Canad. Math. Bull. Vol. **50** (1), 2007 pp. 71–84

# Polynomials for Kloosterman Sums

S. Gurak

*Abstract.* Fix an integer $m > 1$, and set $\zeta_m = \exp(2\pi i/m)$. Let $\bar{x}$ denote the multiplicative inverse of $x$ modulo $m$. The Kloosterman sums $R(d) = \sum_x \zeta_m^{x+d\bar{x}}$, $1 \le d \le m$, $(d, m) = 1$, satisfy the polynomial

$$f_m(x) = \prod_d (x - R(d)) = x^{\phi(m)} + c_1 x^{\phi(m)-1} + \cdots + c_{\phi(m)},$$

where the sum and product are taken over a complete system of reduced residues modulo $m$. Here we give a natural factorization of $f_m(x)$, namely,

$$f_m(x) = \prod_\sigma f_m^{(\sigma)}(x),$$

where $\sigma$ runs through the square classes of the group $\mathbf{Z}_m^*$ of reduced residues modulo $m$. Questions concerning the explicit determination of the factors $f_m^{(\sigma)}(x)$ (or at least their beginning coefficients), their reducibility over the rational field $\mathbf{Q}$ and duplication among the factors are studied. The treatment is similar to what has been done for period polynomials for finite fields.

## 1 Introduction

For fixed integers $a$ and $m$ with $m > 1$ and $(a, m) = 1$, the *Kloosterman sums of order m* are

$$R(a, d, m) = R(d) = \sum_x \zeta_m^{a(x+d\bar{x})} \quad 1 \le d \le m, (d, m) = 1, \tag{1}$$

where $\zeta_m = \exp(2\pi i/m)$ and $\bar{x}$ denotes the multiplicative inverse of $x$ modulo $m$. (The sum is over a complete system of reduced residues modulo $m$.) The Kloosterman sums (1) satisfy the polynomial

$$f_m(x) = \prod_d (x - R(d)) = x^{\phi(m)} + c_1 x^{\phi(m)-1} + \cdots + c_{\phi(m)}, \tag{2}$$

where the product is taken over a complete system of reduced residues modulo $m$. The polynomial $f_m(x)$ is independent of the choice of $a$, so we will choose $a = 1$ throughout.

The Kloosterman sums (1) and their generalizations have been widely studied, particularly their connections to modular forms [9, 13]. Little attention has been given to the Kloosterman polynomial (2) though, so here we study questions regarding the factorization of $f_m(x)$ over the rational field $\mathbf{Q}$, and certain arithmetic

Received by the editors December 17, 2004; revised July 5, 2005.
AMS subject classification: 11L05, 11T24.

properties of the $n$-th power sums associated to its factors. The treatment is similar to what has been done for period polynomials for finite fields [6, 7, 11].

We begin by stating results known for the case $m = p$, an odd prime, which essentially date back to Salie [12]. For $m = p$, an odd prime, it is known that

$$f_p(x) = f_p^+(x) \cdot f_p^-(x) \tag{3}$$

as a product of two distinct irreducible polynomials, each of degree $(p-1)/2$, where

$$f_p^+(x) = \prod_{\left(\frac{d}{p}\right)=1} (x - R(d)) = x^{(p-1)/2} + c_1^+ x^{(p-3)/2} + \cdots + c_{(p-1)/2}^+ \tag{4}$$

and

$$f_p^-(x) = \prod_{\left(\frac{d}{p}\right)=-1} (x - R(d)) = x^{(p-1)/2} + c_1^- x^{(p-3)/2} + \cdots + c_{(p-1)/2}^-. \tag{5}$$

Salie evaluated the power sums

$$\begin{gathered} S_n^+(p) = \sum_{\left(\frac{d}{p}\right)=1} R(d)^n, \quad S_n^-(p) = \sum_{\left(\frac{d}{p}\right)=-1} R(d)^n, \\ S_n(p) = \sum_{(d,p)=1} R(d)^n = S_n^+(p) + S_n^-(p) \end{gathered} \tag{6}$$

for small values of $n$. Namely,

$$\begin{gathered} S_1 = 1, \quad S_2 = p^2 - p - 1, \quad S_3 = \left(\tfrac{-3}{p}\right)p^2 + 2p + 1, \\ S_4 = 2p^3 - 3p^2 - 3p - 1, \quad S_1^+ = \frac{1}{2}\left(1 + \left(\tfrac{-1}{p}\right)p\right), \\ S_2^+ = \frac{1}{2}(p^2 - 2p - 1), \quad S_1^- = \frac{1}{2}\left(1 - \left(\tfrac{-1}{p}\right)p\right), \quad S_2^- = \frac{1}{2}(p^2 - 1), \end{gathered} \tag{7}$$

where $\left(\tfrac{-}{-}\right)$ denotes the usual Legendre symbol.

Later, D. Lehmer [10] showed that

$$S_3^+ = p^2 + 2p\left(1 + 2\left(\tfrac{-1}{p}\right)A^2\right) \quad \text{or} \quad S_3^+ = p^2\left(2\left(\tfrac{-1}{p}\right) - 1\right) + 2p$$

and

$$S_3^- = p^2 + 2p\left(1 - 2\left(\tfrac{-1}{p}\right)A^2\right) \quad \text{or} \quad S_3^- = -p^2\left(2\left(\tfrac{-1}{p}\right) + 1\right) + 2p$$

as $p \equiv 1$ or $5 \pmod 6$, where $p = A^2 + 3B^2$ when $p \equiv 1 \pmod 6$. But beyond this, little else is known in the case $m = p$.

Of course, from the Newton identities

$$c_r = -\frac{1}{r}(S_r + c_1 S_{r-1} + \cdots + c_{r-1}S_1) \quad \text{for } 1 \le r \le p-1, \tag{8}$$

one obtains the formulas

$$c_1 = -1, \quad c_2 = -\frac{1}{2}(p^2 - p - 2), \quad c_3 = -\frac{1}{6}\big(p^2(2\left(\tfrac{-3}{p}\right) - 3) + 7p + 6\big),$$

and similarly,

$$c_1^+ = -\frac{1}{2}(1 + \left(\tfrac{-1}{p}\right)p), \quad c_2^+ = -\frac{1}{8}(p^2 - 2p\big(2 + \left(\tfrac{-1}{p}\right)\big) - 3),$$

and

$$c_3^+ = \frac{1}{48}\big(5\left(\tfrac{-1}{p}\right)p^3 - p^2\big(5 + 12\left(\tfrac{-1}{p}\right)\big) - p\big(28 + \left(\tfrac{-1}{p}\right)(9 + 32A^2)\big) - 15\big)$$

or

$$c_3^+ = \frac{1}{48}\big(5\left(\tfrac{-1}{p}\right)p^3 + p^2\big(11 - 28\left(\tfrac{-1}{p}\right)\big) - p(28 + \left(\tfrac{-1}{p}\right)9) - 15\big)$$

as $p \equiv 1$ or $5 \pmod 6$; and

$$c_1^- = -\frac{1}{2}(1 - \left(\tfrac{-1}{p}\right)p), \quad c_2^- = -\frac{1}{8}(p^2 + 2\left(\tfrac{-1}{p}\right)p - 3)$$

and

$$c_3^- = \frac{1}{48}\Big(-5\left(\tfrac{-1}{p}\right)p^3 - 5p^2 + p\big(\left(\tfrac{-1}{p}\right)(9 + 32A^2) - 16\big) - 15\Big)$$

or

$$\frac{1}{48}\Big(-5\left(\tfrac{-1}{p}\right)p^3 + p^2\big(11 + 16\left(\tfrac{-1}{p}\right)\big) - p\big(16 - 9\left(\tfrac{-1}{p}\right)\big) - 15\Big)$$

as $p \equiv 1$ or $5 \pmod 6$, for the beginning coefficients of $f_p(x)$, $f_p^+(x)$ and $f_p^-(x)$, respectively.

Here we investigate the general case for composite $m$, first giving a natural factorization of $f_m(x)$ as in (3), namely,

$$f_m(x) = \prod_\sigma f_m^{(\sigma)}(x)$$

with $\sigma$ running through the various square classes $(\bmod\ m)$ and each $f_m^{(\sigma)}(x)$ either irreducible or a power of an irreducible over $\mathbf{Q}$. The $n$-th power sums $S_n^{(\sigma)}$ associated with each factor of $f_m^{(\sigma)}(x)$ are seen to be products of the Salie sums (6) or their prime power analogs. Consequences of Salie's explicit evaluation of $R(1, d, p^\alpha)$ for prime powers $p^\alpha$ with $\alpha > 1$ are detailed next in Section 3. In particular, the sums $S_n^{(\sigma)}(p^\alpha)$ are explicitly given, together with formulas for the corresponding factors $f_m^{(\sigma)}(x)$. In the last section, questions concerning duplication and reducibility among the factors $f_m^{(\sigma)}(x)$ of $f_m(x)$ are examined in general for composite $m$. Evidence suggested that $f_m^{(\sigma)}(x)$ is either of the form $x^k$ or irreducible, and indeed we demonstrate this is always the case.

We consider only the classical Kloosterman sums (1) here. There are natural extensions of the theory for higher dimensional Kloosterman sums, hyper Kloosterman sums and certain Kloosterman sums defined over residue rings of algebraic integers. These generalizations will appear in a sequel.

## 2 Factorization of the Kloosterman Polynomial

Here we give a generalization of the factorization of $f_m(x)$ in (3) for any composite $m$. First note that the set of conjugates of a given Kloosterman sum $R(1,d,m)$ is

$$\{R(a,d,m) = R(1,da^2,m) \mid 1 \le a \le [m/2], (a,m) = 1\},$$

since $R(1,d,m)$ is sent to $R(a,d,m) = \sum_x \zeta_m^{ax+ad\bar{x}} = \sum_{ax} \zeta_m^{ax+a^2d\bar{a}\bar{x}} = \sum_x \zeta_m^{x+da^2\bar{x}} = R(1,da^2,m)$ under the action induced by $\zeta_m \to \zeta_m^a$. Further, $R(1,d,m)$ is fixed by the actions induced by $\zeta_m \to \zeta_m^c$ where $c^2 \equiv 1 \pmod{m}$, and so lies in the field $K$ which is the compositum of the real cyclotomic subfields $\mathbf{Q}(\zeta_{p^\alpha} + \zeta_{p^\alpha}^{-1})$ for odd primes $p$ where $p^\alpha || m$ and also $\mathbf{Q}(\zeta_{2^{\alpha-1}} + \zeta_{2^{\alpha-1}}^{-1})$ when $2^\alpha || m$ with $\alpha > 3$. In any case, it follows from Galois theory that $f_m(x)$ factors in $\mathbf{Z}[x]$ as

$$f_m(x) = \prod_{\sigma \in \mathbf{Z}_m^*/\mathbf{Z}_m^{*2}} f_m^{(\sigma)}(x) \tag{9}$$

with each factor

$$f_m^{(\sigma)}(x) = \prod_{d \in \sigma \mathbf{Z}_m^{*2}} (x - R(d)) = x^k + c_1^{(\sigma)} x^{k-1} + \cdots + c_k^{(\sigma)} \tag{10}$$

irreducible or a power of an irreducible, and of degree $k = [K:\mathbf{Q}] = |\mathbf{Z}_m^{*2}|$. We may distinguish the various square classes (mod $m$) by denoting the *signature of* $d$, $s(d) = (s_p(d))$ as a tuple of $\pm 1$'s for each prime $p|m$, where

$$s_2(d) = \begin{cases} (\,) & \text{if } 2||m, \\ \left(\frac{-1}{d}\right) & \text{if } 4||m, \\ \left(\left(\frac{-1}{d}\right), \left(\frac{2}{d}\right)\right) & \text{if } 8|m, \end{cases}$$

$$s_2(d) = (\,) \text{ if } 2||m \text{ or } \left(\frac{-1}{d}\right) \text{ if } 4||m \text{ or } \left(\left(\frac{-1}{d}\right), \left(\frac{2}{d}\right)\right) \text{ if } 8|m$$

and

$$s_p(d) = \left(\frac{d}{p}\right) \text{ for any odd prime } p|m.$$

A square class $\sigma\mathbf{Z}_m^{*2}$ is then identified by the common signature of any $d$ in $\sigma\mathbf{Z}_m^{*2}$.

To illustrate, consider the case $m = 15 = 3 \cdot 5$. Then $\mathbf{Z}_{15}^{*2} = \{1,4\}$, so $k = 2$ and $s(d) = (\left(\frac{d}{3}\right), \left(\frac{d}{5}\right))$. One finds

$$f_{15}(x) = (x^2 + 3x - 1)(x^2 - 2x - 4)(x^2 - 6x + 4)(x^2 + 4x - 16),$$

with respective factors $f^{(1,1)}$, $f^{(1,-1)}$, $f^{(-1,1)}$ and $f^{(-1,-1)}$ irreducible and distinct.

When $m = 48 = 16 \cdot 3$, $\mathbf{Z}_{48}^{*2} = \{1, 25\}$, so again $k = 2$, now with $s(d) = \left(\left(\frac{-1}{d}\right), \left(\frac{2}{d}\right), \left(\frac{d}{3}\right)\right)$. One finds

$$f_{48}(x) = (x^2 - 32)(x^2 - 128)x^2 \cdot x^2(x^2 - 32)(x^2 - 128)x^2 \cdot x^2$$

https://doi.org/10.4153/CMB-2007-007-2 Published online by Cambridge University Press

with respective factors $f^{(1,1,1)}$, $f^{(1,1,-1)}$, $f^{(-1,-1,1)}$, $f^{(-1,-1,-1)}$, $f^{(1,-1,1)}$, $f^{(1,-1,-1)}$, $f^{(-1,1,1)}$ and $f^{(-1,1,-1)}$. Here, duplications and some reducibility occur.

Next, consider the power sums associated with each factor $f_m^{(\sigma)}(x)$,

$$S_n^{(\sigma)}(m) = \sum_{d,s(d)=\sigma} (R(d,m))^n, \tag{11}$$

so

$$S_n(m) = \sum_{\sigma\in \mathbf{Z}_m^*/\mathbf{Z}_m^{*2}} S_n^{(\sigma)}(m), \tag{12}$$

where $m = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ as a product of distinct prime powers with $p_1 < p_2 < \cdots < p_r$ and $\alpha_i > 0 (1 \le i \le r)$. Then it is easily seen that $k = |\mathbf{Z}_m^{*2}| = \phi(m)/2^{r-1}$, $\phi(m)/2^r$ or $\phi(m)/2^{r+1}$ according as (i) $2||m$, (ii) $m$ odd or $4||m$ or (iii) $8|m$, respectively. Now identify each square class $\sigma = (\sigma_{p_1},\dots,\sigma_{p_r})$, where $\sigma_{p_i} = s_{p_i}(d)$ for any $d$ in $\sigma\mathbf{Z}_m^{*2}$. Then the sums $S_n^{(\sigma)}(m)$ and $S_n(m)$ factor nicely as a product of their respective prime power components. Namely,

***Theorem 2.1*** *With notation as above,*

$$S_n^{(\sigma)}(m) = \prod_{i=1}^r S_n^{\sigma_{p_i}}(p_i^{\alpha_i}) \quad \textit{and} \quad S_n(m) = \prod_{i=1}^r S_n(p_i^{\alpha_i}).$$

Before proving the theorem we require the following lemma.

***Lemma 2.2*** *Let $m = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ as a product of prime powers as above. Then for any $(d,m) = 1$, $R(1,d,m) = \prod_{i=1}^r R(1,d_i,p_i^{\alpha_i})$ with $d_i$ uniquely determined by the congruences*

$$d_i \equiv d(\bar{m}_i)^2 \mod p_i^{\alpha_i} \quad (1 \le i \le r), \tag{13}$$

*where $m_i = mp_i^{-\alpha_i}$, $(1 \le i \le r)$.*

**Proof** Now each $R(1,d_i,p_i^{\alpha_i}) = \sum_{x_i} \zeta_m^{m_i(x_i+d_i\bar{x}_i)}$ $(1 \le i \le r)$, so

$$\begin{aligned}\prod_{i=1}^r R(1,d_i,p_i^{\alpha_i}) &= \sum_{x_1,\dots,x_r} \zeta_m^{m_1x_1+\cdots+m_rx_r+m_1d_1\bar{x}_1+\cdots+m_rd_r\bar{x}_r}\\ &= \sum_{x_1,\dots,x_r} \zeta_m^{m_1x_1+\cdots+m_rx_r+d\bar{d}(m_1d_1\bar{x}_1+\cdots+m_rd_r\bar{x}_r)}.\end{aligned}$$

Since the congruences $x \equiv m_ix_i \pmod{p_i^{\alpha_i}}$ $(1 \le i \le r)$ have a unique solution $x \pmod m$ for each choice of $x_i$ relatively prime to $p_i^{\alpha_i}$, $(1 \le i \le r)$, it follows from the Chinese Remainder Theorem that $x = m_1x_1 + \cdots + m_rx_r$ runs through a reduced system of residues mod $m$ as the $x_i$ independently run through a reduced

https://doi.org/10.4153/CMB-2007-007-2 Published online by Cambridge University Press

system of residues mod $p_i^{\alpha_i}$ $(1 \leq i \leq r)$. To establish the lemma it suffices to show that $\bar{d}(m_1 d_1 \bar{x}_1 + \cdots + m_r d_r \bar{x}_r)$ equals $\bar{x}$ precisely when (13) holds. But $x\bar{d}(m_1 d_1 \bar{x}_1 + \cdots + m_r d_r \bar{x}_r) \equiv m_i x_i \bar{d} m_i d_i \bar{x}_i \equiv m_i^2 \bar{d} d_i \equiv 1 \pmod{p_i^{\alpha_i}}$ if and only if $d_i \equiv d(\bar{m}_i)^2 \pmod{p_i^{\alpha_i}}$ $(1 \leq i \leq r)$, so the last assertion follows readily from the Chinese Remainder Theorem. ∎

**Proof of Theorem 2.1** From Lemma 2.2,

$$S_n^{(\sigma)}(m) = \sum_{d, s(d)=\sigma} R(d)^n = \sum_{d, s(d)=\sigma} \prod_{i=1}^{r} R(1, d_i, p_i^{\alpha_i})^n,$$

where $d_i \equiv d(\bar{m}_i)^2 \pmod{p_i^{\alpha_i}}$ $(1 \leq i \leq r)$. Expanding the right-hand side and comparing terms with those obtained in expanding the product

$$\prod_{i=1}^{r} \sum_{d_i, s_{p_i}(d_i)=\sigma_{p_i}} R(1, d_i, p_i^{\alpha_i})^n,$$

one finds equality by the Chinese Remainder Theorem, since $s_{p_i}(d_i) = s_{p_i}(d)$ for $1 \leq i \leq r$, from (13). This establishes the first product identity. The latter follows similarly by considering all $d$ with $(d, m) = 1$. ∎

The following corollary is readily deduced from Lemma 2.2 and Theorem 2.1 using Galois theory and the fact $R(1, 1, 2) = 1$.

***Corollary 2.3*** *For odd $m > 1$, $f_{2m}^{(\sigma)}(x) = f_m^{(\sigma)}(x)$.*

## 3 The Prime Power Case $m = p^\alpha$, $\alpha > 1$

Here we give explicit expressions for the sums $S_n^{(\sigma)}(p^\alpha)$ and formulas for the factors $f_m^{(\sigma)}(x)$ for prime powers $p^\alpha$ when $\alpha > 1$, using the results of Salie [12]. To this end, we first mention some facts concerning the minimal polynomials for certain Gauss periods and their quadratic twists [8] which will be needed. Note that the quantity $2\cos(2\pi/2^\alpha) = \zeta_{2^\alpha} + \zeta_{2^\alpha}^{-1}$ for $\alpha \geq 3$ has minimal polynomial $Q_{2^\alpha}(x)$ of degree $2^{\alpha-2}$ given recursively by

$$Q_8(x) = x^2 - 2, \quad Q_{2^\alpha}(x) = Q_{2^{\alpha-1}}(x^2 - 2) \quad \text{for } \alpha \geq 4, \tag{14}$$

since $(2\cos(2\pi/2^\alpha))^2 - 2 = 2\cos(2\pi/2^{\alpha-1})$. The corresponding sums of $n$-th powers of zeros of $Q_{2^\alpha}(x)$ are seen [8] to satisfy $S_n = 0$ if $n$ is odd; otherwise for even $n$,

$$S_n = 2^{\alpha-2}\binom{n}{n/2} + 2^{\alpha-1} \sum_{t=1}^{[n2^{1-\alpha}]} (-1)^t \binom{n}{(n - 2^{\alpha-1}t)/2}. \tag{15}$$

The polynomial $Q_{2^\alpha}(x)$ is just $A_{2^{\alpha-2}}(x)$ (chiefly, [8, Corollary 1]), where

$$A_d(x) = \sum_{n=0}^{[d/2]} (-1)^n \frac{d}{d-n} \binom{d-n}{n} x^{d-2n} \tag{16}$$

is defined for any integer $d > 0$. Here [ ] denotes the greatest integer function.

When $p$ is an odd prime with $\alpha \geq 2$, the quantity $2\cos(2\pi/p^\alpha) = \zeta_{p^\alpha} + \zeta_{p^\alpha}^{-1}$ has minimal polynomial $Q_{p^\alpha}(x)$ of degree $\phi(p^\alpha)/2$ and sums of $n$-th powers of zeros satisfying [8]

(17)
$$S_n = \binom{n}{n/2} \frac{\phi(p^\alpha)}{2} + p^\alpha \sum_{t=1}^{[np^{-\alpha}/2]} \binom{n}{n/2 - p^\alpha t} - p^{\alpha-1} \sum_{t=1}^{[np^{1-\alpha}/2]} \binom{n}{n/2 - p^{\alpha-1} t}$$

if $n$ is even, or

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

if $n$ is odd. Its minimal polynomial is explicitly given (chiefly, [8, Corollary 2]) by

$$Q_{p^\alpha}(x) = 1 + \sum_{j=0}^{(p-3)/2} A_{p^{\alpha-1}(p-1-2j)/2}(x) \tag{18}$$

in terms of the polynomials $A_d(x)$, with coefficient $c_r$ of $x^{\phi(p^\alpha)/2 - r}$ for $1 \leq r < \phi(p^\alpha)/2$ given by

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

and $c_{\phi(p^\alpha)/2} = \left(\frac{-2}{p}\right)$, where $t_j = (r - p^{\alpha-1} j)/2$.

Finally, consider the quantity $i^* \sqrt{p}(\zeta_{p^\alpha} + (-1)^{(p-1)/2} \zeta_{p^\alpha}^{-1})$ when $p$ is an odd prime with $\alpha \geq 2$, where $i^* = i^{(p-1)^2/4}$. It has minimal polynomial $U_{p^\alpha}(x)$ of degree $\phi(p^\alpha)/2$ with sums of $n$-th powers of zeros satisfying [8]

$$\begin{aligned} S_n = p^{n/2} \frac{\phi(p^\alpha)}{2} \binom{n}{n/2} &+ p^{\alpha+n/2} \sum_{t=1}^{[np^{-\alpha}/2]} (-1)^{t(p-1)/2} \binom{n}{n/2 - tp^\alpha} \\ &- p^{\alpha-1+n/2} \sum_{t=1}^{[np^{1-\alpha}/2]} (-1)^{t(p-1)/2} \binom{n}{n/2 - tp^{\alpha-1}}, \end{aligned} \tag{19}$$

https://doi.org/10.4153/CMB-2007-007-2 Published online by Cambridge University Press

if $n$ is even, or

$$p^{\alpha-1+(n+1)/2}\sum_{t=1,(t,2p)=1}^{[np^{1-\alpha}]}(-1)^{(p-1)(1+tp^{\alpha-1})/4}\left(\tfrac{t}{p}\right)\binom{n}{(n-tp^{\alpha-1})/2},$$

if $n$ is odd. The minimal polynomial $U_{p^\alpha}(x)$ is explicitly described in terms of the coefficients of the Aurifeuille factors of the $p$-th cyclotomic polynomial $x^{p-1}+x^{p-2}+\cdots+1$. It has the form

$$U_{p^\alpha}(x)=a_{(p-1)/2}p^{p^{\alpha-1}[(p+1)/4]}+\sum_{j=0}^{[(p-3)/4]}a_{2j}p^{p^{\alpha-1}j}B_{p^{\alpha-1}(\frac{p-1}{2}-2j)}(x)+\sum_{j=0}^{[(p-1)/4]}a_{2j-1}p^{(p^{\alpha-1}(2j-1)+1)/2}B_{p^{\alpha-1}(\frac{p-1}{2}-2j+1)}(x) \tag{20}$$

in terms of the polynomials

$$B_d(x)=\sum_{n=0}^{[d/2]}(-1)^np^n\frac{d}{d-n}\binom{d-n}{n}x^{d-2n} \tag{21}$$

(chiefly, in [8, Corollary 3]), with coefficient $c_r$ of $x^{\phi(p^\alpha)/2-r}$ given for $1\le r<\phi(p^\alpha)/2$ by

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

where $t_j=(r-p^{\alpha-1}j)/2$ as before, and

$$c_{\phi(p^\alpha)/2}=\begin{cases}\left(\frac{2}{p}\right)p^{\phi(p^\alpha)/4} & \text{if } p\equiv 1\pmod 4,\\ (-1)^N\left(\frac{2}{p}\right)(-p)^{(\phi(p^\alpha)+2)/4} & \text{if } p\equiv 3\pmod 4,\end{cases}$$

where $N$ is the number of quadratic non-residues of $p$ in $(0,p/2)$. Here the coefficients $a_i$ arise from an Aurifeuille factor

$$a_0+a_2x+\cdots+a_{p-1}x^{(p-1)/2}+\sqrt{px}(a_1+a_3x+\cdots+a_{p-2}x^{(p-3)/2})$$

of the $p$-th cyclotomic polynomial. The reader is referred to [8, §3] for details.

Now, from Salie [12] one finds the Kloosterman sums $R(1,d,p^\alpha)$ for $\alpha>1$ explicitly up to conjugacy. Namely,

$$R(1,1,4)=-2,\quad R(1,3,4)=2,\quad R(1,3,8)=-4,\quad R(1,7,8)=4,$$

$$R(1,1,8)=R(1,5,8)=0,\quad R(1,d,16)=\begin{cases}0 & \text{if } d\equiv 3(\text{mod } 4),\\ \pm4\sqrt{2} & \text{if } d\equiv 1(\text{mod } 4),\end{cases}$$

$$R(1,d,32)=\begin{cases}0 & \text{if } d\equiv 1,3,7(\text{mod } 8),\\ \text{a conjugate of } 16\cos(2\pi/16) & \text{if } d\equiv 5(\text{mod } 8),\end{cases}$$

and for $\alpha \geq 6$, $R(1, d, 2^\alpha)$ is a conjugate of $2^{(\alpha+3)/2} \cos(2\pi/2^{\alpha-1})$ or 0 as $d \equiv 1$ or not (mod 8).

For odd primes $p$ with $\alpha > 1$, $R(1, d, p^\alpha) = 0$ if $\left(\frac{d}{p}\right) = -1$. If $\left(\frac{d}{p}\right)$, then $R(1, d, p^\alpha)$ is a conjugate of

$$\begin{cases} 2p^{\alpha/2} \cos(2\pi/p^\alpha) & \text{if } \alpha \text{ is even,} \\ 2\sqrt{p}\,p^{(\alpha-1)/2} \cos(2\pi/p^\alpha) & \text{if } \alpha \text{ is odd and } p \equiv 1 \pmod 4, \\ 2\left(\frac{-2}{p}\right)\sqrt{p}\,p^{(\alpha-1)/2} \sin(2\pi/p^\alpha) & \text{if } \alpha \text{ is odd and } p \equiv 3 \pmod 4. \end{cases}$$

The corresponding sums $S_n^{(\sigma)}(p^\alpha)$ are, in view of (15), (17) and (19), tabulated below.

***Proposition 3.1*** (i) *For $n > 0$,*

$$S_n^{\pm 1}(4) = (\mp 2)^n, \quad S_n^{(1,\pm 1)}(8) = 0, \quad S_n^{(-1,\pm 1)}(8) = (\pm 4)^n,$$

$$S_n^{(-1,\pm 1)}(16) = 0, \quad S_n^{(1,\pm 1)}(16) = \begin{cases} 0 & n \text{ odd,} \\ 2(32)^{n/2} & n \text{ even,} \end{cases}$$

$$S_n^{(-1,\pm 1)}(32) = S_n^{(1,1)}(32) = 0,$$

$$S_n^{(1,-1)}(32) = \begin{cases} 0 & n \text{ odd,} \\ 8^n\left(4\binom{n}{n/2} + 8\left(\sum_{n=1}^{[n/8]}(-1)^t\binom{n}{(n-2^{\alpha-1}t)/2}\right)\right. & n \text{ even.} \end{cases}$$

*For $\alpha \geq 6$,*

$$S_n^{(\pm 1,-1)}(2^\alpha) = S_n^{(-1,\pm 1)}(2^\alpha) = 0$$

$$S_n^{1,1}(2^\alpha) = \begin{cases} 0 & n \text{ odd,} \\ 2^{(\alpha+1)n/2}\left(2^{\alpha-3}\binom{n}{n/2} + 2^{\alpha-2}\sum_{t=1}^{[n2^{2-\alpha}]}(-1)^t\binom{n}{(n-2^{\alpha-2}t)/2}\right) & n \text{ even.} \end{cases}$$

(ii) *Assume $\alpha \geq 2$. For $n > 0$, $S_n^-(p^\alpha) = 0$.*
*For $n$ even, $S_n^+(p^\alpha)$ equals*

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

*if $\alpha$ is even or $p \equiv 1 \pmod 4$, and equals*

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

https://doi.org/10.4153/CMB-2007-007-2 Published online by Cambridge University Press

*if $\alpha$ is odd and $p \equiv 3 \pmod 4$.*

*For n odd with $\alpha$ even, $S_n^+(p^\alpha)$ equals*

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

*For n odd with $\alpha$ odd, $S_n^+(p^\alpha)$ equals*

$$p^{(n\alpha+1)/2}\cdot p^{\alpha-1} \sum_{t=1,(t,2p)=1}^{[np^{1-\alpha}]} \left(\frac{t}{p}\right)\binom{n}{(n-tp^{\alpha-1})/2}$$

*if $p \equiv 1 \pmod 4$, and equals*

$$(-1)^{(p-3)/4} p^{(n\alpha+1)/2}\cdot p^{\alpha-1} \sum_{t=1,(t,2p)=1}^{[np^{1-\alpha}]} (-1)^{(1+t)/2}\left(\frac{t}{p}\right)\binom{n}{(n-tp^{\alpha-1})/2}$$

*if $p \equiv 3 \pmod 4$.*

From the above proposition, formula (16) and remarks at the beginning of this section, one finds $f_{p^\alpha}^{(\sigma)}(x)$ for $\alpha > 1$ In particular,

$$\begin{aligned} &f_4^{\pm}(x) = x \pm 2, \quad f_8^{(-1,\pm1)}(x) = x \mp 4,\\ &f_{16}^{(1,\pm1)}(x) = x^2 - 32 \quad f_{32}^{(1,-1)}(x) = x^4 - 256x^2 + 8192,\\ &f_{2^\alpha}^{(1,1)}(x) = \sum_{n=0}^{2^{\alpha-4}} (-1)^n \frac{2^{\alpha-3}}{2^{\alpha-3}-n} 2^{(\alpha+1)i}\binom{2^{\alpha-3}-n}{n} x^{2^{\alpha-3}-2n} \end{aligned} \tag{22}$$

for $\alpha \geq 6$. For $p$ odd, $f_{p^\alpha}^+(x)$ equals $p^{\alpha\phi(p^\alpha)/4}\cdot Q_{p^\alpha}(x/p^{\alpha/2})$ if $\alpha$ is even; otherwise $f_{p^\alpha}^+(x)$ equals $p^{(\alpha-1)\phi(p^\alpha)/4}\cdot U_{p^\alpha}(x/p^{(\alpha-1)/2})$ if $p \not\equiv 7 \pmod 8$ or $-p^{(\alpha-1)\phi(p^\alpha)/4}\cdot U_{p^\alpha}(-x/p^{(\alpha-1)/2})$ if $p \equiv 7 \pmod 8$ when $\alpha > 1$ is odd, in terms of the polynomials $Q_{p^\alpha}(x)$ and $U_{p^\alpha}(x)$ described before. In each of these cases with $p$ odd, the first $p^{\alpha-1}$ coefficients of $f_{p^\alpha}^+(x)$ are seen to satisfy

$$c_r = 0 \quad \text{or} \quad (-1)^{r/2} p^{\alpha r/2} \frac{\phi(p^\alpha)}{\phi(p^\alpha)-r}\binom{\phi(p^\alpha)/2 - r/2}{r/2} \tag{23}$$

according as $r$ is odd or even with $1 \leq r < p^{\alpha-1}$.

Each of the aforementioned polynomials is irreducible. In all other cases with $\alpha > 1$, $f_{p^\alpha}^{(\sigma)}(x) = x^k$.

https://doi.org/10.4153/CMB-2007-007-2 Published online by Cambridge University Press

## 4 Duplications and Reducibility among the $f_m^{(\sigma)}(x)$

Here we examine what duplications and reducibility may appear among the factors $f_m^{(\sigma)}(x)$ of $f_m(x)$ in (9). Using Theorem 2.1 and Proposition 3.1, it is easy to determine the conditions for a given factor $f_m^{(\sigma)}(x)$ to equal $x^k$ (necessarily some component sum $S_n^{(\sigma_p)}(p^\alpha)$ equals 0 for all $n > 0$). Additional duplications can occur among the factors $f_m^{(\sigma)}(x)$ when $16||m$ for $\sigma_2 = (1,1)$ and $(1,-1)$. In particular, one notes the following.

***Proposition 4.1*** *A factor $f_m^{(\sigma)}(x) = x^k$ if and only if one of the following holds:*

(i) *$p^2|m$ for some odd prime $p$ with $\sigma_p = -1$,*
(ii) *$8||m$ with $\sigma_2 = (1, \pm 1)$,*
(iii) *$16||m$ with $\sigma_2 = (-1, \pm 1)$,*
(iv) *$32||m$ with $\sigma_2 \neq (1, -1)$,*
(v) *$64|m$ with $\sigma_2 \neq (1, 1)$.*

***Corollary 4.2*** *Factors $f_m^{(\sigma')}(x) = f_m^{(\sigma)}(x)$ if and only if one of the conditions* (i)–(v) *of Proposition* 4.1 *holds or $16||m$ with $\sigma'_p = \sigma_p$ for all odd primes $p|m$ and $\sigma'_2, \sigma_2 \in \{(1,1),(1,-1)\}$.*

Computational evidence seems to suggest that $f_m^{(\sigma)}(x)$ is irreducible whenever $f_m^{(\sigma)}(x) \neq x^k$. Indeed we can show this holds in full generality. For this we require some elementary class field theory and a generalization of the argument regarding "Lagrange" resolvents [5, Appendix].

Consider a congruence group $H$ of conductor $m$ and let $L$ be the subfield of $\mathbf{Q}(\zeta_m)$ corresponding to $H$ through class field theory, say with $[L:\mathbf{Q}] = k$. Choose coset representatives $t_1 = 1, t_2, \dots, t_k$ in $Z_m^*$ for $\mathrm{Gal}(L/\mathbf{Q})$ with each $t_i$ relatively prime to $k$, and any element $\eta$ in $L$. Label the conjugates of $\eta$ as $\eta_i = \sigma_{t_i}(\eta)$ $(1 \leq i \leq k)$, where $\sigma_t$ denotes the automorphism of $L/\mathbf{Q}$ induced by sending $\zeta_m \to \zeta_m^t$. Finally, set

$$T(\chi) = \sum_{i=1}^{k} \chi(t_i)\eta_i \tag{24}$$

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

$$\eta_i = \frac{1}{k}\sum_{\chi} \bar{\chi}(t_i)T(\chi) \quad (1 \leq i \leq k),$$

the sum taken over $\chi$ annihilating $H$. Generalizing the argument in [5, Appendix], one finds in view of the lemma there that

***Proposition 4.3*** *The $\eta_i$ $(1 \leq i \leq k)$ are distinct if $T(\chi) \neq 0$ for all $\chi$ annihilating $H$ with conductor $f(\chi) > 1$ satisfying $(m/f(\chi), f(\chi)) = 1$ where $m/f(\chi)$ is square-free.*

In the classical case $m = p$, an odd prime, with primitive root $g$ and congruence group $H = \{\pm 1\}$ of conductor $p$, one may choose $t_i = g^{i-1}$ with $\eta_i = R(1, dg^{2i-2}, p)$ $(1 \leq i \leq (p-1)/2)$ in (24) where $d \in \mathbf{Z}_p^*$.

***Proposition 4.4*** *With $H = \{\pm 1\}$ modulo $p$ and $\eta_i = R(1, dg^{2i-2}, p)$ $(1 \le i \le (p-1)/2)$ as above, $T(\chi) \neq 0$ for any even character $\chi$ modulo $p$. In particular, each $\eta_i$ generates $\mathbf{Q}(\zeta_p + \zeta_p^{-1})$.*

**Proof** Fix a character $\psi$ to generate the group of numerical characters modulo $p$. Any character which annihilates $H$ is even and of the form $\psi^{2\nu}$ for $0 \le \nu < (p-1)/2$. Using [12, (59)] to express the Kloosterman sums for $m = p$ in terms of the Gauss sums $G(\chi) = \sum_{x \in Z_p^*} \chi(x)\zeta_p^x$ for characters $\chi$ modulo $p$ and setting $\rho = \left(\frac{\cdot}{p}\right)$, one finds

$$
\begin{aligned}
T(\psi^{2\nu}) &= \sum_{i=1}^{\frac{p-1}{2}} \psi^{2\nu}(g^{i-1})\eta_i = \frac{1}{p-1} \sum_{i=1}^{\frac{p-1}{2}} \psi^{2\nu}(g^{i-1}) \sum_{j=1}^{p-1} \bar{\psi}^j(dg^{2i-2})G(\psi^j)^2 \\
&= \frac{1}{p-1} \sum_{j=1}^{p-1} \bar{\psi}^j(d)G(\psi^j)^2 \sum_{i=1}^{\frac{p-1}{2}} \psi^{\nu-j}(g^{2i-2}) \\
&= \frac{1}{2}(\bar{\psi}^\nu(d)G(\psi^\nu)^2 + \bar{\psi}^\nu\rho(d)G(\psi^\nu\rho)^2),
\end{aligned}
$$

since

$$
\sum_{i=1}^{\frac{p-1}{2}} \psi^{\nu-j}(g^{2i-2}) = \begin{cases} \frac{p-1}{2} & \text{if } j \equiv \nu \pmod{\frac{p-1}{2}} \\ 0 & \text{otherwise.} \end{cases}
$$

Choosing $\psi$ to be the Teichmuller character one readily confirms that $T(\psi^{2\nu}) \neq 0$ for $1 \le \nu < \frac{p-1}{2}$ using Stickelberger's theorem [1, Theorem 11.2.1]; whereas $T(1) = (1 \pm p)/2 \neq 0$ from (7). Thus $T(\chi) \neq 0$ for any even character $\chi$ modulo $p$, and so the last assertion of the proposition follows now from Proposition 4.3. ■

We now can establish

***Theorem 4.5*** *Each factor $f_m^{(\sigma)}(x)$ of $f_m(x)$ in (9) is either irreducible or equals $x^k$.*

**Proof** In view of Salie's results and Corollary 2.3, it suffices to consider square classes $\sigma$ where, in Theorem 2.1, no component sum $S_n^{(\sigma_p)}(p^\alpha)$ is 0 for all $n > 0$ and with $16|m$ if $m$ is even. We assert that the corresponding factors $f_m^{(\sigma)}(x)$ are irreducible. We consider the case $m$ is odd first, and choose any $d$ in $\sigma Z_m^{*2}$. Set $\eta = R(1, d, m)$, which by Lemma 2.2 is the product of $R(1, d_j, p_j^{\alpha_j})$ $(1 \le j \le r)$, with each $R(1, d_j, p_j^{\alpha_j})$ generating the real subfield $K_j$ of $\mathbf{Q}(\zeta_{p_j^{\alpha_j}})$ of degree $e_j = \phi(p_j^{\alpha_j})/2$ by our assumptions on $\sigma$ above. Here, $d_j \equiv d(\bar{m}_j)^2 \pmod{p_j^{\alpha_j}}$ $(1 \le j \le r)$, where $m_j = mp_j^{-\alpha_j}$ as before. Now $\eta$ lies in $K$, the compositum of the fields $K_j$, and corresponds to the congruence group $H = \{x \equiv \pm 1 \pmod{p_j^{\alpha_j}}\ (1 \le j \le r)\}$ of conductor $m$.

https://doi.org/10.4153/CMB-2007-007-2 Published online by Cambridge University Press

Next choose generators $s_j$ for $Z^*_{p_j^{\alpha_j}}/(\pm 1)$ with $s_j$ prime to $k$ and $s_j \equiv 1 \pmod{m_j}$ $(1 \le j \le r)$. Any coset representative $s$ in $Z^*_m/H$ can be uniquely expressed $s_1^{v_1} \cdots s_r^{v_r}$ with $0 \le v_j < e_j$ $(1 \le j \le r)$ via the canonical identification

$$Z^*_m/H \simeq \prod_{j=1}^{r} Z^*_{p_j^{\alpha_j}}/(\pm 1).$$

Given a character $\chi$ of $Z^*_m$ annihilating $H$, let $\chi = \prod_{j=1}^r \chi_j$ denote its corresponding decomposition into $p$-components, where each $\chi_j(-1) = 1$. Specifically, we obtain $\chi_j(x)$ for any $x$ in $Z^*_{p^\alpha}$, by setting $\chi_j(x) = \chi(x')$ for $x'$ satisfying $x' \equiv x \pmod{p_j^{\alpha_j}}$, $x' \equiv 1 \pmod{m_j}$. If $\chi$ has conductor $f(\chi) = p_1^{\beta_1} \cdots p_r^{\beta_r}$ where $0 \le \beta_j \le \alpha_j$, then $\chi_j$ has conductor $p_j^{\beta_j}$.

Now consider the sum

$$T_j(\chi_j) = \sum_{v_j=0}^{e_j-1} \chi_j(s_j^{v_j}) R(1, d_j s_j^{2v_j}, p_j^{\alpha_j})$$

associated to $R(1, d_j, p_j^{\alpha_j})$. We first assert that $T_j(\chi_j) \ne 0$ when $\chi_j$ has conductor $p_j^{\alpha_j}$ $(\alpha_j > 1)$. Indeed, in view of Salie's results $R(1, d_j, p_j^{\alpha_j})$ is, up to sign conjugate, equal to $i^{(p^\alpha-1)^2/4} p^{\alpha/2} (\zeta_{p^\alpha} + (\frac{-1}{p})^\alpha \zeta_{p^\alpha}^{-1})$, where for convenience we put $\alpha = \alpha_j$ and $p = p_j$. Thus up to a fourth root of unity $T_j(\chi_j)$ equals

$$\sum_{s \in Z^*_{p^\alpha}/(\pm 1)} \chi_j(s) \left(\tfrac{s}{p}\right)^\alpha p^{\alpha/2} \left(\zeta^s_{p^\alpha} + \left(\tfrac{-1}{p}\right)^\alpha \zeta^{-s}_{p^\alpha}\right) = p^{\alpha/2} \sum_{s \in Z^*_{p^\alpha}} \chi_j(s) \left(\tfrac{s}{p}\right)^\alpha \zeta^s_{p^\alpha},$$

just a non-zero multiple of the non-vanishing Gauss sum $\sum_{s \in Z^*_{p^\alpha}} \chi_j(s) \left(\frac{s}{p}\right)^\alpha \zeta^s_{p^\alpha}$ since $\chi_j \left(\frac{\cdot}{p}\right)^\alpha$ has conductor $p^\alpha$. Note also that $T_j(\chi) \ne 0$ from Proposition 4.4 for any even character $\chi$ modulo $p$ when $\alpha_j = 1$. We now assert that $T(\chi) = \prod_{j=1}^r T_j(\chi_j)$. Expanding the right side yields a sum of terms

$$\chi_1(s_1^{v_1}) \cdots \chi_r(s_r^{v_r}) R(1, d_1 s_1^{2v_1}, p_1^{\alpha_1}) \cdots R(1, d_r s_r^{2v_r}, p_r^{\alpha_r}) = \chi(s_1^{v_1} \cdots s_r^{v_r}) R(1, d(s_1^{v_1} \cdots s_r^{v_r})^2, m)$$

by the choice of $s_j$ and Lemma 2.2, one for each choice of exponents $0 \le v_j < e_j$ $(1 \le j \le r)$. But this sum is just $T(\chi)$.

Suppose further that $\chi$ has conductor $f(\chi) > 1$ with $(m/f(\chi), f(\chi)) = 1$ and $m/f(\chi)$ square-free. Then a given $p$-component $\chi_j$ has conductor $p_j^{\alpha_j}$ or may be trivial if $\alpha_j = 1$, so satisfies $T_j(\chi_j) \ne 0$. Thus $T(\chi) \ne 0$ as claimed. From Proposition 4.3, it now follows that $\eta$ generates $K$ with $f_m^{(\sigma)}(x)$ irreducible.

The case $m$ even is argued similarly, though now $H$ has conductor $m/2$, with $K_1$, the real subfield of $\mathbf{Q}(\zeta_{2^{\alpha_1-1}})$ of degree $2^{\alpha_1-2}$ corresponding to the congruence group $\{\pm 1 \pmod{2^{\alpha_1-1}}\}$. One chooses $s_1 \equiv 5 \pmod{2^{\alpha_1}}$ to simultaneously generate $Z^*_{2^{\alpha_1}}/\{\pm 1, \pm 1 + 2^{\alpha_1-1}\}$ isomorphic to $Z^*_{2^{\alpha_1-1}}/(\pm 1)$ with $s_1 \equiv 1 \pmod{m_1}$ and $\eta$ as before. The details are left to the reader.

This concludes the proof of the theorem. ■

https://doi.org/10.4153/CMB-2007-007-2 Published online by Cambridge University Press

## References

[1] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums.* Canadian Mathematical Society Series of Monographs and Advanced Texts. Wiley-Interscience, New York, 1998.

[2] Z. Borevich and I. Shafarevich, *Number Theory.* Pure and Applied Mathematics 20, Academic Press, New York, 1966.

[3] L. Gaal, *Classical Galois Theory with Examples.* Chelsea, New York, 1973.

[4] S. Gupta and D. Zagier, *On the coefficients of the minimal polynomial of Gaussian periods.* Math. Comp. **60**(1993), 385–398.

[5] S. Gurak, *Minimal polynomials for circular numbers.* Pacific J. Math **112**(1984), no. 2, 313–331.

[6] ———, *Factors of period polynomials for finite fields. I.* In: The Rademacher Legacy to Mathematics, Contemp. Math. 166, American Mathematical Society, Providence, RI, 1994), pp. 309–333.

[7] ———, *On the minimal polynomials for certain Gauss periods over finite fields.* In: Finite Fields and their Applications, London Math. Soc. Lecture Note Ser. 233, Cambridge, Cambridge University Press, 1996, pp. 85–96.

[8] ———, *Minimal polynomials for Gauss periods with $f = 2$.* Acta Arith. **121**(2006), 233–257.

[9] H. Iwaniec, *Topics in classical automorphic forms.* Graduate Studies in Mathematics 17, American Mathematical Society, Providence, RI, 1997.

[10] D. Lehmer, *On the cubes of Kloosterman sums.* Acta Arith. **6**(1960), 15–22.

[11] G. Myerson, *Period polynomials and Gauss sums for finite fields.* Acta Arith. **39**(1981), no. 3, 251–264.

[12] H. Salie, *Über die Kloostermanschen Summen $S(u, v; q)$.* Math Z. **34**(1932), no. 1, 91–109.

[13] P. Sarnak, *Some applications of modular forms.* Cambridge Tracts in Mathematics 99, Cambridge University Press, Cambridge, 1990.

*University of San Diego*
*San Diego, CA 92110*
*USA*
*e-mail: gurak@sandiego.edu*