PACIFIC JOURNAL OF MATHEMATICS
Vol. 152, No. 1, 1992

NOTE ON THE DISCRIMINANT OF CERTAIN CYCLOTOMIC PERIOD POLYNOMIALS

JOHN BRILLHART

In this note we determine the discriminant of the period polynomial for certain binomial periods in the nth cyclotomic field, where $n = pq$ and p, q are distinct, odd primes.

1. Introduction. The binomial cyclotomic periods η_j for an odd prime p are defined as

$$(1) \qquad \eta_j = \theta_j = \zeta^j + \zeta^{-j}, \qquad 1 \le j \le \frac{p-1}{2},$$

where $\zeta = \zeta_p$ denotes a primitive pth root of unity, which in the standard Gaussian notation is the case where $e = (p-1)/2$ and $f = 2$. The associated period polynomial is defined to be

$$(2) \qquad \Psi_p(x) = \prod_{j=1}^{\frac{p-1}{2}} (x - \theta_j) = x^e + a_1 x^{e-1} + \cdots + a_e,$$

where

$$a_k = (-1)^{[\frac{k}{2}]} \binom{e - [\frac{k+1}{2}]}{[\frac{k}{2}]}, \qquad 1 \le k \le e.$$

(Here we use θ_j when η_j is real. The square bracket is the greatest integer function.)

The formula for the discriminant of this polynomial is

$$(3) \qquad D(\Psi_p(x)) = p^{\frac{p-3}{2}}.$$

It is also useful to introduce the polynomial

$$(4) \qquad \Psi_p^{(m)}(x) = \prod_{j=1}^{\frac{p-1}{2}} (x - \theta_j^m), \qquad m \ge 0.$$

(See [**4**] for references to the above.)

In [**4**], the Lehmers investigated the period polynomial for another species of binomial period, the case where $n = pq$, p and q being distinct, odd primes. As in the prime case, $\zeta = \zeta_n$ denotes a primitive nth root of unity and $f = 2$. Here $e = \phi(n)/2 = (p-1)(q-1)/2$.

To define the periods in this case, first solve the congruence $x^2 \equiv 1 \pmod{n}$ for the two values of $x = a \not\equiv \pm 1 \pmod{n}$. (Sylvester [7] had investigated the case in which $a \equiv -1 \pmod{n}$.) In what follows, we will only treat the case where $a \equiv -1 \pmod{p}$ and $a \equiv 1 \pmod{q}$ as in [**4**]. (The other case is the same with the values of p and q interchanged.) Then the binomial periods $\eta_j(a)$ are defined by

$$(5) \qquad \eta_j(a) = \zeta^j + \zeta^{aj}, \qquad 1 \le j \le \tfrac{n-1}{2}, \ (j, n) = 1,$$

and the associated period polynomial is

$$(6) \qquad \Psi_n(a, x) = \prod_{\substack{j=1 \\ (j,n)=1}}^{\frac{n-1}{2}} (x - \eta_j(a)).$$

Also established is the useful formula

$$(7) \qquad \Psi_n(a, x) = \Psi_p^{(q)}(x^q)/\Psi_p(x).$$

(Observe that the polynomial division on the right is exact.) It is also shown in [**4**] that $D(\Psi_n(a, x))$ is divisible by the product $p^{(p-3)(q-1)/2} q^{(p-1)(q-2)/2}$.

This note had its origin in the observation that when the quotient

$$D(\Psi_n(a, x))/p^{\frac{(p-3)(q-1)}{2}} q^{\frac{(p-1)(q-2)}{2}}$$

was computed for small values of p and q, it was always found to be a power of some integer. In what follows, we will prove that this is true in general by showing that the quotient is actually $(U_q^{(p)})^{2q-4}$, where the integer $U_q^{(p)}$ is a particular function of the θ_i's, a function mentioned by E. Lucas in [**6**, p. 317]. Unfortunately, Lucas never fully discussed these and related functions before his tragic and untimely death in 1891 or explained their uses in developing the properties of a certain species of elliptic-like functions he claimed he had discovered and their connection with Fermat's Last Theorem. (See Bell [**1**].)

The multiplicative properties of the resultant were used in this note, instead of the more usual direct arguments based on the discriminant defined in terms of the roots, because this "exterior" approach gives the results almost automatically when the discriminant is computed in terms of the resultant using (7). (The form of (12) was originally found in this way.)

2. The discriminant formula. In the following derivation we will use some of the familiar properties of the discriminant and the resultant. (See [7, pp. 279-289], [2, p. 51].)

Let $f(x) = a_0x^r + \cdots + a_r$ and $g(x) = b_0x^s + \cdots + b_s$, $r, s \geq 1$. Then it is not difficult to prove that

$$(8)\quad D(f(g(x))) = (-1)^{r\binom{s}{2}} a_0^{s-1} b_0^{r(rs-s-1)} [D(f)]^s R(f(g(x)), g'(x)),$$

from which we get the special case

$$(9)\qquad D(f(x^s)) = (-1)^{r\binom{s}{2}} (a_0a_r)^{s-1} s^{rs} [D(f)]^s, \qquad s \geq 1.$$

We will also need the following

LEMMA. *Let* $h(x) = c_0x^k + \cdots + c_k$, $k \geq 1$, *and suppose that* $f(x) = g(x)h(x)$ *has no multiple zeros. Then*

$$(10)\qquad D\left(\frac{f}{g}\right) = b_0^2 \frac{D(f)D(g)}{R^2(f', g)}.$$

Proof. Since f has no multiple zero, we have that $0 \neq D(f) = D(g)D(h)R^2(g, h)$, so

$$(11)\qquad D(h) = \frac{D(f)}{D(g)R^2(g, h)}.$$

Also, $f'(x) = g(x)h'(x) + g'(x)h(x)$, so, if α_i are the (distinct) zeros of $g(x)$, then $f'(\alpha_i) = g'(\alpha_i)h(\alpha_i)$. Since $g'(\alpha_i) \neq 0$,

$$\begin{aligned} R(g, h) &= b_0^k \prod_{i=1}^{n} h(\alpha_i) = b_0^k \prod_{i=1}^{s} \frac{f'(\alpha_i)}{g'(\alpha_i)} = \frac{b_0^k \prod_{i=1}^{s} f'(\alpha_i)}{(-1)^{\frac{s(s-1)}{2}} b_0^{2-s} D(g)} \\ &= \frac{(-1)^{\frac{s(s-1)}{2}} b_0^{s+k-2} \prod_{i=1}^{s} f'(\alpha_i)}{D(g)} = \frac{(-1)^{\frac{s(s-1)}{2}} R(g, f')}{b_0 D(g)}. \end{aligned}$$

(Note deg $f' = s + k - 1$.) Substituting this result into (11) gives (10). □

THEOREM 1.

$$(12)\qquad D(\Psi_n(a, x)) = (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{(p-3)(q-1)}{2}} q^{\frac{(p-1)(q-2)}{2}} (U_q^{(p)})^{2q-4},$$

where

$$U_q^{(p)} = \prod_{1\le i<j\le \frac{p-1}{2}} \left(\frac{\theta_j^q - \theta_i^q}{\theta_j - \theta_i}\right)$$

is a rational integer.

Proof. Since $\Psi_n(a, x) = \Psi_p^{(q)}(x^q)/\Psi_p(x)$, then (10) gives

$$D(\Psi_n(a, x)) = \frac{D(\Psi_p(x))D(\Psi_p^{(q)}(x^q))}{[R(\Psi_p(x), (\Psi_p^{(q)}(x^q))')]^2}.$$

In the numerator, $D(\Psi_p(x)) = p^{(p-3)/2}$ by (3), and using (9) with $s = q$ and $r = (p-1)/2$,

$$D(\Psi_p^{(q)}(x^q)) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} q^{q(\frac{p-1}{2})}[D(\Psi_p^{(q)}(x))]^q.$$

In the denominator, the second argument in the resultant will have the factor qx^{q-1} because of the chain rule. Thus, we can use the multiplicativity of the resultant to obtain:

(13) $$\begin{aligned} &R(\Psi_p(x), (\Psi_p^{(q)}(x^q))') \\ &\quad = R(\Psi_p(x), qx^{q-1})R\left(\Psi_p(x), \frac{(\Psi_p^{(q)}(x^q))'}{qx^{q-1}}\right) \\ &\quad = R(\Psi_p(x), qx^{q-1})R(\Psi_p^{(q)}(x), (\Psi_p^{(q)}(x))'). \end{aligned}$$

Now, using the properties in [2, p. 51],

$$R(\Psi_p(x), qx^{q-1}) = q^{\frac{p-1}{2}}[\Psi_p(0)]^{q-1} = q^{\frac{p-1}{2}}.$$

Thus, (13) becomes

$$R(\Psi_p(x), (\Psi_p^{(q)}(x^q))') = q^{\frac{p-1}{2}} D(\Psi_p^{(q)}(x)).$$

Substituting these results in (11) gives:

(14) $$D(\Psi_n(a, x)) = (-1)^{\frac{(p-1)(q-1)}{4}} p^{\frac{p-3}{2}} q^{\frac{(p-1)(q-2)}{2}} [D(\Psi_p^{(q)}(x))]^{q-2}.$$

But

$$\begin{aligned} D(\Psi_p^{(q)}(x)) &= \prod_{1\le i<j\le \frac{p-1}{2}} (\theta_j^q - \theta_i^q)^2 \\ &= \prod_{1\le i<j\le \frac{p-1}{2}} (\theta_j - \theta_i)^2 \prod_{1\le i<j\le \frac{p-1}{2}} \left(\frac{\theta_j^q - \theta_i^q}{\theta_j - \theta_i}\right)^2 \\ &= D(\Psi_p(x))(U_q^{(p)})^2 = p^{\frac{p-3}{2}}(U_q^{(p)})^2. \end{aligned}$$

Substituting this result into (14) gives the theorem. Note that $U_q^{(p)}$ is symmetric in the θ's, so it is a rational integer. □

In [**5**] the Lehmers published the special case when $p = 5$, i.e. when $n = 5q$. They observed in this case that the polynomial $P_n(x) = \Psi_n(a, x)$ has the Fibonacci numbers F_n as their coefficients. They also established that $5^{n-1}n^{2n-4}$ divides $D(P_n(x))$. In [**3**] we proved that the discriminant in this case has the simple formula

$$D(P_n(x)) = 5^{n-1}n^{2n-4}F_n^{2n-4}.$$

References

[1] E. T. Bell, *Analogies between the U_n, V_n of Lucas and elliptic functions*, Bull. Amer. Math. Soc., **29** (1923), 401-406.

[2] J. Brillhart, *On the Euler and Bernoulli polynomials*, J. Reine Angew. Math., **234** (1969), 45-64.

[3] ——, *Letter to the Editor*, Fibonacci Quart., **21** (1983), 259.

[4] D. H. and Emma Lehmer,*Cyclotomy with short periods*, Math. Comp., **41** (1983), 743-758.

[5] ——, *Properties of polynomials having Fibonacci numbers for coefficients*, Fibonacci Quart., **21** (1983), 62-64.

[6] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., **1** (1878), 184-240, 289-321.

[7] J. J. Sylvester, *On certain ternary cubic equations*, Collected Papers, vol. 3, Cambridge, 1904; Amer. J. Math., **2** (1879), 357-381.

[8] J. V. Uspensky, *Theory of Equations*, McGraw-Hill, New York, 1948.

Received May 9, 1990 and in revised form February 10, 1991.

University of Arizona
Tucson, AZ 85721