector is reduced when $A_n = 0$, and the reduction is accomplished by simply writing the replacement instruction

$$A_j = A_j - A_n \qquad (j = 1(1)n).$$

Rational integers are recognized by having all their components A_j for $j \leqslant n$ equal to each other when $n = p$, the value of the integer being $-A_1$. For $n = pq$, the condition is that there be three sets of equal components represented by A_p, A_q and A_1, the value of the rational integer in this case being $A_1 - A_p - A_q$. The period such as

$$\eta = \zeta + \zeta^a + \zeta^{a^2} + \zeta^{a^3},$$

for example, is simply a very sparse vector, and so is the difference between two periods. The multiplication of a normalized cyclotomic integer by a period (or by the difference between two periods) is reduced to the adding or subtracting of the components of the first vector. This can be done in very few operations on a parallel machine.

The polynomial $\psi_n(x)$ is the eth term of the sequence $G_1(x)$, $G_2(x)$, $G_3(x)$ formed recursively by

$$G_0(x) = 1, \qquad G_k(x) = (x - \eta)G_{k-1}(x).$$

This method of producing a polynomial from its roots is very much cheaper than the use of symmetric functions, especially when the multiplication method just described is employed.

To calculate $S_k(n, a)$, using only addition, one uses the multiplication algorithm described above to produce η^k from η^{k-1} and then adds the corresponding components.

To compute the discriminant Δ_n of $\psi_n(x)$ use was made of the factorization

$$\Delta_n = P_1P_2 \cdots P_{e-1},$$

where P_j is the norm of the difference between η and one of its conjugates.

Department of Mathematics
University of California
Berkeley, California 94720

1. William Adams & Daniel Shanks, "Strong primality tests that are not sufficient," *Math. Comp.*, v. 39, 1982, pp. 255–300.

2. S. Gurak, "Minimal polynomials for Gauss circulants and cyclotomic units," *Pacific J. Math.*, v. 102, 1982, pp. 347–353.

3. S. Gurak, "Minimal polynomials for circular numbers." (To appear).

4. E. E. Kummer, *Theorie der idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln der Gleichung $w^n = 1$ gebildet sind, wenn n eine zusammengesetzte Zahl ist*, Collected Papers, Vol. 1, Springer-Verlag, Berlin and New York, 1975, pp. 583–629.

→ D. H. Lehmer, "An extended theory of Lucas functions," *Ann. of Math.*, v. 52, 1930, pp. 293–304.

6. D. H. Lehmer, "The Terry-Escott problem," *Scripta Math.*, v. 13, 1947, pp. 37–41.

7. D. H. Lehmer & Emma Lehmer, *Cyclotomy for Non-Squarefree Moduli*, Lecture Notes in Math., Vol. 899, Springer-Verlag, Berlin and New York, 1981, pp. 276–300.

8. D. H. Lehmer & Emma Lehmer, "Properties of polynomials having Fibonacci numbers for coefficients," *Fibonacci Quart*, v. 21, 1983, pp. 62–64.

9. J. J. Sylvester, "On certain ternary cubic equations," *Collected Papers*, Vol. 3, Cambridge, 1909, pp. 325–339; *Amer. J. Math.*, v. 2, 1879, pp. 357–381.