ON THE MINIMAL POLYNOMIAL OF GAUSS PERIODS FOR PRIME POWERS

S. GURAK

Abstract. For a positive integer m, set $\zeta_m = \exp(2\pi i/m)$ and let $\mathbb{Z}_m^*$ denote the group of reduced residues modulo m. Fix a congruence group $H$ of conductor m and of order f. Choose integers $t_1, \ldots, t_e$ to represent the $e = \phi(m)/f$ cosets of $H$ in $\mathbb{Z}_m^*$. The Gauss periods

$\theta_j = \sum_{x \in H} \zeta_m^{t_j x} \quad (1 \leq j \leq e)$

corresponding to $H$ are conjugate and distinct over $\mathbb{Q}$ with minimal polynomial

$g(x) = x^e + c_1 x^{e-1} + \cdots + c_{e-1} x + c_e.$

To determine the coefficients of the period polynomial $g(x)$ (or equivalently, its reciprocal polynomial $G(X) = X^e g(X^{-1})$) is a classical problem dating back to Gauss. Previous work of the author, and Gupta and Zagier, primarily treated the case $m = p$, an odd prime, with $f > 1$ fixed. In this setting, it is known for certain integral power series $A(X)$ and $B(X)$, that for any positive integer $N$

$G(X) \equiv A(X) \cdot B(X) \pmod{X^N}$

holds in $\mathbb{Z}[X]$ for all primes $p \equiv 1 (\text{mod } f)$ except those in an effectively determinable finite set. Here we describe an analogous result for the case $m = p^\alpha$, a prime power ($\alpha > 1$). The methods extend for odd prime powers $p^\alpha$ to give a similar result for certain twisted Gauss periods of the form

$\psi_j = i^* \sqrt{p} \sum_{x \in H} \left(\frac{t_j x}{p}\right) \zeta_m^{t_j x} \quad (1 \leq j \leq e),$

where $\left(\frac{.}{.}\right)$ denotes the usual Legendre symbol and $i^* = i^{(p-1)/2}$. 

1. Introduction

For any positive integer m, set $\zeta_m = \exp(2\pi i/m)$ and let $\mathbb{Z}_m^*$ denote the group of reduced residues modulo m. Fix a congruence group $H$ defined modulo m of order f and conductor m. Choose integers $t_1, t_2, \ldots, t_e$ to represent the $e = \phi(m)/f$ cosets of $H$ in $\mathbb{Z}_m^*$. The Gauss periods

$\theta_j = \sum_{x \in H} \zeta_m^{t_j x} \quad (1 \leq j \leq e)$

corresponding to $H$ lie in the subfield $K$ of $\mathbb{Q}(\zeta_m)$ fixed by the Galois actions induced by sending $\zeta_m \rightarrow \zeta_m^x$ for $x \in H$. They are conjugate and distinct over $\mathbb{Q}$.
and have minimal polynomial
\[ g(x) = g_H(x) = x^e + c_1 x^{e-1} + \cdots + c_{e-1} x + c_e \]
of degree \( e \). For any numerical character \( \chi \) defined modulo \( m \), the Gauss sum \( G(\chi) \) is given by
\[ G(\chi) = \sum_{x \in \mathbb{Z}_m^*} \chi(x) \zeta_m^x. \]
The Gauss periods (1) are intimately related with the sums (3); namely,
\[ G(\chi) = \sum_{j=1}^{e} \chi(t_j) \theta_j \]
for any character \( \chi \) annihilating \( H \), and
\[ \theta_j = \frac{1}{e} \sum_{\chi} \chi(t_j) G(\chi) \quad (1 \leq j \leq e), \]
where \( \chi \) runs through the characters defined modulo \( m \) which annihilate \( H \). (Here \( \tilde{\chi} \) denotes the multiplicative inverse of the \( \chi \).)

It is well known from the theory of equations [4] that the coefficients \( c_r \) of \( g(x) \) in (2) can be computed in terms of the symmetric power sums \( S_n = \sum (\theta_j)^n \) using Newton’s identities
\[ S_r + c_1 S_{r-1} + \cdots + c_{r-1} S_1 + r c_r = 0 \quad (1 \leq r \leq e), \]
\[ S_n + c_1 S_{n-1} + \cdots + c_{e-1} S_{n-e+1} + c_e S_{n-e} = 0 \quad (n > e). \]
Alternatively, if
\[ G(X) = G_H(X) = X^e g(X^{-1}) = 1 + c_1 X + \cdots + c_e X^e \]
is the reciprocal polynomial of \( g(x) \), its logarithm is formally expressed as
\[ \log G(X) = \log \prod_{j=1}^{e} (1 - \theta_j X) = -\sum_{n=1}^{\infty} \frac{S_n X^n}{n} \]
in terms of the power sums \( S_n \).

To determine the coefficients of the period polynomial \( g(x) \) in (2) (or equivalently its reciprocal polynomial in (7)) is a classical problem dating back to Gauss [5]. When \( f = 1 \) one has \( \theta_1 = \zeta_m \) in (1) whose minimal polynomial is the well-known cyclotomic polynomial
\[ \psi_m(x) = \prod_{d|m} (x^d - 1)^{\mu(m/d)}, \]
with \( \psi_p^\alpha(x) = x^{p^\alpha-1} + \cdots + x^1 + 1 \)
when \( m = p^\alpha \), a prime power. Henceforth, we shall assume \( f > 1 \) throughout this paper.

Previous work of the author [7] and Gupta and Zagier [6] primarily treated the case \( m = p \), an odd prime, with \( f > 1 \) fixed. In this case, the beginning coefficients of \( g(x) \) exhibit a polynomial dependence on \( p \) for all sufficiently large primes \( p \equiv 1(\mod f) \). More precisely, Gupta and Zagier [6] showed for certain integral
power series $A(X)$ and $B(X)$ depending only on simple arithmetic properties of the $f$-roots of unity $\zeta_f^v$ ($1 \leq v \leq f$), that for any positive integer $N$

\[(10) \quad G(X) \equiv A(X) \cdot B(X)^{(p-1)/f} \pmod{X^N}\]

holds in $\mathbb{Z}[X]$ for all primes $p \equiv 1 (\text{mod } f)$ except for those in an effectively determinable finite set. Moreover, they give an elegant algorithm to compute the exceptional sets. For $f = 2$, the congruence (10) holds for $N = p$, so $G(X)$ is uniquely determined. Indeed,

\[(11) \quad G(X) = \sum_{r=0}^{\infty} (-1)^{\lfloor r/2 \rfloor} \left( \left\lfloor \frac{e - r}{2} \right\rfloor \right) X^r\]

exactly in closed form, a formula known to Gauss [5]. (Here $\lfloor \cdot \rfloor$ denotes the greatest integer function.) Some extensions of these results for certain congruence groups $H$ of square-free conductor $m = p_1 \cdots p_r$ with a fixed number of prime factors of specified types have been suggested (see [8] and also [6]). However, the prime power case $m = p^\alpha$, $\alpha > 1$, seems to have been overlooked. It is this situation we describe here. The case $p = 2$ is treated first, separately in Section 2, where closed form formulas are known for $G_H(X)$ for any congruence group $H$ of conductor $2^\alpha$. In Section 3 we give an analog of (10) for Gauss periods corresponding to congruence groups $H$ of odd prime power conductor $p^\alpha$, $\alpha > 1$, together with an adaptation of Gupta and Zagier’s algorithm to determine exceptional prime powers. When $f = 2$ this congruence is shown to hold modulo $X^{r^\alpha+1}$, not enough though to completely determine $G(X)$. However, we have recently found [9] closed form formulas in this case for $G(X)$ which generalize (11). In the final section, we extend the results for odd prime powers $p^\alpha$ to certain twisted Gauss periods of the form

\[(12) \quad \psi_j = i^* \sqrt{p} \sum_{x \in H} \left( \frac{t}{p} \right) \zeta_{p^\alpha}^j x \quad (1 \leq j \leq e),\]

where $\left( \frac{\cdot}{p} \right)$ denotes the usual Legendre symbol and $i^* = i^{(p-1)^2/4}$. Such quadratic twists or integer multiples of them arise classically as values of Kloosterman sums [10], [13] for odd prime powers $p^\alpha$, $\alpha > 1$.

#### 2. Gauss periods for $2^\alpha$

Throughout this section $H$ is a congruence group of conductor $2^\alpha$ ($\alpha > 1$) and order $f > 1$. It is known that there are only two possible choices for $H$. For the sake of completeness we include a brief rationale for this fact.

**Proposition 1.** A congruence group $H$ of conductor $2^\alpha$, $\alpha > 1$, and order $f > 1$ must be either $\{1, 2^\alpha - 1\}$ or $\{1, 2^\alpha - 2^\alpha - 1\}$ modulo $2^\alpha$.

**Proof.** Since $H$ has conductor $2^\alpha$ with $f > 1$, it is known from class field theory that the field $K$ corresponding to $H$ is a proper subfield of $\mathbb{Q}(\zeta_{2^\alpha})$ not contained in $\mathbb{Q}(\zeta_{2^{\alpha-1}})$, and so $\alpha > 2$. Since $2|f$, $H$ contains an element of order two modulo $2^\alpha$—either $2^\alpha - 1$, $2^\alpha - 2^\alpha - 1$ or $2^\alpha + 1$. The last choice can be eliminated since $H$ has conductor $2^\alpha$. Thus $K$ is contained in one of the cyclic fields $\mathbb{Q}(\zeta_{2^\alpha} + \zeta_{2^\alpha}^{-1})$ or $\mathbb{Q}(\zeta_{2^\alpha} - \zeta_{2^\alpha}^{-1})$ which correspond to the congruence groups $\{1, 2^\alpha - 1\}$ or $\{1, 2^\alpha - 2^\alpha - 1\}$ modulo $2^\alpha$, respectively. But any proper subfield of $\mathbb{Q}(\zeta_{2^\alpha} + \zeta_{2^\alpha}^{-1})$ or $\mathbb{Q}(\zeta_{2^\alpha} - \zeta_{2^\alpha}^{-1})$ is a subfield of $\mathbb{Q}(\zeta_{2^{\alpha-1}} + \zeta_{2^{\alpha-1}}^{-1})$ contained in $\mathbb{Q}(\zeta_{2^{\alpha-1}})$. Thus either $K = \mathbb{Q}(\zeta_{2^\alpha} + \zeta_{2^\alpha}^{-1})$ or $\mathbb{Q}(\zeta_{2^\alpha} - \zeta_{2^\alpha}^{-1})$, so $H$ equals $\{1, 2^\alpha - 1\}$ or $\{1, 2^\alpha - 2^\alpha - 1\}$. □
From the proposition above the only possibilities for $\theta_1$ in (1) here is $\zeta_{2^\alpha} + \zeta_{2^\alpha}^{-1}$ or $\zeta_{2^\alpha} - \zeta_{2^\alpha}^{-1}$, each with $f = 2$ and $\alpha > 2$. The corresponding minimal polynomials are classically known from the properties of Chebyshev polynomials. We quote results from [9] relevant to the discussion here.

**Theorem 1.** The minimal polynomial for $\zeta_{2^\alpha} + \zeta_{2^\alpha}^{-1}$ for $\alpha > 2$ is equivalently characterized by

$$g(x) = \sum_{n=0}^{2^{\alpha-3}} (-1)^n \frac{2^{\alpha-2}}{2^{\alpha-2} - n} \left( \frac{2^{\alpha-2} - n}{n} \right) x^{2^{\alpha-2} - 2n}$$

or the power sums

$$S_n = \begin{cases} 2^{\alpha-2} \binom{n}{n/2} & \text{if } n \text{ is even}, \\ 0 & \text{if } n \text{ is odd}, \end{cases}$$

for $1 \leq n \leq 2^{\alpha-2}$, or the congruence

$$G(X) \equiv B_+(X)^{2^{\alpha-2}} \pmod{X^{2^{\alpha-1}}},$$

where

$$B_+(X) = \exp\left( -\sum_{n=1}^{\infty} \frac{(2n)}{n} \frac{X^{2n}}{2n} \right) = \frac{1}{2} \left( 1 + \sqrt{1 - 4X^2} \right).$$

The minimal polynomial for $\zeta_{2^\alpha} - \zeta_{2^\alpha}^{-1}$ for $\alpha > 2$ is characterized equivalently by

$$g(x) = \sum_{n=0}^{2^{\alpha-3}} \frac{2^{\alpha-2}}{2^{\alpha-2} - n} \left( \frac{2^{\alpha-2} - n}{n} \right) x^{2^{\alpha-2} - 2n}$$

or the power sums

$$S_n = \begin{cases} -2^{\alpha-2} \binom{n}{n/2} & \text{if } 2|n \\ 2^{\alpha-2} \binom{n}{n/2} & \text{if } 4|n \\ 0 & \text{if } n \text{ is odd}, \end{cases}$$

for $1 \leq n \leq 2^{\alpha-2}$, or the congruence

$$G(X) \equiv B_-(X)^{2^{\alpha-2}} \pmod{X^{2^{\alpha-1}}},$$

where

$$B_-(X) = \exp\left( -\sum_{n=1}^{\infty} (-1)^n \frac{(2n)}{n} \frac{X^{2n}}{2n} \right) = \frac{1}{2} \left( 1 + \sqrt{1 + 4X^2} \right).$$

We treat the case when $H$ has an odd prime power conductor next.
3. Gauss periods for odd prime powers

Throughout this section we assume the congruence group $H$ in (1) has conductor $m = p^\alpha$ with $p$ odd and $\alpha > 1$. Since $\mathbb{Z}_{p^\alpha}$ is cyclic, $H = (\mathbb{Z}_{p^\alpha})^{\phi(p^\alpha)/f}$, or equivalently $H$ equals the group of $f$-roots of unity in $\mathbb{Z}_{p^\alpha}$. In particular, since $H$ has conductor $p^\alpha$, $p/f$ so $p \equiv 1 (\text{mod } f)$. To compute the symmetric power sums $S_n$, we introduce certain counting functions $T_n(p^\gamma)$ for $0 < \gamma \leq \alpha$ as in [8]. Specifically, let $T_n(p^\gamma)$ count the number of times

\[ x_1 + \cdots + x_n \equiv 0 \pmod{p^\gamma} \]

for choice of tuples $(x_1, \ldots, x_n)$ with $x_i \in (\mathbb{Z}_{p^\gamma})^{\phi(p^\gamma)/f}$ \ ($1 \leq i \leq n$). These counting functions possess the following useful property.

**Lemma 1.** For $\gamma > 1$, $T_n(p^{\gamma-1}) - T_n(p^\gamma)$ equals the number of tuples $(x_1, \ldots, x_n)$ with $x_i \in (\mathbb{Z}_{p^\gamma})^{\phi(p^\gamma)/f}$ for which $p^{\gamma-1} \mid (x_1 + \cdots + x_n)$.

**Proof.** First observe that any $f$-root of unity $x \bmod p^{\gamma-1}$ lifts to a unique $f$-root of unity $x' \bmod p^\gamma$, since

\[ (x + tp^{\gamma-1})^f \equiv x^f + ft p^{\gamma-1} \equiv 1 \pmod{p^\gamma} \]

has a unique solution $t$ satisfying $-ft \equiv (x^f - 1)/p^{\gamma-1} \pmod{p}$. Thus each solution $x_1 + \cdots + x_n \equiv 0 (\text{mod } p^{\gamma-1})$ with $x_i \in (\mathbb{Z}_{p^{\gamma-1}})^{\phi(p^{\gamma-1})/f}$ lifts to a unique solution $x'_1 + \cdots + x'_n \equiv 0 (\text{mod } p^\gamma)$ with $x'_i \in (\mathbb{Z}_{p^\gamma})^{\phi(p^\gamma)/f}$. The statement of the lemma now readily follows.

Now observe in the expansion (8)

\[ \log G(X) = -\sum_{n=1}^{\infty} S_n X^n / n = -\sum_{n=1}^{\infty} \sum_{j=1}^{\gamma} (\sum_{x \in H} \zeta_{p^\alpha}^{x})^n X^n / n, \]

that $S_n$ equals the inner sum

\[ \sum_{j=1}^{\gamma} (\sum_{x \in H} \zeta_{p^\alpha}^{x})^n = \frac{1}{f} \sum_{r \in \mathbb{Z}_{p^\alpha}} \sum_{x_1+\cdots+x_n \in H} \zeta_{p^\alpha}^{r(x_1+\cdots+x_n)}. \]

But in view of the lemma above, and since

\[ \sum_{r \in \mathbb{Z}_{p^\alpha}} \zeta_{p^\alpha}^{rx} = \begin{cases} \phi(p^\alpha) & \text{if } p^\alpha | x \\ -p^{\alpha-1} & \text{if } p^{\alpha-1} | x \\ 0 & \text{otherwise}, \end{cases} \]

\[ \sum_{r \in \mathbb{Z}_{p^\alpha}} \sum_{x_1+\cdots+x_n \in H} \zeta_{p^\alpha}^{r(x_1+\cdots+x_n)} = \phi(p^\alpha)T_n(p^\alpha) - p^{\alpha-1}(T_n(p^{\alpha-1}) - T_n(p^\alpha)) \]

\[ = p^\alpha T_n(p^\alpha) - p^{\alpha-1}T_n(p^{\alpha-1}). \]

Thus,

\[ S_n = \frac{p^{\alpha-1}}{f} (p T_n(p^\alpha) - T_n(p^{\alpha-1})). \]

Now let $\beta_f(n)$ count the number of times $\epsilon_1 + \cdots + \epsilon_n = 0$ for $f$-roots of unity $\epsilon_i$ in $\mathbb{Q}(\zeta_f)$, so $T_n(p^{\alpha-1}) \geq T_n(p^\alpha) \geq \beta_f(n)$. Thus as long as $T_n(p^{\alpha-1}) = \beta_f(n)$,

\[ S_n = \frac{\phi(p^\alpha)}{f} \beta_f(n) \]
above. Letting $\xi_f(n)$ be the set of odd prime powers $p^\alpha$ ($\alpha > 1$, $p \equiv 1(\text{mod } f)$, for which $T_n(p^{\alpha-1}) > \beta_f(n)$ and putting

$$B(X) = \exp(-\sum_{n=1}^{\infty} \beta_f(n)X^n/n),$$

one obtains from (8) and (15) the following analog of Gupta and Zagier’s result [6] Theorem 1].

\textbf{Theorem 2.} For each natural number $N$, the congruence

$$G(X) \equiv B(X)^{\phi(p^n)/f} \pmod{X^N}$$

holds in $\mathbb{Z}[X]$ for all odd prime powers $p^\alpha$ ($\alpha > 1$, $p \equiv 1(\text{mod } f)$, except those lying in $\xi_f(n)$ for some $n < N$.

Before giving some examples, some comments concerning the result above and the computation of the exceptional sets $\xi_f(n)$ are in order. The power series $B(X)$ in (16) is the same integral power series appearing in [6]. The counting function $\beta_f(n)$ has a nice expression when $f$ is a prime power or twice a prime (chiefly, Theorem 2 in [6]) In particular, one has

$$\beta_l(n) = \begin{cases} 0 & \text{if } l \nmid n \\ \frac{n!}{(\lfloor n/l \rfloor)!} & \text{if } l | n \end{cases}$$

when $l$ is a prime and

$$\beta_4(n) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ \left(\frac{n}{2}\right)^2 & \text{if } n \text{ is even} \end{cases}$$

(see also Corollary 2 in [6]).

Gupta and Zagier [6] give an elegant alternative expression for $\beta_f(n)$ which is useful in computing the exceptional sets $\xi_f(n)$. For any tuple $\vec{i} = (i_1, \ldots, i_n)$ in $(\mathbb{Z}/f\mathbb{Z})^n$, let $P_\vec{i}(x)$ denote the polynomial $x^{i_1} + \cdots + x^{i_n}$ with $i_v$ ($1 \leq v \leq n$) chosen to be the least nonnegative representative of the class $i_v \pmod{f}$. Then

$$\beta_f(n) = \text{card}(\{\vec{i} = (i_1, \ldots, i_n) \in (\mathbb{Z}/f\mathbb{Z})^n | \psi_f(x) \text{ divides } P_\vec{i}(x)\})$$

where $\psi_f(x)$ denotes the $f$th cyclotomic polynomial (9). If one fixes a prime $\bar{p}$ lying above $p$ in $\mathbb{Q}(\zeta_f)$, then

$$T_n(p^\gamma) = \text{card}(\{\tilde{i} = (i_1, \ldots, i_n) \in (\mathbb{Z}/f\mathbb{Z})^n | \tilde{\bar{p}}^\gamma \text{ divides } \zeta_f^{i_1} + \cdots + \zeta_f^{i_n}\})$$

in (13), independent of the choice of $\bar{p}$. Clearly $T_n(p^{\alpha-1}) > \beta_f(n)$ if and only if for some tuple $\tilde{i} = (i_1, \ldots, i_n)$ in $(\mathbb{Z}/f\mathbb{Z})^n$

$$\tilde{\bar{p}}^{\alpha-1}|(\zeta_f^{i_1} + \cdots + \zeta_f^{i_n}) \text{ but } \zeta_f^{i_1} + \cdots + \zeta_f^{i_n} \neq 0.$$ 

Thus $\xi_f(n)$ consists of all odd prime powers $p^\alpha$, $p \equiv 1(\text{mod } f)$ for which (21) holds for some tuple $\tilde{i}$ in $(\mathbb{Z}/f\mathbb{Z})^n$. Now a necessary condition for $\tilde{i}$ to satisfy (21) is $R_\tilde{i} \equiv 0(\text{mod } p^{\alpha-1})$, but $R_\tilde{i} \neq 0$, where $R_\tilde{i}$ denotes the resultant of $P_\tilde{i}(x)$ and $\psi_f(x)$. The resultant $R_\tilde{i} = 0$ if $\psi_f(x)$ divides $P_\tilde{i}(x)$. When $\psi_f(x)/P_\tilde{i}(x)$ (so $(\psi_f, R_\tilde{i}) = 1$), $R_\tilde{i}$ is essentially the smallest positive integer $R$ for which the equation $g(x)\psi_f(x) + h(x)P_\tilde{i}(x) = R$ is solvable with polynomials $g, h \in \mathbb{Z}[x]$, or equivalently, the norm $N_{\mathbb{Q}(\zeta_f)/\mathbb{Q}}(\zeta_f)$. Thus to determine which prime powers lie in $\xi_f(n)$, one
Table 1.

| \( f = 4, n = 7 \) : \( \tilde{p}_5 = 2 - \zeta_5 \) where \( \zeta_4 \equiv 7(\text{mod } \tilde{p}_5^2) \) | \( \tilde{i} \) | \( R_{\tilde{i}} \) | \( \zeta_{f_1}^{i_1} + \cdots + \zeta_{f_n}^{i_n} \) factors |
|---|---|---|
| 0000002 | 25 | \( 5 = (2 + \zeta_4)(2 - \zeta_4) \) |
| 0000111 | 25 | \( 4 + 3\zeta_4 = \zeta_4(2 - \zeta_4)^2 \) |
| 0000333 | 25 | \( 4 - 3\zeta_4 = -\zeta_4(2 + \zeta_4)^2 \) |
| 0111112 | 25 | \( 5\zeta_4 = \zeta_4(2 + \zeta_4)(2 - \zeta_4) \) |

| \( f = 5, n = 7 \) : \( \tilde{p}_{11} = 2 + \zeta_5^2 \) where \( \zeta_5 \equiv 3(\text{mod } \tilde{p}_{11}^2) \) | \( \tilde{i} \) | \( R_{\tilde{i}} \) | \( \zeta_{f_1}^{i_1} + \cdots + \zeta_{f_n}^{i_n} \) factors |
|---|---|---|
| 0000123 | 121 | \( 3 - \zeta_5^4 = -\zeta_5^2(1 + \zeta_5^2)(2 + \zeta_5^3)^2 \) |
| 0000124 | 121 | \( 3 - \zeta_5^4 = -\zeta_5^2(1 + \zeta_5^2)(2 + \zeta_5^3)^2 \) |
| 0000134 | 121 | \( 3 - \zeta_5^4 = -\zeta_5^2(1 + \zeta_5^2)(2 + \zeta_5^3)^2 \) |
| 0000234 | 121 | \( 3 - \zeta_5 = -\zeta_5(1 + \zeta_5)(2 + \zeta_5^3)^2 \) |
| 0001113 | 121 | \( 3 + 3\zeta_5 + \zeta_5^3 = -\zeta_5^2(1 + \zeta_5^2)(2 + \zeta_5^3)^2 \) |
| 0001222 | 121 | \( 3 + 3\zeta_5^2 + \zeta_5 = -\zeta_5^2(1 + \zeta_5^2)(2 + \zeta_5^3)^2 \) |

| \( f = 3, n = 11 \) : \( \tilde{p}_7 = \zeta_3 - 2 \) where \( \zeta_4 \equiv -19(\text{mod } \tilde{p}_7^2) \) | \( \tilde{i} \) | \( R_{\tilde{i}} \) | \( \zeta_{f_1}^{i_1} + \cdots + \zeta_{f_n}^{i_n} \) factors |
|---|---|---|
| 0000000111 | 49 | \( 8 + 3\zeta_3 = -\zeta_3^2(3 - 2)^2 \) |
| 0000000222 | 49 | \( 8 + 3\zeta_3^2 = -\zeta_3(3 - 2)^2 \) |

First restricts to those prime powers \( p^\alpha, p \equiv 1(\text{mod } f) \) for which \( R_{\tilde{i}} \equiv 0(\text{mod } p^{\alpha - 1}) \) but \( R_{\tilde{i}} \neq 0 \) for some tuple \( \tilde{i} \) in \((\mathbb{Z}/f\mathbb{Z})^n\). For such a prime power \( p^\alpha \), select a primitive \( f \)-root of unity \( g \) modulo \( p^{\alpha - 1} \) for which \( \tilde{p}^{\alpha - 1}(\zeta_f - g) \). Then in view of (21), \( p^\alpha \in \xi_f(n) \) if and only if

\[
g^{i_1} + \cdots + g^{i_n} \equiv 0 \pmod{p^{\alpha - 1}} \text{ with } \zeta_f^{i_1} + \cdots + \zeta_f^{i_n} \neq 0
\]

for some tuple \( \tilde{i} = (i_1, \ldots, i_n) \) in \((\mathbb{Z}/f\mathbb{Z})^n\). It is enough to consider tuples \( \tilde{i} \), inequivalent under translation and permutation.

Table 1 shows the results of this computation for finding exceptional prime powers \( p^3 \) among the inequivalent \( n \)-tuples \( \tilde{i} \) for which \( R_{\tilde{i}} \equiv 0(\text{mod } p^2) \), \( R_{\tilde{i}} \neq 0 \) in cases \((f, n) = (4, 7), (5, 7) \) and \((3, 11)\).

To illustrate when \( f = 5 \) and \( n = 7 \), one finds six inequivalent classes of 7-tuples \( \tilde{i} \) with \( p^2 | R_{\tilde{i}} \) and \( R_{\tilde{i}} \neq 0 \). Representatives for each such class are given in Table 1 all have resultant \( R_{\tilde{i}} = 121 \). To check if \( 11^3 \in \xi_5(7) \) one may choose \( \tilde{p}_{11} = 2 + \zeta_5^2 \), where \( \zeta_5 \equiv 3(\text{mod } \tilde{p}_{11}) \). One of these tuples satisfies (21) with \( \tilde{p}_{11} = 2 + \zeta_5^2 \) and \( \alpha = 3 \); namely, 0000234, so \( 11^3 \in \xi_5(7) \). There are \( \frac{7!}{4!} = 210 \) permutations of 0000234 with five translations each, so

\[
T_{7}(121) = \beta_5(7) + 210 \cdot 5 = 1250
\]
as \( \beta_5(7) = 0 \).

The “new” exceptional prime powers for given \( n \) are the elements of \( \xi_f(n) \) which do not appear in \( \xi_f(n') \) for some \( n' < n \). Table 2 lists the “new” exceptional prime powers for \( 3 \leq f \leq 8 \) and small values of \( n \).
Example 1. Consider the case $p = 7$ with $f = 3$, so

$$\beta_3(n) = \begin{cases} n!/(n/3)!^3 & \text{if } 3 | n, \\ 0 & \text{otherwise} \end{cases}$$

from (17) with

$$B(X) = 1 - 2X^3 - 13X^6 - 158X^9 - 2431X^{12} - \ldots$$

in (16). The power 49 first appears in the exceptional set $\xi_3(4)$ with $T_4(7) = 12 > \beta_3(4) = 0$, whereas 343 first appears in the exceptional set $\xi_3(11)$ with $T_{11}(49) = 495 > \beta_3(11) = 0$. The minimal polynomials $G(X)$ for $\theta_{49}^{-1} = (\zeta_{49} + \zeta_{49}^{18} + \zeta_{49}^{-19})^{-1}$ begins

$$1 - 28X^3 + 7X^4 + 14X^5 + 189X^6 + \cdots,$$

whereas that for $\theta_{1}^{-1} = (\zeta_{343} + \zeta_{343}^{18} + \zeta_{343}^{-19})^{-1}$ begins

$$1 - 196X^3 + 7^2 \cdot 362X^6 - 7^3 \cdot 2872X^9 + 7^2 \cdot 15X^{11} + 7^3 \cdot 109733X^{12} + \cdots.$$  

The underscored coefficients deviate as expected from the pattern of the beginning coefficients given by Theorem 2.

Example 2. Consider next $p = 5$ with $f = 4$, so $\beta_4(n)$ is given by (18) with

$$B(X) = 1 - 2X^2 - 7X^4 - 50X^6 - 456X^8 - \ldots$$

in (16). The power 25 first appears in $\xi_4(3)$ with $T_5(5) = 12 > \beta_4(3) = 0$, whereas 125 first appears in the exceptional set $\xi_4(7)$ with $T_7(25) = 140 > \beta_4(7) = 0$. Here

<table>
<thead>
<tr>
<th>$n$</th>
<th>$f = 3$</th>
<th>$f = 4$</th>
<th>$f = 6$</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>5</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>7</td>
<td></td>
<td>13</td>
</tr>
<tr>
<td>5</td>
<td>13</td>
<td>19</td>
<td>19</td>
</tr>
<tr>
<td>6</td>
<td>31</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>5^2</td>
<td>37</td>
<td>37</td>
</tr>
<tr>
<td>8</td>
<td>31</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>5^2</td>
<td>31</td>
<td>7</td>
</tr>
<tr>
<td>10</td>
<td>7^2</td>
<td>7^2</td>
<td>3</td>
</tr>
<tr>
<td>11</td>
<td>7^3</td>
<td>7^3, 7^2</td>
<td>97</td>
</tr>
<tr>
<td></td>
<td>61</td>
<td>73</td>
<td>103</td>
</tr>
</tbody>
</table>

Here are a couple of examples to illustrate Theorem 2.
one may take $H = \{ \pm 1, \pm 7 \}$ for $m = 25$ and $H = \{ \pm 1, \pm 57 \}$ for $m = 125$. The minimal polynomial $G(X)$ for $\theta_1^{-1} = (\zeta_{25} + \zeta_{25}^{-1} + \zeta_{57} + \zeta_{57}^{-1})^{-1}$ is

$$1 - 10X^2 + 5X^3 + 10X^4 + X^5.$$  
That for $\theta_1^{-1} = (\zeta_{125} + \zeta_{125}^{-1} + \zeta_{57} + \zeta_{125}^{-1} + \zeta_{57}^{-1})^{-1}$ begins

$$1 - 50X^2 + 1025X^4 - 11250X^6 + 125X^7 + \cdots.$$  
The underscored coefficients deviate as expected from the pattern of the beginning coefficients given by Theorem 2.

We conclude this section with a discussion of the case $f = 2$ where a closed formula for $G(X)$ has been obtained [9]. The power series $B(X)$ in (16) is just

$$B(X) = \frac{1}{2}(1 + \sqrt{1 - 4X^2}) = 1 - \sum_{n=0}^{\infty} \binom{2n}{n} \frac{X^{2n+2}}{n + 1}$$  
with $\beta_2(n)$ given by (17). The minimal polynomial $G(X)$ for $(2\cos 2\pi/p^\alpha)^{-1}$ is seen to have the form

$$G(X) = \frac{1 + \sqrt{1 - 4X^2}}{2} \phi(p^\alpha)/2 + 1 - \frac{(1 - \sqrt{1 - 4X^2})p^\alpha}{1 - (1 - \sqrt{1 - 4X^2})p^\alpha}$$  
with power sums $S_n$ satisfying

$$S_n = p^\alpha \sum_{t=1, \text{odd}}^{[np^{-1}] \phi(p^\alpha)/2} \left( \frac{n - p^\alpha t}{2} \right) - p^{\alpha-1} \sum_{t=1, \text{odd}}^{[np^{-1}] \phi(p^\alpha)/2} \left( \frac{n - p^{\alpha-1} t}{2} \right)$$  
if $n$ is odd, or

$$\frac{\phi(p^\alpha)}{2} \left( \frac{n}{n/2} \right) + p^\alpha \sum_{t=1}^{[np^{-1}/2]} \left( \frac{n - p^\alpha t}{2} \right) - p^{\alpha-1} \sum_{t=1}^{[np^{-1}/2]} \left( \frac{n - p^{\alpha-1} t}{2} \right)$$  
if $n$ is even. A closed form formula for $G(X)$ is

$$G(X) = X^{\phi(p^\alpha)/2} + \sum_{j=0}^{(p^\alpha-3)/2} X^{p^\alpha-1} \text{C}_{p^\alpha-1}(\frac{1}{2} - j)(X),$$  
where

$$\text{C}_d(X) = \sum_{n=0}^{[d/2]} (-1)^n \frac{d}{d-n} \binom{d-n}{n} X^{2n},$$  
or equivalently with coefficients in (7) satisfying for $1 \leq \phi(p^\alpha)/2$,

$$c_r = \sum_{j=0, \text{odd}}^{[p^{\alpha-1}]} (-1)^{t_j} \frac{p^{\alpha-1} (p^{\alpha-1} - j)}{p^{\alpha-1}(p^{\alpha-1} - j) - t_j} \left( \frac{p^{\alpha-1}(2 - j) - t_j}{t_j} \right)$$  
with $c_{\phi(p^\alpha)/2} = (\frac{1}{2})^2$, where $t_j = (r - p^{\alpha-1} j)/2$.

From (22) or (24), it follows that the congruence

$$G(X) \equiv B(X)^{\phi(p^\alpha)/2} \pmod{X^N}$$  
holds in $\mathbb{Z}[X]$ for $N = p^{\alpha-1}$ but not for $N > p^{\alpha-1}$, and thus fails to determine $G(X)$ which is of degree $\phi(p^\alpha)/2$. Indeed, one can show $p^\alpha$ first appears in the exceptional set $\xi_2(n)$ for $n = p^{\alpha-1}$.
4. Twisted Gauss periods for $p^\alpha$

Here we consider quadratic twists of Gauss periods for prime powers $p^\alpha$, $\alpha > 1$. When $p = 2$ with $\alpha > 3$, the twisted Gauss periods have the form $\sqrt{2}(\zeta_{2^n}^\alpha + \zeta_{2^n}^{-\alpha})$ or $\sqrt{2}(\zeta_{2^n}^\alpha - \zeta_{2^n}^{-\alpha})$ for some odd integer $v$, and their corresponding minimal polynomials are easily obtained from the Theorem 1 in Section 2. With no loss of generality then we restrict attention to the case in which $p$ is odd, and consider the twisted Gauss periods

$$
\psi_j = i^* \sqrt{p} \sum_{x \in H} \left( \frac{j \cdot x}{p} \right) \zeta_{p^\alpha}^{j \cdot x} \quad (1 \leq j \leq e),
$$

with $H$ a congruence group of conductor $p^\alpha$ ($\alpha > 1$) and order $f > 1$ as in (1). The twisted Gauss periods (26) also lie in the subfield $K$ of $\mathbb{Q}(\zeta_{p^\alpha})$ corresponding to $H$ with $[K : \mathbb{Q}] = \phi(p^\alpha)/f$. In fact $\psi_j = \text{Tr}_{\mathbb{Q}(\zeta_{p^\alpha})/K}(i^* \sqrt{p} \zeta_{p^\alpha}^j)$ $(1 \leq j \leq e)$, and each is seen to generate $K$.

**Proposition 2.** Each twisted Gauss period $\psi_j$ in (26) generates the field $K$ over $\mathbb{Q}$.

**Proof.** It suffices to show the conjugates $\psi_j \quad (1 \leq j \leq e)$ are all distinct. For this purpose set

$$
T(\chi) = \sum_{j=1}^{e} \chi(t_j) \psi_j
$$

for any numerical character $\chi$ annihilating $H$. Then

$$
\psi_j = \frac{1}{e} \sum_{\chi} \chi(t_j) T(\chi) \quad (1 \leq j \leq e),
$$

the sum taken over the characters $\chi$ annihilating $H$. Generalizing the argument in the Appendix of [8] one finds in view of the lemma there that the $\psi_j$ $(1 \leq j \leq e)$ will be distinct provided $T(\chi) \neq 0$ for all $\chi$ annihilating $H$ with conductor $\text{ord}(\chi)$ satisfying $(p^\alpha/f(\chi), f(\chi)) = 1$, where $p^\alpha/f(\chi)$ is square-free. We assert that this hypothesis above holds here so that the $\psi_j$ are distinct. Indeed for any character $\chi$ annihilating $H$, $T(\chi)$ equals

$$
\sum_{j=1}^{e} \chi(t_j) i^* \sqrt{p} \sum_{x \in H} \left( \frac{j \cdot x}{p} \right) \zeta_{p^\alpha}^{j \cdot x} = i^* \sqrt{p} \sum_{x \in \mathbb{Z}_{p^\alpha}} \chi(x) \left( \frac{x}{p} \right) \zeta_{p^\alpha}^x,
$$

or $i^* \sqrt{p} G(\chi \psi)$ in terms of a Gauss sum (3), where $\psi$ is the quadratic character $(\frac{\cdot}{p})$ considered modulo $p^\alpha$. But any such character $\chi$ with $(p^\alpha/f(\chi), f(\chi)) = 1$ and $p^\alpha/f(\chi)$ square-free must have conductor $f(\chi) = p^\alpha$. Hence $\chi \psi$ must also have conductor $p^\alpha$ so $G(\chi \psi) \neq 0$, and thus $T(\chi) \neq 0$.

The proof of the proposition is now complete. \qed

Our goal here is to give an analog of Theorem 2 in Section 3 for the minimal polynomial $G(X)$ for the reciprocals of the $\psi_j$ in (26). Two situations arise naturally depending on whether $(p - 1)/f$ is even or odd. To deal with the case $(p - 1)/f$ is even, we set

$$
\hat{\beta}_f(n) = \begin{cases} 
\beta_f(n) & \text{if } n \text{ is even} \\
0 & \text{if } n \text{ is odd},
\end{cases}
$$

where
where $\beta_f(n)$ is the counting function in (15). In terms of this adjusted counting function $\beta_f(n)$ and the exceptional sets $\xi_f(n)$ as before, we find

**Theorem 3.** Suppose $(p-1)/f$ is even where $B(X) = \exp(-\sum_{n=1}^{\infty} \beta_f(n)X^n/n)$ with $\beta_f(n)$ defined by (27). Then for each natural number $N$, the congruence

$$G(X) \equiv \hat{B}(i^* \sqrt[7]{X})^{\phi(p^\alpha)/f} \pmod{X^N}$$

holds in $\mathbb{Z}[X]$ for all odd prime powers $p^\alpha$ ($\alpha > 1$) except those lying in $\xi_f(n)$ for some $n < N$.

**Proof.** Here $\log G(X) = -\sum_{n=1}^{\infty} S_n X^n/n$ takes the form

$$-\sum_{n=1}^{\infty} \frac{(i^* \sqrt[7]{X})^n}{n} \left( \sum_{j=1}^{\infty} \left( \sum_{H \in \mathbb{Z}_p^*} \left( \frac{j^H}{p^r} \right) \zeta^{j^H(p^r)} \right)^n \right)$$

with inner sum

$$\sum_{j=1}^{\infty} \left( \sum_{H \in \mathbb{Z}_p^*} \left( \frac{j^H}{p^r} \right) \zeta^{j^H(p^r)} \right)^n = \frac{1}{f} \sum_{r \in \mathbb{Z}_p^*} \left( \sum_{x \in H} \left( \frac{p^r}{p} \right) \zeta^{r(p^x)} \right)^n = \frac{1}{f} \sum_{r \in \mathbb{Z}_p^*} \left( \frac{p^r}{p} \right)^n \left( \sum_{H \in \mathbb{Z}_p^*} \zeta^{r(p^x)} \right)^n,$$

since $H$ is contained in $\mathbb{Z}_p^2$ as $(p-1)/f$ is even. When $n$ is even, this last sum is just

$$\frac{1}{f} \sum_{r \in \mathbb{Z}_p^*} \zeta^{r(p^x)} = \frac{1}{f} \left( \frac{p^\alpha T_n(p^\alpha) - p^{\alpha-1} T_n(p^{\alpha-1})}{p} \right) = \frac{\phi(p^\alpha)}{f} \beta_f(n),$$

as in the proof of Theorem 2 when $p^\alpha$ does not lie in $\xi_f(n)$ for $n < N$. When $n$ is odd this sum becomes

$$\frac{1}{f} \sum_{r \in \mathbb{Z}_p^*} \left( \sum_{x \in H} \left( \frac{p^r}{p} \right) \zeta^{r(x_1+\cdots+x_n)} \right) = \frac{1}{f} \sum_{x_1, \ldots, x_n} \sum_{r \in \mathbb{Z}_p^*} \left( \frac{p^r}{p} \right)^{\alpha} \zeta^{r(x_1+\cdots+x_n)} = 0$$

for any prime power $p^\alpha$ not in $\xi_f(n)$ for some $n < N$, since $\sum_{r \in \mathbb{Z}_p^*} \left( \frac{p^r}{p} \right)^{\alpha} \zeta^{r(x_1+\cdots+x_n)} = 0$ unless $p^{\alpha-1} \mid \alpha$. This establishes the theorem with $\hat{B}(X)$ defined in terms of the adjusted counting function $\beta_f(n)$ in (27).

**Example 3.** Consider $p = 7$ with $f = 3$, so

$$\hat{\beta}_3(n) = \begin{cases} n!/(n/3)!^3 & \text{if } 6 \mid n, \\ 0 & \text{otherwise,} \end{cases}$$

in (27) with

$$\hat{B}(X) = 1 - 15X^6 - 2775X^{12} - 910202X^{18} - \cdots$$

in Theorem 3. Then

$$\hat{B}(i\sqrt[7]{X}) = 1 + 7^3 \cdot 15X^6 - 7^6 \cdot 2775X^{12} + 7^9 \cdot 910202X^{18} - \cdots.$$
The underscored coefficients deviate as expected from the pattern given in Theorem 3.

Now consider the case \((p - 1)/f\) is odd, so \(f\) must be even. For any positive integer \(n\), let \(\beta_f^+ (n)\) count the number of times a sum satisfies \(\epsilon_1 + \cdots + \epsilon_n = 0\) for \(f\)-roots of unity \(\epsilon_i\) in \(\mathbb{Q}(\zeta_f)\) with an even number of the \(\epsilon_i\) actually being \(f/2\)-roots of unity. Similarly, let \(\beta_f^- (n)\) count the number of times a sum satisfies \(\epsilon_1 + \cdots + \epsilon_n = 0\) for \(f\)-roots of unity \(\epsilon_i\) in \(\mathbb{Q}(\zeta_f)\) with an odd number of the \(\epsilon_i\) actually being \(f/2\)-roots of unity. Clearly \(\beta_f^+ (n) + \beta_f^- (n) = \beta_f (n)\) for any \(n\), and also \(\beta_f^+ (n) = \beta_f^- (n)\) if \(n\) is odd. Define an adjusted counting function \(\hat{\beta}_f (n)\) by

\[
(28) \quad \hat{\beta}_f (n) = \beta_f^+ (n) - \beta_f^- (n)
\]

for any positive integer \(n\). Note that \(\hat{\beta}_f (n) = 0\) if \(n\) is odd.

In terms of this adjusted counting function and exceptional sets \(\xi_f (n)\) as before, we find

**Theorem 4.** Suppose \((p - 1)/f\) is odd where \(\hat{B}(X) = \exp (- \sum_{n=1}^\infty \hat{\beta}_f (n) X^n/n)\) with \(\hat{\beta}_f (n)\) defined by (28). Then for each natural number \(N\), the congruence

\[
G(X) \equiv \hat{B}(i^* \sqrt{n}X)^\phi(p^n)/f \quad (\text{mod } X^N)
\]

holds in \(\mathbb{Z}[X]\) for all odd primes powers \(p^\alpha\) (\(\alpha > 1\)) except those lying in \(\xi_f (n)\) for some \(n < N\).

**Proof.** In this case the inner sum in the expansion for \(\log G(X)\) in the proof of Theorem 3 can be expressed

\[
(29) \quad \sum_{j=1}^e \left( \sum_{H \cap \mathbb{Z}_{p^n}^*} \frac{t_j x}{p} \left( \frac{c_{t_j x}}{p} \right)^n \right) = \frac{1}{f} \sum_{r \in \mathbb{Z}_{p^n}^*} \left( \sum_{x \in H \cap \mathbb{Z}_{p^n}^*} \frac{r x}{p} \left( \frac{c_{r x}}{p} \right)^n \right)
\]

since \((\frac{2}{x}) = -1\) for any \(x \in H - H^2\). Here \(H^2\) is just the set of \(f/2\)-roots of unity in \(\mathbb{Z}_{p^n}^*\), \(\sum^+\) is the sum over tuples \((x_1, \ldots, x_n)\) with an even number of components lying in \(H - H^2\) and \(\sum^-\) is the analogous sum over tuples \((x_1, \ldots, x_n)\) with an odd number of components lying in \(H - H^2\). If \(p^\alpha\) is not in any \(\xi_f (n')\) for \(n'< N\), then each term \(\sum_{r \in \mathbb{Z}_{p^n}^*} (\frac{r}{p})^\phi(p^n) \zeta^{r(x_1 + \cdots + x_n)} = 0\) in (29) and hence \(S_n = 0\) when \(n\) is odd, since no sum \(x_1 + \cdots + x_n\) is exactly divisible by \(p^{\alpha - 1}\). When \(n\) is even, there may be sums \(x_1 + \cdots + x_n\) divisible by \(p^{\alpha}\), each such sum \(\sum_{r \in \mathbb{Z}_{p^n}^*} \zeta^{r(x_1 + \cdots + x_n)}\) contributing \(\phi(p^n)\) in (29). Overall, there are \(\beta_f^+(n)\) of these with a + sign and \(\beta_f^-(n)\) with a - sign, so (29) matches \(\frac{\phi(p^n)}{f} (\beta_f^+(n) - \beta_f^-(n))\). This establishes the assertion of the theorem with \(\hat{B}(X)\) defined in terms of the adjusted sums \(\hat{\beta}_f (n)\) in (28). \(\square\)
Example 4. Consider $p = 7$ with $f = 6$. Here one finds $\beta_6^+(1) = \beta_6^-(1) = 0$, $\beta_6^+(2) = 0$, $\beta_6^-(2) = 6$, $\beta_6^+(3) = \beta_6^-(3) = 6$, $\beta_6^+(4) = 90$, $\beta_6^-(4) = 0$, $\beta_6^+(5) = \beta_6^-(5) = 180$, $\beta_6^+(6) = 180$ and $\beta_6^-(6) = -1860$ to obtain values $\hat{\beta}_6(2) = -6$, $\hat{\beta}_6(4) = 90$ and $\hat{\beta}_6(6) = -1680$ in (28). Then

$$\hat{B}(X) = 1 + 3X^2 - 18X^4 + 217X^6 + \cdots$$

in Theorem 4 so

$$\hat{B}(i\sqrt{7}X) = 1 - 21X^2 - 18 \cdot 7^2X^4 - 217 \cdot 7^3X^6 - \cdots.$$ 

One may take $H = \{\pm 1, \pm 18, \pm 19\}$ for $m = 49$ or 343. From Table 2 one finds that 49 first appears in $\xi_6(3)$, whereas 343 first appears in $\xi_6(8)$. The minimal polynomial for the reciprocal of $\psi_1 = i\sqrt{7}(\xi_{49} + \zeta_{49}^{18} + \zeta_{49}^{-19} - \zeta_{49}^{-1} - \zeta_{49}^{-18} - \zeta_{49}^{19})$ in (26)

is

$$1 - 7^2 \cdot 3X^2 - \frac{7^3}{2}X^3 + \frac{7^4}{2}X^4 + 2 \cdot \frac{7^5}{2}X^5 - \frac{7^6}{2}X^6,$$

whereas that for the reciprocal of $\psi_1 = i\sqrt{7}(\xi_{343} + \zeta_{343}^{18} + \zeta_{343}^{-19} - \zeta_{343}^{-1} - \zeta_{343}^{-18} - \zeta_{343}^{19})$ begins

$$1 - 7^3 \cdot 3X^2 - 7^4 \cdot 198X^4 - 7^6 \cdot 1111X^6 + 7^7 \cdot 29027X^8 + 7^8 \cdot 6X^9 + \cdots.$$

The underscored coefficients deviate as expected from the pattern of the beginning coefficients given in Theorem 4.

Example 5. Next consider $p = 5$ with $f = 4$. One readily finds that

$$\hat{\beta}_4(n) = \begin{cases} n^2 & \text{if } n \text{ is even} \\ n/2 & \text{if } n \text{ is odd} \end{cases}$$

in (28) so

$$\hat{B}(X) = 1 - 2X^2 - 7X^4 - 50X^6 - 456X^8 - \cdots$$

in Theorem 4 and hence

$$\hat{B}(\sqrt{5}X) = 1 - 10X^2 - 52 \cdot 7X^4 - 5^5 \cdot 2X^6 - 5^4 \cdot 456X^8 - \cdots.$$ 

Here we take $H = \{\pm 1, \pm 7\}$ for $m = 25$ and $H = \{\pm 1, \pm 57\}$ for $m = 125$ again as in Example 2, where 25 first appears in $\xi_4(3)$ and 125 first appears in $\xi_4(7)$. The minimal polynomial for the reciprocal of $\psi_1 = \sqrt{5}(\xi_{25} + \zeta_{25}^{-1} - \zeta_{25}^{-7} - \zeta_{25}^{-5})$ is

$$1 - 50X^2 + 125X^3 + 125X^4 - 500X^5,$$

whereas that for the reciprocal of $\psi_1 = \sqrt{5}(\xi_{125} + \zeta_{125}^{-1} - \zeta_{125}^{57} - \zeta_{125}^{-57})$ begins

$$1 - 250X^2 + 5^4 \cdot 41X^4 - 5^7 \cdot 18X^7 - 5^7 \cdot 7X^7 + \cdots.$$ 

The underscored coefficients deviate as expected from the pattern given in Theorem 4.

One may have noticed that $\hat{\beta}_4(n) = \beta_4(n)$ in the last example. More generally,

Proposition 3. For $\nu > 1$, $\hat{\beta}_{2\nu}(n)$ in (28) satisfies $\hat{\beta}_{2\nu}(n) = \beta_{2\nu}(n)$. 

Proof. We first note that no sum of an odd number of $2^\nu$-roots of unity for $\nu \geq 1$ can vanish since each such root of unity is congruent to 1 mod $\pi_2$, where $\pi_2$ is the unique prime above 2 in $\mathbb{Q}(\zeta_2)$. Now we assert no sum of an odd number of primitive $2^\nu$-roots of unity can lie in $\mathbb{Q}(\zeta_{2\nu-1})$ for $\nu > 1$. Suppose to the contrary a sum $\zeta_{2\nu}^i + \cdots + \zeta_{2\nu}^{i_k}$ lies in $\mathbb{Q}(\zeta_{2\nu-1})$, where $\nu > 1$ and the $i_j$ and $n$ are odd. Then $\zeta_{2\nu}(\zeta_{2\nu-1})^{i/2} + \cdots + \zeta_{2\nu}(\zeta_{2\nu-1})^{i_k/2}$ lies in $\mathbb{Q}(\zeta_{2\nu-1})$ so $\zeta_{2\nu-1}^{i/2} + \cdots + \zeta_{2\nu-1}^{i_k/2} = 0$ contradicting our first remark. It follows easily now that for $\nu > 1$ any sum of an even number of $2^\nu$-roots of unity which vanishes must always contain an even number of primitive $2^\nu$-roots of unity. Hence $\beta_2(n) = 0$ for $n$ even. The statement of the proposition readily follows.

We conclude this section with a remark concerning the case $f = 2$, which is not governed by the last proposition. One finds in this case that the counting function $\beta_2(n) = \beta(n)$ in (27) whenever $p \equiv 1 (\text{mod } 4)$, whereas $\beta_2(n) = (-1)^{n/2}\beta_2(n)$ in (28) for $p \equiv 3 (\text{mod } 4)$. In each case, the respective power series $\hat{B}(X) = \exp(-\sum_{n=1}^{\infty} \beta_2(n)X^n/n)$ in Theorems 3 or 4 satisfies

$$B(i^*X) = \exp\left(-\sum_{n=1}^{\infty} \left(\frac{2n}{n}\frac{x^{2n}}{2n}\right)\right) = \frac{1}{2}(1 + \sqrt{1-4X^2}).$$

In particular for the case $f = 2$, one finds for any odd prime power $p^\alpha$, $\alpha > 1$ that the congruence

$$G(X) = B(\sqrt[p^\alpha]{X})^{\phi(p^\alpha)/2} \mod X^N$$

holds in $\mathbb{Z}[X]$ for $N = p^{\alpha-1}$ but not for $N > p^{\alpha-1}$, where

$$B(X) = \exp\left(-\sum_{n=1}^{\infty} \left(\frac{2n}{n}\frac{x^{2n}}{2n}\right)\right).$$

Indeed, we had previously remarked in Section 3 that $p^0$ first appears in an exceptional set $\xi_2(n)$ for $n = p^{\alpha-1}$. One consequence is that the first $p^{\alpha-1}$ coefficients of $G(X)$ satisfy

$$(31) \quad c_r = \begin{cases} (-1)^{r/2}p^{r/2} & \frac{\phi(p^\alpha)}{\phi(p^\alpha)-r} \left(\frac{\phi(p^\alpha)/2 - r/2}{r/2}\right) \quad \text{if } r \text{ is even} \\ 0 \quad \text{if } r \text{ is odd} \end{cases}$$

for $1 \leq r < p^{\alpha-1}$ (chiefly, Corollary 3 in [9]). While (31) is not enough to determine $G(X)$, we have recently found a closed form formula for the coefficients of $G(X)$ analogous to (25) expressed in terms of an Aurifeuillian factor $\xi_b$ of the cyclotomic polynomial $\psi_b$. The reader is referred to [9] for details.

References


DEPARTMENT OF MATHEMATICS, UNIVERSITY OF SAN DIEGO, SAN DIEGO, CALIFORNIA 92110
E-mail address: gurak@sandiego.edu