

## 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  $\mathbf{Z}_m^*$  denote the group of reduced residues modulo  $m$ . Fix a congruence group  $H$  of conductor  $m$  and of order  $f$ . Choose integers  $t_1, \dots, t_e$  to represent the  $e = \phi(m)/f$  cosets of  $H$  in  $\mathbf{Z}_m^*$ . 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  $\mathbf{Q}$  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  $N$

$$G(X) \equiv A(X) \cdot B(X)^{\frac{p-1}{f}} \pmod{X^N}$$

holds in  $\mathbf{Z}[X]$  for all primes  $p \equiv 1 \pmod{f}$  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

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

where  $\left(\frac{\cdot}{p}\right)$  denotes the usual Legendre symbol and  $i^* = i^{\frac{(p-1)^2}{4}}$ .

### 1. INTRODUCTION

For any positive integer  $m$ , set  $\zeta_m = \exp(2\pi i/m)$  and let  $\mathbf{Z}_m^*$  denote the group of reduced residues modulo  $m$ . Fix a congruence group  $H$  defined modulo  $m$  of order  $f$  and conductor  $m$ . Choose integers  $t_1 = 1, t_2, \dots, t_e$  to represent the  $e = \phi(m)/f$  cosets of  $H$  in  $\mathbf{Z}_m^*$ . The Gauss periods

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

corresponding to  $H$  lie in the subfield  $K$  of  $\mathbf{Q}(\zeta_m)$  fixed by the Galois actions induced by sending  $\zeta_m \rightarrow \zeta_m^x$  for  $x \in H$ . They are conjugate and distinct over  $\mathbf{Q}$

---

Received by the editor June 2, 2005.

2000 *Mathematics Subject Classification*. Primary 11L05, 11T22, 11T23.

©2006 American Mathematical Society  
 Reverts to public domain 28 years from publication

[8, 11], and have minimal polynomial

$$(2) \quad g(x) = g_H(x) = x^e + c_1x^{e-1} + \cdots + c_{e-1}x + c_e$$

of degree  $e$ . For any numerical character  $\chi$  defined modulo  $m$ , the Gauss sum  $G(\chi)$  is given by

$$(3) \quad G(\chi) = \sum_{x \in \mathbf{Z}_m^*} \chi(x) \zeta_m^x.$$

The Gauss periods (1) are intimately related with the sums (3); namely,

$$(4) \quad G(\chi) = \sum_{j=1}^e \chi(t_j) \theta_j$$

for any character  $\chi$  annihilating  $H$ , and

$$(5) \quad \theta_j = \frac{1}{e} \sum_{\chi} \bar{\chi}(t_j) G(\chi) \quad (1 \leq j \leq e),$$

where  $\chi$  runs through the characters defined modulo  $m$  which annihilate  $H$ . (Here  $\bar{\chi}$  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

$$(6) \quad S_r + c_1 S_{r-1} + \cdots + c_{r-1} S_1 + r c_r = 0 \quad (1 \leq r \leq e),$$

$$S_n + c_1 S_{n-1} + \cdots + c_{e-1} S_{n-e+1} + c_e S_{n-e} = 0 \quad (n > e).$$

Alternatively, if

$$(7) \quad G(X) = G_H(X) = X^e g(X^{-1}) = 1 + c_1 X + \cdots + c_e X^e$$

is the reciprocal polynomial of  $g(x)$ , its logarithm is formally expressed as

$$(8) \quad \log G(X) = \log \prod_{j=1}^e (1 - \theta_j X) = - \sum_{n=1}^{\infty} \frac{S_n X^n}{n}$$

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

$$(9) \quad \psi_m(x) = \prod_{d|m} (x^d - 1)^{\mu(m/d)},$$

$$\text{with } \psi_{p^\alpha}(x) = x^{p^{\alpha-1}(p-1)} + \cdots + x^{p^\alpha} + 1$$

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  $p \equiv 1 \pmod{f}$ . 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  $\mathbf{Z}[X]$  for all primes  $p \equiv 1 \pmod{f}$  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,

$$(11) \quad G(X) = \sum_{r=0}^e (-1)^{\lfloor r/2 \rfloor} \binom{\lfloor e - r/2 \rfloor}{\lfloor r/2 \rfloor} X^r$$

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  $X^{p^{\alpha-1}}$ , 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

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

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  $\{1, 2^{\alpha-1} - 1\}$  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  $\mathbf{Q}(\zeta_{2^\alpha})$  not contained in  $\mathbf{Q}(\zeta_{2^{\alpha-1}})$ , and so  $\alpha > 2$ . Since  $2|f$ ,  $H$  contains an element of order two modulo  $2^\alpha$ —either  $2^\alpha - 1$ ,  $2^{\alpha-1} - 1$  or  $2^{\alpha-1} + 1$ . The last choice can be eliminated since  $H$  has conductor  $2^\alpha$ . Thus  $K$  is contained in one of the cyclic fields  $\mathbf{Q}(\zeta_{2^\alpha} + \zeta_{2^\alpha}^{-1})$  or  $\mathbf{Q}(\zeta_{2^\alpha} - \zeta_{2^\alpha}^{-1})$  which correspond to the congruence groups  $\{1, 2^\alpha - 1\}$  or  $\{1, 2^{\alpha-1} - 1\}$  modulo  $2^\alpha$ , respectively. But any proper subfield of  $\mathbf{Q}(\zeta_{2^\alpha} + \zeta_{2^\alpha}^{-1})$  or  $\mathbf{Q}(\zeta_{2^\alpha} - \zeta_{2^\alpha}^{-1})$  is a subfield of  $\mathbf{Q}(\zeta_{2^{\alpha-1}} + \zeta_{2^{\alpha-1}}^{-1})$  contained in  $\mathbf{Q}(\zeta_{2^{\alpha-1}})$ . Thus either  $K = \mathbf{Q}(\zeta_{2^\alpha} + \zeta_{2^\alpha}^{-1})$  or  $\mathbf{Q}(\zeta_{2^\alpha} - \zeta_{2^\alpha}^{-1})$ , so  $H$  equals  $\{1, 2^\alpha - 1\}$  or  $\{1, 2^{\alpha-1} - 1\}$ .  $\square$

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*

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

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

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

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

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

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

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

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  $\mathbf{Z}_{p^\alpha}^*$  is cyclic,  $H = (\mathbf{Z}_{p^\alpha}^*)^{\phi(p^\alpha)/f}$ , or equivalently  $H$  equals the group of  $f$ -roots of unity in  $\mathbf{Z}_{p^\alpha}^*$ . In particular, since  $H$  has conductor  $p^\alpha$ ,  $p \not\equiv 1 \pmod f$  so  $p \equiv 1 \pmod f$ . 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

$$(13) \quad x_1 + \dots + x_n \equiv 0 \pmod{p^\gamma}$$

for choice of tuples  $(x_1, \dots, x_n)$  with  $x_i$  in  $(\mathbf{Z}_{p^\gamma}^*)^{\phi(p^\gamma)/f}$  ( $1 \leq i \leq n$ ). 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  $(x_1, \dots, x_n)$  with  $x_i$  in  $(\mathbf{Z}_{p^\gamma}^*)^{\phi(p^\gamma)/f}$  for which  $p^{\gamma-1} \mid (x_1 + \dots + x_n)$ .*

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

$$(x + tp^{\gamma-1})^f \equiv x^f + ftp^{\gamma-1} \equiv 1 \pmod{p^\gamma}$$

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

Now observe in the expansion (8)

$$\log G(X) = - \sum_{n=1}^{\infty} S_n X^n / n = - \sum_{n=1}^{\infty} \sum_{j=1}^e \left( \sum_{x \in H} \zeta_{p^\alpha}^{t_j x} \right)^n \frac{X^n}{n},$$

that  $S_n$  equals the inner sum

$$\sum_{j=1}^e \left( \sum_{x \in H} \zeta_{p^\alpha}^{t_j x} \right)^n = \frac{1}{f} \sum_{r \in \mathbf{Z}_{p^\alpha}^*} \sum_{x_i \in H} \zeta_{p^\alpha}^{r(x_1 + \dots + x_n)}.$$

But in view of the lemma above, and since

$$\sum_{r \in \mathbf{Z}_{p^\alpha}^*} \zeta_{p^\alpha}^{rx} = \begin{cases} \phi(p^\alpha) & \text{if } p^\alpha \mid x \\ -p^{\alpha-1} & \text{if } p^{\alpha-1} \parallel x \\ 0 & \text{otherwise,} \end{cases}$$

$$\sum_{r \in \mathbf{Z}_{p^\alpha}^*} \sum_{x_i \in H} \zeta_{p^\alpha}^{r(x_1 + \dots + x_n)} = \phi(p^\alpha) T_n(p^\alpha) - p^{\alpha-1} (T_n(p^{\alpha-1}) - T_n(p^\alpha))$$

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

Thus,

$$(14) \quad S_n = \frac{p^{\alpha-1}}{f} (p T_n(p^\alpha) - T_n(p^{\alpha-1})).$$

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

$$(15) \quad S_n = \frac{\phi(p^\alpha)}{f} \beta_f(n)$$

above. Letting  $\xi_f(n)$  be the set of odd prime powers  $p^\alpha$  ( $\alpha > 1$ ),  $p \equiv 1 \pmod f$ , for which  $T_n(p^{\alpha-1}) > \beta_f(n)$  and putting

$$(16) \quad B(X) = \exp\left(-\sum_{n=1}^{\infty} \beta_f(n) \frac{X^n}{n}\right),$$

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

**Theorem 2.** *For each natural number  $N$ , the congruence*

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

*holds in  $\mathbf{Z}[X]$  for all odd prime powers  $p^\alpha$  ( $\alpha > 1$ ),  $p \equiv 1 \pmod f$ , 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

$$(17) \quad \beta_l(n) = \begin{cases} 0 & \text{if } l \nmid n \\ \frac{n!}{((n/l)!)^l} & \text{if } l \mid n \end{cases}$$

when  $l$  is a prime and

$$(18) \quad \beta_4(n) = \begin{cases} 0 & \text{if } n \text{ is odd} \\ \binom{n}{n/2}^2 & \text{if } n \text{ is even} \end{cases}$$

(see also Corollary 2 in [8]).

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  $\bar{i} = (i_1, \dots, i_n)$  in  $(\mathbf{Z}/f\mathbf{Z})^n$ , let  $P_{\bar{i}}(x)$  denote the polynomial  $x^{i_1} + \dots + x^{i_n}$  with  $i_v$  ( $1 \leq v \leq n$ ) chosen to be the least nonnegative representative of the class  $i_v \pmod f$ . Then

$$(19) \quad \beta_f(n) = \text{card}(\{\bar{i} = (i_1, \dots, i_n) \in (\mathbf{Z}/f\mathbf{Z})^n \mid \psi_f(x) \text{ divides } P_{\bar{i}}(x)\}),$$

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

$$(20) \quad T_n(p^\gamma) = \text{card}(\{\bar{i} = (i_1, \dots, i_n) \in (\mathbf{Z}/f\mathbf{Z})^n \mid \tilde{p}^\gamma \text{ divides } \zeta_f^{i_1} + \dots + \zeta_f^{i_n}\})$$

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

$$(21) \quad \tilde{p}^{\alpha-1} \mid (\zeta_f^{i_1} + \dots + \zeta_f^{i_n}) \text{ but } \zeta_f^{i_1} + \dots + \zeta_f^{i_n} \neq 0.$$

Thus  $\xi_f(n)$  consists of all odd prime powers  $p^\alpha$ ,  $p \equiv 1 \pmod f$  for which (21) holds for some tuple  $\bar{i}$  in  $(\mathbf{Z}/f\mathbf{Z})^n$ . Now a necessary condition for  $\bar{i}$  to satisfy (21) is  $R_{\bar{i}} \equiv 0 \pmod{p^{\alpha-1}}$ , but  $R_{\bar{i}} \neq 0$ , where  $R_{\bar{i}}$  denotes the resultant of  $P_{\bar{i}}(x)$  and  $\psi_f(x)$ . The resultant  $R_{\bar{i}} = 0$  if  $\psi_f(x)$  divides  $P_{\bar{i}}(x)$ . When  $\psi_f(x) \nmid P_{\bar{i}}(x)$  (so  $(\psi_f, P_{\bar{i}}) = 1$ ),  $R_{\bar{i}}$  is essentially the smallest positive integer  $R$  for which the equation  $g(x)\psi_f(x) + h(x)P_{\bar{i}}(x) = R$  is solvable with polynomials  $g, h \in \mathbf{Z}[x]$ , or equivalently, the norm  $N_{\mathbf{Q}(\zeta_f)/\mathbf{Q}} P_{\bar{i}}(\zeta_f)$ . 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 $\zeta_4 \equiv 7 \pmod{\tilde{p}_5^2}$		
$\bar{i}$	$R_{\bar{i}}$	$\zeta_f^{i_1} + \dots + \zeta_f^{i_n}$ 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 $\zeta_5 \equiv 3 \pmod{\tilde{p}_{11}^2}$		
$\bar{i}$	$R_{\bar{i}}$	$\zeta_f^{i_1} + \dots + \zeta_f^{i_n}$ factors
0000123	121	$3 - \zeta_5^4 = -\zeta_5^4(1 + \zeta_5^4)(2 + \zeta_5^3)^2$
0000124	121	$3 - \zeta_5^3 = -\zeta_5^3(1 + \zeta_5^3)(2 + \zeta_5)^2$
0000134	121	$3 - \zeta_5^2 = -\zeta_5^2(1 + \zeta_5^2)(2 + \zeta_5^4)^2$
0000234	121	$3 - \zeta_5 = -\zeta_5(1 + \zeta_5)(2 + \zeta_5^2)^2$
0001113	121	$3 + 3\zeta_5 + \zeta_5^3 = -\zeta_5^2(1 + \zeta_5^2)(2 + \zeta_5)(2 + \zeta_5^4)$
0001222	121	$3 + 3\zeta_5^2 + \zeta_5 = -\zeta_5^4(1 + \zeta_5^4)(2 + \zeta_5^2)(2 + \zeta_5^3)$
$f = 3, n = 11 : \tilde{p}_7 = \zeta_3 - 2$ where $\zeta_3 \equiv -19 \pmod{\tilde{p}_7^2}$		
$\bar{i}$	$R_{\bar{i}}$	$\zeta_f^{i_1} + \dots + \zeta_f^{i_n}$ factors
00000000111	49	$8 + 3\zeta_3 = -\zeta_3^2(\zeta_3 - 2)^2$
00000000222	49	$8 + 3\zeta_3^2 = -\zeta_3(\zeta_3^2 - 2)^2$

first restricts to those prime powers  $p^\alpha, p \equiv 1 \pmod{f}$  for which  $R_{\bar{i}} \equiv 0 \pmod{p^{\alpha-1}}$  but  $R_{\bar{i}} \not\equiv 0$  for some tuple  $\bar{i}$  in  $(\mathbf{Z}/f\mathbf{Z})^n$ . 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

$$g^{i_1} + \dots + g^{i_n} \equiv 0 \pmod{p^{\alpha-1}} \text{ with } \zeta_f^{i_1} + \dots + \zeta_f^{i_n} \neq 0$$

for some tuple  $\bar{i} = (i_1, \dots, i_n)$  in  $(\mathbf{Z}/f\mathbf{Z})^n$ . It is enough to consider tuples  $\bar{i}$ , 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  $\bar{i}$  for which  $R_{\bar{i}} \equiv 0 \pmod{p^2}$ ,  $R_{\bar{i}} \neq 0$  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  $\bar{i}$  with  $p^2 | R_{\bar{i}}$  and  $R_{\bar{i}} \neq 0$ . Representatives for each such class are given in Table 1; all have resultant  $R_{\bar{i}} = 121$ . To check if  $11^3 \in \xi_5(7)$  one may choose  $\tilde{p}_{11} = 2 + \zeta_5^2$ , where  $\zeta_5 \equiv 3 \pmod{\tilde{p}_{11}^2}$ . 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  $n$ .

TABLE 2.

$n$	$f = 3$	$f = 4$	$f = 6$
3	---	$5^2$	$7^2$
4	$7^2$	---	$13^2$
5	$13^2$	$13^2, 17^2$	$19^2$
6	---	---	$31^2$
7	$19^2, 31^2$	$5^3, 29^2, 37^2$	$37^2, 43^2$
8	$43^2$	---	$7^3$
9	---	$41^2, 53^2$	$61^2, 67^2, 73^2$
10	$37^2, 73^2$	---	$79^2$
11	$7^3, 67^2$	$61^2, 73^2, 101^2$	$97^2, 103^2$

  

$n$	$f = 5$	$f = 7$	$f = 8$
3	$11^2$	$43^2$	$17^2$
4	$61^2$	$29^2, 71^2, 547^2$	$41^2$
5	$41^2$	$113^2, 197^2,$ $421^2, 463^2$	$73^2, 89^2, 97^2$ $113^2, 257^2$
6	$31^2, 71^2$ $181^2, 521^2$	$211^2, 379^2, 449^2$ $751^2, 2689^2$	$137^2, 313^2$
7	$11^3, 101^2, 151^2$ $191^2, 461^2$	$239^2, 281^2, 337^2$ $1583^2, 1597^2$	$17^3, 193^2, 233^2$ $241^2, 281^2, 337^2$ $353^2, 409^2, 433^2,$ $641^2, 1297^2$

Here are a couple of examples to illustrate Theorem 2.

**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

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

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

$$1 - 28X^3 + \underline{7}X^4 + \underline{14}X^5 + \underline{189}X^6 + \dots,$$

whereas that for  $\theta_1^{-1} = (\zeta_{343} + \zeta_{343}^{18} + \zeta_{343}^{-19})^{-1}$  begins

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

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

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

in (16). The power 25 first appears in  $\xi_4(3)$  with  $T_3(5) = 12 > \beta_4(3) = 0$ , whereas 125 first appears in the exceptional set  $\xi_4(7)$  with  $T_7(25) = 140 > \beta_4(7) = 0$ . Here

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  $\theta_1^{-1} = (\zeta_{25} + \zeta_{25}^{-1} + \zeta_{25}^{57} + \zeta_{25}^{-57})^{-1}$  is

$$1 - 10X^2 + \underline{5}X^3 + \underline{10}X^4 + \underline{1}X^5.$$

That for  $\theta_1^{-1} = (\zeta_{125} + \zeta_{125}^{-1} + \zeta_{125}^{57} + \zeta_{125}^{-57})^{-1}$  begins

$$1 - 50X^2 + 1025X^4 - 11250X^6 + \underline{125}X^7 + \dots$$

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

$$(22) \quad G(X) = \left(\frac{1 + \sqrt{1 - 4X^2}}{2}\right)^{\phi(p^\alpha)/2} \cdot \frac{1 - \left(\frac{1 - \sqrt{1 - 4X^2}}{2X}\right)^{p^\alpha}}{1 - \left(\frac{1 - \sqrt{1 - 4X^2}}{2X}\right)^{p^{\alpha-1}}}$$

with power sums  $S_n$  satisfying

$$(23) \quad S_n = p^\alpha \sum_{t=1, t \text{ odd}}^{[np^{-\alpha}]} \binom{n}{(n - p^\alpha t)/2} - p^{\alpha-1} \sum_{t=1, t \text{ odd}}^{[np^{1-\alpha}]} \binom{n}{(n - p^{\alpha-1}t)/2}$$

if  $n$  is odd, or

$$\frac{\phi(p^\alpha)}{2} \binom{n}{n/2} + p^\alpha \sum_{t=1}^{[np^{-\alpha}/2]} \binom{n}{n/2 - p^\alpha t} - p^{\alpha-1} \sum_{t=1}^{[np^{1-\alpha}/2]} \binom{n}{n/2 - p^{\alpha-1}t}$$

if  $n$  is even. A closed form formula for  $G(X)$  is

$$(24) \quad G(X) = X^{\phi(p^\alpha)/2} + \sum_{j=0}^{(p-3)/2} X^{p^{\alpha-1}j} C_{p^{\alpha-1}(\frac{p-1}{2}-j)}(X),$$

where

$$C_d(X) = \sum_{n=0}^{[d/2]} (-1)^n \frac{d}{d-n} \binom{d-n}{n} X^{2n},$$

or equivalently with coefficients in (7) satisfying for  $1 \leq r < \phi(p^\alpha)/2$ ,

$$(25) \quad c_r = \sum_{j=0, j \equiv r \pmod{2}}^{[rp^{1-\alpha}]} (-1)^{t_j} \frac{p^{\alpha-1}(\frac{p-1}{2}-j)}{p^{\alpha-1}(\frac{p-1}{2}-j)-t_j} \binom{p^{\alpha-1}(\frac{p-1}{2}-j)-t_j}{t_j}$$

with  $c_{\phi(p^\alpha)/2} = \binom{-2}{p}$ , 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  $\mathbf{Z}[X]$  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  $\sqrt{2}(\zeta_{2^\alpha}^v + \zeta_{2^\alpha}^{-v})$  or  $\sqrt{2}(\zeta_{2^\alpha}^v - \zeta_{2^\alpha}^{-v})$  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

$$(26) \quad \psi_j = i^* \sqrt{p} \sum_{x \in H} \left(\frac{t_j x}{p}\right) \zeta_{p^\alpha}^{t_j x} \quad (1 \leq j \leq e),$$

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  $\mathbf{Q}(\zeta_{p^\alpha})$  corresponding to  $H$  with  $[K : \mathbf{Q}] = \phi(p^\alpha)/f$ . In fact  $\psi_j = \text{Tr}_{\mathbf{Q}(\zeta_{p^\alpha})/K}(i^* \sqrt{p} \zeta_{p^\alpha}^{t_j})$  ( $1 \leq j \leq e$ ), and each is seen to generate  $K$ .

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

*Proof.* It suffices to show the conjugates  $\psi_j$  ( $1 \leq j \leq e$ ) 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

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

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  $f(\chi)$  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

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

or  $i^* \sqrt{p} G(\chi\psi)$  in terms of a Gauss sum (3), where  $\psi$  is the quadratic character  $(\frac{x}{p})$  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. □

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

$$(27) \quad \hat{\beta}_f(n) = \begin{cases} \beta_f(n) & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd,} \end{cases}$$

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

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

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

holds in  $\mathbf{Z}[X]$  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

$$-\sum_{n=1}^\infty \frac{(i^* \sqrt{p}X)^n}{n} \left( \sum_{j=1}^e \left( \sum_H \left( \frac{t_j x}{p} \right)_{\zeta_{p^\alpha}^{t_j x}} \right)^n \right)$$

with inner sum

$$\sum_{j=1}^e \left( \sum_H \left( \frac{t_j x}{p} \right)_{\zeta_{p^\alpha}^{t_j x}} \right)^n = \frac{1}{f} \sum_{r \in Z_{p^\alpha}^*} \left( \sum_{x \in H} \left( \frac{rx}{p} \right)_{\zeta_{p^\alpha}^{rx}} \right)^n = \frac{1}{f} \sum_{r \in Z_{p^\alpha}^*} \left( \frac{r}{p} \right)^n \left( \sum_H \zeta_{p^\alpha}^{rx} \right)^n,$$

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

$$\frac{1}{f} \sum_{r \in Z_{p^\alpha}^*} \left( \sum_H \zeta_{p^\alpha}^{rv} \right)^n = \frac{1}{f} (p^\alpha T_n(p^\alpha) - p^{\alpha-1} T_n(p^{\alpha-1})) = \frac{\phi(p^\alpha)}{f} \beta_f(n)$$

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

$$\frac{1}{f} \sum_{r \in Z_{p^\alpha}^*} \sum_{x_i \in H} \left( \frac{r}{p} \right)_{\zeta_{p^\alpha}^{r(x_1 + \dots + x_n)}} = \frac{1}{f} \sum_{x_i \in H} \sum_{r \in Z_{p^\alpha}^*} \left( \frac{r}{p} \right)_{\zeta_{p^\alpha}^{r(x_1 + \dots + x_n)}} = 0$$

for any prime power  $p^\alpha$  not in  $\xi_f(n)$  for some  $n < N$ , since  $\sum_{r \in Z_{p^\alpha}^*} \left( \frac{r}{p} \right)_{\zeta_{p^\alpha}^{rv}} = 0$  unless  $p^{\alpha-1} || v$ . This establishes the theorem with  $\hat{B}(X)$  defined in terms of the adjusted counting function  $\hat{\beta}_f(n)$  in (27). □

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

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

in (27) with

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

in Theorem 3. Then

$$\tilde{B}(i\sqrt{7}X) = 1 + 7^3 \cdot 15X^6 - 7^6 \cdot 2775X^{12} + 7^9 \cdot 910202X^{18} - \dots$$

One may again take  $H = \{1, 18, -19\}$  for  $m = 49$  or  $343$  as in Example 1, where 49 first appears in  $\xi_3(4)$  and 343 first appears in  $\xi_3(11)$ . The minimal polynomial for the reciprocal of  $\psi_1 = i * \sqrt{7}(\zeta_{49} + \zeta_{49}^{18} + \zeta_{49}^{-19})$  begins

$$1 + \underline{7}^3 X^4 + \underline{7}^4 \cdot \underline{2} X^5 + \underline{7}^4 \cdot \underline{29} X^6 + \dots,$$

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

$$1 + 7^5 \cdot 36X^6 - \underline{7}^8 \cdot \underline{165} X^{11} + 7^9 \cdot 2325X^{12} + \dots$$

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  $\epsilon_1 + \dots + \epsilon_n = 0$  for  $f$ -roots of unity  $\epsilon_i$  in  $\mathbf{Q}(\zeta_f)$  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  $\epsilon_1 + \dots + \epsilon_n = 0$  for  $f$ -roots of unity  $\epsilon_i$  in  $\mathbf{Q}(\zeta_f)$  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*

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

holds in  $\mathbf{Z}[X]$  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

$$(29) \quad \begin{aligned} \sum_{j=1}^e \left( \sum_H \left( \frac{t_j x}{p} \right) \zeta_{p^\alpha}^{t_j x} \right)^n &= \frac{1}{f} \sum_{r \in \mathbf{Z}_{p^\alpha}^*} \left( \sum_{x \in H} \left( \frac{rx}{p} \right) \zeta_{p^\alpha}^{rx} \right)^n \\ &= \frac{1}{f} \sum_{x_i \in H}^+ \sum_{r \in \mathbf{Z}_{p^\alpha}^*} \left( \frac{r}{p} \right)^n \zeta_{p^\alpha}^{r(x_1 + \dots + x_n)} - \frac{1}{f} \sum_{x_i \in H}^- \sum_{r \in \mathbf{Z}_{p^\alpha}^*} \left( \frac{r}{p} \right)^n \zeta_{p^\alpha}^{r(x_1 + \dots + x_n)} \end{aligned}$$

since  $(\frac{x}{p}) = -1$  for any  $x \in H - H^2$ . Here  $H^2$  is just the set of  $f/2$ -roots of unity in  $\mathbf{Z}_{p^\alpha}^*$ ,  $\sum^+$  is the sum over tuples  $(x_1, \dots, x_n)$  with an **even** number of components lying in  $H - H^2$  and  $\sum^-$  is the analogous sum over tuples  $(x_1, \dots, x_n)$  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  $\sum_{r \in \mathbf{Z}_{p^\alpha}^*} (\frac{r}{p}) \zeta_{p^\alpha}^{r(x_1 + \dots + x_n)} = 0$  in (29) and hence  $S_n = 0$  when  $n$  is odd, since no sum  $x_1 + \dots + x_n$  is exactly divisible by  $p^{\alpha-1}$ . When  $n$  is even, there may be sums  $x_1 + \dots + x_n$  divisible by  $p^\alpha$ , each such sum  $\sum_{r \in \mathbf{Z}_{p^\alpha}^*} \zeta_{p^\alpha}^{r(x_1 + \dots + x_n)}$  contributing  $\phi(p^\alpha)$  in (29). Overall, there are  $\beta_f^+(n)$  of these with a  $+$  sign and  $\beta_f^-(n)$  with a  $-$  sign, so (29) matches  $\frac{\phi(p^\alpha)}{f}(\beta_f^+(n) - \beta_f^-(n))$ . 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

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

in Theorem 4 so

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

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  $\psi_1 = i\sqrt{7}(\zeta_{49} + \zeta_{49}^{18} + \zeta_{49}^{-19} - \zeta_{49}^{-1} - \zeta_{49}^{-18} - \zeta_{49}^{19})$  in (26) is

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

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

$$1 - 7^3 \cdot 3X^2 - 7^4 \cdot 198X^4 - 7^6 \cdot 1111X^6 + \underline{7^7} \cdot \underline{29027}X^8 + \underline{7^8} \cdot \underline{6}X^9 + \dots$$

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

$$\hat{\beta}_4(n) = \begin{cases} \binom{n}{n/2}^2 & \text{if } n \text{ is even} \\ 0 & \text{if } n \text{ is odd} \end{cases}$$

in (28) so

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

in Theorem 4 and hence

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

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  $\psi_1 = \sqrt{5}(\zeta_{25} + \zeta_{25}^{-1} - \zeta_{25}^7 - \zeta_{25}^{-7})$  is

$$1 - 50X^2 + \underline{125}X^3 + \underline{125}X^4 - \underline{500}X^5,$$

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

$$1 - 250X^2 + 5^4 \cdot 41X^4 - 5^7 \cdot 18X^7 - \underline{5^7}X^7 + \dots$$

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  $\mathbf{Q}(\zeta_{2^\nu})$ . Now we assert no sum of an **odd** number of primitive  $2^\nu$ -roots of unity can lie in  $\mathbf{Q}(\zeta_{2^{\nu-1}})$  for  $\nu > 1$ . Suppose to the contrary a sum  $\zeta_{2^\nu}^{i_1} + \cdots + \zeta_{2^\nu}^{i_n}$  lies in  $\mathbf{Q}(\zeta_{2^{\nu-1}})$ , where  $\nu > 1$  and the  $i_j$  and  $n$  are odd. Then  $\zeta_{2^\nu}(\zeta_{2^{\nu-1}}^{(i_1-1)/2} + \cdots + \zeta_{2^{\nu-1}}^{(i_n-1)/2})$  lies in  $\mathbf{Q}(\zeta_{2^{\nu-1}})$  so  $\zeta_{2^{\nu-1}}^{(i_1-1)/2} + \cdots + \zeta_{2^{\nu-1}}^{(i_n-1)/2} = 0$  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  $\beta_{2^\nu}^-(n) = 0$  for  $n$  even. The statement of the proposition readily follows.  $\square$

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  $\hat{\beta}_2(n) = \beta_2(n)$  in (27) whenever  $p \equiv 1 \pmod{4}$ , whereas  $\hat{\beta}_2(n) = (-1)^{[n/2]}\beta_2(n)$  in (28) for  $p \equiv 3 \pmod{4}$ . In each case, the respective power series  $\hat{B}(X) = \exp(-\sum_{n=1}^{\infty} \hat{\beta}_2(n)X^n/n)$  in Theorems 3 or 4 satisfies

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

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

$$(30) \quad G(X) \equiv B(\sqrt{p}X)^{\phi(p^\alpha)/2} \pmod{X^N}$$

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

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

Indeed, we had previously remarked in Section 3 that  $p^\alpha$  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

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

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 [3] of the cyclotomic polynomial  $\psi_p$ . The reader is referred to [9] for details.

#### REFERENCES

- [1] B.C. Berndt, R.J. Evans and K.S. Williams, *Gauss and Jacobi sums*, Wiley-Interscience, New York, (1998). MR1625181 (99d:11092)
- [2] Z. Borevich and I. Shafarevich. *Number Theory*, Academic Press, New York, (1966). MR0195803 (33:4001)
- [3] R.P. Brent, "On computing factors of cyclotomic polynomials," *Math. Comp.* 61 (1993), 131-149. MR1205459 (93m:11131)
- [4] L.E. Dickson, *Elementary Theory of Equations*, Wiley, New York.
- [5] C.F. Gauss, *Disquisitiones Arithmeticae*, Yale University Press, New Haven, (1966). MR0197380 (33:5545)

- [6] S. Gupta and D. Zagier, "On the coefficients of the minimal polynomial of Gaussian periods," *Math. Comp.* 60 (1993), 385-398. MR1155574 (93d:11086)
- [7] S. Gurak, "Minimal polynomials for Gauss circulants and cyclotomic units," *Pac. J. Math.* 102 (1982), 347-353. MR0686555 (84c:10032)
- [8] S. Gurak, "Minimal polynomials for circular numbers," *Pac. J. Math.* 112 (1984), 313-331. MR0743988 (85i:11107)
- [9] S. Gurak, "Minimal polynomials for Gauss periods with  $f=2$ ," *Acta Arith.* 121 (2006), 233-257.
- [10] S. Gurak, "Explicit evaluation of multi-dimensional Kloosterman sums for prime powers" (to appear).
- [11] H. Hasse, *Vorlesungen über Zahlentheorie*, Springer-Verlag, Berlin, (1950). MR0051844 (14:534c)
- [12] J. Neukirch, *Class Field Theory*, Springer-Verlag, New York, (1986). MR0819231 (87i:11005)
- [13] H. Salie, "Über die Kloostermanschen Summen  $S(u,v;q)$ ," *Math. Z.* 34 (1932), 91-109. MR1545243

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