MATHEMATICS OF COMPUTATION
VOLUME 48, NUMBER 177
JANUARY 1987, PAGES 211-216

Cyclotomic Resultants

By D. H. Lehmer and Emma Lehmer

Dedicated to Daniel Shanks on his 70th birthday

Abstract. This paper examines the eth power character of the divisors of two cyclotomic period polynomials of degree e_1 and e_2. The special cases $e_1 = 2$ and $e_2 = 3$, 4, are considered in detail. As corollaries one finds new conditions for cubic and quartic residuacity.

The computational method consists in representing cyclotomic numbers in the form $c_1\zeta + c_2\zeta^2 + \cdots + c_{p-1}\zeta^{p-1}$, where $\zeta = e^{2\pi i/p}$. Multiplication is reduced to addition and subtraction, which are carried out in a multi-precision system.

The Gaussian f-nomial periods η_i for a prime $p = ef + 1$ can be written

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

where $\zeta = e^{2\pi i/p}$ and g is a primitive root of p. The periods are roots of a monic polynomial of degree e with integer coefficients,

$$\psi_e(x) = \prod_{i=0}^{e-1}(x - \eta_i) = x^e + x^{e-1} + c_2x^{e-2} + \cdots + c_e. \tag{2}$$

It is well known that the discriminant D_e of ψ_e splits into $e - 1$ factors, where

$$D_e = \prod_{i<j=0}^{e-1}(\eta_i - \eta_j)^2 = \prod_{k=1}^{e-1} P_k \tag{3}$$

and

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

Kummer [3] showed that all the prime factors of the numbers represented by $\psi_e(x)$ are eth power residues of p, except those that divide P_k for $(k, e) > 1$. The primes that divide D_e and are not eth power residues of p are called *exceptional* if they divide $\psi_e(x)$ for some integer x.

This also holds for a generalized cyclotomy in which η_i is replaced by

$$\theta_j = \sum_{i=0}^{e-1} \varepsilon_i \eta_i, \tag{4}$$

where $\varepsilon_i = 0$, 1 or -1.

Received February 28, 1986.
1980 *Mathematics Subject Classification*. Primary 12A35.

Another cyclotomic invariant which does not appear to have been studied before is the resultant $R(e_1, e_2)$ of two period polynomials ψ_{e_1} and ψ_{e_2} for the same prime $p = ef + 1$, where e is the least common multiple of e_1 and e_2. By definition,

$$R(e_1, e_2) = \prod_{i=0}^{e_1 - 1} \psi_{e_2}(\eta'_i) \tag{5}$$

or, what is the same thing,

$$R(e_1, e_2) = \prod_{i=0}^{e_1 - 1} \prod_{j=0}^{e_2 - 1} (\eta'_i - \eta''_j), \tag{6}$$

where η'_i and η''_j are the roots of $\psi_{e_1}(x)$ and $\psi_{e_2}(x)$. The following theorem is an analogue of (3).

Theorem 1. *Let e_1 and e_2 be two distinct divisors of $p - 1$. Let e be the least common multiple and δ be the greatest common divisor of e_1 and e_2. Let $R(e_1, e_2)$ be the resultant of $\psi_{e_1}(x)$ and $\psi_{e_2}(x)$ as defined in* (5). *Then*

$$R(e_1, e_2) = \prod_{\lambda=0}^{\delta - 1} R_\lambda(e_1, e_2), \tag{7}$$

where

$$R_\lambda(e_1, e_2) = \prod_{i=0}^{e_1 - 1} \prod_{n=1}^{e_2/\delta} F_\lambda(i, n) \tag{8}$$

and where

$$F_\lambda(i, n) = \sum_{k=1}^{e_2/\delta} \eta_{i+ke_1} - \sum_{m=1}^{e_1/\delta} \eta_{i+\lambda+n\delta+me_2} \tag{9}$$

and where η_ν are the roots of $\psi_e(x)$. The factors $R_\lambda(e_1, e_2)$ are rational integers.

Proof. We arrange the factors of (6) so that R is the product of those subsets of $\eta_i - \eta_j$ for which

$$j \equiv i + \lambda \pmod{\delta} \qquad (i = 0, 1, \ldots, \delta - 1).$$

Then we use the identities

$$\eta'_\nu = \sum_{k=1}^{e_1/\delta} \eta_{\nu+ke_1}, \qquad \eta''_\nu = \sum_{m=1}^{e_2/\delta} \eta_{\nu+me_2}.$$

This proves (8). To prove that $R(e_1, e_2)$ is a rational integer, we rearrange the factors $F(i, n)$ in (8) into a linear array as follows. Let

$$\theta_0^{(\lambda)} = F_\lambda(0, 0) = \sum_{k=0} \eta_{ke_1} - \sum_{m=0} \eta_{\lambda+me_2}.$$

Then we define $\theta_\nu^{(\lambda)}$ by

$$\theta_\nu^{(\lambda)} = \sum_{k=0} \eta_{\nu+ke_1} - \sum_{m=0} \eta_{\nu+\lambda+me_2}.$$

We see that

$$\theta_\nu^{(\lambda)} = \sum \varepsilon_j \eta_j \qquad (\varepsilon_j = 0, 1, -1),$$

so that all the $\theta_j^{(\lambda)}$ satisfy the generalized cyclotomic polynomial $\psi_e^{(\lambda)}(x)$. Then

$$|R_\lambda(e_1, e_2)| = \psi_e^{(\lambda)}(0)$$

is a rational integer. □

COROLLARY. *Let e be the least common multiple of e_1 and e_2. Then the prime factors of $R_\lambda(e_1, e_2)$ that do not divide pe are eth power residues of p, except possibly those which divide*

$$(10) \qquad P_k^{(\lambda)} = \prod_{i=0}^{e-1} \left(\theta_i^{(\lambda)} - \theta_{i+k}^{(\lambda)}\right)$$

for some k not prime to e.

We next consider two extreme cases in which $\delta = 1$ and $\delta = e/2$.

Case I. Let e_1 and e_2 be coprime. Then $\delta = 1$, $e = e_1 \cdot e_2$ and hence

$$R(e_1, e_2) = R_0(e_1, e_2) = \prod_{i=0}^{e_1 - 1} \psi_{e_2}(\eta_i')$$

by (5).

For example, let $e_1 = 2$ and $e_2 = 3$ and

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

If we substitute

$$\eta_i' = \begin{cases} (-1 \pm \sqrt{p})/2 & \text{if } p = 12n + 1, \\ (-1 \pm \sqrt{-p})/2 & \text{if } p = 12n + 7 \end{cases}$$

into the cyclotomic cubic [1],

$$\psi_3(x) = x^3 + x^2 - \frac{p-1}{3}x - \frac{p(L+3) - 1}{27} = \prod_{i=0}^{2} (x - \eta_i''),$$

we obtain, with $c = -[p(L+3) - 1]/27$,

$$(11) \qquad 4R(2,3) = \begin{cases} \left(2c + \frac{p-1}{12}\right)^2 - p\left(\frac{p-1}{12}\right)^2 & \text{if } p = 12n + 1, \\ \left(2c + \frac{7p-1}{12}\right)^2 + p\left(\frac{7p-1}{12}\right)^2 & \text{if } p = 12n + 7. \end{cases}$$

$R(2,3)$ is then the constant term of a sextic $\psi_6^*(x)$ whose roots are

$$\theta_i = \eta_{i+2} - \eta_{i+3} + \eta_{i+4}.$$

All the divisors of $R(2,3)$ are sextic residues of p unless they divide P_2^* or P_3^* for $\psi_6^*(x)$. But

$$P_2^* = \prod_{i=0}^{5} (\theta_i - \theta_{i+2}) = \prod_{i=0}^{2} (\eta_{i+2}'' - \eta_i'')^2 = D_3 = p^M$$

and

$$P_3^* = \prod_{i=0}^{5} (\theta_i - \theta_{i+3}) = \left(\sqrt{p}\right)^6 = p^3.$$

Therefore, if a prime q divides $R(2,3)$, q is a sextic residue of p unless q divides M. But it is well known that all the prime factors of M are cubic residues of p. The form (11) for $R(2,3)$ tells us that every divisor of R is a quadratic residue of p. Hence $R(2,3)$ has no exceptional divisors.

We note that $R(2,3)$ increases very rapidly with p. Thus for $p = 307$

$$R(2,3) = 2475149 = 17 \cdot 19 \cdot 79 \cdot 97,$$

and all the prime factors of $R(2,3)$ are sextic residues of 307.

Case II. If $e_1 = 2e_2 = e$, then $\delta = e/2$ and (8) becomes

$$R_\lambda\left(\frac{e}{2}, e\right) = \prod_{i=0}^{e-1} (\eta_i + \eta_{i+e/2} - \eta_{i+e/2+\lambda}), \tag{12}$$

so that if $\lambda = 0$ then $\theta_i^{(0)} = \eta_i$ and

$$R_0\left(\frac{e}{2}, e\right) = \prod_{i=0}^{e-1} \eta_i = \psi_e(0).$$

This generates an interesting family of $e/2$ generalized period polynomials which includes $\psi_e(x)$.

If e is a prime, then only $P_2^{(\lambda)}$ and $P_{e/2}^{(\lambda)}$ have to be examined for possible divisors which are not eth power residues of p.

In the simplest case of $e = 4$, $p = a^2 + b^2$, $a \equiv 1 \pmod 4$, there are two cases: $p = 8n + 1$ and $p = 8n + 5$.

It is well known that [1]

$$256R_0(2,4) = \begin{cases} \left[(p-1)^2 - 4p(a-1)^2\right] & \text{if } p \equiv 1 \pmod 8, \\ \left[(3p+1)^2 - 4p(a-1)^2\right] & \text{if } p \equiv 5 \pmod 8) \end{cases}$$

and that $P_2^{(0)} = pb^2$. We find similarly that

$$256R_1(2,4) = \begin{cases} \left[(7p+1)^2 - 4p(a+3)^2\right] & \text{if } p \equiv 1 \pmod 8, \\ \left[(11p+1)^2 - 4p(a+3)^2\right] & \text{if } p \equiv 5 \pmod 8, \end{cases}$$

and since by (12)

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

we have

$$P_2^{(1)} = \prod_{i=0}^{3} (\theta_i^{(1)} - \theta_{i+2}^{(1)}) = \prod_{i=0}^{3} (\eta_i - \eta_{i+2}) = P_2 = pb^2.$$

Therefore, by the corollary to Theorem 1, any exceptional divisors of R_0 or R_1 must divide b. But for $p = 8n + 1$ all the divisors of b are quartic residues of p. For $p = 8n + 5$ the primes of the form $4m + 3$ dividing b may be only quadratic residues of p[2, 4]. They must appear to at least the second power in $R_\lambda(2, 4)$.

For example, for $p = 1789$, $a = 5$, $b = 42$, we find

$$R_0(2,4) = 112113 = 3^2 \cdot 12457,$$

$$R_1(2,4) = 1511111 = 7^2 \cdot 30839.$$

Both 3 and 7 are quartic nonresidues of 1789. Hence they are exceptional primes.

In considering these resultants it is important to be able to compute numerical examples with any given value of p, e_1 and e_2. With today's narrow computing machines and the very considerable size of the resultants, a nonconventional method of computing is called for.

The key to the problem is the cylotomic field $Q(\zeta)$.

We recall that

$$\zeta = \exp(2\pi i/p) \quad \text{and} \quad \sum_{\nu=0}^{p-1} \zeta^\nu = 0.$$

The general element of the field is of the form

$$\alpha = c_0 + c_1\zeta + \cdots + c_{p-1}\zeta^{p-1},$$

where the c's are rational integers. The unique reduced representative of α is

$$\alpha = k_1\zeta + k_2\zeta^2 + \cdots + k_{p-1}\zeta^{p-1},$$

where $k_i = c_i - c_0$. If

$$(13) \qquad \beta = j_1\zeta + j_2\zeta^2 + \cdots + j_{p-1}\zeta^{p-1},$$

then $\alpha = \beta$ if and only if $k_i = j_i$ because of the irreducibility of $1 + x + x^2 + \cdots + x^{p-1}$.

We can easily recognize when α is a rational integer n. Indeed, in the representation (13), $\alpha = n$ if and only if $k_1 = k_2 = \cdots = k_{p-1} = -n$.

Similarly, we can recognize numbers of the form

$$\alpha = A + B\sqrt{(-1)^{(p-1)/2}p},$$

where A and B are rational integers. The components k_i have just two values. Those with subscripts that are quadratic residues of p are equal to $B - A$, and those with nonresidue subscripts are equal to $-(A + B)$. By recognizing this phenomenon we cut the running time in two.

In practice we use the redundant vector

$$(c_0, c_1, \ldots, c_{p-1})$$

of dimension p to represent elements of the field. We perform vector operations on such vectors, including reduction.

Let

$$\sigma = (a_0, a_1, \ldots, a_{p-1}) \quad \text{and} \quad \tau = (b_0, b_1, \ldots, b_{p-1})$$

be two arbitrary elements. Then

$$\sigma + \tau = (a_0 + b_0, a_1 + b_1, \ldots, a_{p-1} + b_{p-1}),$$

$$\sigma\tau = (c_0, c_1, \ldots, c_{p-1}),$$

where

$$(14) \qquad c_i = \sum_{j+k \equiv i \ (\mathrm{mod}\ p)} a_j b_k.$$

We see from (1) that

$$\eta_i = \sum_{j=0}^{p-1} d_j\zeta^j,$$

where $d_j = 0$ or 1. In fact, η_i is represented by the reduced vector

$$\eta_i = (0, d_1, \ldots, d_{p-1}).$$

This is a sparse vector since only 1 in e of its components differs from 0.

In calculating $R_\lambda(e_1, e_2)$ in Theorem 1 we have to consider the product of factors $F_\lambda(i, n)$ defined by (9). If we write

$$F_\lambda(i, n) = \sum_{k=1}^{p-1} b_k\zeta^k,$$

then $b_k = 0, 1$ or -1. This means that in all the multiplications by $F_\lambda(i, n)$ in arriving at $R_\lambda(e_1, e_2)$ in (8), terms of the summation (14) can be replaced by additions or subtractions.

Since the resultants can be large, it becomes necessary to employ some sort of multi-precision system to perform addition and subtraction. The simplest scheme is to write the components of the vectors to base 2^{15} (for a machine with 15-bit words) and use subroutines to add and subtract. This assures the calculation does not overflow and it maintains the exactness of the result, despite the narrowness in the arithmetic unit.

We give below a table showing all the resultants for $p = 31$. The factors of the various R's are given in parentheses.

e	e_1	e_2	$R(e_1, e_2)$ for $p = 31$.
6	2	3	$(2^4 \cdot 157)$
6	2	6	$(2^2 \cdot 47)(2^{11})$
6	3	6	$(2^5)(2^{10})(2 \cdot 1163)$
10	2	5	$(5 \cdot 41603)$
10	2	10	$(5^2)(5 \cdot 7193)$
10	5	10	$(5^2)(5 \cdot 1307)(5^5)(5^3 \cdot 149)(5 \cdot 2113)$
15	3	5	(-33851)
15	3	15	$(11719)(-2417)(1352777)$
15	5	15	$(1)(10169)(61^2)(-1301)(61^2)$
30	2	15	$(311 \cdot 2031970151441)$
30	2	30	$(373 \cdot 12535147973)(683 \cdot 310120586219)$
30	3	10	$(1613 \cdot 581458693)$
30	3	30	$(311 \cdot 3091817)(37201 \cdot 428297)(1303 \cdot 1427 \cdot 36767)$
30	5	6	$(27529 \cdot 12724447)$
30	5	30	$(1946801)(418700509)(4985483)(311 \cdot 406907)(1303 \cdot 19531)$
30	6	10	$(2737397093)(1448203937)$
30	6	15	$(11719 \cdot 41479)(373 \cdot 22674083)(100926391799)$
30	6	30	$(1155247)(89653)(5688390013)(471614347)$ $(110043677)(311 \cdot 374047)$
30	10	15	$(5953)(2^5 \cdot 571331)(2^5 \cdot 373.71549)(8091683)(1427 \cdot 1861)$
30	10	30	$(1)(464939)(2^5 \cdot 22259)(2^5 \cdot 311^2)(38069)(1907617)$ $(5537593)(46439)(62497)(20781781)$
30	15	30	$(1)(38069)(2^5 \cdot 1489)(27901)(5953)(34721)$ $(5953)(20089)(5^3 \cdot 1117)(2^5 \cdot 311)(46439)$ $(2^5 \cdot 683)(16741)(6263)$.

All the primes in this table are eth power residues of 31, except 2 and 5 which divide e. Hence $R(e_1, e_2)$ has no exceptional divisors for $p = 31$.

Department of Mathematics
University of California
Berkeley, California 94720

1. PAUL BACHMANN, *Die Lehre von der Kreistheilung*, B. G. Teubner, Leipzig, 1872, pp. 210–213, 224–230.

2. RONALD J. EVANS, "The octic period polynomial," *Proc. Amer. Math. Soc.*, v. 87, 1983, pp. 389–393.

3. E. E. KUMMER, "Über die Divisoren gewisser Formen der Zahlen welche aus der Theorie der Kreistheilung entstehen," *J. Reine Angew. Math.*, v. 30, 1846, pp. 107–116, Collected papers, v. 1, pp. 193–239.

4. J. J. SYLVESTER, "On the multisection of roots of unity," *Johns Hopkins Univ. Circular*, v. 1, 1881, pp. 150–151, Collected papers, v. 3, pp. 477–478.