Minimal polynomials for Gauss periods with \( f = 2 \)

by

S. Gurak (San Diego, CA)

1. Introduction. For an integer \( m > 1 \), fix a primitive \( m \)th root of unity \( \zeta_m = \exp(2\pi i/m) \) and let \( \mathbb{Z}_m^\ast \) denote the multiplicative group of reduced residues modulo \( m \). Let \( H \) be a congruence group of conductor \( m \) and of order \( f \). It is a classical problem dating back to Gauss [4] to determine the minimal polynomial \( f(x) \) of the Gauss periods

\[
\theta_v = \sum_{x \in H} \zeta_m^{vx} \quad (v \in \mathbb{Z}_m^\ast/H)
\]

(1)

corresponding to \( H \), or equivalently its reciprocal \( F(X) = X^e f(X^{-1}) \) where \( e = \phi(m)/f \). (It is known that the \( \theta_v \) are distinct and \( f(x) \) is irreducible over the rational field \( \mathbb{Q} \) and that \( H \) has conductor \( m \equiv 0 \pmod{4} \) if \( m \) is even [6, 8].)

For \( f = 1 \), the minimal polynomial is the classical cyclotomic polynomial \( \psi_m(x) \) given by

\[
\psi_m(x) = \prod_{d|m} (1 - x^{m/d})^{\mu(d)} = \sum_{k=0}^{\phi(m)} b_k x^k
\]

(2)

which satisfies

\[
\psi_m(x) = \frac{\psi_{m/p}(x^p)}{\psi_{m/p}(x)}
\]

(3)

for any odd prime \( p | m \). The polynomial \( \psi_m(x) \) is self-reciprocal, that is, the coefficients \( b_k \) satisfy

\[
b_0 = 1, \quad b_{\phi(m)-i} = b_i \quad \text{for} \ 0 \leq i \leq [\phi(m)/2].
\]

(Here \( [ \cdot ] \) denotes the greatest integer function, and \( \phi \) and \( \mu \) are the usual Euler-phi and Möbius functions, respectively.)

2000 Mathematics Subject Classification: Primary 11L05, 11T22, 11T23.
Gauss himself settled the case \( f = 2 \) when \( m = p \) is an odd prime, giving the
explicit formula (see [4])

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

for the reciprocal polynomial for \( \zeta_p + \zeta_p^{-1} \). For \( f > 2 \) it is known [5, 7] that
no such closed formula exists, but that the beginning coefficients, at least,
satisfy a predictable pattern depending polynomially on the distinct prime
factors of \( m \).

Here I treat the general case \( f = 2 \), showing in Section 2 how to compute
the minimal polynomial \( F(X) \) for the reciprocals of the Gauss periods (1)
when \( m \) is composite. This determination is seen to rely on the special cases
\( H = \{ \pm 1 \} \) (and \( H = \{ 1, m/2 - 1 \} \) when \( 8 \mid m \) of conductor \( m \), for which
I give a closed formula generalizing (4) for \( F(X) \), expressed in terms of
the coefficients of the cyclotomic polynomial \( \psi_{m'}(x) \) in (2), where \( m' \) is the
product of the distinct primes dividing \( m \). The details appear in Section 2.
Later in Section 3, I give analogous formulas for quadratic twists of the
form \( i^* \sqrt{l} (\zeta_m + (-1)^{(l-1)/2} \zeta_m^{-1}) \), when \( l \mid m' \) with \( m' \) odd and \( i^* = i^{(l-1)^2/4} \).
The latter formulas are expressed in terms of an appropriate Aurifeuille
or Schinzel factor [3, 9, 13] of \( \psi_{m'}((-1)^{(l-1)/2} x) \). Such quadratic twists or
integer multiples of them arise classically [12] as values of Kloosterman sums
for odd prime powers \( p^\alpha \), \( \alpha > 1 \).

2. Minimal polynomials for Gauss periods with \( f = 2 \). My principal aim here is to first give an explicit formula for the minimal polynomial \( f(x) \) of the Gauss periods \( \theta_v \) in (1) when \( H = \{ \pm 1 \} \) (and for
\( H = \{ 1, m/2 - 1 \} \) when \( 8 \mid m \)). Then I will show how to employ it to compute
\( f(x) \) in general when \( f = 2 \). It will be more convenient to express the results
in terms of the reciprocal polynomial

\[
F(X) = \prod_{v \in \mathbb{Z}_m^*/H} (1 - \theta_v X) = 1 + c_1 X + \cdots + c_e X^e
\]

where \( e = \phi(m)/2 \). Then \( \log F(X) = - \sum_{n=1}^{\infty} S_n X^n / n \) as a formal power
series, with \( n \)th power sums \( S_n = \sum_{v \in \mathbb{Z}_m^*/H} \theta_v^n \) \((n \geq 1) \) satisfying the Newton
identities

\[
S_r + c_1 S_{r-1} + \cdots + c_{r-1} S_1 + c_r r = 0 \quad (1 \leq r \leq e),
\quad S_n + c_1 S_{n-1} + \cdots + c_e S_{n-e} = 0 \quad (n > e).
\]

I first consider the case \( H = \{ \pm 1 \} \) with corresponding Gauss period
\( \theta_1 = \zeta_m + \zeta_m^{-1} \) in (1), and denote its minimal polynomial by \( f_m(x) \) and
corresponding reciprocal polynomial by \( F_m(X) \). The following result will be
crucial to the determination of the minimal polynomials here as well as quite useful later in Section 3.

**Proposition 1.** The reciprocal polynomials

\[ C_d(X) = \prod_{v=1, v \neq (d+1)/2}^d (1 - (\zeta_{4d}^{2v-1} + \zeta_{4d}^{-2v+1})X) \quad \text{for } d \geq 1 \]  

of degree \( 2[d/2] \) are equivalently given by the closed formula

\[ C_d(X) = \left( \frac{1 + \sqrt{1 - 4X^2}}{2} \right)^d \left( \frac{1 - \sqrt{1 - 4X^2}}{2} \right)^d \quad (d \geq 1), \]  

by the recursion

\[ C_0 = 2, \quad C_1(X) = 1, \quad C_d(X) = C_{d-1}(X) - X^2C_{d-2}(X) \quad \text{for } d > 1, \]  

by the generating function

\[ \sum_{d=0}^\infty C_d(X)T^d = \frac{2 - T}{1 - T + X^2T^2}, \]  

by the expansion

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

or the power sums

\[ S_n = d \binom{n}{n/2} \text{ or } 0 \quad \text{for } 1 \leq n \leq 2[d/2], \]  

according as \( n \) is even or odd.

**Proof.** The argument follows that of Gupta and Zagier’s in the proof of Theorem 2 in [5], first establishing the equivalence of (8)–(12). With \( C_d(X) \) defined by (8),

\[ \sum_{d=0}^\infty C_d(X)T^d = \frac{1}{1 + (1 + \sqrt{1 - 4X^2})T/2} + \frac{1}{1 - (1 - \sqrt{1 - 4X^2})T/2} \]

\[ = \frac{2 - T}{1 - T + X^2T^2}, \]

which gives (10). The recursion (9) follows by multiplying both sides of (10) by \( 1 - T + X^2T^2 \) and then comparing corresponding coefficients of \( T^d \). The formula (11) follows by expanding the right-hand side of (10) as a geometric series and using the binomial theorem. Specifically,

\[ \frac{2 - T}{1 - T + X^2T^2} = (1 + (1 - T)) \sum_{n=0}^\infty \frac{(-1)^n T^{2n} X^{2n}}{(1 - T)^{n-1}} \]
\[
\begin{align*}
&= \sum_{n=0}^{\infty} \frac{(-1)^n T^{2n} X^{2n}}{(1 - T)^{n+1}} + \sum_{n=0}^{\infty} \frac{(-1)^n T^{2n} X^{2n}}{(1 - T)^n} \\
&= 1 + \sum_{n=0}^{\infty} T^n + \sum_{n=1}^{\infty} (-1)^n T^{2n} X^{2n} \left( \sum_{j=0}^{\infty} \binom{n+j}{j} T^j + \sum_{j=0}^{\infty} \binom{n+j-1}{j} T^j \right) \\
&= 1 + \sum_{n=0}^{\infty} T^n + \sum_{n=1}^{\infty} \sum_{j=0}^{\infty} (-1)^n \binom{n+j}{j} + \binom{n+j-1}{j} X^{2n} T^{2n+j} \\
&= 1 + \sum_{n=0}^{\infty} T^n + \sum_{n=1}^{\infty} \sum_{j=0}^{\infty} (-1)^n \frac{2n+j}{n+j} \binom{n+j}{n} X^{2n} T^{2n+j} \\
&= 2 + \sum_{d=1}^{\infty} T^d \left( \sum_{n=0}^{\left[\frac{d}{2}\right]} (-1)^n \frac{d}{d-n} \binom{d-n}{n} X^{2n} \right).
\end{align*}
\]

To establish (12), write \( C_d(X) \) in (8) as
\[
C_d(X) = \left( \frac{1 + \sqrt{1 - 4X^2}}{2} \right)^d \left( 1 + \left( \frac{1 - \sqrt{1 - 4X^2}}{2X} \right)^{2d} \right).
\]

Then
\[
\log C_d(X) = d \log \left( \frac{1 + \sqrt{1 - 4X^2}}{2} \right) - \sum_{\nu=1}^{\infty} \frac{(-1)^\nu X^{2\nu}}{\nu} \left( \sum_{n=0}^{\infty} \binom{2n}{n} X^{2n} \right)^{2\nu}
\]

since
\[
A(X) = \frac{1 - \sqrt{1 - 4X^2}}{2X} = X \cdot \sum_{n=0}^{\infty} \binom{2n}{n} X^{2n} + 1
\]

from the expansion
\[
E(X) = \frac{1 + \sqrt{1 - 4X^2}}{2} = 1 - \sum_{n=0}^{\infty} \binom{2n}{n} X^{2n+2} + 1
\]

given in [5]. Thus, from (6) and (13) (see also (17)), the power sums
\[
S_n = \begin{cases} 0 & \text{if } n \text{ is odd,} \\ d \binom{n}{n/2} & \text{if } n \text{ is even} \end{cases} \quad \text{for } 1 \leq n \leq 2[d/2]
\]

are sufficient to determine \( C_d(X) \) from Newton’s identities (6). This proves the equivalence of (8)–(12).

It remains to show that \( c_d(x) = x^d C_d(x^{-1}) \) has zeros \( 2 \cos(\pi \nu/2d) \) for \( \nu \) odd and \( 1 \leq \nu \leq 2d - 1 \) (this includes the zero \( 2 \cos(\pi/2) = 0 \) when \( \nu = d \).
odd). But from (10), the generating function for the \( c_d(x) \) is
\[
\sum_{d=0}^{\infty} c_d(x)T^d = \sum_{d=0}^{\infty} C_d(x^{-1})(xT)^d = \frac{2 - xT}{1 - xT + T^2}.
\]
Substituting \( x = z + z^{-1} \) yields
\[
\sum_{d=0}^{\infty} c_d(z + z^{-1})T^d = \frac{2 - (z + z^{-1})T}{1 - (z + z^{-1})T + T^2}
= (1 - zT)^{-1} + (1 - z^{-1}T)^{-1} = \sum_{d=0}^{\infty} (z^d + z^{-d})T^d.
\]
Thus \( c_d(z + z^{-1}) = 0 \) iff \( z^d + z^{-d} = 0 \) iff \( z^{4d} = 1 \) with \( z = \pm i \) iff \( z = \zeta_{4d}^{\nu} \) with \( \nu \) odd iff \( z + z^{-1} = 2 \cos(\pi \nu/2d) \) for \( 1 \leq \nu \leq 2d - 1 \) with \( \nu \) odd. But \( c_d(x) \) is monic (\( C_d(X) \) has constant term 1) and has degree \( d \), so \( c_d(x) = \prod_{\nu=1, \nu \text{ odd}}^{2d-1} (x - (\zeta_{4d}^{\nu} + \zeta_{4d}^{-\nu})) \) is the reciprocal polynomial of \( C_d(X) \) as defined in (7). This completes the proof of Proposition 1.

Incidentally, the power series \( A(X) \) in (14) has an important property that will be useful later.

**Lemma 1.** For any positive integers \( n \geq m \), the coefficient of \( X^n \) in the expansion \( A(X)^m \) is \( \frac{m}{n} \binom{n}{m/2} \) or 0 according as \( n \equiv m \pmod{2} \) or not.

**Proof.** The proof proceeds using induction on \( m \). With \( m = 1 \), the coefficient of \( X^n \) is clearly 0 if \( n \) is even or
\[
\frac{2}{n+1} \binom{n-1}{(n-1)/2} = \frac{1}{n} \binom{n}{(n-1)/2}
\]
if \( n \) is odd. With \( m = 2 \), \( A(X)^2 = -1 + A(X)/X \), so by (14),
\[
A(X)^2 = -1 + \sum_{k=0}^{\infty} \binom{2k}{k} \frac{X^{2k}}{k+1}.
\]
It follows that the coefficient of \( X^n \) is
\[
\frac{2}{n+2} \binom{n}{n/2} = \frac{2}{n} \binom{n}{(n-2)/2}
\]
if \( n \) even or 0 if \( n \) odd. Now assume that the conclusion of the lemma holds for all powers \( A(X)^k \) up to \( k = j \) for some \( j \geq 2 \), and consider \( A(X)^{j+1} = -A(X)^{j-1} + A(X)^j/X \) by (16). Thus the coefficient of \( X^n \) in \( A(X)^{j+1} \) is the sum of the coefficient of \( X^n \) in \( -A(X)^{j-1} \) and of the coefficient of \( X^{n+1} \) in \( A(X)^j \). By the induction hypothesis, this sum is 0 if \( n \not\equiv j + 1 \pmod{2} \) but equals...
\[
\frac{j - 1}{n} \binom{n - j + 1}{2} + \frac{j}{n + 1} \binom{n + 1}{n - j + 1} = \frac{j}{n} \binom{n}{n - j + 1/2}
\]
if \(n \equiv j + 1 \pmod{2}\). This completes the induction so the conclusion of the lemma is proved.

When \(m = 2^\alpha, \alpha > 2\), the following result is an immediate consequence of Proposition 1 and the lemma above.

**Corollary 1.**

\[
F_{2^\alpha}(X) = \sum_{n=0}^{2^\alpha-3} (-1)^n \frac{2^{\alpha-2}}{2^{\alpha-2} - n} \binom{2^{\alpha-2} - n}{n} X^{2n}
\]

with power sums \(S_n\) satisfying

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

**Proof.** Clearly \(F_{2^\alpha}(X) = C_{2^{\alpha-2}}(X)\) by Proposition 1. Using the expansion

\[
\log((1 + \sqrt{1 - 4X^2})/2) = -\sum_{n=1}^{\infty} \left(\frac{2n}{n}\right) X^{2n}
\]

and the lemma above, one obtains the expression for the power sums \(S_n\) upon comparing coefficients in the expansion of \(\log C_{2^{\alpha-2}}(X)\) in (13).

I am now ready to describe \(F_m(X)\) in general. For \(d > 0\) put

\[
B_d(X) = \begin{cases} 
\sqrt{1 - 2X} (V(X)^d - W(X)^d) & \text{if } d \text{ is odd,} \\
\sqrt{1 - 4X^2}(V(X)^d - W(X)^d) & \text{if } d \text{ is even,}
\end{cases}
\]

where \(V(X) = \frac{1}{2}(\sqrt{1+2X} + \sqrt{1-2X})\) and \(W(X) = \frac{1}{2}(\sqrt{1+2X} - \sqrt{1-2X})\). This sequence has initial terms \(B_1(X) = 1 - 2X, B_2(X) = 1 - 4X^2, B_3(X) = (1 - 2X)(1 + X), B_4(X) = 1 - 4X^2,\) and satisfies \(B_n(X) = B_{n-2}(X) - X^2B_{n-4}(X)\) for \(n > 4\). We have

**Proposition 2.**

\[
F_m(X) = \prod_{d|m} B_{m/d}(X)^{u(d)}.
\]

**Proof.** I assert that (i) \(B_d(X)\) has degree \((d + 1)/2\) with zeros \((\zeta_d^\nu + \zeta_d^{-\nu})^{-1}, 0 \leq \nu \leq (d-1)/2\), if \(d\) is odd, (ii) \(B_d(X)\) has degree \(d/2 + 1\) with zeros \((\zeta_d^\nu + \zeta_d^{-\nu})^{-1}, 0 \leq \nu \leq d/2\), if \(2 \mid d\), and (iii) \(B_d(X)\) has degree \(d/2\) with zeros \((\zeta_d^\nu + \zeta_d^{-\nu})^{-1}, 0 \leq \nu \leq d/2, \nu \neq d/4,\) if \(4 \mid d\). Then \(B_m(X) = \prod_{d|m} F_d(X)\), since the right side has constant term 1 and accounts for all zeros that are reciprocals of the non-zero values \(\zeta_m^\nu + \zeta_m^{-\nu}\) with \(0 \leq \nu \leq [m/2]\) exactly once. Now the statement of the proposition readily follows by Möbius inversion.
But (i) is essentially Theorem 3 in [5] taking into account the extra factor \(1 - 2X\) for \(\nu = 0\). So it remains to establish (ii) and (iii) of the claim. Now if \(2 \parallel d\), say \(d = 2d'\) with \(d'\) odd, then \(B_d(X) = B_{d'}(X)B_{d'}(-X)\). Thus by (i), \(B_d(X)\) has distinct zeros \((\zeta_{d'} + \zeta_{d'})^{-1} = (\zeta_d + \zeta_d)^{-1}\) and 
\(- (\zeta_{d'} + \zeta_{d'})^{-1} = (\zeta_d^{2\nu} + \zeta_d^{-2\nu})^{-1}\) for \(0 \leq \nu \leq (d' - 1)/2\), or equivalently zeros \((\zeta_{d'} + \zeta_{d'})^{-1}\) for \(0 \leq \nu \leq d' = d/2\), establishing assertion (ii). To settle claim (iii) first note if \(4 \parallel d\), say with \(d = 4d'\) where \(d'\) is odd, then \(B_d(X) = B_{2d'}(X)C_{d'}(X)\) with \(C_{d'}(X)\) as in (7). In this case \(B_d(X)\) has zeros 
\((\zeta_{d'}^{2\nu} + \zeta_{d'}^{-2\nu})^{-1}\) for \(1 \leq \nu \leq d' = d/4\), \(\nu \neq (d + 4)/8\) from Proposition 1, and zeros \((\zeta_d^{2\nu} + \zeta_d^{-2\nu})^{-1}\) for \(0 \leq \nu \leq d' = d/4\) from the above. Restated, \(B_d(X)\) has distinct zeros \((\zeta_{d'}^{2\nu} + \zeta_{d'}^{-2\nu})^{-1}\) for \(0 \leq \nu \leq d/2\), \(\nu \neq d/4\) if \(4 \parallel d\). Arguing similarly using Proposition 1 and the above statement, one obtains (iii) in general when \(8 \parallel d\) by an induction involving the exact power of 2 dividing \(d\). The proof of the proposition is now complete.

I should remark that the statement of Proposition 2 is not new, and was first noted by Watkins and Zeitlin [16] in reciprocal form using the properties of the Chebyshev polynomials \(T_m(x)\), which are defined by

\[
T_m(\cos \theta) = \cos(m\theta)
\]

for positive integers \(m\) and all real \(\theta\). Indeed, defining

\[
b_m(x) = 2(T_{[m/2]+1}(x/2) - T_{([m-1]/2)}(x/2))
\]

they essentially show \(b_m(x)\) has zeros \(2 \cos(2\pi v/m)\) for \(0 \leq v \leq [m/2]\). Here \(B_m(X) = X^{[m/2]+1}b_m(X^{-1})\).

I now give the main result of this section.

**Theorem 1.** For \(m \neq 2^n\),

\[
F_m(X) = b_{\phi(m')/2}X^{\phi(m)/2} + \sum_{j=0}^{\phi(m')/2-1} b_j X^{mj/m'} C_{m'}^{m'}(\phi(m')/2-j)(X)
\]

where the \(b_j\) are the coefficients for \(\psi_m(x)\) given in (2) and the polynomials \(C_d(X)\) are as in (11).

The power sums \(S_n\) satisfy

\[
S_n = \begin{cases} 
\sum_{d|m} \mu(d) \frac{m}{d} \sum_{t=1, mt/d \text{ odd}}^{[nd/m]} \binom{n}{n - mt/d/2} & \text{if } n \text{ is odd}, \\
\phi(m) \frac{1}{2} \binom{n}{n/2} + \sum_{d|m} \mu(d) \frac{m}{d} \sum_{t=1, mt/d \text{ even}}^{[nd/m]} \binom{n}{n - mt/d/2} & \text{if } n \text{ is even}.
\end{cases}
\]

(18)
The coefficients $c_r$ of $F_m(X)$ are given for $1 \leq r < \phi(m)/2$ by

$$c_r = \sum_{j=0}^{[m'/m]} (-1)^{t_j} b_j \times \frac{m}{m'} \left( \phi(m')/2 - j \right) - t_j$$

and

$$c_{\phi(m)/2} = \begin{cases} \left( \frac{-2}{p} \right) & \text{if } m' = p \text{ an odd prime,} \\ 1 & \text{otherwise,} \end{cases}$$

where $t_j = (r - jm/m')/2$.

**Proof.** I first note that if $F_m(X)$ is expressed in terms of the coefficients of $\psi_{m'}(x)$ and the polynomials $C_d(X)$ as given in the initial statement of the theorem, then formula (19) for the coefficients $c_r$ is deduced in routine fashion upon collecting like powers of $X$. The value of $c_{\phi(m)/2}$ is seen to be

$$b_{\phi(m')/2} + 2 \sum_{j=0}^{\phi(m')/2-1} b_j = \sum_{j=0}^{\phi(m')/2} b_j = \psi_{m'}(1) = 1$$

if $m'$ is even (and hence composite since $m \neq 2^\alpha$), or

$$b_{\phi(m')/2} + (-1)^{[(\phi(m')+2)/4]} \sum_{j=0}^{\phi(m')/2-2} (-1)^{[(j+1)/2]} 2b_j$$

if $m'$ is odd. The latter expression is

$$(-1)^{\phi(m')/4} \sum_{j=0}^{\phi(m')/2-1} (-1)^j b_{2j} = (-1)^{\phi(m')/4} (\psi_{m'}(i) + \psi_{m'}(-i))/2$$

if $4 \mid \phi(m')$, or

$$(-1)^{(p-3)/4} \sum_{j=0}^{\phi(p)/2-2} (-1)^j b_{2j+1} = (-1)^{(p-3)/4} (\psi_p(i) - \psi_p(-i))/2i$$

if $m' = p \equiv 3 \pmod{4}$ a prime. Noting that for odd primes $p$, $\psi_p(i) = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ i & \text{if } p \equiv 3 \pmod{4}, \end{cases}$

and using (3), one finds $\psi_{m'}(i) = (-1)^{\phi(m')/4}$ whenever $m'$ is odd and composite. It now follows readily for $m \neq 2^\alpha$ that $c_{\phi(m)/2}$ is $\left( \frac{-2}{p} \right)$ if $m' = p$, an odd prime, and 1 otherwise.
Now I assert that
\[
F_m(X) = E(X)^{\phi(m)/2} \prod_{d|m} (1 - A(X)^{m/d})^{\mu(d)}.
\]

Then
\[
\log F_m(X) = \frac{\phi(m)}{2} \log E(X) + \sum_{d|m} \mu(d) \log(1 - A(X)^{m/d})
\]
\[
= -\frac{\phi(m)}{2} \sum_{n=1}^{\infty} \left(\frac{2n}{n}\right) \frac{X^{2n}}{2n} - \sum_{d|m} \mu(d) \sum_{v=1}^{\infty} \frac{A(X)^{mv/d}}{v}
\]
again by using the formal Taylor series for \(\log(1 - T)\) about \(T = 0\). By Lemma 1 the coefficient of \(X^n\) in \(\sum_{v=1}^{\infty} A(X)^{mv/d}/v\) is
\[
\sum_{t=1, mt/d \equiv n (\mod 2)}^{[nd/m]} \frac{m}{dn} \left(\frac{n}{n - mt/d/2}\right),
\]
and so the statements about the power sums \(S_n\) in the theorem would follow.

In addition, if (20) holds then
\[
F_m(X) = E(X)^{\phi(m)/2}\psi_{m'}(A(X)^{m/m'})
\]
\[
= (E(X)^{m/m'})^{\phi(m')/2} \sum_{j=0}^{\phi(m')/2-1} b_j A(X)^{mj/m'}
\]
\[
= b_{\phi(m')/2} X^{\phi(m)/2} + \sum_{j=0}^{\phi(m')/2-1} b_j X^{mj/m'} E(X)^{m/_{m'} (\phi(m')/2-j)}
\]
\[
+ \sum_{j=0}^{\phi(m')/2-1} b_{\phi(m')-j} X^{m\phi(m')/2m'} A(X)^{m/_{m'} (\phi(m')/2-j)},
\]
since \(E(X)A(X) = X\), or
\[
b_{\phi(m')/2} X^{\phi(m)/2} + \sum_{j=0}^{\phi(m')/2-1} b_j X^{mj/m'} (E(X)^{m/_{m'} (\phi(m')/2-j)} + E(X)^{m/_{m'} (\phi(m')/2-j)})
\]
where \(E(X) = (1 - \sqrt{1 - 4X^2})/2\), since \(\psi_{m'}(x)\) is self-reciprocal and \(XA(X) = E(X)\). But \(E(X)^d + E(X)^d\) is just the polynomial \(C_d(X)\) in Proposition 1, so the expression for \(F_m(X)\) in the theorem would follow.

It remains to prove assertion (20). If \(m\) is odd then from Proposition 3,
\[
F_m(X) = \prod_{d|m} (\sqrt{1 - 2X} (V(X)^{m/d} - W(X)^{m/d}))^{\mu(d)}
\]
\[ = V(X)^{\phi(m)} \prod_{d|m} (1 - A(X)^{m/d})^{\mu(d)} \]
\[ = E(X)^{\phi(m)/2} \prod_{d|m} (1 - A(X)^{m/d})^{\mu(d)} \]
as asserted, since \( A(X) = (\sqrt{1 + 2X} - \sqrt{1 - 2X})/(\sqrt{1 + 2X} + \sqrt{1 - 2X}) \).
For even \( m \) we have \( 4 | m \), so from Proposition 3,
\[ F_m(X) = \prod_{d|m} (\sqrt{1 - 4X^2} (V(X)^{m/d} - W(X)^{m/d}))^{\mu(d)} \]
again equaling \( E(X)^{\phi(m)/2} \prod_{d|m} (1 - A(X)^{m/d})^{\mu(d)} \). Thus the assertion (20) is verified so the proof of the theorem is now complete.

I wish to remark that direct calculation of the power sums using the binomial theorem
\[ (\zeta_m + \zeta_m^{-1})^n = \begin{cases} 
\binom{n}{n/2} + \sum_{j=0}^{n/2-1} \binom{n}{j} (\zeta_m^{n-2j} + \zeta_m^{2j-n}) & \text{if } n \text{ is even}, \\
\sum_{j=0}^{(n-1)/2} \binom{n}{j} (\zeta_m^{n-2j} + \zeta_m^{2j-n}) & \text{if } n \text{ is odd},
\end{cases} \tag{21} \]
and the fact that the trace (see equation (16) in [3]) satisfies
\[ \text{Tr}_{K/Q}(\zeta_m^v + \zeta_m^{-v}) = \sum_{x \in \mathbb{Z}_m^*} \zeta_m^{ux} = \mu(d) \frac{\phi(m)}{\phi(d)} \]
if \((v, m) = m/d\), where \( K = \mathbb{Q}(\zeta_m + \zeta_m^{-1}) \), yield a variant form for the \( S_n \) in (18). Namely,
\[ S_n = \begin{cases} 
\sum_{d|m} \mu(d) \frac{\phi(m)}{\phi(d)} \sum_{t=1, t,d=1, mt/d \text{ odd}}^{[nd/m]} \left( \begin{array}{c} n \\ n - mt/d \end{array} \right) / 2 & \text{if } n \text{ is odd}, \\
\frac{\phi(m)}{2} \left( \begin{array}{c} n \\ n/2 \end{array} \right) + \sum_{d|m} \mu(d) \frac{\phi(m)}{\phi(d)} \sum_{t=1, t,m/d \text{ even}}^{[nd/m]} \left( \begin{array}{c} n \\ n - mt/d \end{array} \right) / 2 & \text{if } n \text{ is even}.
\end{cases} \tag{23} \]
However, these are seen to be equivalent using the alternative expression \( \psi_{m'}(x) = \prod_{v \in \mathbb{Z}_m^*} (1 - \zeta_m^{v}, x) \) to evaluate \( \psi_{m'}(A^{m/m'}) \) in (20) before taking logarithms.

Here are a couple of examples to illustrate Theorem 1.

**Example 1.** Consider \( \theta_1 = \zeta_{27} + \zeta_{27}^{-1} \) in (1). Here \( m = 27, m' = 3 \) and \( \psi_3(x) = 1 + x + x^2 \) in (2). Direct calculation of the power sums \( S_n \) yields...
$S_1 = S_3 = S_5 = S_7 = 0$, $S_9 = -9$, $S_2 = 18$, $S_4 = 54$, $S_6 = 180$ and $S_8 = 630$ with $F_{27}(X) = 1 - 9X^2 + 27X^4 - 30X^6 + 9X^8 + X^9$ in agreement with the formulas in Theorem 1.

**Example 2.** Now consider $\theta_1 = \zeta_{15} + \zeta_{15}^{-1}$ in (1). Here $m = m' = 15$ and $\psi_{15}(x) = 1 - x + x^3 - x^4 + x^5 - x^7 + x^8$ in (2). Direct calculation of the power sums $S_n$ yields $S_1 = 1$, $S_2 = 9$, $S_3 = 1$, $S_4 = 29$ with $F_{15}(X) = 1 - X - 4X^2 + 4X^3 + X^4$ again in agreement with Theorem 1.

The case $m = p^\alpha$, $p$ an odd prime, warrants special consideration.

**Corollary 2.** For an odd prime $p$,

$$F_{p^\alpha}(X) = X^{\phi(p^\alpha)/2} + \sum_{j=0}^{(p-3)/2} X^{p^{\alpha-1}j} C_{p^\alpha-1(p-1-2j)}/2(X)$$

with $n$th power sums $S_n$ equal to

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

if $n$ is odd, or

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

if $n$ is even. The coefficients $c_r$ of $F_{p^\alpha}(X)$ are given for $1 \leq r < \phi(p^\alpha)/2$ by

$$c_r = \sum_{j=0, j \equiv r (\text{mod } 2)}^{[rp^{\alpha-1}]} (-1)^{t_j} p^{\alpha-1} \left( \frac{p^{1/2} - j}{p^{1/2} - (r - t j)} \right)$$

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

I remark that for $m = p$, the above formula for the coefficients $c_r$ reduces to that found by Gauss in (4), in view of the combinatorial identity

$$\sum_{t=0}^{[r/2]} (-1)^t \frac{p^{1/2} - (r - 2t)}{p^{1/2} - (r - t)} \left( \frac{p^{1/2} - (r - t)}{t} \right) = (-1)^{[r/2]} \left( \frac{[(p-1-r)/2]}{[r/2]} \right)$$

for $0 \leq r < (p-1)/2$. This identity follows readily from the fact that

$$\sum_{t=0}^{k} (-1)^t \frac{x - 2k + 2t}{x - 2k + t} \left( \frac{x - 2k + t}{t} \right)$$

$$= \sum_{t=0}^{k} (-1)^t \left( \frac{x - 2k + t}{t} \right) + \sum_{t=1}^{k} (-1)^t \left( \frac{x - 2k + t - 1}{t - 1} \right)$$
with corresponding sums \( S \).

S. Gurak

\[ \sum_{t=0}^{k} (-1)^t \binom{x-2k+t}{t} - \sum_{t=0}^{k-1} (-1)^t \binom{x-2k+t}{t} \]

\[ = (-1)^k \binom{x-k}{k} \]

for \( x > k \).

Next I consider the alternative situation when \( H = \{1, m/2 - 1\} \) with \( 8 | m \), and denote \( F(X) \) in (5) by \( G_m(X) \). Now one has \( \theta_1 = \zeta_m - \zeta_m^{-1} = i(\zeta_m^{m/4-1} + \zeta_m^{-m/4}) \) in (1), so that \( G_m(X) = F_m(iX) \) with corresponding sums \( S_n^- = 0 \) if \( n \) is odd and \( S_n^- = (-1)^n S_{2n} \). The next result now follows immediately from Theorem 1 and Corollary 1.

**Theorem 2.** Let \( 8 | m \) and \( H = \{1, m/2 - 1\} \). The minimal polynomial for the reciprocals of the Gauss periods \( \theta_v = \zeta_m^v - \zeta_m^{-v} \) \( (v \in \mathbb{Z}_m^*/H) \) is

\[
G_m(X) = (-1)^{\phi(m)/4} b_{\phi(m')/2} X^{\phi(m)/2} + \sum_{j=0}^{\phi(m')/2-1} b_j X^{m j/m'} C_{mj/m'}(\phi(m)/2-j)(iX)
\]

when \( m \neq 2^\alpha \), with corresponding sums \( S_n^- = 0 \) if \( n \) is odd, and

\[
S_n^- = (-1)^{n/2} \frac{\phi(m)}{2} \binom{n/2}{n} + (-1)^{n/2} \sum_{d|m} \mu(d) \frac{m}{d} \sum_{t=1}^{[nd/m]} \left( n - mt/d \right) / 2)
\]

if \( n \) is even. The coefficients of \( G_m(X) \) are given for \( 1 \leq r < \phi(m)/2 \) by

\[
c_r = \begin{cases} 
(-1)^{[r/2]} \sum_{j=0}^{[m'r/m]} (-1)^t_j b_j \frac{m}{m'} \left( \frac{\phi(m')}{2} - j \right) - t_j, \\
0
\end{cases}
\]

according as \( r \) is even or odd, respectively, with \( c_{\phi(m)/2} = 1 \). If \( m = 2^\alpha \) \( (\alpha > 2) \), then

\[
G_{2^\alpha}(X) = \sum_{n=0}^{2^{\alpha-3}} 2^{\alpha-2} - n \left( 2^{\alpha-2} - n \right) X^{2^{\alpha-2} - 2n}
\]

with corresponding sums \( S_n^- = 0 \) if \( n \) is odd, and

\[
S_n^- = (-1)^{n/2} 2^{\alpha-2} \binom{n/2}{n} + 2^{\alpha-1} \sum_{t=1}^{[n2^{1-\alpha}]} (-1)^{t+n/2} \left( n - 2^{\alpha-1} t \right) / 2)
\]

if \( n \) is even.

Here is an example to illustrate Theorem 2.
Example 3. Consider \( \theta_1 = \zeta_{40} + \zeta_{40}^{19} = \zeta_{40} - \zeta_{40}^{-1} \) in (1) where \( H = \{1, 19\} \) modulo 40. Here \( m = 40 \) and \( m' = 10 \) with
\[
\psi_{10}(x) = 1 - x + x^2 - x^3 + x^4
\]
in (2). Direct calculation of the power sums \( S_n \) yields \( S_1 = S_3 = S_5 = S_7 = 0 \) and \( S_2 = -16, S_4 = 52, S_6 = -184, S_8 = 668 \) with \( G_{40}(X) = 1 + 8X^2 + 19X^4 + 12X^6 + X^8 \) in agreement with the formulas in Theorem 2.

Now I return to the general problem to compute the minimal polynomial \( F(X) \) for the reciprocals of the Gauss periods (1) for a given congruence group \( H \) of conductor \( m \) and order \( f = 2 \). This determination is seen to rely on the special cases \( H = \{ \pm 1 \} \) and \( H = \{1, m/2 - 1\} \) already discussed. For this purpose some familiarity with congruence groups is needed. (The reader may find the discussion in Section 5 of [6] helpful here.)

Given a congruence group \( H \) of conductor \( m \) and a positive divisor \( d \mid m \), let \( H_d \) denote the congruence group defined modulo \( d \) determined by
\[
H_d = \{ x \in \mathbb{Z} \mid x \equiv x' \pmod{d} \text{ for some } x' \in H \}.
\]
If \( p^\alpha \parallel m \), where \( p \) is prime, then \( H_{p^\alpha} \) has conductor \( p^\alpha \) and order dividing that of \( H \).

The next result is critical in the determination of \( F(X) \).

**Lemma 2.** Let \( H \) be a congruence group of conductor \( m \) and order \( f = 2 \), say \( H = \{1, a\} \) modulo \( m \) for some \( a \in \mathbb{Z}_m^* \). Then \( m = m_0m_1 \) with \((m_0, m_1) = 1\), where \( H_1 = H_{m_0} \cap H_{m_1} \), with \( H_{m_1} = \{1\} \) modulo \( m_1 \) and \( H_{m_0} = \{\pm 1\} \) modulo \( m_0 \) or possibly \( \{1, m_0/2 - 1\} \) modulo \( m_0 \) when \( 8 \mid m_0 \). Moreover, the Gauss period \( \zeta_{m_1} + \zeta_{m_0}^a \) is a conjugate of \( \zeta_{m_1}(\zeta_{m_0} + \zeta_{m_0}^a) \).

**Proof.** Write \( m \) as a product \( p_1^{\alpha_1} \cdots p_r^{\alpha_r} \) of distinct prime powers, where \( p_1 < \cdots < p_r \) and \( \alpha_i > 0 \) (\( 1 \leq i \leq r \)). Since \( H \) has conductor \( m \) and order \( f = 2 \), each congruence group \( H_{p_i^{\alpha_i}} \) has conductor \( p_i^{\alpha_i} \) (\( 1 \leq i \leq r \)) with order equaling 1 or 2. Let \( m_0 \) be the product of the prime powers \( p_i^{\alpha_i} \) for which \( H_{p_i^{\alpha_i}} \) has order 2, and put \( m_1 = m/m_0 \). (Note that if \( p_1 = 2 \) divides \( m_0 \) then necessarily \( \alpha_1 > 2 \).) Then \( a \equiv 1 \pmod{m_1} \) and ord \( p_i^{\alpha_i}, a = 2 \) for each \( p_i \mid m_0 \).

In particular, \( a \equiv -1 \pmod{p_i^{\alpha_i}} \) for any odd \( p_i \mid m_0 \) and \( a \equiv -1 \) or \( 2^{\alpha_i-1} - 1 \pmod{2^{\alpha_i}} \) should \( p_1 = 2 \) divide \( m_0 \). (The choice \( a \equiv 2^{\alpha_i-1} + 1 \pmod{2^{\alpha_i}} \) would contradict the fact that \( H_{2^{\alpha_1}} \) has conductor \( 2^{\alpha_1} > 4 \).) It follows from the Chinese Remainder Theorem (as in (40) of [6]) that \( a \equiv -1 \pmod{m_0} \) or \( a \equiv m_0/2 - 1 \pmod{m_0} \) respectively, so \( H = H_{m_0} \cap H_{m_1} \), where \( H_{m_1} = \{1\} \) modulo \( m_1 \) and \( H_{m_0} = \{\pm 1\} \) or \( \{1, m_0/2 - 1\} \) modulo \( m_0 \) according as \( H_{2^{\alpha_1}} = \{\pm 1\} \) or \( \{1, 2^{\alpha_1-1} - 1\} \). The last statement of the proposition now follows readily from the Chinese Remainder Theorem, using the fact that \( \zeta_{m_1}^v(\zeta_{m_0}^w + \zeta_{m_0}^{aw}) \), for \( v \in \mathbb{Z}_{m_1}^* \) and \( w \in \mathbb{Z}_{m_0}/H_{m_0} \), comprise a complete set of conjugates of \( \zeta_{m_1}(\zeta_{m_0} + \zeta_{m_0}^a) \).
Using the decomposition for $H$ in the lemma above, one can now express the reciprocal polynomial $F(X)$ in terms of the polynomials $F_{m_0}(X)$ or $G_{m_0}(X)$ appearing in Theorems 1 and 2.

**Proposition 3.** Let $H$ be a congruence group of conductor $m$ and order $f = 2$, say with $H = H_{m_0} \cap H_{m_1}$ as in Lemma 2, where $m = m_0m_1$, $(m_0, m_1) = 1$ and $H_{m_0} = \{ \pm 1 \}$ modulo $m_0$ (or possibly $\{ 1, m_0/2 - 1 \}$ when $8 \mid m_0$). Then

$$F(X) = \prod_{v \in \mathbb{Z}_{m_1}^*} F_{m_0}(\zeta_{m_1}^v X) \quad \text{or} \quad \prod_{v \in \mathbb{Z}_{m_1}^*} G_{m_0}(\zeta_{m_1}^v X)$$

according as $H_{m_0} = \{ \pm 1 \}$ or $\{ 1, m_0/2 - 1 \}$ modulo $m_0$. The corresponding sums $S_n$ of $n$th powers satisfy

$$S_n = \mu\left(\frac{m_1}{n, m_1}\right) \frac{\phi(m_1)}{\phi(m)} S_n^* (n > 0),$$

where $S_n^*$ are the $n$th power sums associated with $F_{m_0}(X)$ in Theorem 1 (Corollary 1 if $m_0 = 2^{w_1}$) or $G_{m_0}(X)$ in Theorem 2, respectively.

**Proof.** Much of the proposition’s assertions follow readily from Lemma 2 and its proof. To justify the formula for the power sums $S_n$ note that from Lemma 2,

$$S_n = \sum_{v \in \mathbb{Z}_{m_1}^*, w \in \mathbb{Z}_{m_0}^*/H_{m_0}} \zeta_{m_1}^{nw} (\zeta_{m_0}^w + \zeta_{m_0}^{wa})^n = \sum_{v \in \mathbb{Z}_{m_1}^*} \zeta_{m_1}^{nv} S_n^* (n > 0),$$

where $S_n^* = \sum_{w \in \mathbb{Z}_{m_0}^*/H_{m_0}} (\zeta_{m_0}^w + \zeta_{m_0}^{wa})^n (n > 0)$ are the power sums associated with $F_{m_0}(X)$ or $G_{m_0}(X)$ according as $a \equiv -1$ or $m_0/2 - 1 \pmod{m_0}$. From (22),

$$\sum_{v \in \mathbb{Z}_{m_1}^*} \zeta_{m_1}^{nv} = \mu(d) \frac{\phi(m_1)}{\phi(d)}$$

where $(n, m_1) = m_1/d$, so the formula for $S_n$ given in the proposition follows.

I conclude this section with two examples illustrating Proposition 3.

**Example 4.** Consider $\theta_1 = \zeta_{35} + \zeta_{35}^{29}$ in (1) where $H = \{ 1, 29 \}$ modulo 35. Here $m_0 = 5$ and $m_1 = 7$ with $H_{m_0} = \{ \pm 1 \}$ modulo 5 and $F_5(X) = 1 + X - X^2$ from Theorem 1 or direct calculation. One finds $\theta_1 = \zeta_7^{3}(\zeta_5^2 + \zeta_5^{-2})$ with minimal polynomial

$$F(X) = \prod_{v \in \mathbb{Z}_7} F(\zeta_7^v X) = 1 - X + 2X^2 - 3X^3 + 5X^4 - 8X^5 + 13X^6 + 8X^7 + 5X^8 + 3X^9 + 2X^{10} + X^{11} + X^{12}$$

from Proposition 3. Direct calculation of the power sums $S_n$ yields $S_1 = 1$, $S_2 = -3$, $S_3 = 4$, $S_4 = -7$, $S_5 = 11$, $S_6 = -18$, $S_7 = -174$, $S_8 = -47$,...
$S_9 = 76$, $S_{10} = -123$, $S_{11} = 199$ and $S_{12} = -322$ in agreement with the formula in Proposition 3.

Example 5. Next consider $\theta_1 = \zeta_{120} + \zeta_{120}^{19}$ in (1) where $H = \{1, 19\}$ modulo 120. Here $m_0 = 40$ and $m_1 = 3$ from Lemma 2 with $H_{m_0} = \{1, 19\}$ modulo 40. From Example 3, $G_{40}(X) = 1 + 8X^2 + 19X^4 + 12X^6 + X^8$. One finds $\theta_1, \zeta_{27}/40$ with minimal polynomial

$$F(X) = G_{40}(\zeta_3 X)G_{40}(\zeta_3^2 X) = 1 - 8X^2 + 45X^4 - 128X^6 + 264X^8 - 212X^{10} + 125X^{12} - 12X^{14} + X^{16}$$

from Proposition 3.

3. Minimal polynomial for quadratic twists of $\zeta_m + \zeta_m^{-1}$. Here I consider certain twisted Gauss periods for odd $m$ of the form $\theta = i^* \sqrt{l} (\zeta_m + (-1)^{(l-1)/2}\zeta_m^{-1})$, where $l|m'$ with again $m' = \prod_{p|m} p$ as in the previous section and $i^* = i^{(l-1)/2}$. It is easy to see that $\theta$ generates $K = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ since $\theta = \text{Tr}_{\mathbb{Q}(\zeta_m)/K}(i^* \sqrt{l} \zeta_m)$ and

$$\theta^2 = (-1)^{(l-1)/2} l (\zeta_m^2 + \zeta_m^{-2} + (-1)^{(l-1)/2} 2)$$

already generates $K$. Now I wish to give formulas analogous to those in Theorem 1 for such quadratic twists, which ultimately depend on the Aurifeuille and Schinzel factors $[3, 9, 13]$ of the cyclotomic polynomial $\psi_{m'}$ of the form $\psi_{m'}((-1)^{(l-1)/2}z^2) = a_0 + a_2z^2 + \ldots + a_{\phi(m')}z^{\phi(m')}$

$$+ \sqrt{l} (a_1z + a_3z^3 + \ldots + a_{\phi(m')-1}z^{\phi(m')-1})$$

The conjugates of $\theta$ are

$$\theta_v = \left(\frac{v}{l}\right) i^* \sqrt{l} (\zeta_m^v + (-1)^{(l-1)/2}\zeta_m^{-v}) \quad (v \in \mathbb{Z}_{m'}^*/\{\pm 1\})$$

with power sums $S_n$ equaling

$$l^{(n-1)/2}m_+ \sum_{t=1, (t,l)=1, t \text{ odd}}^{[nm'/m]} (-1)^{(l-1)(1+m+t/m')/4} \times \delta_{m,l}(t) \left(\frac{n}{n - mt/m'}\right)^{\frac{n}{2}},$$

if $n$ is odd, where

$$\delta_{m,l}(t) = \left(\frac{lt/m'}{l}\right) \mu \left(\frac{m_-}{mt/m', m_-}\right) \frac{\phi(m_-)}{\phi\left(\frac{m_-}{mt/m', m_-}\right)},$$

or

$$l^{n/2} \left(\frac{\phi(m)}{2}\right) \left(\frac{n}{n/2}\right) + \sum_{d|m} \mu(d) \left(\frac{\phi(m)}{\phi(d)}\right) \sum_{t=1, (t,d)=1}^{[dn/2m]} (-1)^{(l-1)t/2} \left(\frac{n}{n/2 - mt/d}\right).$$
if \( n \) is even. Here \( m \) is uniquely expressed in the form \( m = m_+ m_- \) where \((m_-, l) = 1\) and \( m_+ > 0 \) is divisible only by primes dividing \( l \). The above formulas for \( S_n \) are readily obtained directly as in (23) using the expansions

\[
\theta_1^n = l^{n/2} \left( n \over n/2 \right) + l^{n/2} \sum_{j=0}^{n/2-1} (-1)^{(l-1)(n+2j)/4} \binom{n}{j} (\zeta_{m_-}^{n-2j} + \zeta_{m_-}^{2j-n})
\]

if \( n \) is even, or

\[
(-1)^{(l-1)(n-1)/4} l^{(n-1)/2} i^* \sqrt{l} \sum_{j=0}^{(n-1)/2} \binom{n}{j} (-1)^{(l-1)j/2} \times (\zeta_{m_-}^{n-2j} + (-1)^{(l-1)/2} \zeta_{m_-}^{2j-n})
\]

if \( n \) is odd, from the binomial theorem together with equation (22), the fact that

\[
\sum_{v \in \mathbb{Z}_m^*/(\pm 1)} \left( \frac{v}{l} \right)^{t \over m} + (-1)^{(l-1)/2} \zeta_{m_-}^{t \over m} = \sum_{v \in \mathbb{Z}_m^*} \left( \frac{v}{l} \right)^{t \over m},
\]

and the lemma below. Details of the calculation, similar to that in establishing (23), are left to the reader.

**Lemma 3.** With notation as above,

\[
\sum_{x \in \mathbb{Z}_m^*} \left( \frac{x}{l} \right)^{t \over m} = i^* \sqrt{l} \frac{m_+}{l} \left( \frac{lt/m}{l} \right) \mu \left( \frac{m_-}{(t, m_-)} \right) \phi \left( \frac{m_-}{(t, m_-)} \right)
\]

if \((m_+, t) = m_+/l\) and 0 otherwise.

**Proof.** First note that

\[
\sum_{x \in \mathbb{Z}_m^*} \zeta_{m}^{t \over m} = \mu(d) \frac{\phi(m)}{\phi(d)}
\]

where \((t, m) = m/d\) from (22). Applying the result of problem 4, p. 336, in [2] with \( m = m_+ m_- \), one finds

\[
\sum_{x \in \mathbb{Z}_m^*} \left( \frac{x}{l} \right)^{t \over m} = \left( \frac{m_-}{l} \right) \sum_{x \in \mathbb{Z}_{m_+}^*} \left( \frac{x}{l} \right)^{t \over m} \sum_{x \in \mathbb{Z}_{m_-}^*} \zeta_{m_-}^{t \over m}. \sum_{x \in \mathbb{Z}_{m_+}^*} \zeta_{m_+}^{t \over m}
\]

The first sum in the product on the right is non-vanishing only when \((t, m_+) = m_+/l\), since otherwise in the factorization of \( \sum_{x \in \mathbb{Z}_{m_+}^*} \left( \frac{x}{l} \right)^{t \over m} \) \( \zeta_{m_+}^{t \over m} \) as a product of Gauss sums defined modulo the distinct prime powers dividing \( m_+ \), at least one such component will be zero (by problem 4, p. 336 in [2] again, and the fact that any imprimitive Gauss sum defined modulo a prime power vanishes). If \((t, m_+) = m_+/l\), say \( t = m_+/v \) with \((v, l) = 1\), then \( \sum_{x \in \mathbb{Z}_{m_+}^*} \left( \frac{x}{l} \right)^{t \over m} \) \( \zeta_{m_+}^{t \over m} \) is just \( m_+/l \) copies of \( \sum_{x \in \mathbb{Z}_{m_+}^*} \left( \frac{x}{l} \right)^{t \over m} \) \( \zeta_{m_+}^{t \over m} \), so equals \( i^* \sqrt{l} \frac{m_+}{l} \left( \frac{lt/m_+}{l} \right) \). The second
sum in the product equals
\[
\mu\left(\frac{m_-}{(l, m_-)}\right) \frac{\phi(m_-)}{\phi\left(\frac{m_-}{(l, m_-)}\right)}
\]
by my initial observation. The result of the lemma now follows since
\[
\left(\frac{m_-}{l}\right) \left(\frac{lt/m_+}{l}\right) = \left(\frac{lt/m}{l}\right)
\]
My aim here is to find a formula for the minimal polynomial of \(\theta\), or more precisely for the reciprocal polynomial \(P_{m,l}(X)\), analogous to that for \(F_m(X)\) in Section 2, whose zeros are the reciprocals of \(\theta\), in (25). To this end I first find an expression for the polynomial \(P(X)\) with zeros \(\{\pm\theta_v^{-1} \mid v \in \mathbb{Z}_m^*/(\pm 1)\}\). From (24), one has \((\zeta_m^2 + \zeta_m^{-2})^{-1} = (-1)^{(l-1)/2}\sqrt{2}(1 - 2\theta^{-2})\), a zero of \(F_m(X)\), so
\[
P(X) = (1 - 2lX^2)^{\phi(m)/2}F_m((-1)^{(l-1)/2}lX^2/(1 - 2lX^2))
\]
\[
= \left(1 - 2lX^2 + \sqrt{1 - 4lX^2}\right)^{\phi(m)/2}
\]
\[
\times \psi_{m'}\left(\left(\frac{1 - 2lX^2 - \sqrt{1 - 4lX^2}}{(-1)^{(l-1)/2}lX^2}\right)^{m/m'}\right)
\]
\[
= \left(1 + \sqrt{1 - 4lX^2}\right)^{\phi(m)/2}\psi_{m'}\left((-1)^{(l-1)/2}\frac{1 - \sqrt{1 - 4lX^2}}{2X}\right)^{2m/m'}
\]
from (20) since \((1 \pm \sqrt{1 - 4lX^2})/2 = (1 - 2lX^2 \pm \sqrt{1 - 4lX^2})/2\). For convenience I write
\[
(28) \quad P(X) = E_l(X)^{\phi(m)/2}\psi_{m'}((-1)^{(l-1)/2}A_l(X)^{2m/m'})
\]
where \(E_l(X) = (1 + \sqrt{1 - 4lX^2})/2, E_l(X) = (1 - \sqrt{1 - 4lX^2})/2\) and \(A_l(X) = (1 - \sqrt{1 - 4lX^2})/(2\sqrt{l}X)\). Now \(P(X) = P_{m,l}(X) \cdot P_{m,l}(-X)\) over \(\mathbb{Z}[X]\), so the strategy is to find the correct factor of \(P(X)\) in (28).

Suppose \(\psi_{m'}((-1)^{(l-1)/2}z^2)\) factors in \(\mathbb{Q}(\sqrt{l})\) as \(g_{m',l}(z)g_{m',l}(-z)\) with \(g_{m',l}(z)\) self-reciprocal and of the form
\[
(29) \quad g_{m',l}(z) = a_0 + a_2z^2 + \cdots + a_{\phi(m')/2}z^\phi(m') + \sqrt{l}(a_1z + a_3z^3 + \cdots + a_{\phi(m')-1}z^{\phi(m')-1})
\]
for integers \(a_j (0 \leq j \leq \phi(m'))\). Then \(a_{\phi(m')-j} = a_j (0 \leq j \leq \phi(m')/2)\) and \(E_l(X)^{\phi(m')/2} \cdot g_{m',l}(A_l(X)^{\phi(m')})\) is a polynomial in \(\mathbb{Z}[X]\). In fact, since \(E_l(X)A_l(X) = \sqrt{l}X\) and \(\sqrt{l}XA_l(X) = E_l(X)\), this polynomial is
\[ E_t(X) \frac{m}{m'} \phi(m')}{2} \times \left( \sum_{j=0}^{\phi(m')/2} a_{2j}(A_t(X)^{m'/m'})^{2j} + \sum_{j=1}^{\phi(m')/2} a_{2j-1} \sqrt{l}(A_t(X)^{m'/m'})^{2j-1} \right), \]

which equals
\[
(30) \quad a_{\phi(m')/2} l^{[(\phi(m)+2)/4]} X^{\phi(m)/2} + \sum_{j=0}^{\phi(m')/2} a_{2j}(lX^2)^{mj/m'} C_{m'/m'}(\phi(m')/2-2j)(\sqrt{l}X) + \sum_{j=1}^{\phi(m')/2} a_{2j-1} l^{(m(2j-1)/m'+1)/2} X^{m(2j-1)/m'} C_{m'/m'}(\phi(m')/2-2j+1)(\sqrt{l}X). \]

To find such a factor \( g_{m',l}(z) \) first consider
\[ g(x) = \prod_{v \in \mathbb{Z}_{m'}^*} \left( 1 - \left( \frac{v}{l} \right) \zeta_{m'}^v X \right), \]

a polynomial over \( \mathbb{Q}(i^* \sqrt{l}) \) with power sums given by (see Lemma 3)
\[
(31) \quad \sum_{v \in \mathbb{Z}_{m'}^*} \left( \frac{v}{l} \right) \zeta_{m'}^v = \begin{cases} 
  i^* \sqrt{l} \left( \frac{ln/m'}{l} \right) \mu \left( \frac{m'/l}{(n,m'/l)} \right) \phi((n,m'/l)) & \text{if } (n,l) = 1, \\
  0 & \text{if } (n,l) \neq 1
\end{cases}
\]

when \( n \) is odd, or by
\[ \sum_{v \in \mathbb{Z}_{m'}^*} \zeta_{m'}^v = \mu(d) \phi(m'/d) \]

when \( n \) is even, where \( (n,m') = m'/d \). I assert that \( g_{m',l}(z) = g(\varepsilon z) \), where
\[
(32) \quad \varepsilon = (-1)^{(l-1)(1-m/m')/4} i^* = \begin{cases} 
  1 & \text{if } l \equiv 1 \pmod{4}, \\
  (-1)^{(1-m/m')/2} i & \text{if } l \equiv 3 \pmod{4}
\end{cases}
\]

has the desirable characteristics in (29). From (31) its associated power sums for odd \( n \) are
\[
(33) \quad S_n = \begin{cases} 
  i^* \varepsilon^n \left( \frac{ln/m'}{l} \right) \mu \left( \frac{m'/l}{(n,m'/l)} \right) \phi((n,m'/l)) \sqrt{l} & \text{if } (n,l) = 1, \\
  0 & \text{otherwise}
\end{cases}
\]

and
\[ S_n = (-1)^{(l-1)n/4} \mu(d) \phi(m'/d) \quad \text{if } n \text{ is even}, \]
where \((n, m') = m'/d\). From Newton’s identities (6) one readily finds that \(g_{m', l}(z)\) has the form (29) with \(a_j\) satisfying a polynomial dependence on \(l\) of degree \(\leq [j/2]\). Furthermore, \(a_{\phi(m')-j} = a_j\) since \(g_{m', l}(z)\) is seen to be self-reciprocal. In fact, \(g_{m', m'}(z)\) is just the polynomial \(L_m(z)\) or \(L_m(-z)\) in equation (24) in [3], so is expressible in terms of the Auri feuille factors \(\psi\). More generally, \(g_{m', l}(z)\) is seen to be expressible in terms of the Schinzel factors [13] of \(\psi\). Brent [3] gives an efficient algorithm to compute \(g_{m', m'}(z)\) from Newton’s identities, basically due to Dirichlet, that readily generalizes to compute \(g_{m', l}(z)\) here.

I assert that \(P_{m,l}(X) = E_l(X)^{\phi(m)/2} g_{m', l}(A_l(X)^{m/m'})\) is the correct choice with zeros \(\theta_{\nu}^{-1}\) for \(\theta_{\nu}\) in (25). Indeed:

**Theorem 3.** Let \(g_{m', l}(z)\) be the self-reciprocal polynomial of the form (29) and of degree \(\phi(m')\) over \(\mathbb{Q}(\sqrt{l})\) determined from the power sums in (33). Then \(P_{m,l}(X)\) is given by (30) with coefficients \(c_r\) for \(X^r\) satisfying

\[
(34) \quad c_r = \left[\frac{r+1}{2}\right] \sum_{j=0, j \equiv r (\text{mod } 2)}^{[m'/m]} (-1)^{t_j} a_j \times \frac{m}{m'} \left( \frac{\phi(m')}{2} - j \right) \left( \frac{m}{m'} \left( \frac{\phi(m')}{2} - j \right) - t_j \right)
\]

for \(1 \leq r < \phi(m)/2\), and

\[
c_{\phi(m)/2} = \left[\frac{\phi(m)+2}{4}\right] \times \left( a_{\phi(m')/2} + (-1)^{[\phi(m')+2]/4} \sum_{j=0, j \equiv \phi(m)/2 (\text{mod } 2)}^{\phi(m')/2-2} (-1)^{[(j+1)/2]} 2a_j \right),
\]

where \(t_j = (r - mj/m')/2\).

**Proof.** In view of the remarks already made it suffices to show that \(E_l(X)^{\phi(m)/2} g_{m', l}(A_l(X)^{m/m'})\), which yields the polynomial expression in (30) above, has associated power sums matching those in (26). Again, expanding \(\log(1 - T)\) about \(T = 0\), one finds \(\log E_l(X)^{\phi(m)/2} g_{m', l}(A_l(X)^{m/m'})\) equals

\[
\frac{\phi(m)}{2} \log E_l(X) + \sum_{w \in \mathbb{Z}_{m'}} \log \left( 1 - \left( \frac{w}{l} \right) \varepsilon_{s_{m'}} \right) A_l(X)^{m/m'}
\]

\[
= - \frac{\phi(m)}{2} \sum_{n=1}^{\infty} \left( \frac{2n}{n} \right) \frac{\ln X^{2n}}{2n} - \sum_{w \in \mathbb{Z}_{m'}} \sum_{v=1}^{\infty} \varepsilon^v \left( \frac{w}{l} \right) \varepsilon_{s_{m'}} A_l(X)^{mv/m'}
\]
\[ -\frac{\phi(m)}{2n} \sum_{n=1}^{\infty} \binom{2n}{n} l^n X^{2n} \frac{m}{2n} - \sum_{v=1}^{\infty} \frac{\varepsilon^v}{v} A_l(X)^{mv/m'} \sum_{w \in \mathbb{Z}_{m'}} \left( \frac{w}{l} \right)^v \zeta_{wv}. \]

In view of (31) and Lemma 1, this last expression is seen to have the coefficient of \( X^n \) equal to
\[ -\frac{\phi(m)}{2n} \binom{n}{n/2} - \frac{1}{n} \sum_{d|m'} \mu(d) \times \frac{\phi(m')}{\phi(d)} \sum_{t=1, (t,d)=1}^{[dn/2m]} (-1)^{(l-1)t/2} \frac{m}{m'} \left( \frac{n}{n/2 - mt/d} \right) \]
if \( n \) is even, or
\[ -\frac{l^{(n-1)/2}}{n} \sum_{t=1, (t,l)=1, t \text{ odd}}^{[m'n/m]} i^* \varepsilon^t \left( \frac{lt/m'}{l} \right) \mu \left( \frac{m'/l}{t, m'/l} \right) \frac{\phi(m')/l}{\phi \left( \frac{m'/l}{t, m'/l} \right)} \times \frac{lm}{m'} \left( \frac{n}{n/2 - mt/2m'} \right) \]
if \( n \) is odd. Since for \((t, l) = 1, \)
\[ (mt/m', m_-) = \left( \frac{m_- t}{m'/l}, m_- \right) = \frac{m_-}{m'/l} (t, m'/l), \]
on one finds
\[ \frac{m'/l}{(t, m'/l)} = \frac{m_-}{mt/m', m_-} \quad \text{and} \quad \frac{\phi(m'/l)}{\phi \left( \frac{m'/l}{(t, m'/l)} \right)} = \frac{m'/l}{m_-} \frac{\phi(m_-)}{\phi \left( \frac{m_-}{mt/m', m_-} \right)}, \]
so this last expression for odd \( n \) equals
\[ -\frac{l^{(n-1)/2} m_+}{n} \sum_{t=1, (t,l)=1, t \text{ odd}}^{[nm'/m]} i^* \varepsilon^t \delta_{m,l}(t) \left( \frac{n}{n - mt/m'} / 2 \right), \]
with \( \delta_{m,l}(t) \) as in (26). But for \( t \) odd, \( i^* \varepsilon^t = (-1)^{(l-1)(1+mt/m')/4} \) from (32), so the polynomial \( E_l(X)^{\phi(m)/2} g_{m', l}(A_l(X)^{m/m'}) \) has associated power sums as in (26).

The formulas for the coefficients \( c_r \) are obtained in a straightforward fashion from the expression (30). This completes the proof of the theorem.

Next I give a few examples to illustrate Theorem 3.

**Example 6.** Consider \( \theta_1 = i\sqrt{15} (\zeta_{15} - \zeta_{15}^{-1}) \) in (25). Here \( l = m_+ = m = m' = 15 \) and \( m_- = 1 \) with \( \psi_{15}(x) = 1 - x + x^3 - x^4 + x^5 - x^7 + x^8. \)
One finds
\[ g_{15,15}(z) = 1 + 8z^2 + 13z^4 + 8z^6 + z^8 + \sqrt{15} (z + 3z^3 + 3z^5 + z^7) \]
is the correct “Aurifeuille” factor of $\psi_{15}(-z^2)$ satisfying (32). Indeed direct computation of $P_{15,15}(X)$ yields

$$P_{15,15}(X) = 1 + 15X + 60X^2 - 225X^4,$$

whose coefficients agree with those obtained from (34). Note that $\theta = i\sqrt{15}(\zeta_{45} - \zeta_{45}^{-1})$ with $l = m' = 15$, $m_+ = m = 45$ and $m_- = 1$ requires the conjugate factor

$$g_{15,15}(z) = 1 + 8z^2 + 13z^4 + 8z^6 + z^8 - \sqrt{15}(z + 3z^3 + 3z^5 + z^7)$$

in the computation of

$$P_{45,15}(X) = 1 - 180X^2 - 225X^3 + 54 \cdot 15^2X^4 + 9 \cdot 15^3X^5 - 104 \cdot 15^3X^6 - 27 \cdot 15^4X^7 + 57 \cdot 15^4X^8 + 27 \cdot 15^5X^9 + 36 \cdot 15^5X^{10} - 15^6X^{12}.$$ 

**Example 7.** Next consider $\theta_1 = i\sqrt{3}(\zeta_{45} - \zeta_{45}^{-1})$ in (25) with $m = 45$, $l = 3$, $m_+ = 9$, $m' = 15$ and $m_- = 5$, and again $\psi_{15}(x) = 1 - x + x^3 - x^4 + x^5 - x^7 + x^8$. One finds here that

$$g_{15,3}(z) = 1 + 2z^2 + z^4 + 2z^6 + z^8 - \sqrt{3}(z + z^3 + z^5 + z^7)$$

is the correct “Schinzel” factor of $\psi_{15}(-z^2)$ satisfying (32). Direct computation of the power sums $S_n$ yields $S_1 = 0$, $S_2 = 72$, $S_3 = 27$, $S_4 = 3^4 \cdot 8$, $S_5 = 3^4 \cdot 5$, $S_6 = 3^4 \cdot 79$, $S_7 = 3^6 \cdot 7$, $S_8 = 3^5 \cdot 272$, $S_9 = 3^7 \cdot 28$, $S_{10} = 3^8 \cdot 107$, $S_{11} = 3^8 \cdot 110$ and $S_{12} = 3^8 \cdot 1159$, with

$$P_{45,3}(X) = 1 - 36X^2 - 9X^3 + 3^5 \cdot 2X^4 + 3^5X^5 - 3^3 \cdot 110X^6 - 3^7X^7 + 3^4 \cdot 93X^8 + 3^5 \cdot 29X^9 - 3^7 \cdot 2X^{10} - 3^7 \cdot 2X^{11} - 3^6X^{12}$$

in agreement with the formulas in Theorem 3. If instead one takes $\theta_1 = \sqrt{5}(\zeta_{45} + \zeta_{45}^{-1})$ in (25) so $m = 45$, $l = m_+ = 5$, $m' = 15$ and $m_- = 9$, then the correct “Schinzel” factor of $\psi_{15}(z^2)$ satisfying (32) is

$$g_{15,5}(z) = 1 + 2z^2 + 3z^4 + 2z^6 + z^8 - \sqrt{5}(z + z^3 + z^5 + z^7).$$

Direct computation yields

$$P_{45,5}(X) = 1 - 60X^2 - 25X^3 + 5^2 \cdot 54X^4 + 5^3 \cdot 9X^5 - 5^4 \cdot 22X^6 - 5^4 \cdot 27X^7 + 5^4 \cdot 93X^8 + 5^5 \cdot 29X^9 - 5^5 \cdot 18X^{10} - 5^6 \cdot 6X^{11} + 5^6X^{12},$$

whose coefficients agree with those determined from (34).

**Example 8.** Now consider $\theta_1 = \sqrt{21}(\zeta_{21} + \zeta_{21}^{-1})$ in (25). Here $l = m_+ = m = m' = 21$ and $m_- = 1$, with $\psi_{21}(x) = 1 - x + x^3 - x^4 + x^6 - x^8 + x^9 - x^{11} + x^{12}$. One finds here that

$$g_{21,21}(z) = 1 + 10z^2 + 13z^4 + 7z^6 + 13z^8 + 10z^{10} + x^{12} - \sqrt{21}(x + 3x^3 + 2x^5 + 2x^7 + 3x^9 + x^{11})$$
is the correct “Aurifeuille” factor of \( \psi_{21}(z^2) \) satisfying (32). Direct computation yields

\[ P_{21,21}(X) = 1 - 21X + 84X^2 + 882X^3 - 7938X^4 + 18522X^5 - 9261X^6, \]
whose coefficients agree with those found from (34).

If one considers instead \( \theta_1 = i\sqrt{7}(\zeta_{21} - \zeta_{21}^{-1}) \) in (25), so \( l = m_+ = 7, m' = m = 21 \) and \( m_- = 3 \), one finds that

\[
g_{21,7}(x) = 1 + 4z^2 - z^4 - 7z^6 - z^8 + 4z^{10} + z^{12} + \sqrt{7}(z + z^3 - 2z^5 - 2z^7 + z^9 + z^{11})
\]
is the correct “Schinzel” factor of \( \psi_{21}(-z^2) \) satisfying (32) with

\[ P_{21,7}(X) = 1 + 7X - 14X^2 - 7^2 \cdot 4X^3 - 7^2 \cdot 8X^4 + 7^3X^6 \]
from (34).

The special case \( m = p^\alpha \) warrants special consideration. Here I simply write \( P_{p^\alpha}(X) \) for \( P_{p^\alpha,p}(X) \).

**Corollary 3.** For an odd prime \( p \), \( P_{p^\alpha}(X) \) has the form

\[
a_{(p-1)/2}p^{\alpha-1}(p+1)/4 X^{p^{\alpha-1}(p-1)/2} + \sum_{j=0}^{[(p-3)/4]} a_{2j}(pX^2)^{p^{\alpha-1}j} C_{p^{\alpha-1}(p-1)/4-2j}(\sqrt{p} X)
\]

\[
+ \sum_{j=1}^{[(p-1)/4]} a_{2j-1}p^{(p^{\alpha-1}(2j-1)+1)/2} X^{p^{\alpha-1}(2j-1)/2} C_{p^{\alpha-1}(p-1)/4-2j+1}(\sqrt{p} X),
\]

with coefficient \( c_r \) for \( X^r \) satisfying

\[
c_r = p^{[(r+1)/2]} \sum_{j=0, j \equiv r \pmod{2}}^{[rp^{1-\alpha}]} (-1)^j a_j \times \frac{p^{\alpha-1}(p^{1-1}/2 - j)}{p^{\alpha-1}(p^{1-1}/2 - j)} \left( p^{\alpha-1}(p^{1-1}/2 - j) - t_j \right)
\]

for \( 1 \leq r < \phi(p^\alpha)/2 \), where \( t_j = (r - p^{\alpha-1}j)/2 \), and with

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

where \( N \) is the number of quadratic non-residues of \( p \) in \((0, p/2)\).

**Proof.** I need only justify the determination of the last coefficient \( c_{\phi(p^\alpha)/2} = (-1)^{\phi(p^\alpha)/2} N_{K/\mathbb{Q}}(i^* \sqrt{p} (\zeta_{p^\alpha} + (-1)^{(p-1)/2} \zeta_{p^\alpha}^{-1})) \), where \( K = \mathbb{Q}(\zeta_{p^\alpha} + \zeta_{p^\alpha}^{-1}) \).
For $p \equiv 1 \pmod{4}$, one immediately has $c_{\phi(p^a)/2} = \left(\frac{2}{p}\right)p^{\phi(p^a)/4}$ since $N_{K/Q}(\zeta_{p^a} + \zeta_{p^a}^{-1}) = \left(\frac{2}{p}\right)$ from (19). For $p \equiv 3 \pmod{4}$, one notes that (see problem 14, p. 355 in [2]; see also (35) below)

\[
\prod_{v=1, p|v}^{[p^a/2]} (\zeta_{p^a}^v - \zeta_{p^a}^{-v}) = \prod_{v=1}^{[p/2]} (\zeta_p - \zeta_p^{-v}) = i\sqrt{p}\left(-\frac{2}{p}\right),
\]

so that

\[
c_{\phi(p^a)/2} = -\prod_{v=1, p|v}^{[p^a/2]} i\sqrt{p}\left(\frac{v}{p}\right)(\zeta_{p^a}^v - \zeta_{p^a}^{-v}) = \left(\frac{2}{p}\right)(-1)^N(-p)^{(\phi(p^a)+2)/4},
\]

where $N$ counts the number of times $\left(\frac{v}{p}\right) = -1$ for $1 \leq v \leq (p-1)/2$.

Actually it is no more difficult to determine the last coefficient $c_{\phi(m)/2}$ for the polynomial $P_{m,l}(X)$ in Theorem 3 in general. For odd composite $m'$, $c_{\phi(m)/2}$ is the norm of $\theta_1$ in (25) so equals $\pm l^{\phi(m)/4}$ since $i^*(\zeta_m + (-1)^{(l-1)/2}\zeta_m^{-1})$ is a unit of $K$. The correct sign is given by

**PROPOSITION 4.** For odd composite $m'$ in Theorem 3,

\[
c_{\phi(m)/2} = (-1)^N l^{\phi(m)/4},
\]

where $N$ counts the number of reduced residues $v$ modulo $m'$ in $(0, m'/2)$ with $\left(\frac{v}{m'}\right) = -1$.

**Proof.** First note that for any integer $a$ with $(a, m') = 1$,

\[
(35) \prod_{v \in \mathbb{Z}_{m'}, v \equiv a \pmod{m'}} (\zeta_m^v \pm \zeta_m^{-v}) = \prod_{\lambda=0}^{m/m'-1} (\zeta_{m/m'\lambda}^v \pm \zeta_{m/m'}^{-\lambda} \zeta_m^a \pm \zeta_{m/m'}^{-a}) = \zeta_m^a \pm \zeta_m^{-a}
\]

since $\zeta_m^a + \lambda m' = \zeta_{m/m'}^\lambda \cdot \zeta_m^a$ for $0 \leq \lambda < m/m'$. Moreover, I assert here that

\[
(36) \prod_{v=1, (v, m')=1}^{(m'-1)/2} 2\sin\frac{2\pi v}{m'} = \prod_{v=1, (v, m')=1}^{(m'-1)/2} 2\cos\frac{2\pi v}{m'} = 1
\]

since $m'$ is odd and composite. To verify (36) observe that up to sign $\prod 2\sin(2\pi v/m')$ is the norm from $K$ to $Q$ of the unit $i(\zeta_{m'} - \zeta_{m'}^{-1})$, so it equals $\pm 1$. But $2\sin(2\pi v/m') > 0$ for $1 \leq v \leq (m'-1)/2$, so that the product must be 1 and hence also the product of its conjugates $2\sin(4\pi v/m')$ for $1 \leq v \leq (m'-1)/2$. Since

\[
2\cos(2\pi v/m') = \frac{2\sin(4\pi v/m')}{2\sin(2\pi v/m')},
\]
the product of cosines must also equal 1. Now from (35),
\[
c_{\phi(m)/2} = \prod_{v=1, (v,m')=1}^{[m'/2]} i^* \sqrt{\frac{
u}{l}} \left( \zeta_{m'}^\nu + (-1)^{(l-1)/2} \zeta_{m'}^{-\nu} \right)
\]
or just
\[
((-1)^{(l-1)/2} l)^{\phi(m)/4} \prod_{v=1, (v,m')=1}^{[m'/2]} \left( \frac{
u}{l} \right)^{\phi(m)/4} \zeta_{m'}^\nu + (-1)^{(l-1)/2} \zeta_{m'}^{-\nu}
\]
by (36), where \(N\) counts the number of reduced residues \(v\) modulo \(m'\) in the interval \((0, m'/2)\) with \(\left( \frac{v}{l} \right) = -1\). This completes the proof of the proposition.

Before concluding this section I wish to remark that one obtains a variant for the sums \(S_n\) in (26) when \(n\) is even using the fact that \(P(X) = P_{m,l}(X) \cdot P_{m,l}(-X)\), so that \(S_n = \frac{1}{2} S'_n\), where \(S'_n\) is the \(n\)th power sum associated to \(P(X)\) with \(n\) even. Now from (28),
\[
\log P(X) = \phi(m) \log E_l(X) + \sum_{d|m'} \mu(d) \log(1 - (-1)^{(l-1)/2} A_l(X)^{2m/m'})
\]
\[
= -\phi(m) \sum_{n=1}^{\infty} \frac{(2n)^n X^{2n}}{2n} \frac{1}{n} + \sum_{d|m'} \mu(d) \sum_{v=1}^{\infty} \frac{(-1)^{(l-1)v/2}}{v} A_l(X)^{2mv/m'}.
\]
Thus if \(n\) is even,
\[
S_n = l^{n/2} \frac{\phi(m)}{2} \binom{n}{n/2} + l^{n/2} \sum_{d|m} \mu(d) \frac{m}{d} \sum_{t=1}^{[nd/2m]} (-1)^{(l-1)t/2} \binom{n}{n/2 - mt/d}
\]
as an alternative expression for \(S_n\) in (26).

References

Minimal polynomials for Gauss periods


University of San Diego
San Diego, CA 92110, U.S.A.
E-mail: gurak@sandiego.edu

*Received on 13.6.2005*

*and in revised form on 4.11.2005*