THE OCTIC PERIOD POLYNOMIAL

RONALD J. EVANS

Abstract. The coefficients and the discriminant of the octic period polynomial $\psi_{8}(z)$ are computed, where, for a prime $p = 8f + 1$, $\psi_{8}(z)$ denotes the minimal polynomial over $\mathbb{Q}$ of the period $(1/p)\sum_{n=1}^{p-1} \exp(2\pi in^8/p)$. Also, the finite set of prime octic nonresidues (mod $p$) which divide integers represented by $\psi_{8}(z)$ is characterized.

1. Introduction. In this paper we extend certain results of E. Lehmer in [7]. Let $p = 8f + 1$ be prime, and define the Gauss sum $G_e$ of order $e$ by

$$G_e = \sum_{n=1}^{p} \exp(2\pi in^e/p).$$

Let $F_e(z)$ denote the minimal polynomial of $G_e$ over $\mathbb{Q}$, so that $F_e(z)$ has degree $e$. Let $\psi_e(z)$ denote the minimal polynomial over $\mathbb{Q}$ of the Gauss period $\eta_0 = (G_e - 1)/e$. Then $\psi_e(z)$, the period polynomial of order $e$, equals

$$\psi_e(z) = e^{-eF_e(ex + 1)}.$$ 

Explicit determinations of the coefficients of $F_e(z)$ have been made for all $e \leq 6$; see [2] for references, and also [5] for $e = 6$.

In §2, we determine the coefficients of $F_e(z)$, and hence of $\psi_e(z)$, in terms of $p$, $C$, and $X$, where

$$(1) \quad p = 8f + 1 = X^2 + Y^2 = C^2 + 2D^2, \quad C \equiv X \equiv 1 \pmod{4}.$$ 

The discriminant of $\psi_{8}(z)$ is computed in §3. A theorem of Kummer [7, p. 436; 4, p. 197] shows that the set $E_p$ of odd prime $e$th power nonresidues (mod $p$) which divide integers represented by $\psi_e(z)$ is a subset of the set of divisors of the discriminant of $\psi_e(z)$. (A generalization of Kummer's theorem, in which $p$ is replaced by any composite $n > 0$, is proved in [3].) In §4, we prove that for $e = 8$, $E_p$ consists precisely of the odd prime nonoctic quartic residues (mod $p$) which divide $DY$. A characterization of $E_p$ for $e = 4$ was known to Sylvester [9, p. 392]. It is given in the Appendix. Further results of this type are proved in [3, §§3–5].

We will generally merely sketch proofs, omitting a number of lengthy calculations. The formulas for the discriminant and coefficients of the period polynomial have been double-checked by computer for primes $p = 8f + 1 < 200$.
We are indebted to E. Lehmer for many helpful comments. Also, the counsel of J. Sutton has been helpful.

2. Determination of \( F_8(z) \). Define

\[
E = (-1)^f
\]

and

\[
N = 1 \text{ or } -1, \text{ according as } 2 \text{ is quartic or not (mod } p).\]

A special case of the following theorem is given in [7, (33)].

**Theorem 1.** In the notation of (1)–(3),

\[
F_8(z) = z^8 + 4p(-3 - 4E)z^6 - 16p(A_1 - 2A_3)z^5
\]

\[
+ 2p(A_0 + 2pA_2^2 - 8A_2^2 + 16A_4)z^4
\]

\[
- 32p(pA_1A_2 + A_4A_5 + A_3)z^3 + 4p(pA_1A_2 + 8A_3A_5 + 16pA_1^2 - 4A_2^2)z^2
\]

\[-16p(pA_0A_1 - 2A_3A_4)z + p(pA_0^3 - 16A_3^2),\]

where

\[
A_0 = p(9 - 24E + 16N) - 16XC(1 + E - N) + 4X^2 + 8C^2,
\]

\[
A_1 = X(1 - 2N) + 2C(E - N),
\]

\[
A_2 = 1 - 4E,
\]

\[
A_3 = 2pC(2 - 3E + 2N) - pX(1 + 4E - 4N) - 2XC^2,
\]

\[
A_4 = p(1 + 4E - 4N) - 4NCX,
\]

\[
A_5 = X + 2EC.
\]

**Proof.** Define

\[
S = \sqrt{p}, \quad R = \sqrt{2p - 2SX}, \quad R_1 = \sqrt{2p + 2SX},
\]

\[
U = 2E(S - C)(2S + ENR), \quad U_1 = 2E(S + C)(2S - ENR_1),
\]

\[
V = 2E(S - C)(2S - ENR), \quad V_1 = 2E(S + C)(2S + ENR_1).
\]

It follows from [1, Theorem 3.18] and Galois theory that the eight conjugates of \( G_8 \) over \( \mathbb{Q} \), i.e., the eight zeros of \( F_8(z) \), are given by

\[
S + R \pm \sqrt{U}, \quad S - R \pm \sqrt{V},
\]

\[
- S + R_1 \pm \sqrt{U_1}, \quad - S - R_1 \pm \sqrt{V_1}.
\]

The four numbers in (4) are the conjugates of \( G_8 \) over \( \mathbb{Q}(S) \). From (4), one easily finds the quartic irreducible polynomial \( E_S(z) \) of \( G_8 - S \) over \( \mathbb{Q}(S) \). Then \( F_8(z) \) can be computed by the formula \( F_8(z) = E_S(z - S)E_{-S}(z + S) \). In this way, calculations with the numbers in (5) can be avoided.
3. The discriminant of $\psi_8(z)$. In the notation of (1)-(3), define

$$J = (4N - 2)CX - C^2 - X^2 + 4p(1 + N - 2E) + 4DY(2N - E - 1)$$

and

$$K = 2Y(3D^2 + 2pE - 2pN) + 4D(2pE - 2pN - p + CX),$$

where the choices of $Y$ and $D$ in (6) must be the same as those in (7).

**Theorem 2.** The discriminant $\Delta$ of $\psi_8(z)$ is $\Delta = B_2B_3B_4p^7$, where

$$B_4 = 2^8Y^2D^4, \quad B_3 = 2^{-16}(pJ^2 - K^2),$$

$$B_2 = 2^{-12}Y^2((2p - 2pE - D2)^2 - p(X + C - 2EC)^2),$$

and $B_1$ is obtained from $B_3$ by replacing $Y$ by $-Y$ (or, equivalently, $D$ by $-D$).

**Proof.** The eight zeros of $\psi_8(z)$ are the periods

$$\eta_k = \sum_{v=1}^{\infty} \exp(2\pi i g^8v + k/p) \quad (k = 0, 1, \ldots, 7),$$

where $g$ is a primitive root of $p$. Thus $\Delta = P_2P_3P_4$, where $P_r = \prod_{k=0}^{7}(\eta_k - \eta_{r+k})$.

It remains to prove that

$$P_r = pB_r \quad (r = 1, 2, 3, 4).$$

It is easy to verify (8) for $r = 2, 4$ with use of (4). Suppose that $r = 1$ or 3. One can compute $\eta_0 - \eta_r$ from (4) and (5). Then $P_r$, the norm of $\eta_0 - \eta_r$ from $Q(\eta_0)$ to $Q$, can be found by successively computing the norm first down to $Q(R)$, then down to $Q(S)$, and then down to $Q$. The computations are facilitated by use of the formula

$$4\sqrt{U_1} = 2D(R - R_1 + 2ENS).$$

4. Prime factors of $\psi_8(n)$. Let $G_p$ denote the infinite set of odd primes which divide $\psi_8(n)$ for some $n$. Let $E_p$ denote the set of octic nonresidues (mod $p$) in $G_p$. The set $E_p$ is finite; indeed, Kummer showed that $E_p$ is contained in the set of divisors of $\Delta$.

The following theorem characterizes $E_p$.

**Theorem 3.** $E_p$ equals the set of odd prime nonoctic quartic residues (mod $p$) which divide $DY$.

**Proof.** Let $q \in E_p$. By Kummer's theorem [7, p. 436], either

$$q \text{ is quartic and } q \mid P_4,$$

or

$$q \text{ is quadratic and } q \mid (\eta_0 - \eta_2)(\eta_1 - \eta_3) \text{ in } \Omega,$$

where $\Omega$ is the ring of algebraic integers. By (8) and Theorem 2, $q \mid DY$ when (9) holds. Thus suppose that (10) holds. We will show that $q \mid Y$; it will then also follow that $q$ is quartic, since every odd prime factor of $Y$ is quartic by the law of biquadratic reciprocity [8, p. 77].
By [7, (3)], we have

\[(11) \quad (\eta_0 - \eta_2)(\eta_1 - \eta_3) = \sum_{k=0}^{7} C_k \eta_k,\]

where \(C_k = (1, k) + (1, k - 2) - (3, k) - (1, k - 1)\), and the \((i, j)\) denote cyclotomic numbers \((\text{mod } p)\) of order 8. From the table of values of the \((i, j)\) given in [6, pp. 116–117], we see that

\[(12) \quad C_3 + C_4 = \pm \sqrt{4}.\]

By (10) and (11), \(q \mid C_k\) for each \(k\). Hence \(q \mid Y\) by (12).

Conversely, suppose that \(q\) is an odd prime quartic nonoctic residue \((\text{mod } p)\) which divides \(DY\). Since \(P_4 = p2^{-8}Y^2D^4\), \(q \mid P_4\). Let \(\mathcal{O}\) denote the ring of integers of \(\mathbb{Q}(\eta_0)\), and let \(N(\alpha)\) denote the norm of \(\alpha\) from \(\mathbb{Q}(\eta_0)\) to \(\mathbb{Q}\). Since \(q \mid P_4\), we have \(q \mid N(\eta_0 - \eta_4)\), so \(\eta_0 \equiv \eta_4 \pmod{Q}\) for some prime ideal \(Q\) of \(\mathcal{O}\) dividing \(q\mathcal{O}\). Since \(q\) is quartic but not octic,

\[\eta_0^q = \left(\sum_{v=1}^{f} \exp(2\pi i g^{8v}/p)\right)^q \equiv \sum_{v=1}^{f} \exp(2\pi i g^{8v+4}/p) = \eta_4 \pmod{q}.\]

Thus \(\eta_0^q = \eta_0 \pmod{Q}\). The polynomial \(x^q - x\) equals \(\prod_{j=0}^{q-1} (x - j) \pmod{q}\), so

\[0 \equiv N(\eta_0^q - \eta_0) \equiv \prod_{j=0}^{q-1} N(\eta_0 - j) = \prod_{j=0}^{q-1} \psi_8(j) \pmod{q}.\]

Thus \(q \mid \psi_8(j)\) for some \(j\), so \(q \in E_p\).

**Example.** For \(p = 193\), \(q = 3\), we have \(q \mid Y\), \(q \mid F_8(0)\), and \(q \in E_p\). For \(p = 1193\), \(q = 11\), we have \(q \mid D\), \(q \mid F_8(0)\), and \(q \in E_p\).

**Appendix.** Sylvester [9, p. 392] characterized \(E_p\) for \(e = 4\) as follows. Write \(p = A^2 + B^2\) with \(A \equiv 1 \pmod{4}\).

If \(p = 8k + 1\), then \(E_p\) is empty; if \(p = 8k + 5\), then \(E_p\) is the set of primes \(\equiv 3 \pmod{4}\) which divide \(B\).

Since Sylvester’s proof [10] is erroneous, we sketch a proof below.

Suppose that \(p = 8k + 1\). From the well-known formula for \(\eta_0 = (G_4 - 1)/4\) [1, Theorem 3.11], it is easily seen that the discriminant of the period polynomial \(\psi_4(z)\) is \(\Delta = 2^{-10}p^3B^6\). Suppose \(q \in E_p\). By Kummer’s theorem [7, p. 436], \(q \mid \Delta\), so \(q \mid B\). By the law of biquadratic reciprocity [8, p. 77], every odd prime factor of \(B\) is quartic \((\text{mod } p)\), so \(q \not\in E_p\). Thus \(E_p\) is empty.

Finally, suppose that \(p = 8k + 5\). Let \(q\) be a prime divisor of \(B\) with \(q \equiv 3 \pmod{4}\). Then \(q\) is not quartic, by the biquadratic reciprocity law. Furthermore, the formula for \(\eta_0\) [1, Theorem 3.11] can be used to show easily that \(B \mid F_4(-A)\), so \(q \mid \psi_4(n)\) for some integer \(n\). Thus \(q \in E_p\). Conversely, suppose that \(q\) is any odd prime in \(E_p\). By Kummer’s theorem, \(q \mid P_2\). Since \(P_2 = pB^2/4\), \(q \mid B\). If \(q \equiv 1 \pmod{4}\), then \(q\) would be quartic by the law of biquadratic reciprocity, which contradicts \(q \in E_p\). Thus \(q \equiv 3 \pmod{4}\).
References

6. E. Lehmer, On the number of solutions of $u^4 + D \equiv w^2 \pmod{p}$, Pacific J. Math. 5 (1955), 103–118.