Number Theory, *Richard A. Mollin (ed.)*
© 1990 by Walter de Gruyter · Berlin · New York

Explicit evaluation of certain Eisenstein sums

Kenneth S. Williams[1], *Kenneth Hardy*[2] *and Blair K. Spearman*
with the assistance of Nicholas Buck and Iain deMille

0. Notation

The following notation will be used throughout this paper: p is an odd prime, m is an integer ≥ 2 coprime with p, and f is a positive integer such that $p^f - 1$ is divisible by m.

1. Introduction

The finite field with $q = p^f$ elements is denoted by F_q. The prime subfield of F_q is $F_p = \{0,1,2,\ldots,p-1\}$. The trace of an element $\alpha \in F_q$ is defined by

$$tr(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \ldots + \alpha^{p^{f-1}} \in F_p . \tag{1.1}$$

The trace function has the following properties:

$$tr(\alpha+\beta) = tr(\alpha) + tr(\beta), \quad \forall\, \alpha, \beta \in F_q , \tag{1.2}$$

$$tr(k\alpha) = ktr(\alpha), \quad \forall\, \alpha \in F_q,\ k = 0,1,2,\ldots, \tag{1.3}$$

$$tr(\alpha^p) = tr(\alpha), \quad \forall\, \alpha \in F_q , \tag{1.4}$$

$$tr(k) = kf, \quad k = 0,1,2,\ldots . \tag{1.5}$$

---

[1]Research supported by Natural Sciences and Engineering Research Council of Canada Grant A–7233.

[2]Research supported by Natural Sciences and Engineering Research Council of Canada Grant A–7823.

We also set $F_q^* = F_q - \{0\}$. With respect to multiplication, F_q^* is a cyclic group of order $q-1$. We fix once and for all a generator γ of F_q^*. For $\alpha \in F_q^*$. For $\alpha \in F_q^*$ the unique integer r such that $\alpha = \gamma^r$, where $0 \le r \le q-2$, is called the *index* of α with respect to γ and is denoted by $\text{ind}_\gamma(\alpha)$. We have $\text{ind}_\gamma(-1) = (q-1)/2$. Since γ generates F_q^*,

$$g = \gamma^{(q-1)/(p-1)} \in F_p \tag{1.6}$$

generates F_q^*. For $k \in F_q^*$ the unique integer s such that $k = g^s$, where $0 \le s \le p-2$, is called the *index* of k with respect to g and is denoted by $\text{ind}_g(k)$. The relationship between $\text{ind}_\gamma(k)$ and $\text{ind}_g(k)$ is given by

$$\text{ind}_\gamma(k) \equiv \frac{(q-1)}{(p-1)} \text{ind}_g(k) \pmod{q-1}. \tag{1.7}$$

For m a positive integer (≥ 2) dividing $q-1$ and any integer n, the Eisenstein sum $E_q(w_m^n)$ is defined by

$$E_q(w_m^n) = \sum_{\substack{\alpha \in F_q^* \\ tr(\alpha)=1}} w_m^{n\,\text{ind}_\gamma(\alpha)}, \tag{1.8}$$

where $w_m = \exp(2\pi i/m)$. Clearly $E_q(w_m^n)$ is an integer of the cyclotomic field $Q(w_m)$. We remark that if $n \equiv n' \pmod m$ then

$$E_q(w_m^n) = E_q(w_m^{n'}). \tag{1.9}$$

In particular, if $n \equiv 0 \pmod m$, we have

$$E_q(w_m^n) = E_q(1) = \sum_{\substack{\alpha \in F_q^* \\ tr(\alpha)=1}} 1 = p^{f-1}.$$

We also note that if GCD $(m,n) = d > 1$, say $m = m_1 d$, $n = n_1 d$, where GCD $(m_1, n_1) = 1$, then $m_1 | q-1$ and

$$E_q(w_m^n) = E_q(w_{m_1}^{n_1}). \tag{1.10}$$

Thus it suffices to consider only those $E_q(w_m^n)$ for which $1 \leq n < m$, GCD $(n,m) = 1$. Further, if σ_n is the automorphism of $Q(w_m)$ such that $\sigma_n(w_m) = w_m^n$ (GCD $(n,m) = 1$), then $\sigma_n(E_q(w_m)) = E_q(w_m^n)$, and we can further restrict our attention to $E_q(w_m)$.

It is the purpose of this paper to evaluate explicitly the Eisenstein sums $E_q(w_m)$ for $m = 2,3,\ldots,8$. The evaluation of $E_q(w_m)$ for $m = 2,3,4,5,6,7,8$ is given in Theorem 1, 2, 3, 4, 5, 6, 7, respectively. Examples are given in Tables 1–29 (§11). It is planned to treat additional values of m in another paper, as well as to apply the results of this paper to the determination of cyclotomic numbers over F_q and the determination of binomial coefficients modulo p.

These evaluations are accomplished by using the basic facts about Eisenstein sums established by Stickelberger [19] together with the theory of Gauss sums, including the important results on Gauss sums established by Davenport and Hasse in [4]. Our results include and extend those of Berndt and Evans in [2] in the case $f = 2$.

We make use of the Gauss sums $G_q(w_m^n)$, $g_q(w_m^n)$, and $g_p(w_m^n)$ defined for any integer n by

$$G_q(w_m^n) = \sum_{\alpha \in F_q^*} w_m^{\text{nind}_\gamma(\alpha)} \exp(2\pi i\ tr(\alpha)/p), \tag{1.11}$$

$$g_q(w_m^n) = \sum_{k \in F_p^*} w_m^{\text{nind}_\gamma(k)} \exp(2\pi ik/p), \tag{1.12}$$

$$g_p(w_m^n) = \sum_{k \in F_p^*} w_m^{\text{nind}_g(k)} \exp(2\pi ik/p), \quad \text{provided } p \equiv 1 \pmod{m}, \tag{1.13}$$

as well as the Jacobi sum $J_p(w_m^r, w_m^s)$ defined for any integers r and s by

$$J_p(w_m^r, w_m^s) = \sum_{k=2}^{p-1} w_m^{r\,\text{ind}_g(k) + s\,\text{ind}_g(1-k)}, \quad \text{provided } p \equiv 1 \pmod{m}. \tag{1.14}$$

It is well–known (see for example [17: Chapter 5]) that

$$G_q(w_m^n)G_q(w_m^{-n}) = w_m^{n(q-1)/2}q, \quad \text{if } m \nmid n, \tag{1.15}$$

$$g_q(w_m^n)g_q(w_m^{-n}) = w_m^{n(q-1)/2}p, \quad \text{if } m \nmid n\left[\frac{q-1}{p-1}\right], \tag{1.16}$$

and if $p \equiv 1 \pmod{m}$

$$g_p(w_m^n)g_p(w_m^{-n}) = w_m^{n(p-1)/2}p, \quad \text{if } m \nmid n, \tag{1.17}$$

$$J_p(w_m^r, w_m^s) = \frac{g_p(w_m^r)g_p(w_m^s)}{g_p(w_m^{r+s})}, \quad m \nmid r,\ m \nmid s,\ m \nmid r+s. \tag{1.18}$$

We close this section by emphasizing that the Eisenstein sum $E_q(w_m^n)$ depends upon the generator γ as well as upon m, n and q. On the few occasions when we wish to indicate this dependence, we write $E_q(w_m^n, \gamma)$ for $E_q(w_m^n)$. If γ' is another generator of F_q^* we have

$$E_q(w_m^n, \gamma) = E_q\left(w_m^{n\,\mathrm{ind}_\gamma(\gamma')}, \gamma'\right), \tag{1.19}$$

as $\mathrm{ind}_\gamma(\alpha) \equiv \mathrm{ind}_g(\gamma')\,\mathrm{ind}_{\gamma'}(\alpha) \pmod{q-1}$, and so

$$E_q(w_m^n, \gamma) = E_q(w_m^n, \gamma'), \quad \text{if } \mathrm{ind}_\gamma(\gamma') \equiv 1 \pmod{m/\mathrm{GCD}(m,n)}. \tag{1.20}$$

2. Eisenstein sums

The following basic results concerning Eisenstein sums are implicit in the work of Stickelberger [19].

Theorem A. (Stickelberger)

(a) [19: p. 338] $E_q(w_m^n) = E_q(w_m^{np})$.

(b) [19: p. 339] $E_q(w_m^n) = \begin{cases} G_q(w_m^n)/g_q(w_m^n), & \text{if } m \nmid n\left[\frac{q-1}{p-1}\right], \\ -G_q(w_m^n)/p, & \text{if } m \mid n\left[\frac{q-1}{p-1}\right],\ m \nmid n. \end{cases}$

(c) [19: p. 339] $E_q(w_m^n)E_q(w_m^{-n}) = \begin{cases} p^{f-1}, & \text{if } m \nmid n\left[\frac{q-1}{p-1}\right], \\ (w_m^{n(q-1)/2}p^{f-2}, & \text{if } m \mid n\left[\frac{q-1}{p-1}\right],\ m \nmid n. \end{cases}$

(d) [19: p. 361] *For* $i = 0,1,2,\ldots, f-1$ *set*

$$a_i = \text{least positive residue of } p^i \pmod m. \tag{2.1}$$

Let

$$A_0 = \text{least nonnegative residue of } \frac{q-1}{p-1} \pmod m. \tag{2.2}$$

Define the integer B_0 *by*

$$B_0 = \left(\sum_{i=0}^{f-1} a_i - A_0\right)/m. \tag{2.3}$$

Then, for some prime ideal $\mathfrak{P}$ *of* $Q(w_m)$ *dividing* p, *we have*

$$E_q(w_m) \equiv (-1)^{B_0}p^{f-1-B_0}\,\frac{\left[\frac{pa_0}{m}\right]!\cdots\left[\frac{pa_{f-1}}{m}\right]!}{\left[\frac{pA_0}{m}\right]} \pmod{\mathfrak{P}^{f-B_0}}. \tag{2.4}$$

Next we relate $E_q(w_m^n)$ to $E_{p^\ell}(w_m^n)$, where ℓ is the least positive integer such that m divides $p^\ell - 1$, so that ℓ is a divisor of f. The sum $E_{p^\ell}(w_m^n)$ is taken with respect to the generator $\gamma' = \gamma^{(q-1)/(p^\ell-1)}$. We prove

Theorem B. *Let* ℓ *denote the least positive integer such that* $p^\ell - 1$ *is divisible by* m, *so that* ℓ *is a divisor of* f. *Then*

$$E_q(w_m^n) = \begin{cases} (-1)^{\frac{f}{\ell}-1}\,\dfrac{g_{p^\ell}(w_m^n)^{f/\ell}}{g_{p^\ell}\left[w_m^{n\left[\frac{p^f-1}{p^\ell-1}\right]}\right]}\,(E_{p^\ell}(w_m^n))^{f/\ell}, & \text{if } m \nmid n\left[\frac{p^f-1}{p-1}\right], \\ (-1)^{f/\ell}\,\dfrac{(g_{p^\ell}(w_m^n))^{f/\ell}}{p}\,(E_{p^\ell}(w_m^n))^{f/\ell}, & \text{if } m \nmid n\left[\frac{p^\ell-1}{p-1}\right], m \mid n\left[\frac{p^f-1}{p-1}\right], \\ p^{\frac{f}{\ell}-1}(E_{p^\ell}(w_m^n))^{f/\ell}, & \text{if } m \mid n\left[\frac{p^\ell-1}{p-1}\right],\ m \nmid n. \end{cases}$$

Proof. From the Davenport–Hasse theorem [4: p. 153] (see also [17: p. 197]), we have

$$G_q(w_m^n) = (-1)^{\frac{f}{\ell}-1}(G_{p^\ell}(w_m^n))^{f/\ell}. \tag{2.5}$$

Also, as

$$\mathrm{ind}_\gamma(k) \equiv \left(\frac{q-1}{p^\ell-1}\right) \mathrm{ind}_{\gamma'}(k) \pmod{q-1},$$

where $\gamma' = \gamma^{(q-1)/(p^\ell-1)}$, we have appealing to (1.12)

$$g_q(w_m^n) = g_{p^\ell}(w_m^{n\left[\frac{p^f-1}{p^\ell-1}\right]}). \tag{2.6}$$

(a): $m \nmid n\left[\frac{p^f-1}{p-1}\right]$. We have

$$E_q(w_m^n) = \frac{G_q(w_m^n)}{g_q(w_m^n)} \quad \text{(by Theorem A(b))}$$

$$= \frac{(-1)^{f/\ell-1}(G_{p^\ell}(w_m^n))^{f/\ell}}{g_{p^\ell}\left(w_m^{n(q-1)/(p^\ell-1)}\right)} \quad \text{(by (2.5) and (2.6))}$$

$$= (-1)^{f/\ell-1}\frac{g_{p^\ell}(w_m^n)^{f/\ell}}{g_{p^\ell}\left(w_m^{n(q-1)/(p^\ell-1)}\right)}(E_{p^\ell}(w_m^n))^{f/\ell},$$

by Theorem A(b).

(b): $m \mid n\left(\frac{q-1}{p-1}\right)$, $m \nmid n\left(\frac{p^\ell-1}{p-1}\right)$. We have

$$E_q(w_m^n) = -\frac{G_q(w_m^n)}{p} \quad \text{(by Theorem A(b))}$$

$$= (-1)^{f/\ell}\left(G_{p^\ell}(w_m^n)\right)^{f/\ell}/p \quad \text{(by (2.5))}$$

$$= (-1)^{f/\ell} \frac{\left(g_{p\ell}(w_m^n)\right)^{f/\ell}}{p} \left(E_{p\ell}(w_m^n)\right)^{f/\ell},$$

by Theorem A(b).

(c): $m \mid n\left(\frac{p^\ell-1}{p-1}\right)$, $m \nmid n$ (so that $m \mid n\left(\frac{q-1}{p-1}\right)$). We have

$$E_q(w_m^n) = -\frac{G_q(w_m^n)}{p} \quad \text{(by Theorem A(b))}$$

$$= \frac{(-1)^{f/\ell}\left(G_{p\ell}(w_m^n)\right)^{f/\ell}}{p} \quad \text{(by (2.5))}$$

$$= \frac{(-1)^{f/\ell}\left(-pE_{p\ell}(w_m^n)\right)^{f/\ell}}{p} \quad \text{(by Theorem A(b))}$$

$$= p^{f/\ell-1}\left(E_{p\ell}(w_m^n)\right)^{f/\ell}.$$

The special case of Theorem B when $p \equiv 1 \pmod{m}$, so that $\ell = 1$, gives the following corollary.

Corollary 1. *If $p \equiv 1 \pmod{m}$ then*

$$E_q(w_m) = \begin{cases} (-1)^{f-1} \dfrac{g_p(w_m)^f}{g_p(w_m^f)}, & \text{if } m \nmid f, \\ (-1)^f \dfrac{(g_p(w_m))^f}{p}, & \text{if } m \mid f. \end{cases}$$

Proof. As $p \equiv 1 \pmod{m}$ we have $\ell = 1$. By Theorem B with $n = 1$ we obtain

$$E_q(w_m) = \begin{cases} (-1)^{f-1} \dfrac{g_p(w_m)^f}{g_p\left(w_m^{\left(\frac{p^f-1}{p-1}\right)}\right)} E_p(w_m))^f, & \text{if } m \nmid \dfrac{p^f-1}{p-1}, \\ (-1)^f \dfrac{(g_p(w_m))^f}{p} (E_p(w_m))^f, & \text{if } m \Big| \dfrac{p^f-1}{p-1}. \end{cases}$$

The required result now follows as

$$E_q(w_m) = 1, \quad \frac{p^f-1}{p-1} = p^{f-1} + \ldots + p + 1 \equiv f \pmod{m},$$

and $\gamma^{\frac{p^f-1}{p^\ell-1}} = \gamma^{\frac{p^f-1}{p-1}} = g.$

The next theorem gives the value of $E_q(w_m)$ when there is an integer r such that $p^r \equiv -1 \pmod{m}$.

Theorem C. *Let p be a prime for which there is an integer r such that $p^r \equiv -1 \pmod{m}$. Let ℓ be the least positive integer such that*

$$p^\ell \equiv -1 \pmod{m}.$$

Then, for $f \equiv 0 \pmod{2\ell}$, we have

$$E_q(w_m) = (-1)^{\frac{f}{2\ell}\left(\frac{p^\ell-(m-1)}{m}\right)} p^{f/2-1}.$$

Proof. By Theorem A(a) we have

$$E_q(w_m) = E_q(w_m^p) = E_q(w_m^{p^2}) = \ldots = E_q(w_m^{p^\ell}),$$

that is

$$E_q(w_m) = E_q(w_m^{m-1}), \tag{2.7}$$

showing that $E_q(w_m)$ is real. Next set

$$\frac{f}{2\ell} = 2^r s, \quad r \geq 0, \quad s \text{ odd}, \tag{2.8}$$

so that

$$p^{f/2^{r+1}} = p^{\ell s} = \left(p^{\ell}\right)^{s} \equiv (-1)^{s} \equiv -1 \pmod{m}. \tag{2.9}$$

Then we have

$$\frac{q-1}{p-1} = \left(\frac{p^{f/2^{r+1}} - 1}{p-1}\right)\left(p^{f/2^{r+1}} + 1\right)\left(p^{f/2^{r}} + 1\right) \cdots \left(p^{f/2} + 1\right) \equiv 0 \pmod{m},$$

and

$$(q-1)/2 = \frac{\left(p^{f/2^{r+1}} - 1\right)}{2}\left(p^{f/2^{r+1}} + 1\right)\left(p^{f/2^{r}} + 1\right) \cdots \left(p^{f/2} + 1\right) \equiv 0 \pmod{m},$$

so, by Theorem A(c), we have

$$E_q(w_m)E_q(w_m^{m-1}) = p^{f-2}. \tag{2.10}$$

From (2.7) and (2.10), we deduce that

$$E_q(w_m) = \theta p^{f/2-1}, \tag{2.11}$$

where $\theta = \pm 1$.

Next, since $p^{\ell} \equiv -1 \pmod{m}$, for $k = 0,1,2,\ldots$, we have (with the notation of (2.1))

$$a_k = \begin{cases} a_{k-\ell[k/\ell]}, & \text{if } [k/\ell] \equiv 0 \pmod 2, \\ m - a_{k-\ell[k/\ell]}, & \text{if } [k/\ell] \equiv 1 \pmod 2. \end{cases} \tag{2.12}$$

Thus we have

$$\left[\frac{p\,a_0}{m}\right]!\left[\frac{p\,a_1}{m}\right]!\cdots\left[\frac{p\,a_{f-1}}{m}\right]!$$

$$= \prod_{i=1}^{2^{r+1}s} \prod_{j=0}^{\ell-1} \left[\frac{p a_{(i-1)\ell+j}}{m}\right]!$$

$$= \prod_{\substack{i=1 \\ i \text{ odd}}}^{2^{r+1}s} \prod_{j=0}^{\ell-1} \left[\frac{pa_j}{m}\right]! \prod_{\substack{i=1 \\ i \text{ even}}}^{2^{r+1}s} \prod_{j=0}^{\ell-1} \left[\frac{p(m-a_j)}{m}\right]!$$

$$= \left(\prod_{j=0}^{\ell-1} \left[\frac{pa_j}{m}\right]!\right)^{2^r s} \left(\prod_{j=0}^{\ell-1} \left[p - \frac{pa_j}{m}\right]!\right)^{2^r s}$$

$$= \left(\prod_{j=0}^{\ell-1} \left[\frac{pa_j}{m}\right]! \left[p - \frac{pa_j}{m}\right]!\right)^{f/2\ell}$$

$$= \left(\prod_{j=0}^{\ell-1} \left[\frac{pa_j}{m}\right]! \left(p - 1 - \left[\frac{pa_j}{m}\right]\right)!\right)^{f/2\ell}$$

$$\equiv \left(\prod_{j=0}^{\ell-1} (-1)^{\left[\frac{pa_j}{m}\right]+1}\right)^{f/2\ell} \pmod{p}$$

$$\equiv (-1)^{f/2\ell\left(\sum_{j=0}^{\ell-1} \left[\frac{pa_j}{m}\right]+\ell\right)} \pmod{p},$$

that is

$$\prod_{k=0}^{f-1} \left[\frac{pa_k}{m}\right]! \equiv (-1)^{f/2\ell \sum_{j=0}^{\ell-1}\left[\frac{pa_j}{m}\right]+f/2} \pmod{p}. \tag{2.13}$$

Clearly we have

$$a_k = p^k - m[p^k/m] \quad (k = 0,1,2,\ldots)$$

so that

$$\left[\frac{pa_k}{m}\right] = \left[\frac{p^{k+1}}{m} - p[p^k/m]\right]$$

$$= \left[\frac{p^{k+1}}{m}\right] - p\left[\frac{p^k}{m}\right]$$

$$\equiv \left[\frac{p^{k+1}}{m}\right] - \left[\frac{p^{k}}{m}\right] \pmod 2,$$

and thus

$$\sum_{k=0}^{\ell-1} \left[\frac{p\,a_k}{m}\right] \equiv \left[\frac{p^{\ell}}{m}\right] \pmod 2,$$

that is

$$\sum_{k=0}^{\ell-1} \left[\frac{p\,a_k}{m}\right] \equiv \frac{p^{\ell} - (m-1)}{m} \pmod 2. \tag{2.14}$$

From (2.13) and (2.14), we obtain

$$\prod_{k=0}^{f-1} \left[\frac{p\,a_k}{m}\right]! \equiv (-1)^{(f/2\ell)\left(\frac{p^{\ell}-(m-1)}{m}\right)+f/2} \pmod p. \tag{2.15}$$

Next, with the notation of (2.3), we have $A_0 = 0$ and

$$\begin{aligned} mB_0 &= \sum_{k=0}^{f-1} a_k \\ &= \sum_{i=1}^{2^{r+1}s} \sum_{j=0}^{\ell-1} a_{(i-1)\ell+j} \\ &= \sum_{\substack{i=1 \\ i \text{ odd}}}^{2^{r+1}s} \sum_{j=0}^{\ell-1} a_j + \sum_{\substack{i=1 \\ i \text{ even}}}^{2^{r+1}s} \sum_{j=0}^{\ell-1} (m-a_j) \\ &= 2^r s \sum_{j=0}^{\ell-1} a_j + 2^r s \sum_{j=0}^{\ell-1} (m-a_j) \\ &= 2^r sm\ell, \end{aligned}$$

so that

$$B_0 = 2^r s\ell = f/2. \tag{2.16}$$

Hence, by Stickelberger's congruence (2.4), we have

$$E_q(w_m) \equiv (-1)^{(f/2\ell)\left(\frac{p^\ell-(m-1)}{m}\right)} p^{f/2-1} \pmod{p^{f/2}}. \tag{2.17}$$

From (2.11) and (2.17), we deduce that

$$\theta = (-1)^{(f/2\ell)\left(\frac{p^\ell-(m-1)}{m}\right)},$$

so that

$$E_q(w_m) = (-1)^{(f/2\ell)\left(\frac{p^\ell-(m-1)}{m}\right)} p^{f/2-1}.$$

This completes the proof of Theorem C.

We conclude this section with two lemmas which we will need later.

Lemma 1. *For* $k = 0,1,2,\ldots,m-1$ *we have*

$$\sum_{\substack{\alpha \in F_q \\ tr(\alpha)=1}} \alpha^{k(q-1)/m} = 0, \quad \text{if} \quad m \Big| \frac{q-1}{p-1}.$$

Proof. Let

$$F_q^o = \{\beta \in F_q \mid tr(\beta) = 0\}.$$

It is easily checked that F_q^o is a $(f-1)$–dimensional subspace of the vector space F_q over F_p. We let $\beta_1,\ldots,\beta_{f-1}$ be a basis for F_q^o over F_p, and let α_1 be a fixed element of F_q with $tr(\alpha_1) = 1$. Let α be any element of F_q with $tr(\alpha) = 1$. Then we have $tr(\alpha - \alpha_1) = 0$, and so $\alpha - \alpha_1 \in F_q^o$, and thus $\alpha = \alpha_1 + \beta$, for some $\beta \in F_q^o$. Hence every element of F_q having trace 1 is given uniquely by

$$\alpha = \alpha_1 + b_1\beta_1 + \ldots + b_{f-1}\beta_{f-1},$$

where $b_1,b_2,\ldots,b_{f-1} \in F_p$. Then we have, for $k = 0,1,2,\ldots,m-1$, by the Multinomial theorem,

$$\sum_{\substack{\alpha \in F_q \\ tr(\alpha)=1}} \alpha^{k(q-1)/m}$$

$$= \sum_{b_1,\ldots,b_{f-1}\epsilon F_p} (\alpha_1 + b_1\beta_1 + \ldots + b_{f-1}\beta_{f-1})^{k(q-1)/m}$$

$$= \sum_{b_1,\ldots,\, b_{f-1}\epsilon F_p} \sum_{n_0+\ldots+n_{f-1}=k(q-1)/m} \binom{k(q-1)/m}{n_0,n_1,\ldots,n_{f-1}} \alpha_1^{n_0}(b_1\beta_1)^{n_1} \ldots (b_{f-1}\beta_{f-1})^{n_{f-1}}$$

$$= \sum_{n_0+\ldots+n_{f-1}=k(q-1)/m} \binom{k(q-1)/m}{n_0,n_1,\ldots,n_{f-1}} \alpha_1^{n_0}\beta_1^{n_1}\ldots\beta_{f-1}^{n_{f-1}} \prod_{i=1}^{f-1} \left(\sum_{b_i \in F_p} b_i^{n_i}\right)$$

$$= \sum_{\substack{n_0+\ldots+n_{f-1}=k(q-1)/m \\ p-1\,|\,n_1,\ \ldots,\ p-1\,|\,n_{f-1}}} \binom{k(q-1)/m}{n_0,n_1,\ldots,n_{f-1}} \alpha_1^{n_0}\beta_1^{n_1}\ldots\beta_{f-1}^{n_{f-1}}.$$

As $m \left| \frac{q-1}{p-1} \right.$ we have $p-1 \left| \frac{q-1}{m} \right.$, and so $p-1 \,|\, n_0$. Now Genocchi [9] has shown that

$$\binom{a_1 + a_2 + \ldots + a_r}{a_1, a_2, \ldots, a_r} \equiv 0 \pmod{p},$$

provided the nonnegative integers a_1, a_2, ..., a_r satisfy

$$p-1 \,|\, a_1, \ldots, p-1 \,|\, a_r\ , \quad a_1 + a_2 + \ldots + a_r < p^r - 1.$$

Thus we have

$$\binom{k(q-1)/m}{n_0, n_1, \ldots, n_{f-1}} \equiv 0 \pmod{p}$$

for

$$p-1 \,|\, n_0, \ldots, p-1 \,|\, n_{f-1}\ , \ n_0 + n_1 + \ldots + n_{f-1} = k(q-1)/m.$$

This completes the proof of Lemma 1.

Lemma 2. *Let h and k be integers such that*

$$h+k=\tfrac{1}{2}(p-1), \quad h\geq 0,\ k\geq 0.$$

Then we have

$$h!\equiv\frac{(-1)^k 2^{2k}k!\left(\frac{p-1}{2}\right)!}{(2k)!}\pmod{p}.$$

Proof. Modulo p we have

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! &\equiv 2^{p-1}\left(\frac{p-1}{2}\right)!\\
&\equiv \left(\frac{2}{p}\right)2\cdot 4\cdot 6\ldots(p-1)\\
&\equiv \left(\frac{2}{p}\right)2\cdot 4\ldots(2h)(2h+2)\ldots(p-1)\\
&\equiv \left(\frac{2}{p}\right)2^h h!\,(2h+2)\ldots(p-1)\\
&\equiv \left(\frac{2}{p}\right)2^h h!\,(-1)^{\frac{p-1}{2}-h}(p-(2h+2))\ldots(p-(p-1))\\
&\equiv \left(\frac{2}{p}\right)2^h h!\,(-1)^k(2k-1)(2k-3)\ldots 1\\
&\equiv \left(\frac{2}{p}\right)2^h h!\,(-1)^k\frac{(2k)!}{2^k k!}\\
&\equiv \left(\frac{2}{p}\right)2^{\frac{p-1}{2}}h!\,(-1)^k\frac{(2k)!}{2^{2k}k!}\\
&\equiv (-1)^k\frac{h!(2k)!}{2^{2k}k!},
\end{aligned}$$

completing the proof of Lemma 2.

3. Evaluation of Eisenstein sums: $m = 2$.

We prove the following theorem.

Theorem 1.

$$E_q(w_2) = \begin{cases} (-1)^{\frac{p-1}{2}\cdot\frac{f}{2}} \, p^{\frac{f}{2}-1}, & \text{if } f \equiv 0 \pmod 2, \\ (-1)^{\frac{p-1}{2}\cdot\frac{f-1}{2}} \, p^{\frac{f-1}{2}}, & \text{if } f \equiv 1 \pmod 2. \end{cases}$$

Proof. The theorem follows immediately from Corollary 1 (with $m = 2$) and the classical result

$$g_p(w_2) = i^{\left(\frac{p-1}{2}\right)^2} p^{1/2}, \tag{3.1}$$

see for example [17: p. 199]. We remark that for $f \equiv 0 \pmod 2$ the result also follows from Theorem C.

4. Evaluation of Eisenstein sums: $m = 3$

In this case the condition $m \mid p^f - 1$ holds if and only if

$$\begin{cases} \text{(a) } p \equiv 1 \pmod 3, & \text{or} \\ \text{(b) } p \equiv 2 \pmod 3, & f \equiv 0 \pmod 2. \end{cases} \tag{4.1}$$

Case (a): $p \equiv 1 \pmod 3$. By Corollary 1 with $m = 3$ we have

$$E_q(w_3) = \begin{cases} (-1)^{f-1} \, \dfrac{g_p(w_3)^f}{g_p(w_3^f)}, & \text{if } f \not\equiv 0 \pmod 3, \\ (-1)^f \, \dfrac{g_p(w_3)^f}{p}, & \text{if } f \equiv 0 \pmod 3. \end{cases} \tag{4.2}$$

As $p \equiv 1 \pmod 3$ there are integers L and M such that

$$4p = L^2 + 27M^2. \tag{4.3}$$

The positive integers $|L|$ and $|M|$ are determined uniquely by (4.3). We specify L uniquely by choosing between L and $-L$ so that

$$L \equiv -1 \pmod 3. \tag{4.4}$$

The two non–trivial cube roots of unity modulo p are $\frac{L+9M}{L-9M}$ and $\frac{L-9M}{L+9M}$. As $g^{\frac{p-1}{3}}$ is a non–trivial cube root of unity (mod p), we can distinguish between M and $-M$ by choosing M so that

$$g^{\frac{p-1}{3}} \equiv \frac{L+9M}{L-9M} \pmod p. \tag{4.5}$$

The integers L and M are uniquely determined by (4.3), (4.4) and (4.5). It is a classical result (see for example [10: pp. 443–444]) that

$$\begin{cases} J_p(w_3, w_3) &= -\frac{1}{2}(L + 3M\sqrt{-3}), \\ g_p(w_3)^3 &= -\frac{1}{2}(L+3M\sqrt{-3})\,p, \\ g_p(w_3^2)^3 &= -\frac{1}{2}(L-3M\sqrt{-3})\,p, \\ g_p(w_3)\,g_p(w_3^2) &= p. \end{cases} \tag{4.6}$$

Subcase (i): $f \equiv 0 \pmod 3$. From (4.2) and (4.6), we have

$$E_q(w_3) = (-1)^f g_p(w_3)^f / p = p^{f/3-1} \left(\frac{L + 3M\sqrt{-3}}{2}\right)^{f/3}.$$

Subcase (ii): $f \equiv 1 \pmod 3$. From (4.2) and (4.6), we have

$$E_q(w_3) = (-1)^{f-1} g_p(w_3)^{f-1} = p^{\frac{f-1}{3}} \left(\frac{L + 3M\sqrt{-3}}{2}\right)^{\frac{f-1}{3}}.$$

Subcase (iii): $f \equiv 2 \pmod 3$. From (4.2) and (4.6), we have

$$E_q(w_3) = (-1)^{f-1} \frac{g_p(w_3)^f}{g_p(w_3^2)}$$

$$= (-1)^{f-1} \frac{g_p(w_3)^{f+1}}{p}$$

$$= p^{\frac{f-2}{3}} \left(\frac{L + 3M\sqrt{-3}}{2}\right)^{\frac{f+1}{3}}.$$

Case (b): $p \equiv 2 \pmod 3$, $f \equiv 0 \pmod 2$. Taking $m = 3$ and $\ell = 1$ in Theorem C, we obtain

$$E_q(w_3) = (-1)^{\frac{f}{2}\cdot\frac{p-2}{3}} p^{f/2-1} = (-1)^{\frac{f}{2}} p^{\frac{f}{2}-1}.$$

This completes the proof of the following theorem.

Theorem 2. *(a) If* $p \equiv 1 \pmod 3$ *let* (L,M) *be the unique solution of*

$$4p = L^2 + 27M^2, \quad L \equiv -1 \pmod 3,$$

$$M \equiv \left(\frac{g^{\frac{p-1}{3}} - 1}{g^{\frac{p-1}{3}} + 1}\right) \frac{L}{9} \pmod p.$$

Then we have

$$E_q(w_3) = p^{\alpha}\left(\tfrac{1}{2}(L + 3M\sqrt{-3})\right)^{\beta},$$

where

$$\alpha = \begin{cases} f/3 - 1, & \text{if } f \equiv 0 \pmod 3, \\ (f-1)/3, & \text{if } f \equiv 1 \pmod 3, \\ (f-2)/3, & \text{if } f \equiv 2 \pmod 3, \end{cases}$$

$$\beta = \begin{cases} f/3, & \text{if } f \equiv 0 \pmod 3, \\ (f-1)/3, & \text{if } f \equiv 1 \pmod 3, \\ (f+1)/3, & \text{if } f \equiv 2 \pmod 3. \end{cases}$$

(b) If $p \equiv 2 \pmod 3$ *then we have*

$$E_q(w_3) = (-1)^{f/2} p^{f/2-1}.$$

For some numerical examples illustrating Theorem 2(a) see Tables 1–5 at the end of the paper.

5. Evaluation of Eisenstein sums: m = 4.

In this case the condition $m|p^f-1$ holds if and only if

$$\begin{cases}\text{(a)} & p \equiv 1 \pmod 4 \text{ or} \\ \text{(b)} & p \equiv 3 \pmod 4, \quad f \equiv 0 \pmod 2.\end{cases} \tag{5.1}$$

Case (a): $p \equiv 1 \pmod 4$. As $p \equiv 1 \pmod 4$ there are integers A and B such that

$$p = A^2 + B^2. \tag{5.2}$$

If A is chosen to be odd and B even, the relation (5.2) determines $|A|$ and $|B|$ uniquely. Replacing A by $-A$, if necessary, we may specify A uniquely by requiring

$$A \equiv 1 \pmod 4. \tag{5.3}$$

As $(\pm B/A)^4 \equiv 1 \pmod p$, $(\pm B/A)^2 \equiv -1$, we may choose between B and $-B$ by requiring

$$B/A \equiv g^{\frac{p-1}{4}} \pmod p. \tag{5.4}$$

Thus A and B are determined uniquely by (5.2), (5.3) and (5.4). With this normalization we have [10: p. 443]

$$\begin{cases} g_p(w_4)^2 = -(A+Bi)p^{1/2} \\ g_p(w_4^3)^2 = -(A-Bi)p^{1/2} \\ g_p(w_4)g_p(w_4^3) = (-1)^{(p-1)/4}\, p. \end{cases} \tag{5.5}$$

Next, by Corollary 1 (with $m = 4$), we have

$$E_q(w_4) = \begin{cases} (-1)^{f-1}\dfrac{g_p(w_4)^f}{g_p(w_4^f)}, & \text{if } f \not\equiv 0 \pmod 4, \\ \dfrac{g_p(w_4)^f}{p}, & \text{if } f \equiv 0 \pmod 4. \end{cases} \tag{5.6}$$

Subcase (i): $f \equiv 0 \pmod 4$. From (5.5) and (5.6), we have

$$E_q(w_4) = (-(A + Bi)p^{1/2})^{f/2}/p$$
$$= p^{\frac{f}{4}-1}(A + Bi)^{f/2}.$$

Subcase (ii): $f \equiv 1 \pmod 4$. From (5.5) and (5.6), we have

$$E_q(w_4) = g_p(w_4)^{f-1}$$
$$= (-(A + Bi)p^{1/2})^{\frac{f-1}{2}}$$
$$= p^{\frac{f-1}{4}}(A + Bi)^{\frac{f-1}{2}}.$$

Subcase (iii): $f \equiv 2 \pmod 4$. From (5.5), (5.6) and (3.1), we have

$$E_q(w_4) = (-1)\frac{g_p(w_4)^f}{g_p(w_2)}$$
$$= (-1)(-(A + Bi)p^{1/2})^{f/2}/p^{1/2}$$
$$= p^{\frac{f-2}{4}}(A + Bi)^{f/2}.$$

Subcase (iv): $f \equiv 3 \pmod 4$. From (5.5) and (5.6), we have

$$E_q(w_4) = \frac{g_p(w_4)^f}{g_p(w_4^3)}$$
$$= \frac{g_p(w_4)^{f+1}}{(-1)^{\frac{p-1}{4}}p}$$
$$= (-(A + Bi)p^{1/2})^{\frac{f+1}{2}}(-1)^{\frac{p-1}{4}}/p$$
$$= (-1)^{\frac{p-1}{4}}p^{\frac{f-3}{4}}(A + Bi)^{\frac{f+1}{2}}.$$

Case (b): $p \equiv 3 \pmod 4$, $f \equiv 0 \pmod 2$. Taking $m = 4$ and $\ell = 1$ in Theorem C, we obtain

$$E_q(w_4) = (-1)^{\frac{f}{2}\cdot\frac{p-3}{4}} p^{\frac{f}{2}-1}.$$

This completes the proof of the following theorem.

Theorem 3. *(a) If* $p \equiv 1 \pmod 4$ *let* (A,B) *be the unique solution of*

$$\begin{cases} p = A^2 + B^2, & A \equiv 1 \pmod 4, \\ B \equiv g^{\frac{p-1}{4}} A \pmod p. \end{cases}$$

Then we have

$$E_q(w_4) = \epsilon p^{\alpha}(A + Bi)^{\beta},$$

where

$$\alpha = \begin{cases} f/4 - 1, & \text{if } f \equiv 0 \pmod 4, \\ [f/4], & \text{if } f \not\equiv 0 \pmod 4, \end{cases}$$

$$\beta = \begin{cases} f/2, & \text{if } f \equiv 0 \pmod 2, \\ (f - (-1)^{\frac{f-1}{2}})/2, & \text{if } f \equiv 1 \pmod 2, \end{cases}$$

$$\epsilon = \begin{cases} 1, & \text{if } f \not\equiv 3 \pmod 4, \\ (-1)^{(p-1)/4}, & \text{if } f \equiv 3 \pmod 4. \end{cases}$$

(b) If $p \equiv 3 \pmod 4$ *and* $f \equiv 0 \pmod 2$ *then we have*

$$E_q(w_4) = (-1)^{\frac{f}{2}\cdot\frac{p-3}{4}} p^{\frac{f}{2}-1}.$$

Some numerical examples illustrating Theorem 3(a) are given in Tables 6–10.

6. Evaluation of Eisenstein sums: $m = 5$

The condition $m \mid p^f - 1$ in this case holds if and only if

$$\begin{cases}\text{(a) } p \equiv 1 \pmod 5, & \text{or} \\ \text{(b) } p \equiv 2,3 \pmod 5, & f \equiv 0 \pmod 4, \text{ or} \\ \text{(c) } p \equiv 4 \pmod 5, & f \equiv 0 \pmod 2. \end{cases} \tag{6.1}$$

Case (a): $p \equiv 1 \pmod 5$. As $p \equiv 1 \pmod 5$ there are integers x,u,v,w, (see [5]) such that

$$\begin{cases} 16p = x^2 + 50u^2 + 50v^2 + 125w^2, \\ xw = v^2 - 4uv - u^2. \end{cases} \tag{6.2}$$

If (x,u,v,w) is a solution of (6.2), all solutions are given by

$$\pm(x,u,v,w),\ \pm(x,-v,u,-w),\ \pm(x,-u,-v,w),\ \pm(x,v,-u,-w). \tag{6.3}$$

Thus the diophantine equation system (6.2) determines $|x|$ uniquely. We distinguish between x and $-x$ by choosing

$$x \equiv 1 \pmod 5. \tag{6.4}$$

Set

$$\begin{cases} R = R(x,w) = x^2 - 125w^2, \\ S = S(x,u,v,w) = 2xu - xv - 25vw, \\ e(x,u,v,w) \equiv \dfrac{R-10S}{R+10S} \pmod p. \end{cases} \tag{6.5}$$

Then (see for example [14: p. 72]) $e(x,u,v,w)$, $e(x,-v,u,-w) \equiv e(x,u,v,w)^2 \pmod p$, $e(x,v,-u,-w) \equiv e(x,u,v,w)^3 \pmod p$, $e(x,-u,-v,w) \equiv e(x,u,v,w)^4 \pmod p$ are the four primitive fifth roots of unity modulo p. Of the four solutions of (6.2) and (6.4), we choose (x,u,v,w) to be the one such that

$$g^{\frac{p-1}{5}} \equiv e(x,u,v,w) \pmod p. \tag{6.6}$$

Then (6.2), (6.4) and (6.6) determine x,u,v,w uniquely. For this solution we set

$$\tau(x,u,v,w) = \frac{1}{4}\left(x + (u+2v)\, i\sqrt{10+2\sqrt{5}} + (2u-v)\, i\sqrt{10-2\sqrt{5}} + 5w\sqrt{5}\right). \tag{6.7}$$

Then we have [14: Theorem 1]

$$\begin{cases} J_p(w_5,w_5) = J_p(w_5,w_5^3) = \tau(x,u,v,w), \\ J_p(w_5^2,w_5^2) = J_p(w_5,w_5^2) = \tau(x,v,-u,-w), \\ J_p(w_5^3,w_5^3) = J_p(w_5^3,w_5^4) = \tau(x,-v,u,-w), \\ J_p(w_5^4,w_5^4) = J_p(w_5^2,w_5^4) = \tau(x,-u,-v,w). \end{cases} \tag{6.8}$$

Now [12: Prop. 8.3.3]

$$g_p(w_5)^5 = pJ_p(w_5,w_5)J_p(w_5,w_5^2)J_p(w_5,w_5^3), \tag{6.9}$$

so that

$$\begin{cases} g_p(w_5)^5 = p\tau(x,u,v,w)^2\tau(x,v,-u,-w), \\ g_p(w_5^2)^5 = p\tau(x,v,-u,-w)^2\tau(x,-u,-v,w), \\ g_p(w_5^3)^5 = p\tau(x,-v,u,-w)^2\tau(x,u,v,w), \\ g_p(w_5^4)^5 = p\tau(x,-u,-v,w)^2\tau(x,-v,u,-w). \end{cases} \tag{6.10}$$

Next, from (1.17), we have

$$g_p(w_5)g_p(w_5^4) = g_p(w_5^2)g_p(w_5^3) = p. \tag{6.11}$$

Appealing to Corollary 1, we obtain

$$E_q(w_5) = \begin{cases} (-1)^{f-1}\dfrac{g_p(w_5)^f}{g_p(w_5^f)}, & \text{if } f \not\equiv 0 \pmod 5, \\ (-1)^f\dfrac{g_p(w_5)^f}{p}, & \text{if } f \equiv 0 \pmod 5. \end{cases} \tag{6.12}$$

Subcase (i): $f \equiv 0 \pmod 5$. From (6.10) and (6.12), we obtain

$$\begin{aligned} E_q(w_5) &= (-1)^f\Big(p\tau(x,u,v,w)^2\tau(x,v,-u,-w)\Big)^{f/5}/p \\ &= (-1)^f p^{f/5-1}\tau(x,u,v,w)^{2f/5}\tau(x,v,-u,-w)^{f/5}. \end{aligned}$$

Subcase (ii): $f \equiv 1 \pmod 5$. From (6.10) and (6.12), we obtain

$$\begin{aligned} E_q(w_5) &= (-1)^{f-1} g_p(w_5)^{f-1} \\ &= (-1)^{f-1} \left(p\tau(x,u,v,w)^2 \tau(x,v,-u,-w) \right)^{\frac{f-1}{5}} \\ &= (-1)^{f-1} \; p^{\frac{f-1}{5}} \; \tau(x,u,v,w)^{\frac{2(f-1)}{5}} \tau(x,v,-u,-w)^{\frac{(f-1)}{5}}. \end{aligned}$$

Subcase (iii): $f \equiv 2 \pmod 5$. From (6.8), (6.10), (6.12) and (1.18), we obtain

$$\begin{aligned} E_q(w_5) &= (-1)^{f-1} \; \frac{g_p(w_5)^f}{g_p(w_5^2)} \\ &= (-1)^{f-1} g_p(w_5)^{f-2} \; \frac{g_p(w_5)^2}{g_p(w_5^2)} \\ &= (-1)^{f-1} \left(p\tau(x,u,v,w)^2 \tau(x,v,-u,-w) \right)^{\frac{f-2}{5}} J_p(w_5, w_5) \\ &= (-1)^{f-1} \; p^{\frac{f-2}{5}} \; \tau(x,u,v,w)^{\frac{2f+1}{5}} \tau(x,v,-u,-w)^{\frac{f-2}{5}}. \end{aligned}$$

Subcase (iv): $f \equiv 3 \pmod 5$. From (1.18), (6.8), (6.10) and (6.12), we obtain

$$\begin{aligned} E_q(w_5) &= (-1)^{f-1} \; \frac{g_p(w_5)^f}{g_p(w_5^3)} \\ &= (-1)^{f-1} g_p(w_5)^{f-3} \cdot \frac{g_p(w_5)^2}{g_p(w_5^2)} \cdot \frac{g_p(w_5)\, g_p(w_5^2)}{g_p(w_5^3)} \\ &= (-1)^{f-1} \left(g_p(w_5)^5 \right)^{\frac{f-3}{5}} J_p(w_5, w_5) J_p(w_5, w_5^2) \\ &= (-1)^{f-1} \left(p\tau(x,u,v,w)^2 \tau(x,v,-u,-w) \right)^{\frac{f-3}{5}} \tau(x,u,v,w)\tau(x,v,-u,-w) \\ &= (-1)^{f-1} \; p^{\frac{f-3}{5}} \tau(x,u,v,w)^{\frac{2f-1}{5}} \; \tau(x,v,-u,-w)^{\frac{f+2}{5}}. \end{aligned}$$

Subcase (v): $f \equiv 4 \pmod 5$. From (6.10) and (6.12), we obtain

$$\begin{aligned} E_q(w_5) &= (-1)^{f-1}\,\frac{g_p(w_5)^f}{g_p(w_5^4)} \\ &= (-1)^{f-1}\,\frac{g_p(w_5)^{f+1}}{p} \\ &= (-1)^{f-1}\left(p\tau(x,u,v,w)^2\tau(x,v,-u,-w)\right)^{\frac{f+1}{5}}/p \\ &= (-1)^{f-1}\,p^{\frac{f-4}{5}}(\tau(x,u,v,w))^{\frac{2f+2}{5}}\,\tau(x,v,-u,-w)^{\frac{f+1}{5}}. \end{aligned}$$

Case (b): $p \equiv 2$ or $3 \pmod 5$, $f \equiv 0 \pmod 4$. Taking $m = 5$ and $\ell = 2$ in Theorem C, we obtain

$$E_q(w_5) = (-1)^{f/4\left(\frac{p^2-4}{5}\right)}p^{f/2-1} = (-1)^{f/4}\,p^{f/2-1}.$$

Case (c): $p \equiv 4 \pmod 5$, $f \equiv 0 \pmod 2$. Taking $m = 5$ and $\ell = 1$ in Theorem C, we obtain

$$E_q(w_5) = (-1)^{f/2\left(\frac{p-4}{5}\right)}p^{f/2-1} = (-1)^{f/2}\,p^{f/2-1}.$$

This completes the proof of the following theorem.

Theorem 4. *(a) If $p \equiv 1 \pmod 5$, let (x,u,v,w) be the unique solution of*

$$\begin{cases} 16p = x^2 + 50u^2 + 50v^2 + 125w^2, \\ xw = v^2 - 4uv - u^2, \\ x \equiv 1 \pmod 5, \\ \dfrac{(x^2-125w^2) - 10(2xu-xv-25vw)}{(x^2-125w^2) + 10(2xu-xv-25vw)} \equiv g^{\frac{p-1}{5}} \pmod p. \end{cases}$$

Set

$$\tau(x,u,v,w) = \frac{1}{4}\left(x + (u+2v)\,i\sqrt{10+2\sqrt{5}} + (2u-v)\,i\sqrt{10-2\sqrt{5}} + 5w\sqrt{5}\right).$$

Then we have

$$E_q(w_5) = \epsilon p^{\alpha} \tau(x,u,v,w)^{\beta} \tau(x,v,-u,-w)^{\delta},$$

where

$$\alpha = \begin{cases} f/5-1, & \text{if } f \equiv 0 \pmod 5, \\ [f/5], & \text{if } f \not\equiv 0 \pmod 5, \end{cases}$$

$$\beta = \begin{cases} [2f/5], & \text{if } f \equiv 0,1,3 \pmod 5, \\ [2f/5]+1, & \text{if } f \equiv 2,4 \pmod 5, \end{cases}$$

$$\delta = \begin{cases} [f/5], & \text{if } f \equiv 0,1,2 \pmod 5, \\ [f/5]+1, & \text{if } f \equiv 3,4 \pmod 5, \end{cases}$$

$$\epsilon = \begin{cases} (-1)^{f}, & \text{if } f \equiv 0 \pmod 5, \\ (-1)^{f-1}, & \text{if } f \not\equiv 0 \pmod 5. \end{cases}$$

(b) If $p \equiv 2$ *or* $3 \pmod 5$ *and* $f \equiv 0 \pmod 4$ *then we have*

$$E_q(w_5) = (-1)^{f/4} p^{f/2-1}.$$

(c) If $p \equiv 4 \pmod 5$ *and* $f \equiv 0 \pmod 2$ *then we have*

$$E_q(w_5) = (-1)^{f/2} p^{f/2-1}.$$

For some numerical examples illustrating Theorem 4(a) see Tables 11–15.

7. Evaluation of Eisenstein sums: $m = 6$.

The condition $m \mid p^f - 1$ in this case holds if and only if

$$\begin{cases} \text{(a) } p \equiv 1 \pmod 6, & \text{or} \\ \text{(b) } p \equiv 5 \pmod 6, & f \equiv 0 \pmod 2. \end{cases} \tag{7.1}$$

Case (a): $p \equiv 1 \pmod 6$. As $p \equiv 1 \pmod 6$ we may determine L and M uniquely (as in §4) by (4.3), (4.4) and (4.5). By Jacobi's theorem [13: p. 167] (see also [5: p. 407]) we have

$$\begin{cases} w_3^{\operatorname{ind} g(2)} g_p(w_6) g_p(w_3^2) = g_p(w_3) g_3(w_2), \\ w_3^{2 \operatorname{ind} g(2)} g_p(w_6^5) g_p(w_3) = g_p(w_3^2) g_p(w_2), \end{cases} \tag{7.2}$$

so that (by 3.1))

$$\begin{cases} g_p(w_6) = w_3^{2\,\mathrm{ind}_g(2)}\, i^{\left(\frac{p-1}{2}\right)^2} p^{1/2} g_p(w_3)/g_p(w_3^2), \\ g_p(w_6^5) = w_3^{\mathrm{ind}_g(2)}\, i^{\left(\frac{p-1}{2}\right)^2} p^{1/2} g_p(w_3^2)/g_p(w_3). \end{cases} \tag{7.3}$$

By (1.17) or (7.3) we have

$$g_p(w_6) g_p(w_6^5) = (-1)^{\frac{p-1}{2}}\, p. \tag{7.4}$$

Thus we have

$$\begin{aligned} J_p(w_6, w_6) &= (g_p(w_6)^2/g_p(w_3) \quad \text{(by (1.18))} \\ &= w_3^{\mathrm{ind}_g(2)} (-1)^{\frac{p-1}{2}}\, p\, g_p(w_3)/(g_p(w_3^2))^2 \quad \text{(by (7.3))} \\ &= w_3^{\mathrm{ind}_g(2)} (-1)^{\frac{p-1}{2}} g_p(w_3)^2/g_p(w_3^2) \quad \text{(by (4.6))} \\ &= (-1)^{\frac{p-1}{2}}\, w_3^{\mathrm{ind}_g(2)} J_p(w_3, w_3) \quad \text{(by (1.18))}, \end{aligned}$$

that is (by (4.6)),

$$J_p(w_6, w_6) = (-1)^{\frac{p+1}{2}}\, w_3^{\mathrm{ind}_g(2)} \left(\frac{L + 3M\sqrt{-3}}{2}\right). \tag{7.5}$$

Cubing the first equation in (7.3), and appealing to (4.6), we obtain

$$g_p(w_6)^3 = i^{3\left(\frac{p-1}{2}\right)^2}\, p^{3/2}\, g_p(w_3)^6/p^3,$$

that is (by (4.6)),

$$g_p(w_6)^3 = (-1)^{\frac{p-1}{2}}\, i^{\left(\frac{p-1}{2}\right)^2} \left(\frac{1}{2}(L + 3M\sqrt{-3})\right)^2 p^{1/2}. \tag{7.6}$$

Squaring (7.7) we deduce that

$$g_p(w_6)^6 = (-1)^{\frac{p-1}{2}} \left(\frac{1}{2}(L + 3M\sqrt{-3})\right)^4 p. \tag{7.7}$$

Also, by Corollary 1, we have

$$E_q(w_6) = \begin{cases} (-1)^{f-1} g_p(w_6)^f / g_p(w_6^f), & \text{if } f \not\equiv 0 \pmod 6, \\ g_p(w_6)^f / p, & \text{if } f \equiv 0 \pmod 6. \end{cases} \tag{7.8}$$

Subcase (i): $f \equiv 0 \pmod 6$. From (7.7) and (7.8), we obtain

$$\begin{aligned} E_q(w_6) &= (g_p(w_6)^6)^{f/6}/p \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{f}{6}} \left(\frac{L+3M\sqrt{-3}}{2}\right)^{2f/3} p^{f/6-1}. \end{aligned}$$

Subcase (ii): $f \equiv 1 \pmod 6$. From (7.7) and (7.8), we obtain

$$\begin{aligned} E_q(w_6) &= g_p(w_6)^{f-1} \\ &= \left((-1)^{\frac{p-1}{2}}\left(\frac{L+3M\sqrt{-3}}{2}\right)^4 p\right)^{\frac{f-1}{6}} \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{f-1}{6}} p^{\frac{f-1}{6}} \left(\frac{L+3M\sqrt{-3}}{2}\right)^{\frac{2f-2}{3}}. \end{aligned}$$

Subcase (iii): $f \equiv 2 \pmod 6$. From (7.5), (7.7) and (7.8), we obtain

$$\begin{aligned} E_q(w_6) &= -\frac{g_p(w_g)^f}{g_p(w_6^2)} \\ &= -g_p(w_6)^{f-2} \frac{g_p(w_6)^2}{g_p(w_6^2)} \\ &= -\left\{(-1)^{\frac{p-1}{2}} \left(\frac{L+3M\sqrt{-3}}{2}\right)^4 p\right\}^{\frac{f-2}{6}} J_p(w_6, w_6) \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{f+4}{6}} w_3^{\operatorname{ind}_g(2)} p^{\frac{f-1}{6}} \left(\frac{L+3M\sqrt{-3}}{2}\right)^{\frac{2f-1}{3}}. \end{aligned}$$

Subcase (iv): $f \equiv 3 \pmod 6$. By (3.1), (7.6) and (7.8), we have

$$E_q(w_6) = \frac{g_p(w_6)^f}{g_p(w_2)}$$

$$= \left\{(-1)^{\frac{p-1}{2}} i^{(\frac{p-1}{2})^2}\left(\frac{L+3M\sqrt{-3}}{2}\right)^2 p^{1/2}\right\}^{f/3} / i^{(\frac{p-1}{2})^2} p^{1/2}$$

$$= (-1)^{\frac{p-1}{2}\cdot\frac{f+3}{6}}\, p^{\frac{f-3}{6}} \left(\frac{L+3M\sqrt{-3}}{2}\right)^{2f/3}.$$

Subcase (v): $f \equiv 4 \pmod 6$. Appealing to (1.18), (4.6), (7.5), (7.7), and (7.8), we obtain

$$\begin{aligned} \mathrm{E}_q(w_6) &= -\frac{g_p(w_6)^f}{g_p(w_6^4)} \\ &= -g_p(w_6)^{f-4}\left(\frac{g_p(w_6)^2}{g_p(w_6^2)}\right)^2 \frac{g_p(w_6^2)^2}{g_p(w_6^4)} \\ &= -g_p(w_6)^{f-4}\,(J_p(w_6,w_6))^2\, J_p(w_6^2,w_6^2) \\ &= -g_p(w_6)^{f-4}(J_p(w_6,w_6))^2\, J_p(w_3,w_3) \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{f-4}{6}}\, w_3^{2\mathrm{ind}\, g(2)}\, p^{\frac{f-4}{6}} \left(\frac{L+3M\sqrt{-3}}{2}\right)^{\frac{2f+1}{3}}. \end{aligned}$$

Subcase (vi): $f \equiv 5 \pmod 6$. By (7.4), (7.7) and (7.8), we have

$$\begin{aligned} E_q(w_6) &= \frac{g_p(w_6)^f}{g_p(w_6^5)} \\ &= g_p(w_6)^{f+1}/(-1)^{\frac{p-1}{2}}\, p \\ &= (-1)^{\frac{p-1}{2}\,\frac{f-5}{6}}\, p^{\frac{f-5}{6}} \left(\frac{L+3M\sqrt{-3}}{2}\right)^{\frac{2f+2}{3}}. \end{aligned}$$

Case (b): $p \equiv 5 \pmod 6$, $f \equiv 0 \pmod 2$. Taking $m = 6$ and $\ell = 1$ in Theorem C, we obtain

$$E_q(w_6) = (-1)^{\frac{f}{2}\cdot\frac{p-5}{6}}\, p^{f/2-1}.$$

This completes the proof of the following theorem.

Theorem 5. *(a) If* $p \equiv 1 \pmod 6$ *let* (L,M) *be the unique solution of*

$$\begin{cases} 4p = L^2 + 27M^2, \quad L \equiv -1 \pmod 3, \\ M \equiv \left[\dfrac{g^{\frac{p-1}{3}} - 1}{g^{\frac{p-1}{3}} + 1} \right] \dfrac{L}{9} \pmod p. \end{cases}$$

Then we have

$$E_q(w_6) = \epsilon p^{\alpha} \left(\frac{1}{2}(L + 3M\sqrt{-3}) \right)^{\beta},$$

where

$$\alpha = \begin{cases} f/6 - 1, & \text{if } f \equiv 0 \pmod 6 \\ [f/6], & \text{if } f \not\equiv 0 \pmod 6, \end{cases}$$

$$\beta = \begin{cases} 2f/3, & \text{if } f \equiv 0 \pmod 3, \\ (2f-2)/3, & \text{if } f \equiv 1 \pmod 6, \\ (2f-1)/3, & \text{if } f \equiv 2 \pmod 6, \\ (2f+1)/3, & \text{if } f \equiv 4 \pmod 6, \\ (2f+2)/3, & \text{if } f \equiv 5 \pmod 6, \end{cases}$$

$$\epsilon = \begin{cases} (-1)^{\left(\frac{p-1}{2}\right)[f/6]}, & \text{if } f \equiv 0,1,5 \pmod 6 \\ (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{f+3}{6}\right)}, & \text{if } f \equiv 3 \pmod 6, \\ (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{f+4}{6}\right)} w_3^{\operatorname{ind}_g(2)}, & \text{if } f \equiv 2 \pmod 6, \\ (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{f-4}{6}\right)} w_3^{2\operatorname{ind}_g(2)}, & \text{if } f \equiv 4 \pmod 6. \end{cases}$$

(b) If $p \equiv 5 \pmod 6$ *and* $f \equiv 0 \pmod 2$ *then we have*

$$E_q(w_6) = (-1)^{\frac{f}{2} \cdot \frac{p-5}{6}} p^{\frac{f}{2}-1}.$$

For some numerical examples illustrating Theorem 5(a) see Tables 16–19.

8. Evaluation of Eisenstein sums: $m = 7$

The condition $m|p^f-1$ in this case holds if and only if

$$\begin{array}{lll} \text{(a)} & p \equiv 1 \pmod 7, & \text{or} \\ \text{(b)} & p \equiv 2,4 \pmod 7, & f \equiv 0 \pmod 3, \text{ or} \\ \text{(c)} & p \equiv 3,5 \pmod 7, & f \equiv 0 \pmod 6, \text{ or} \\ \text{(d)} & p \equiv 6 \pmod 7, & f \equiv 0 \pmod 2. \end{array} \tag{8.1}$$

Case (a): p ≡ 1 (mod 7). This case can be handled similarly to Case (a) of §6. The appropriate diophantine system and Jacobi sums are given in [6]. The details are complicated and will be included in a sequel to this paper.

Case (b): $p \equiv 2,4 \pmod 7$, $f \equiv 0 \pmod 3$. As $p \equiv 2,4 \pmod 7$ there are integers G,H such that

$$p = G^2 + 7H^2. \tag{8.2}$$

If (G,H) is a solution of (8.2), all four solutions are given by $(\pm G,\pm H)$. We distinguish between G and $-G$ by requiring

$$G \equiv \begin{cases} 4 \pmod 7, & \text{if } p \equiv 2 \pmod 7, \\ 2 \pmod 7, & \text{if } p \equiv 4 \pmod 7. \end{cases} \tag{8.3}$$

Next we determine a unique solution $S \pmod p$ of

$$S^2 \equiv -7 \pmod p \tag{8.4}$$

by means of

$$S \equiv \gamma^{\left(\frac{q-1}{7}\right)} + \gamma^{2\left(\frac{q-1}{7}\right)} - \gamma^{3\left(\frac{q-1}{7}\right)} + \gamma^{4\left(\frac{q-1}{7}\right)} - \gamma^{5\left(\frac{q-1}{7}\right)} - \gamma^{6\left(\frac{q-1}{7}\right)} \pmod p. \tag{8.5}$$

Replacing S by $S+p$, if necessary, we can suppose that S is odd. As

$$H^2 \equiv -G^2/7 \equiv (SG/7)^2 \pmod p, \tag{8.6}$$

we can distinguish between H and $-H$ by choosing

$$H \equiv SG/7 \pmod p. \tag{8.7}$$

The pair of integers (G,H) is now uniquely determined by (8.2), (8.3) and (8.7).

As $p \equiv 2,4 \pmod 7$ the least positive integer ℓ such that $p^\ell \equiv 1 \pmod 7$ is $\ell = 3$. We first determine $E_{p^3}(w_7) = E_{p^3}(w_7, \gamma^{(q-1)/(p^3-1)})$. Appealing to Theorem A(a), we have

$$\begin{cases} E_{p^3}(w_7) = E_{p^3}(w_7^2) = E_{p^3}(w_7^4), \\ E_{p^3}(w_7^3) = E_{p^3}(w_7^5) = E_{p^3}(w_7^6). \end{cases} \tag{8.8}$$

Thus $E_{p^3}(w_7)$ is fixed under the automorphism $\sigma_2 : w_7 \longrightarrow w_7^2$. Hence $E_{p^3}(w_7)$ belongs to the field $Q(w_7 + w_7^2 + w_7^4) = Q(\sqrt{-7})$. As $E_{p^3}(w_7)$ is an algebraic integer, we must have $E_{p^3}(w_7) \in Z + Z\left(\frac{-1+\sqrt{-7}}{2}\right)$ (the ring of integers of $Q(\sqrt{-7})$, which is a unique factorization domain). By (2.4), for some prime $\pi \in Z + Z\left(\frac{-1+\sqrt{-7}}{2}\right)$ dividing p, we have

$$E_{p^3}(w_7) \equiv -p\left(\left[\frac{p}{7}\right]!\left[\frac{2p}{7}\right]!\left[\frac{4p}{7}\right]!\right) \pmod{\pi^2}. \tag{8.9}$$

As $p = \pi\bar{\pi}$, from (8.2) we see that $\pi = \theta(G \pm H\sqrt{-7})$ for some unit θ of $Z + Z\left(\frac{-1+\sqrt{-7}}{2}\right)$, that is $\theta = \pm 1$. Replacing π by $-\pi$, if necessary, we may suppose that

$$\pi = G + H_1\sqrt{-7}, \quad \text{where } H_1 = \pm H. \tag{8.10}$$

Next, for $p \equiv 2 \pmod 7$, we have

$$\begin{aligned} &\left[\frac{p}{7}\right]!\left[\frac{2p}{7}\right]!\left[\frac{4p}{7}\right]! \\ &\equiv \left(\frac{p-2}{7}\right)!\left(\frac{2p-4}{7}\right)!\left(\frac{4p-1}{7}\right)! \pmod p \\ &\equiv \frac{\left(\frac{p-2}{7}\right)!\left(\frac{2p-4}{7}\right)!}{\left(\frac{3p-6}{7}\right)!} \pmod p \quad \text{(by Wilson's theorem)} \end{aligned}$$

$$\equiv \begin{bmatrix} \frac{3p-6}{7} \\ \frac{p-2}{7} \end{bmatrix}^{-1} \pmod{p}$$

$$\equiv -1/2G \pmod{p} \qquad ([7: \text{p. } 126])$$

and, for $p \equiv 4 \pmod 7$, we have

$$\left[\frac{p}{7}\right]!\left[\frac{2p}{7}\right]!\left[\frac{4p}{7}\right]!$$

$$\equiv \left(\frac{p-4}{7}\right)!\left(\frac{2p-1}{7}\right)!\left(\frac{4p-2}{7}\right)! \pmod{p}$$

$$\equiv -\frac{\left(\frac{p-4}{7}\right)!\left(\frac{2p-1}{7}\right)!}{\left(\frac{3p-5}{7}\right)!} \pmod{p} \quad \text{(by Wilson's theorem)}$$

$$\equiv -\begin{bmatrix} \frac{3p-5}{7} \\ \frac{p-4}{7} \end{bmatrix}^{-1} \pmod{p}$$

$$\equiv -1/2G \pmod{p} \qquad ([7: \text{p. } 126]).$$

Hence we have

$$E_{\mathfrak{p}^3}(w_7) \equiv \pi\overline{\pi}/(2G) \pmod{\pi^2}. \tag{8.11}$$

From (8.11) we see that

$$E_{\mathfrak{p}^3}(w_7) = \lambda\pi, \tag{8.12}$$

where $\lambda(\epsilon Z + Z\left(\frac{-1+\sqrt{-7}}{2}\right))$ is not divisible by π. Mapping $w_7 \longrightarrow w_7^6$ in (8.12), we obtain

$$E_{\mathfrak{p}^3}(w_7^6) = \overline{\lambda}\,\overline{\pi}. \tag{8.13}$$

Now, by Theorem A(c), we have

$$E_{\mathfrak{p}^3}(w_7)E_{\mathfrak{p}^3}(w_7^6) = p, \tag{8.14}$$

so that

$$\lambda\overline{\lambda} = 1. \tag{8.15}$$

This shows that λ is a unit of $Z + Z\left(\frac{-1+\sqrt{-7}}{2}\right)$, thus

$$\lambda = \pm 1. \tag{8.16}$$

From (8.12) and (8.16) we obtain

$$E_{p^3}(w_7) = \pm\pi. \tag{8.17}$$

Appealing to (8.11) and (8.17), we deduce that the sign $\pm$ in (8.17) satisfies

$$\pm 1 \equiv \overline{\pi}/(2G) \equiv (\pi + \overline{\pi})/(2G) \equiv 2G/2G \equiv 1 \pmod{\pi}, \tag{8.18}$$

proving that the + sign holds in (8.17), that is

$$E_{p^3}(w_7) = \pi = G + H_1\sqrt{-7}. \tag{8.19}$$

The next step is to show that $H_1 = H$. As $p \equiv 2$ or $4 \pmod 7$, the cyclotomic polynomial

$$\phi_7(x) = \frac{x^7 - 1}{x - 1} = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$$

is congruent to the product of two distinct irreducible cubic polynomials modulo p, namely,

$$\phi_7(x) \equiv \phi_7^-(x)\phi_7^+(x), \tag{8.20}$$

where

$$\phi_7^-(x) = x^3 + \left(\frac{1-S}{2}\right)x^2 + \left(\frac{-1-S}{2}\right)x - 1, \tag{8.21}$$

$$\phi_7^+(x) = x^3 + \left(\frac{1+S}{2}\right)x^2 + \left(\frac{-1+S}{2}\right)x - 1. \tag{8.22}$$

Hence, by Kummer's theorem, the principal ideal $\langle p\rangle$ of the ring of integers D of $Q(w_7)$ factors into the product of two prime ideals, namely,

$$\langle p\rangle = P_1P_2\ , \tag{8.23}$$

where

$$\begin{cases} P_1 = \langle p, \phi_7^-(w_7)\rangle\ , \quad P_2 = \langle p, \phi_7^+(w_7)\rangle, \\ N(P_1) = N(P_2) = p^3. \end{cases} \tag{8.24}$$

Thus D/P_1 is a finite field with p^3 elements. Hence there exists an isomorphism $\theta : D/P_1 \longrightarrow F_{p^3}$. Let $\lambda : D/P_1$ be the canonical homomorphism defined by

$$\lambda(\alpha) = \alpha + P_1 \quad (\alpha \in D). \tag{8.25}$$

Set $\tau = \theta \circ \lambda$ so that τ is a homomorphism such that

$$\tau : D \xrightarrow{\text{onto}} F_{p^3} . \tag{8.26}$$

Clearly we have $\tau(w_7) \neq 0$, otherwise $\tau(\alpha) = 0$ for all $\alpha \in D = Zw_7 + Zw_7^2 + \ldots + Zw_7^6$. Similarly $\tau(w_7) \neq 1$, otherwise $\tau(D) \subseteq F_p$. Hence $\tau(w_7) \in F_{p^3}^* \backslash \{1\}$ and so, as $F_{p^3}^* = \langle \gamma_1 \rangle$, where $\gamma_1 = \gamma^{(q-1)/(p^3-1)}$, we have $\tau(w_7) = \gamma_1^{k_1}$ for some integer k_1 satisfying $1 \leq k_1 \leq p^3 - 2$. Then we have

$$\gamma_1^{7k_1} = \tau(w_7)^7 = \tau(1) = \theta(\lambda(1)) = \theta(1 + P_1) = 1,$$

and so $(p^3 - 1) | 7k_1$, that is $\frac{p^3-1}{7} | k_1$, say $k_1 = \left(\frac{p^3-1}{7}\right)k$, where $1 \leq k \leq 6$, showing that

$$\tau(w_7) = \gamma_1^{k\left(\frac{p^3-1}{7}\right)}, \quad 1 \leq k \leq 6. \tag{8.27}$$

Next, as

$$\begin{aligned} & 2(w_7 + w_7^2 + w_7^4) + 1 - S \\ &= \left(\frac{(S^2+7)}{2p}(w_7 + w_7^2)\right)p + (2w_7 - 1 + S)\,\phi_7^{-}(w_7) \\ &\in \langle p, \phi_7^{-}(w_7) \rangle = P_1 , \end{aligned}$$

we have

$$\lambda(\sqrt{-7}) = \lambda(2(w_7 + w_7^2 + w_7^4) + 1) = (2(w_7 + w_7^2 + w_7^4) + 1) + P_1 = S + P_1 ,$$

and so

$$\tau(\sqrt{-7}) = \theta(S + P_1) = S. \tag{8.28}$$

But, from (8.27), we have

$$\begin{aligned}\tau(\sqrt{-7}) &= \tau(2(w_7 + w_7^2 + w_7^4) + 1)\\ &= 2\left(\gamma_1^{k\left(\frac{p^3-1}{7}\right)} + \gamma_1^{2k\left(\frac{p^3-1}{7}\right)} + \gamma_1^{4k\left(\frac{p^3-1}{7}\right)}\right) + 1\\ &= 2\left(\gamma^{k\left(\frac{q-1}{7}\right)} + \gamma^{2k\left(\frac{q-1}{7}\right)} + \gamma^{4k\left(\frac{q-1}{7}\right)}\right) + 1\\ &= \begin{Bmatrix} S, & \text{if } k = 1,2,4\\ -S, & \text{if } k = 3,5,6\end{Bmatrix} \qquad \text{(by (8.5))}.\end{aligned}$$

Hence we must have

$$\tau(w_7) = \gamma_1^{k\left(\frac{p^3-1}{7}\right)}, \quad k = 1,2,4. \tag{8.29}$$

Applying the homomorphism τ to (8.19), we obtain

$$\sum_{\substack{\alpha \in F^*_{p^3}\\ tr(\alpha)=1}} \gamma_1^{k\left(\frac{p^3-1}{7}\right)\mathrm{ind}_{\gamma_1}(\alpha)} \equiv G + H_1 S \pmod{p},$$

that is

$$\sum_{\substack{\alpha \in F^*_{p^3}\\ tr(\alpha)=1}} \alpha^{k\left(\frac{p^3-1}{7}\right)} \equiv G + H_1 S \pmod{p}. \tag{8.30}$$

But, by Lemma 1, the left hand side of (8.30) is $\equiv 0 \pmod{p}$, and, by (8.7), the right hand side is $\equiv G + H_1 7H/G \pmod{p}$. Thus we have

$$0 \equiv G^2 + 7HH_1 \pmod{p},$$

that is (as $G^2 \equiv -7H^2 \pmod{p}$) $H_1 \equiv H \pmod{p}$ and so $H_1 = H$ as asserted. Thus (8.19) becomes

$$E_{p^3}(w_7) = G + H\sqrt{-7}. \tag{8.31}$$

Finally, by Theorem B, we obtain

$$E_q(w_7) = p^{f/3-1}(E_{p^3}(w_7))^{f/3} = p^{f/3-1}(G + H\sqrt{-7})^{f/3}.$$

Case (c): $p \equiv 3,5 \pmod 7$, $f \equiv 0 \pmod 6$. In this case $\ell = 3$ is the least positive integer such that $p^\ell \equiv -1 \pmod 7$. Hence, by Theorem C, we have, as $f \equiv 0 \pmod 6$,

$$E_q(w_7) = (-1)^{f/6\left(\frac{p^3-6}{7}\right)}p^{f/2-1} = (-1)^{f/2}\ p^{f/2-1}.$$

Case (d): $p \equiv 6 \pmod 7$, $f \equiv 0 \pmod 2$. In this case $\ell = 1$ is the least positive integer such that $p^\ell \equiv -1 \pmod 7$. Hence, by Theorem C, we have as $f \equiv 0 \pmod 2$,

$$E_q(w_7) = (-1)^{f/2\left(\frac{p-6}{7}\right)}p^{f/2-1} = (-1)^{f/2}\ p^{f/2-1}.$$

This completes the proof of the following theorem.

Theorem 6. *(a) If* $p \equiv 2,4 \pmod 7$ *and* $f \equiv 0 \pmod 3$ *let* (G,H) *be the unique solution of*

$$\begin{cases} p = G^2 + 7H^2, \\ G \equiv \begin{cases} 4 \pmod 7, & \text{if } p \equiv 2 \pmod 7, \\ 2 \pmod 7, & \text{if } p \equiv 4 \pmod 7, \end{cases} \\ H \equiv \left(\sum_{k=1}^{6} \left(\frac{k}{7}\right)\gamma^{k\left(\frac{q-1}{7}\right)}\right) G/7 \pmod p. \end{cases}$$

Then we have

$$E_q(w_7) = p^{f/3-1}(G + H\sqrt{-7})^{f/3}.$$

(b) If $p \equiv 3,5 \pmod 7$ *and* $f \equiv 0 \pmod 6$, *or* $p \equiv 6 \pmod 7$ *and* $f \equiv 0 \pmod 2$, *then we have*

$$E_q(w_7) = (-1)^{f/2}\ p^{f/2-1}.$$

Some numerical examples illustrating Theorem 6(a) are given in Tables 20–21.

9. Evaluation of Eisenstein sums: $m = 8$

The condition $m \mid p^f - 1$ in this case holds if and only if

$$\begin{cases} \text{(a) } p \equiv 1 \pmod 8, & \text{or} \\ \text{(b) } p \equiv 3 \pmod 8, & f \equiv 0 \pmod 2, \text{ or} \\ \text{(c) } p \equiv 5 \pmod 8, & f \equiv 0 \pmod 2, \text{ or} \\ \text{(d) } p \equiv 7 \pmod 8, & f \equiv 0 \pmod 2. \end{cases} \tag{9.1}$$

Case (a): $p \equiv 1 \pmod 8$. As $p \equiv 1 \pmod 8$ we can define integers A, B, C, D uniquely as follows:

$$\begin{cases} p = A^2 + B^2, \\ A \equiv 1 \pmod 4, \quad B \equiv g^{\frac{p-1}{4}} A \pmod p, \end{cases} \tag{9.2}$$

and

$$\begin{cases} p = C^2 + 2D^2, \\ C \equiv 1 \pmod 4, \quad D \equiv \left(g^{\frac{p-1}{8}} + g^{\frac{3(p-1)}{8}}\right) C/2 \pmod p. \end{cases} \tag{9.3}$$

With this normalization, we show that

$$J_p(w_8, w_8^2) = (-1)^{\frac{p+7}{8}} i^{3\operatorname{ind}_g(2)}(A + Bi) \tag{9.4}$$

and

$$J_p(w_8, w_8) = -i^{3\operatorname{ind}_g(2)}(C + D\sqrt{-2}). \tag{9.5}$$

We first prove (9.4). We have

$$J_p(w_8, w_8^2) = \frac{g_p(w_8)\, g_p(w_8^2)}{g_p(w_8^3)} \quad \text{(by (1.18))}$$

$$= (-1)^{\frac{p-1}{8}} \frac{g_p(w_8)\, g_p(w_8^5)}{g_p(w_8^6)} \quad \text{(by (1.17))}$$

$$= (-1)^{\frac{p-1}{8}} w_8^{-2\operatorname{ind}_g(2)} \frac{g_p(w_8^2)\, g_p(w_8^4)}{g_p(w_8^6)} \quad \text{(by Jacobi's theorem [(13: p. 167)], [5: p. 407])}$$

$$= (-1)^{\frac{p-1}{8}} i^{3\mathrm{ind}_g(2)} \frac{g_p(w_4)\, g_p(w_2)}{g_p(w_4^3)}$$

$$= (-1)^{\frac{p-1}{8}} i^{3\mathrm{ind}_g(2)} \frac{g_p(w_4)^2 g_p(w_2)}{p} \quad \text{(by (1.17))}$$

$$= (-1)^{\frac{p-1}{8}} i^{3\mathrm{ind}_g(2)} \frac{(-1)(A+Bi)p^{1/2}\cdot p^{1/2}}{p} \quad \text{(by (3.1) and (5.5))}$$

$$= (-1)^{\frac{p+7}{8}} i^{3\mathrm{ind}_g(2)}(A+Bi),$$

completing the proof of (9.4).

Next we prove (9.5). We have

$$J_p(w_8,w_8) = \frac{g_p(w_8)^2}{g_p(w_4)} \quad \text{(by (1.18))}$$

$$= i^{3\mathrm{ind}_g(2)} \frac{g_p(w_8)\, g_p(w_8^4)}{g_p(w_8^5)} \quad \text{(by Jacobi's theorem [5] [13])}$$

$$= (-1)^{\frac{p-1}{8}} i^{3\mathrm{ind}_g(2)} \frac{g_p(w_8)\, g_p(w_8^3)}{g_p(w_8^4)} \quad \text{(by (1.17))},$$

that is

$$J_p(w_8,w_8) = (-1)^{\frac{p-1}{8}} i^{3\mathrm{ind}_g(2)}\, J_p(w_8,w_8^3) \quad \text{(by (1.18))}. \tag{9.6}$$

As

$$\sigma_3(J_p(w_8,w_8^3)) = J_p(w_8^3,w_8^9) = J_p(w_8,w_8^3),$$

we see that $J_p(w_8,w_8^3) \in Q(w_8+w_8^3) = Q(\sqrt{-2})$. Hence, as $J_p(w_8,w_8^3)$ is an algebraic integer, it must be an integer of $Q(\sqrt{-2})$, that is

$$J_p(w_8,w_8^3) \in Z + Z\sqrt{-2}.$$

The domain $Z + Z\sqrt{-2}$ is a unique factorization domain. Thus, in view of

$$J_p(w_8,w_8^3)J_p(w_8^7,w_8^5) = p = (C+D\sqrt{-2})\,(C-D\sqrt{-2}),$$

we must have

$$J_p(w_8, w_8^3) = \theta(C + D_1\sqrt{-2}), \tag{9.7}$$

where θ is a unit of $Z + Z\sqrt{-2}$, that is $\theta = \pm 1$, and $D_1 = \pm D$. Putting (9.6) and (9.7) together, we obtain

$$J_p(w_8, w_8) = (-1)^{\frac{p-1}{8}} i^{3\text{ind}_g(2)}\ \theta(C + D_1\sqrt{-2}). \tag{9.8}$$

We next show that $\theta = (-1)^{\frac{p+7}{8}}$. From (1.17), (1.18), and (9.7), we have

$$J_p(w_8, w_8^4) = (-1)^{\frac{p-1}{8}}\ J_p(w_8, w_8^3) = (-1)^{\frac{p-1}{8}}\ \theta(C + D_1\sqrt{-2}). \tag{9.9}$$

Further, in the ring R of integers of $Q(w_8)$ (R is a unique factorization domain), we have

$$\sum_{k=2}^{p-1} \left(w_8^{\text{ind}_g(k)} - 1\right)\left(w_8^{4\text{ind}_g(1-k)} - 1\right) \equiv 0 \pmod{2(w_8 - 1)}, \tag{9.10}$$

where $w_8 - 1$ is a prime such that

$$(w_8 - 1)(w_8^3 - 1) = -\sqrt{-2}, \quad (w_8 - 1)(w_8^5 - 1) = 1 - i,$$
$$(w_8 - 1)(w_8^7 - 1) = (\sqrt{2} - 1)\sqrt{2}, \quad (w_8 - 1)(w_8^3 - 1)(w_8^5 - 1)(w_8^7 - 1) = 2.$$

Expanding and summing the left hand side of (9.10), we obtain

$$J_p(w_8, w_8^4) \equiv -1 \pmod{2(w_8 - 1)}. \tag{9.11}$$

From (9.9) and (9.11), we obtain (as $C \equiv 1 \pmod 4$ and $D_1 \equiv 0 \pmod 2$)

$$(-1)^{\frac{p-1}{8}}\ \theta = -1 \pmod{2(w_8 - 1)},$$

proving that $\theta = (-1)^{\frac{p+7}{8}}$ as asserted. Hence (9.8) becomes

$$J_p(w_8, w_8) = -i^{3\text{ind}_g(2)}(C + D_1\sqrt{-2}). \tag{9.12}$$

The next step is to show that $D_1 = D$. As $p \equiv 1 \pmod 8$, the cyclotomic polynomial $\phi_8(x) = \frac{x^8 - 1}{x^4 - 1} = x^4 + 1$ is congruent to the product of four distinct linear polynomials modulo p, namely,

$$\phi_8(x) \equiv (x-g^{\frac{p-1}{8}})(x-g^{3(\frac{p-1}{8})})(x-g^{5(\frac{p-1}{8})})(x-g^{7(\frac{p-1}{8})}) \pmod{p}. \tag{9.13}$$

Hence, by Kummer's theorem, the principal ideal $\langle p\rangle$ of R is the product of four prime ideals, namely

$$\langle p\rangle = P_1P_3P_5P_7 , \tag{9.14}$$

where

$$P_k = \langle p,\ w_8 - g^{k(\frac{p-1}{8})}\rangle,\ N(P_k) = p,\quad k = 1,3,5,7. \tag{9.15}$$

Thus R/P_1 is a finite field with p elements. Hence there exists an isomorphism $\theta : R/P_1 \longrightarrow F_p$. Let $\lambda : R \longrightarrow R/P_1$ be the canonical homomorphism defined by $\lambda(\alpha) = \alpha + P_1 (\alpha \in R)$. Set $\tau = \theta \circ \lambda$ so that τ is a homomorphism such that $\tau : R \xrightarrow{\text{onto}} F_p$. Clearly $\tau(w_8) \neq 0$ otherwise $\tau(R) = \{0\}$. Hence $\tau(w_8) \in F_p^* = \langle g\rangle$ and so there exists an integer k_1 $(0 \leq k_1 \leq p-1)$ such that $\tau(w_8) = g_1^k$. Hence we have

$$g^{8k_1} = (\tau(w_8))^8 = \tau(1) = \theta(\lambda(1)) = \theta(1+P_1) \equiv 1 \pmod{p},$$

so that $(p-1)|8k$, that is, $k_1 = \left(\frac{p-1}{8}\right)k$, for some integer $k (0 \leq k \leq 7)$. Thus

$$\tau(w_8) \equiv g^{(\frac{p-1}{8})k} \pmod{p} \quad (0 \leq k \leq 7).$$

Next we have

$$\begin{aligned}
&\sqrt{-2} - \left(g^{\frac{p-1}{8}} + g^{3(\frac{p-1}{8})}\right) \\
&\quad = (w_8 + w_8^3) - \left(g^{\frac{p-1}{8}} + g^{3(\frac{p-1}{8})}\right) \\
&\quad = \left(w_8 - g^{\frac{p-1}{8}}\right)\left(1 + g^{\frac{p-1}{4}} + g^{\frac{p-1}{8}}\ w_8 + w_8^2\right) \\
&\quad \in P_1 ,
\end{aligned}$$

and so

$$\lambda(\sqrt{-2}) = \sqrt{-2} + P_1 = \left(g^{\frac{p-1}{8}} + g^{3(\frac{p-1}{8})}\right) + P_1 ,$$

giving

$$\tau(\sqrt{-2}) = \theta\left(g^{\frac{p-1}{8}} + g^{3\left(\frac{p-1}{8}\right)} + P_1\right) \equiv g^{\frac{p-1}{8}} + g^{3\left(\frac{p-1}{8}\right)} \pmod{p}.$$

But

$$\tau(\sqrt{-2}) = \tau(w_8 + w_8^3) \equiv g^{\left(\frac{p-1}{8}\right)k} + g^{3\left(\frac{p-1}{8}\right)k} \pmod{p},$$

proving that $k = 1$ or 3. Hence we have

$$\tau(w_8) \equiv g^{\left(\frac{p-1}{8}\right)k} \pmod{p}, \quad k = 1 \text{ or } 3.$$

Applying the homomorphism τ to (9.12), we obtain

$$\sum_{s=0}^{p-1} s^{k\left(\frac{p-1}{8}\right)} (1-s)^{k\left(\frac{p-1}{8}\right)} \equiv -2^{3\left(\frac{p-1}{4}\right)} \left(C + D_1\left(g^{\left(\frac{p-1}{8}\right)k} + g^{3\left(\frac{p-1}{8}\right)k}\right)\right) \pmod{p}$$

$$\equiv -2^{3\left(\frac{p-1}{4}\right)k}(C + D_1(2D/C)) \pmod{p} \qquad \text{(by 9.3)}.$$

By the Binomial theorem we have

$$\sum_{s=0}^{p-1} s^{k\left(\frac{p-1}{8}\right)}(1-s)^{k\left(\frac{p-1}{8}\right)} \equiv 0 \pmod{p},$$

as

$$\sum_{s=0}^{p-1} s^m \equiv \begin{cases} 0 \pmod{p}, & m = 1,2,\ldots,p-2, \\ -1 \pmod{p}, & m = p-1, \end{cases}$$

Hence we have $C^2 + 2DD_1 \equiv 0 \pmod{p}$, that is (as $C^2 \equiv -2D^2 \pmod{p}$) $D \equiv D_1 \pmod{p}$, so $D_1 = D$, as asserted. The result (9.5) now follows from (9.12).

From (1.18), (5.5) and (9.12) we obtain

$$\frac{g_p(w_8)^2}{g_p(w_4)} = -i^{3\operatorname{ind}_g(2)} (C + D\sqrt{-2}), \tag{9.16}$$

$$g_p(w_8)^4 = -(A + Bi)(C + D\sqrt{-2})^2 p^{1/2}. \tag{9.17}$$

Next, by Corollary 1, we have

$$E_q(w_8) = \begin{cases} (-1)^{f-1}\dfrac{g_p(w_8)^f}{g_p(w_8^f)}, & \text{if } f \not\equiv 0 \pmod 8, \\ \dfrac{g_p(w_8)^f}{p}, & \text{if } f \equiv 0 \pmod 8. \end{cases} \tag{9.18}$$

Subcase (i): $f \equiv 0 \pmod 8$. We have

$$\begin{aligned} E_q(w_8) &= (g_p(w_8)^4)^{f/4}/p \quad \text{(by (9.18))} \\ &= p^{f/8-1}(A+Bi)^{f/4}(C+D\sqrt{-2}))^{f/2} \quad \text{(by (9.17)).} \end{aligned}$$

Subcase (ii): $f \equiv 1 \pmod 8$. We have

$$\begin{aligned} E_q(w_8) &= g_p(w_8)^{f-1} \quad \text{(by (9.18))} \\ &= (-(A+Bi)(C+D\sqrt{-2})^2 p^{1/2})^{\frac{f-1}{4}} \quad \text{(by (9.17))} \\ &= p^{\frac{f-1}{8}}(A+Bi)^{\frac{f-1}{4}}(C+D\sqrt{-2})^{\frac{f-1}{2}}. \end{aligned}$$

Subcase (iii): $f \equiv 2 \pmod 8$. We have

$$\begin{aligned} E_q(w_8) &= -\frac{g_p(w_8)^f}{g_p(w_4)} \quad \text{(by (9.18))} \\ &= -g_p(w_8)^{f-2} J_p(w_8, w_8) \quad \text{(by (1.18))} \\ &= i^{3\text{ind}_g(2)} p^{\frac{f-2}{8}}(A+Bi)^{\frac{f-2}{4}}(C+D\sqrt{-2})^{f/2}, \end{aligned}$$

by (9.5) and (9.17).

Subcase (iv): $f \equiv 3 \pmod 8$. We have

$$\begin{aligned} E_q(w_8) &= \frac{g_p(w_8)^f}{g_p(w_8^3)} \quad \text{(by (9.18))} \\ &= g_p(w_8)^{f-3} J_p(w_8, w_8) J_p(w_8, w_8^2) \quad \text{(by (1.18))} \end{aligned}$$

$$= (-1)^{\frac{p-1}{8}}\, p^{\frac{f-3}{8}}\, (A+Bi)^{\frac{f+1}{4}}\, (C+D\sqrt{-2})^{\frac{f-1}{2}},$$

by (9.4), (9.5) and (9.17), as $\mathrm{ind}_g(2) \equiv 0 \pmod 2$.

Subcase (v): $f \equiv 4 \pmod 8$. We have

$$E_q(w_8) = (-1)\,\frac{g_p(w_8)^f}{g_p(w_2)} \quad \text{(by (9.18))}$$

$$= (-1)\,\frac{(g_p(w_8)^4)^{f/4}}{p^{1/2}} \quad \text{(by (3.1))}$$

$$= (-1)\,\frac{((-1)(A+Bi)(C+D\sqrt{-2})^2 p^{1/2})^{f/4}}{p^{1/2}} \quad \text{(by (9.17))}$$

$$= p^{\frac{f-4}{8}}\, (A+Bi)^{f/4} (C+D\sqrt{-2})^{f/2}.$$

Subcase (vi): $f \equiv 5 \pmod 8$. We have

$$E_q(w_8) = \frac{g_p(w_8)^f}{g_p(w_8^5)} \quad \text{(by (9.18))}$$

$$= (-1)^{\frac{p-1}{8}}\, g_p(w_8)^{f-5} \cdot \frac{g_p(w_8)^4}{g_p(w_4)^2} \cdot \frac{g_p(w_8)\, g_p(w_4)}{g_p(w_8^3)} \cdot \frac{g_p(w_8^3)^2}{g_p(w_8^6)} \quad \text{(by (1.17))}$$

$$= (-1)^{\frac{p-1}{8}}\, g_p(w_8)^{f-5} (J_p(w_8,w_8))^2 J_p(w_8,w_8^2) J_p(w_8^3,w_8^3) \quad \text{(by (1.18))}$$

$$= p^{\frac{f-5}{8}}\, (A+Bi)^{\frac{f-1}{4}}\, (C+D\sqrt{-2})^{\frac{f+1}{2}},$$

by (9.4), (9.5) and (9.17), as $\sigma_3\,(J_p(w_8,w_8)) = J_p(w_8^3,w_8^3)$.

Subcase (vii): $f \equiv 6 \pmod 8$. We have

$$E_q(w_8) = (-1)\,\frac{g_p(w_8)^f}{g_p(w_8^6)} \quad \text{(by (9.18))}$$

$$= (-1) g_p(w_8)^{f-6} (J_p(w_8,w_8))^3\; J_p(w_8^2,w_8^2) J_p(w_8^2,w_8^4) \quad \text{(by (1.18))}$$

$$= i^{\mathrm{ind}_g(2)}\, p^{\frac{f-6}{8}}\, (A+Bi)^{\frac{f+2}{4}}(C+D\sqrt{-2})^{f/2},$$

by (1.17), (3.1), (5.5), (9.5) and (9.17).

Subcase (viii): $f \equiv 7 \pmod 8$. We have

$$E_q(w_8) = \frac{g_p(w_8)^f}{g_p(w_8^7)} \quad \text{(by (9.18))}$$

$$= \frac{g_p(w_8)^{f+1}}{(-1)^{\frac{p-1}{8}}\, p} \quad \text{(by (1.17))}$$

$$= (-1)^{\frac{p-1}{8}}\, p^{\frac{f-7}{8}}\, (A+Bi)^{\frac{f+1}{4}}(C+D\sqrt{-2})^{\frac{f+1}{2}} \quad \text{(by (9.17))}.$$

Case (b): $p \equiv 3 \pmod 8$, $f \equiv 0 \pmod 2$. As $p \equiv 3 \pmod 8$ there are integers C and D such that

$$p = C^2 + 2D^2. \tag{9.19}$$

If (C,D) is a solution of (9.19), all (four) solutions are given by $(\pm C, \pm D)$. We distinguish between C and $-C$ by requiring

$$C \equiv 1 \pmod 4. \tag{9.20}$$

Next we determine a unique solution $K \pmod p$ of

$$K^2 \equiv -2 \pmod p \tag{9.21}$$

by means of

$$K \equiv \gamma^{\frac{q-1}{8}} + \gamma^{3\left(\frac{q-1}{8}\right)} \pmod p. \tag{9.22}$$

As

$$D^2 \equiv -C^2/2 \equiv (KC/2)^2 \pmod p,$$

we can distinguish between D and $-D$ by choosing

$$D \equiv KC/2 \pmod p. \tag{9.23}$$

The pair of integers (C,D) is uniquely determined by (9.19), (9.20) and (9.23).

As $p \equiv 3 \pmod 8$ the least positive integer ℓ such that $p^\ell \equiv 1 \pmod 8$ is $\ell = 2$. We first determine $E_{\mathfrak{p}_2}(w_8) = E_{\mathfrak{p}_2}(w_8, \gamma^{\frac{q-1}{p^2-1}})$. Appealing to Theorem A(a), we have

$$\begin{cases} E_{\mathfrak{p}_2}(w_8) = E_{\mathfrak{p}_2}(w_8^3), \\ E_{\mathfrak{p}_2}(w_8^5) = E_{\mathfrak{p}_2}(w_8^7), \end{cases} \tag{9.24}$$

showing that $E_{\mathfrak{p}_2}(w_8) \in Q(w_8 + w_8^2) = Q(\sqrt{-2})$. As $E_{\mathfrak{p}_2}(w_8)$ is an algebraic integer, we have $E_{\mathfrak{p}_2}(w_8) \in Z + Z\sqrt{-2}$ (the ring of integers of $Q(\sqrt{-2})$). $Z + Z\sqrt{-2}$ is a unique factorization domain. By Theorem A(d), for some prime $\pi \in Z + Z\sqrt{-2}$ dividing p, we have

$$E_{\mathfrak{p}_2}(w_8) \equiv p \frac{\left[\frac{p}{8}\right]! \left[\frac{3p}{8}\right]!}{\left[\frac{p}{2}\right]!} \pmod{\pi^2}. \tag{9.25}$$

As $p = \pi\bar{\pi}$, from (9.11) we see that $\pi = \pm C \pm D\sqrt{-2}$. Replacing π by $-\pi$, if necessary, we may suppose that

$$\pi = C + D_1\sqrt{-2}, \quad \text{where } D_1 = \pm D.$$

Now, as $p \equiv 3 \pmod 8$, we have

$$\begin{aligned} \frac{\left[\frac{p}{8}\right]! \left[\frac{3p}{8}\right]!}{\left[\frac{p}{2}\right]!} &\equiv \frac{\left(\frac{p-3}{8}\right)! \left(\frac{3p-1}{8}\right)!}{\left(\frac{p-1}{2}\right)!} \pmod p \\ &\equiv \begin{pmatrix} \frac{p-1}{2} \\ \frac{p-3}{8} \end{pmatrix}^{-1} \pmod p \\ &\equiv \frac{1}{2(-1)^{\frac{p+5}{8}} C} \pmod p, \end{aligned}$$

as

$$\begin{bmatrix} \frac{p-1}{2} \\ \frac{p-3}{8} \end{bmatrix} \equiv 2(-1)^{\frac{p+5}{8}} C \pmod{p}$$

[7: pp. 111–112].

Hence we have

$$E_{p^2}(w_8) \equiv \pi\overline{\pi}(-1)^{\frac{p+5}{8}}(2C)^{-1} \pmod{\pi^2}. \tag{9.26}$$

From (9.26) we see that

$$E_{p^2}(w_8) = \lambda\pi, \tag{9.27}$$

where $\lambda(\epsilon Z + Z\sqrt{-2})$ is not divisible by π. Mapping $w_8 \longrightarrow w_8^7$ in (9.27), we obtain

$$E_{p^2}(w_8^7) = \overline{\lambda}\,\overline{\pi}. \tag{9.28}$$

Now, by Theorem A(c), we have

$$E_{p^2}(w_8)E_{p^2}(w_8^7) = p, \tag{9.29}$$

so that (using (9.27) and (9.28)) $\lambda\overline{\lambda} = 1$. This shows that λ is a unit of $Z + Z\sqrt{-2}$, thus $\lambda = \pm 1$. From (9.26) and (9.27), we obtain

$$\begin{aligned} \lambda &\equiv \overline{\pi}(-1)^{\frac{p+5}{8}}(2C)^{-1} \pmod{\pi} \\ &\equiv (\pi + \overline{\pi})(-1)^{\frac{p+5}{8}}(2C)^{-1} \pmod{\pi} \\ &\equiv (2C)(-1)^{\frac{p+5}{8}}(2C)^{-1} \pmod{\pi} \\ &\equiv (-1)^{\frac{p+5}{8}} \pmod{\pi}, \end{aligned}$$

proving that $\lambda = (-1)^{\frac{p+5}{8}}$, that is

$$E_{p^2}(w_8) = (-1)^{\frac{p+5}{8}}\pi = (-1)^{\frac{p+5}{8}}(C + D_1\sqrt{-2}). \tag{9.30}$$

The next step is to show that $D_1 = D$. As $p \equiv 3 \pmod 8$ the cyclotomic polynomial

$$\phi_8(x) = \frac{x^8 - 1}{x^4 - 1} = x^4 + 1$$

is congruent to the product of two distinct irreducible quadratic polynomials modulo p, namely

$$\phi_8(x) \equiv \phi_8^-(x)\phi_8^+(x),$$

where

$$\phi_8^-(x) = x^2 - Kx - 1, \quad \phi_8^+(x) = x^2 + Kx - 1.$$

Hence, by Kummer's theorem, the principal ideal $\langle p \rangle$ of the ring R of integers of $Q(w_8)$ factors into the product of two prime ideals namely

$$\langle p \rangle = P_1 P_2,$$

where

$$P_1 = \langle p, \phi_8^-(w_8) \rangle, \quad P_2 = \langle p, \phi_8^+(w_8) \rangle, \quad N(P_1) = N(P_2) = p^2.$$

Thus R/P_1 is a finite field with p^2 elements. Hence there exists an isomorphism $\theta : R/P_1 \longrightarrow F_{p^2}$. Let $\lambda : R \longrightarrow R/P_1$ be the canonical homomorphism defined by

$$\lambda(\alpha) = \alpha + P_1 \quad (\alpha \in R).$$

Set $\tau = \theta \circ \lambda$ so that τ is a homomorphism such that

$$\tau : R \xrightarrow{\text{onto}} F_{p^2}.$$

Clearly we have $\tau(w_8) \neq 0$ otherwise $\tau(R) = \{0\}$. Also we have $\tau(w_8) \neq 1$, otherwise $\tau(R) \subseteq F_p$. Hence $\tau(w_8) \in F_{p^2}^*\backslash\{1\}$ and so, as $\gamma^{\frac{p^f-1}{p^2-1}}$ generates $F_{p^2}^*$, there exists an integer $k_1 (1 \leq k_1 \leq p^2 - 2)$ such that

$$\tau(w_8) = \gamma^{\left(\frac{p^f-1}{p^2-1}\right)k_1}.$$

Then we have

$$\gamma^{8\left(\frac{p^f-1}{p^2-1}\right)k_1} = (\tau(w_8))^8 = \tau(1) = \theta(\lambda(1)) = \theta(1 + P_1) \equiv 1 \pmod{p},$$

so that $p^f - 1 \mid 8\left(\frac{p^f-1}{p^2-1}\right)k_1$, that is $\frac{p^2-1}{8} \mid k_1$, say

$$k_1 = \left(\frac{p^2 - 1}{8}\right)k, \quad 1 \le k \le 7,$$

and so

$$\tau(w_8) = \gamma^{\left(\frac{p^f-1}{8}\right)k}, \quad 1 \le k \le 7.$$

Next we have (recall (9.22))

$$\sqrt{-2} - K = \left(\frac{(K^2+2)}{p}w_8\right)p + (K + w_8)\bar{\phi}_8(w_8) \in P_1 ,$$

and so

$$\lambda(\sqrt{-2}) = \sqrt{-2} + P_1 = K + P_1 ,$$

giving

$$\tau(\sqrt{-2}) = \theta(K + P_1) \equiv K \pmod{p}.$$

But

$$\begin{aligned}\tau(\sqrt{-2}) &= \tau(w_8 + w_8^3)\\ &= \gamma^{\left(\frac{q-1}{8}\right)k} + \gamma^{3\left(\frac{q-1}{8}\right)k}\\ &\equiv \begin{cases} K \pmod{p}, & \text{if } k = 1,3,\\ -K \pmod{p}, & \text{if } k = 5,7,\end{cases}\end{aligned}$$

proving that $k = 1$ or 3. Hence

$$\tau(w_8) = \gamma^{\left(\frac{q-1}{8}\right)k}, \quad k = 1 \text{ or } 3.$$

Applying the homomorphism τ to (9.30), we obtain

$$\sum_{\substack{\alpha \in F_{p^2}^* \\ tr(\alpha)=1}} \gamma^{k\left(\frac{q-1}{8}\right)\mathrm{ind}_{\gamma'}(\alpha)} \equiv (-1)^{\frac{p+5}{8}}(C + D_1K) \pmod{p},$$

where $\gamma' = \gamma^{(q-1)/(p^2-1)}$, that is

$$\sum_{\substack{\alpha \in F_{p^2}^* \\ tr(\alpha)=1}} \alpha^{k\left(\frac{p^2-1}{8}\right)} \equiv (-1)^{\frac{p+5}{8}}(C + D_1K) \pmod{p}. \tag{9.31}$$

By Lemma 1, the left hand side of (9.31) is congruent to 0 (mod p) and by (9.23) the right hand side is congruent to $(-1)^{\frac{p+5}{8}}(C + 2DD_1/C)$ (mod p). Hence we have $0 \equiv C^2 + 2DD_1 \pmod{p}$, that is (as $C^2 \equiv -2D^2 \pmod{p}$) $D_1 \equiv D \pmod{p}$, and so $D_1 = D$, as claimed. Hence we have from (9.30)

$$E_{\mathfrak{p}^2}(w_8) = (-1)^{\frac{p+5}{8}}(C + D\sqrt{-2}). \tag{9.32}$$

Next from Theorem B, we deduce

$$E_{\mathfrak{q}}(w_8) = \begin{cases} \dfrac{\left(g_{\mathfrak{p}^2}(w_8)\right)^{f/2}}{g_{\mathfrak{p}^2}(w_8^{f/2})}\,(E_{\mathfrak{p}^2}(w_8))^{f/2}, & \text{if } f \equiv 2 \pmod 4, \\ \dfrac{\left(g_{\mathfrak{p}^2}(w_8)\right)^{f/2}}{p}\,(E_{\mathfrak{p}^2}(w_8))^{f/2}, & \text{if } f \equiv 0 \pmod 4. \end{cases} \tag{9.33}$$

Finally, with $\gamma' = \gamma^{\frac{q-1}{p^2-1}}$, we have for n odd

$$\begin{aligned} g_{\mathfrak{p}^2}(w_8^n) &= \sum_{k \in F_p^*} w_8^{n\,\mathrm{ind}_{\gamma'}(k)} \exp(2\pi ik/p) \\ &= \sum_{k \in F_p^*} w_8^{n(p+1)\mathrm{ind}_g(k)} \exp(2\pi ik/p) \\ &= \sum_{k=1}^{p-1} (-1)^{\mathrm{ind}_g(k)} \exp(2\pi ik/p) \\ &= \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \exp(2\pi ik/p), \end{aligned}$$

that is, by (3.1) as $p \equiv 3 \pmod 4$,

$$g_{\mathfrak{p}^2}(w_8^n) = ip^{1/2}. \tag{9.34}$$

From (9.32), (9.33) and (9.34), we deduce

$$E_q(w_8) = \begin{cases} (-1)^{f/4}\ p^{f/4-1}(C + D\sqrt{-2})^{f/2}, & \text{if } f \equiv 0 \pmod 4, \\ (-1)^{\frac{f-2}{4}+\frac{p+5}{8}}\ p^{\frac{f-2}{4}}(C + D\sqrt{-2})^{f/2}, & \text{if } f \equiv 2 \pmod 4. \end{cases}$$

(c) $p \equiv 5 \pmod 8$, $f \equiv 0 \pmod 2$. As $p \equiv 5 \pmod 8$ we determine integers A and B as in Theorem 3, that is, by

$$\begin{cases} p = A^2 + B^2, & A \equiv 1 \pmod 4, \\ B \equiv g^{\frac{p-1}{4}} A \equiv \gamma^{\frac{q-1}{4}} A \pmod p. \end{cases} \tag{9.35}$$

Set $m = \operatorname{ind}_g(2)$. As $p \equiv 5 \pmod 8$ we have $m \equiv 1 \pmod 2$. Thus, as $(B/A)^2 \equiv -1 \pmod p$, we have

$$2^{\frac{p-1}{4}} \equiv (g^m)^{\frac{p-1}{4}} \equiv \left(g^{\frac{p-1}{4}}\right)^m \equiv (B/A)^m \pmod p,$$

that is

$$2^{\frac{p-1}{4}} \equiv (-1)^{\frac{m-1}{2}} B/A \pmod p. \tag{9.36}$$

Hence, from the work of Gauss [8] (see also [6], [11], [15], [20]), it follows that

$$B \equiv 2(-1)^{(m-1)/2} \pmod 8. \tag{9.37}$$

Before proceeding we prove a lemma we will need.

Lemma 3. $$\left[\begin{matrix} \frac{3p-7}{8} \\ \frac{p-5}{8} \end{matrix}\right] \equiv (-1)^{\frac{p+3}{8}+\frac{m-1}{2}} 2B \pmod p.$$

Proof. We have

$$\left[\begin{matrix} \frac{3p-7}{8} \\ \frac{p-5}{8} \end{matrix}\right] = \frac{\left(\frac{3p-7}{8}\right)!}{\left(\frac{p-5}{8}\right)!\left(\frac{p-1}{4}\right)!}$$

$$= \frac{\left(\frac{3p+1}{8}\right)!}{\left(\frac{p-5}{8}\right)!\left(\frac{p-1}{4}\right)!\left(\frac{3p+1}{8}\right)}$$

$$\equiv \frac{(-1)^{\frac{p-5}{8}}\, 2^{\frac{p-5}{4}} \left(\frac{p-1}{2}\right)!}{\left(\frac{p-5}{4}\right)!\left(\frac{p-1}{4}\right)!\left(\frac{3p+1}{8}\right)} \pmod{p} \text{ (by Lemma 2)}$$

$$\equiv (-1)^{\frac{p-5}{8}}\, 2^{\frac{p-1}{4}} \begin{bmatrix} \frac{p-1}{2} \\ \frac{p-1}{4} \end{bmatrix} \frac{\frac{p-1}{4}}{\frac{3p+1}{4}} \pmod{p}$$

$$\equiv (-1)^{\frac{p-5}{8}}(-1)^{\frac{m-1}{2}} \frac{B}{A} \cdot (2A)\cdot(-1) \pmod{p}$$

$$\equiv (-1)^{\frac{p+3}{8}+\frac{m-1}{2}}\, 2B \pmod{p},$$

where we have used Gauss's result $2A \equiv \binom{\frac{p-1}{2}}{\frac{p-1}{4}} \pmod{p}$. This completes the proof of Lemma 3.

The least positive integer ℓ such that $p^\ell \equiv 1 \pmod 8$ is $\ell = 2$, so we first determine $E_{p^2}(w_8) = E_{p^2}(w_8, \gamma^{\frac{q-1}{p-1}})$. Appealing to Theorem A(a) we have

$$E_{p^2}(w_8) = E_{p^2}(w_8^5), \quad E_{p^2}(w_8^3) = E_{p^2}(w_8^7).$$

Thus $E_{p^2}(w_8)$ is fixed under the automorphism $\sigma_5 : w_8 \longrightarrow w_8^5$. Hence $E_{p^2}(w_8)$ belongs to $Q(w_8^2) = Q(i)$. As $E_{p^2}(w_8)$ is an algebraic integer, we must have $E_{p^2}(w_8) \in Z + Zi$ (the ring of integers of $Q(i)$). $Z + Zi$ is a unique factorization domain. By Theorem A(c), we have

$$E_{p^2}(w_8)E_{p^2}(w_8^7) = p, \tag{9.38}$$

so that in view of (9.35) we must have

$$E_{p^2}(w_8) = \theta(A + B_1 i), \tag{9.39}$$

where θ is a unit of $Z + Zi$ (that is $\theta = \pm 1, \pm i$), and $B_1 = \pm B$.

We show first that $\theta = \pm i$. We have (setting $\gamma' = \gamma^{\frac{q-1}{p^2-1}}$)

$$\sum_{k=0}^{7} E_{p^2}(w_8^k) = \sum_{k=0}^{7} \sum_{\substack{\alpha \in F_{p^2}^* \\ tr(\alpha)=1}} w_8^{\mathrm{kind}_{\gamma'}(\alpha)}$$

$$= \sum_{\substack{\alpha \in F_{p^2}^* \\ tr(\alpha)=1}} \sum_{k=0}^{7} w_8^{\mathrm{kind}_{\gamma'}(\alpha)}$$

$$= 8 \sum_{\substack{\alpha \in F_{p^2}^* \\ tr(\alpha)=1 \\ \mathrm{ind}_{\gamma'}(\alpha) \equiv 0 \pmod 8}} 1$$

that is,

$$\sum_{k=0}^{7} E_{p^2}(w_8^k) \equiv 0 \pmod 8. \tag{9.40}$$

As

$$\begin{cases} E_{p^2}(1) = p \ (\S 1), E_{p^2}(w_8) = 1 & \text{(Theorem 1)}, \\ E_{p^2}(w_4) = A + Bi, \ E_{p^2}(w_4^3) = A - Bi, & \text{(Theorem 3(a))}, \end{cases} \tag{9.41}$$

we obtain from (9.40) and (9.41) (noting $p \equiv 5 \pmod 8$, $A \equiv 1 \pmod 4$)

$$Re(E_{p^2}(w_8)) \equiv 0 \pmod 2,$$

proving that $\theta = \pm i$. Thus we have

$$E_{p^2}(w_8) = \rho i(A + B_1 i), \quad B_1 = \pm B, \quad \rho = \pm 1. \tag{9.42}$$

Next we show that $\rho = (-1)^{(m-1)/2}(B_1/B)$. By Theorem A(d) we have

$$E_{p^2}(w_8) \equiv p \frac{\left[\frac{p}{8}\right]! \left[\frac{5p}{8}\right]!}{\left[\frac{3p}{4}\right]!} \pmod{\pi^2}, \tag{9.43}$$

where $\pi = A + B_1 i$. As $p \equiv 5 \pmod 8$, appealing to Wilson's theorem and Lemma 3, we obtain

$$\frac{\left[\frac{p}{8}\right]!\left[\frac{5p}{8}\right]!}{\left[\frac{3p}{4}\right]!} = \frac{\left(\frac{p-5}{8}\right)!\left(\frac{5p-1}{8}\right)!}{\left(\frac{3p-3}{4}\right)!}$$

$$\equiv (-1)^{\frac{p-5}{8}} \frac{\left(\frac{p-5}{8}\right)!\left(\frac{p-1}{4}\right)!}{\left(\frac{3p-7}{8}\right)!} \pmod p$$

$$\equiv (-1)^{\frac{p-5}{8}} \left[\begin{array}{c} \frac{3p-7}{8} \\ \frac{p-5}{8} \end{array}\right]^{-1} \pmod p$$

$$\equiv (-1)^{\frac{m+1}{2}}/2B \pmod p.$$

Hence we have from (9.43)

$$E_{p^2}(w_8) \equiv \pi\overline{\pi}(-1)^{\frac{m+1}{2}} (2B)^{-1} \pmod{\pi^2},$$

and so, appealing to (9.42), we obtain

$$\rho i \equiv \overline{\pi}(-1)^{\frac{m+1}{2}}(2B)^{-1} \pmod \pi$$

$$\equiv (\overline{\pi} - \pi)(-1)^{\frac{m+1}{2}}(2B)^{-1} \pmod \pi$$

$$\equiv (-2B_1 i)(-1)^{\frac{m+1}{2}}(2B)^{-1} \pmod \pi$$

$$\equiv (-1)^{\frac{m-1}{2}}(B_1/B)i \pmod \pi,$$

proving that $\rho = (-1)^{\frac{m-1}{2}}(B_1/B)$ as asserted. Thus we have shown that

$$E_{p^2}(w_8) = (-1)^{\frac{m-1}{2}}(B_1/B)\, i(A + B_1 i), \quad \text{where } B_1 = \pm B. \tag{9.44}$$

Next we show that $B_1 = B$. As $p \equiv 5 \pmod 8$ the cyclotomic polynomial $\phi_8(x) = \frac{x^8-1}{x^4-1} = x^4 + 1$ is congruent to the product of two distinct irreducible quadratic polynomials modulo p, namely

$$\phi_8(x) \equiv \phi_8^-(x)\phi_8^+(x),$$

where

$$\phi_8^-(x) = x^2 - g^{\frac{p-1}{4}}, \quad \phi_8^+(x) = x^2 + g^{\frac{p-1}{4}}.$$

Hence, by Kummer's theorem, the principal ideal $\langle p \rangle$ of the ring R of integers of $Q(w_8)$ factors into the product of two prime ideals, namely

$$\langle p \rangle = P_1 P_2 ,$$

where

$$P_1 = \langle p, \phi_8^-(w_8) \rangle, \quad P_2 = \langle p, \phi_8^+(w_8) \rangle, \quad N(P_1) = N(P_2) = p^2.$$

Thus R/P_1 is a finite field with p^2 elements. Hence there exists an isomorphism $\theta : R/P_1 \longrightarrow F_{p^2}$. Let $\lambda : R \longrightarrow R/P_1$ be the canonical homomorphism defined by $\lambda(\alpha) = \alpha + P_1 (\alpha \in R)$. Set $\tau = \theta \circ \lambda$ so that τ is a homomorphism such that $\tau : R \xrightarrow{\text{onto}} F_{p^2}$. Clearly we have $\tau(w_8) \neq 0$, otherwise $\tau(R) = \{0\}$. Also we have $\tau(w_8) \neq 1$, otherwise $\tau(R) \subseteq F_p$. Hence $\tau(w_8) \in F_{p^2}^* \backslash \{1\}$ and so, as $\gamma^{\frac{q-1}{p^2-1}}$ generates $F_{p^2}^*$, there exists an integer $k_1 (1 \leq k_1 \leq p^2 - 1)$ such that

$$\tau(w_8) = \gamma^{\left(\frac{p^f-1}{p^2-1}\right)k_1}.$$

Then we have

$$\gamma^{8\left(\frac{p^f-1}{p^2-1}\right)k_1} = (\tau(w_8))^8 = \tau(1) = \theta(\lambda(1)) = \theta(1 + P_1) \equiv 1 \pmod{p},$$

so that $p^f - 1 \mid 8\left(\frac{p^f-1}{p^2-1}\right)k_1$, that is $\frac{p^2-1}{8} \mid k_1$, say $k_1 = \left(\frac{p^2-1}{8}\right)k$, $1 \leq k \leq 7$, and so

$$\tau(w_8) = \gamma^{\left[\frac{p^f-1}{8}\right]k}, \quad 1 \leq k \leq 7.$$

Next we have

$$i - g^{\frac{p-1}{4}} = w_8^2 - g^{\frac{p-1}{4}} = \phi_8^-(w_8) \in P_1 ,$$

and so

$$\lambda(i) = i + P_1 = g^{\frac{p-1}{4}} + P_1 ,$$

giving

$$\tau(i) \equiv g^{\frac{p-1}{4}} \pmod{p}.$$

But

$$\tau(i) = \tau(w_8^2) = \gamma^{(\frac{q-1}{4})k} \equiv g^{(\frac{p-1}{4})k} \pmod{p},$$

showing that $k = 1$ or 5. Hence we have

$$\tau(w_8) = \gamma^{(\frac{q-1}{8})k} \quad (k = 1 \text{ or } 5).$$

Applying the homomorphism τ to (9.44) we obtain

$$\sum_{\substack{a \in F^*_{p^2} \\ tr(a)=1}} \gamma^{k(\frac{q-1}{8})\mathrm{ind}_{\gamma'}(a)} \equiv (-1)^{\frac{m-1}{2}} (B_1/B) g^{(\frac{p-1}{4})k}(A + B_1 g^{(\frac{p-1}{4})}) \pmod{p},$$

where $\gamma' = \gamma^{\frac{q-1}{p^2-1}}$, that is

$$\sum_{\substack{a \in F^*_{p^2} \\ tr(a)=1}} \alpha^{k(\frac{p^2-1}{8})} \equiv (-1)^{\frac{m-1}{2}} (B_1/B) g^{(\frac{p-1}{4})k}(A + B_1 g^{(\frac{p-1}{4})}) \pmod{p}.$$

By Lemma 1 the left hand side is 0 (mod p). Hence, as $g^{\frac{p-1}{4}} \equiv B/A \pmod{p}$, we obtain $A + (B_1 B/A) \equiv 0 \pmod{p}$, showing that $B_1 \equiv B \pmod{p}$ (as $A^2 \equiv -B^2 \pmod{p}$), and thus $B_1 = B$ as asserted. Hence we have

$$E_{p^2}(w_8) = (-1)^{\frac{m-1}{2}} i(A + Bi). \tag{9.45}$$

Next, appealing to Theorem B, we have

$$E_q(w_8) = \begin{cases} (-1)^{f/2-1} \dfrac{\left[g_{p^2}(w_8)\right]^{f/2}}{g_{p^2}(w_8^{f/2})} \, (E_{p^2}(w_8))^{f/2}, & \text{if } f \not\equiv 0 \pmod 8, \\ \dfrac{\left[g_{p^2}(w_8)\right]^{f/2}}{p} \, (E_{p^2}(w_8))^{f/2}, & \text{if } f \equiv 0 \pmod 8. \end{cases} \tag{9.46}$$

Finally with $\gamma' = \gamma^{(q-1)/(p^2-1)}$ we have for any integer n

$$\begin{aligned} g_{p^2}(w_8^n) &= \sum_{k \in F_p^*} w_8^{n \operatorname{ind}_{\gamma'}(k)} \exp(2\pi ik/p) \\ &= \sum_{k \in F_p^*} w_n^{n(p+1)\operatorname{ind}_g(k)} \exp(2\pi ik/p) \\ &= \sum_{k \in F_p^*} w_4^{3n \operatorname{ind}_g(k)} \exp(2\pi ik/p) \\ &= g_p(w_4^{3n}). \end{aligned}$$

This proves that the value of $g_{p^2}(w_8^n)$ only depends upon $n \pmod 4$ not $n \pmod 8$. Appealing to (3.1) and (5.5), we have

$$\begin{cases} (g_{p^2}(w_8^n))^2 = \begin{cases} -(A - Bi)p^{1/2}, & \text{if } n \equiv 1 \pmod 4, \\ -(A + Bi)p^{1/2}, & \text{if } n \equiv 3 \pmod 4. \end{cases} \\ g_{p^2}(w_4) = p^{1/2}, \quad \text{if } n \equiv 2 \pmod 4. \end{cases} \tag{9.47}$$

Putting (9.45), (9.46) and (9.47), together we obtain

$$E_q(w_8) = \begin{cases} p^{\frac{3f}{4}-1}(A + Bi)^{f/4}, & \text{if } f \equiv 0 \pmod 8, \\ (-1)^{\frac{\operatorname{ind}_g(2)-1}{2}} i p^{\frac{3f-6}{8}} (A + Bi)^{\frac{f+2}{4}}, & \text{if } f \equiv 2 \pmod 8, \\ -p^{(3f-4)/8}(A + Bi)^{f/4}, & \text{if } f \equiv 4 \pmod 8, \\ (-1)^{\frac{\operatorname{ind}_g(2)-1}{2}} i p^{\frac{3f-2}{8}} (A + Bi)^{(f-2)/4}, & \text{if } f \equiv 6 \pmod 8. \end{cases}$$

(d) $p \equiv 7 \pmod 8$, $f \equiv 0 \pmod 2$. By Theorem C, with $m = 8$ and $\ell = 1$, we have

$$E_q(w_8) = (-1)^{\frac{f}{2}\left(\frac{p-7}{8}\right)} p^{f/2-1}.$$

This completes the proof of the following theorem.

Theorem 7. *(a) If* $p \equiv 1 \pmod 8$, *let* A,B,C,D *be the unique integers given by*

$$\begin{cases} p = A^2 + B^2, \\ A \equiv 1 \pmod 4,\ B \equiv g^{\frac{p-1}{4}} A \pmod p, \end{cases}$$

and

$$\begin{cases} p = C^2 + 2D^2, \\ C \equiv 1 \pmod 4,\ D \equiv \left(g^{\frac{p-1}{8}} + g^{3\left(\frac{p-1}{8}\right)}\right) C/2 \pmod p. \end{cases}$$

Then we have

$$E_q(w_8) = \epsilon p^{\alpha}(A + Bi)^{\beta}(C + D\sqrt{-2})^{\delta},$$

where

$$\epsilon = \begin{cases} 1, & \text{if } f \equiv 0,1,4,5 \pmod 8, \\ (-1)^{\frac{p-1}{8}}, & \text{if } f \equiv 3,7 \pmod 8, \\ i^{3\operatorname{ind}_g(2)}, & \text{if } f \equiv 2 \pmod 8, \\ i^{\operatorname{ind}_g(2)}, & \text{if } f \equiv 6 \pmod 8; \end{cases}$$

$$\alpha = \begin{cases} f/8 - 1, & \text{if } f \equiv 0 \pmod 8, \\ [f/8], & \text{if } f \not\equiv 0 \pmod 8; \end{cases}$$

$$\beta = \begin{cases} f/4, & \text{if } f \equiv 0 \pmod 4, \\ \frac{f-1}{4}, & \text{if } f \equiv 1 \pmod 4, \\ \frac{f-2}{4}, & \text{if } f \equiv 2 \pmod 8, \\ \frac{f+2}{4}, & \text{if } f \equiv 6 \pmod 8, \\ \frac{f+1}{4}, & \text{if } f \equiv 3 \pmod 4; \end{cases}$$

$$\delta = \begin{cases} f/2, & \text{if } f \equiv 0 \pmod 2, \\ (f-1)/2, & \text{if } f \equiv 1,3 \pmod 8, \\ (f+1)/2, & \text{if } f \equiv 5,7 \pmod 8. \end{cases}$$

(b) If $p \equiv 3 \pmod 8$ *and* $f \equiv 0 \pmod 2$ *define the integers* C, D *uniquely by*

$$\begin{cases} p = C^2 + 2D^2, \ C \equiv 1 \pmod 4, \\ D \equiv \left[\gamma^{\frac{q-1}{8}} + \gamma^{3\left(\frac{q-1}{8}\right)}\right] D/2 \pmod p. \end{cases}$$

Then we have

$$E_q(w_8) = \begin{cases} (-1)^{f/4}\, p^{f/4-1}(C + D\sqrt{-2})^{f/2}, & \text{if } f \equiv 0 \pmod 4, \\ (-1)^{\frac{(f-2)}{4}+\frac{p+5}{8}}\, p^{(f-2)/4}(C + D\sqrt{-2})^{f/2}, & \text{if } f \equiv 2 \pmod 4. \end{cases}$$

(c) If $p \equiv 5 \pmod 8$ *and* $f \equiv 0 \pmod 2$ *define the integers* A, B *uniquely by*

$$\begin{cases} p = A^2 + B^2, \quad A \equiv 1 \pmod 4, \\ B = g^{\frac{p-1}{4}} A \pmod p. \end{cases}$$

Set $m = ind_g(2)$. *Then we have*

$$E_q(w_8) = \begin{cases} p^{3f/4-1}(A + Bi)^{f/4}, & \text{if } f \equiv 0 \pmod 8, \\ (-1)^{\frac{m-1}{2}}\, i\, p^{\frac{3f-6}{8}}(A + Bi)^{\frac{f+2}{4}}, & \text{if } f \equiv 2 \pmod 8, \\ -p^{\frac{3f-4}{8}}(A + Bi)^{f/4}, & \text{if } f \equiv 4 \pmod 8, \\ (-1)^{\frac{m-1}{2}}\, i\, p^{\frac{3f-2}{8}}(A + Bi)^{\frac{f-2}{4}}, & \text{if } f \equiv 6 \pmod 8. \end{cases}$$

(d) If $p \equiv 7 \pmod 8$ *and* $f \equiv 0 \pmod 2$ *then we have*

$$E_q(w_8) = (-1)^{\frac{f}{2}\left(\frac{p-7}{8}\right)}\, p^{f/2-1}.$$

Some numerical examples illustrating Theorem 7(a), (b), (c) are given in Tables 22–31 in §11.

10. Acknowledgement

The authors would like to thank Nicholas Buck and Iain deMille for their valuable assistance in the computer related areas of this project.

11. Tables

The values of the Eisenstein sums given in the tables below were computed on a Honeywell DPS 8/47 computer at Carleton University. The programs were written in PASCAL. For each prime p and integer $f \geq 2$, an irreducible polynomial $x^f + a_{f-1}x^{f-1} + \ldots + a_1x + a_0 \pmod p$ of degree f was found using a modification of Berlekamp's procedure. This gave a concrete realization of F_{p^f} as

$$F_{p^f} = \{b_0 + b_1x + \ldots + b_{f-1}x^{f-1} \mid x^f = -a_{f-1}x^{f-1} - \ldots - a_1x - a_0\}.$$

A generator γ of $F_{p^f}^*$ was then found by checking that $\gamma^{(p^f-1)/p_i} \neq 1$, for every prime $p_i \mid p^f - 1$. The sum $E_q(w_n)$ was then calculated by means of the formula

$$E_q(w_m) = \sum_{t=0}^{m-1} w_m^t \text{ card } \{s \mid 0 \leq s < \tfrac{q-1}{p-1},\ s - \left(\tfrac{q-1}{p-1}\right) \text{ ind}_g(tr(\gamma^s)) \equiv t \pmod m\}.$$

TABLE 1

$m=3$: $f=2$: $p\equiv 1 \pmod 3$ $(\alpha=0, \beta=1)$							
$p\equiv 1 \pmod 3$	$F_{p^2}^* = \langle\gamma\rangle$	$E_{p^2}(\omega_3)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{3}}$	L	M	$\frac{1}{2}(L+3M\sqrt{-3})$
7	$\gamma_2 = 1+x$ $x^2 = -2$	$\frac{1}{2}(-1+3\sqrt{-3})$	3	2	-1	$+1$	$\frac{1}{2}(-1+3\sqrt{-3})$
13	$\gamma_2 = 2+x$ $x^2 = 2$	$\frac{1}{2}(5+3\sqrt{-3})$	2	3	$+5$	$+1$	$\frac{1}{2}(5+3\sqrt{-3})$
19	$\gamma_2 = 2+x$ $x^2 = 2$	$\frac{1}{2}(-7+3\sqrt{-3})$	2	7	-7	$+1$	$\frac{1}{2}(-7+3\sqrt{-3})$
31	$\gamma_2 = 1+x$ $x^2 = -2$	$\frac{1}{2}(-4-6\sqrt{-3})$	3	25	-4	-2	$\frac{1}{2}(-4-6\sqrt{-3})$
37	$\gamma_2 = 2+x$ $x^2 = 2$	$\frac{1}{2}(11-3\sqrt{-3})$	2	26	$+11$	-1	$\frac{1}{2}(11-3\sqrt{-3})$

TABLE 2

$m=3$: $f=3$: $p\equiv 1 \pmod 3$ $(\alpha=0, \beta=1)$							
$p\equiv 1 \pmod 3$	$F_{p^3}^* = \langle\gamma\rangle$	$E_{p^3}(\omega_3)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{3}}$	L	M	$\frac{1}{2}(L+3M\sqrt{-3})$
7	$\gamma_3 = 5+x$ $x^3 = -1-x$	$\frac{1}{2}(-1+3\sqrt{-3})$	3	2	-1	$+1$	$\frac{1}{2}(-1+3\sqrt{-3})$
13	$\gamma_3 = 4+x$ $x^3 = -5-x$	$\frac{1}{2}(5+3\sqrt{-3})$	11	3	$+5$	$+1$	$\frac{1}{2}(5+3\sqrt{-3})$
19	$\gamma_3 = 3+x$ $x^3 = -1-x$	$\frac{1}{2}(-7-3\sqrt{-3})$	10	11	-7	-1	$\frac{1}{2}(-7-3\sqrt{-3})$
31	$\gamma_3 = 4+x$ $x^3 = -3-x$	$\frac{1}{2}(-4-6\sqrt{-3})$	3	25	-4	-2	$\frac{1}{2}(-4-6\sqrt{-3})$
37	$\gamma_3 = 9+x$ $x^3 = -3-x$	$\frac{1}{2}(11+3\sqrt{-3})$	32	10	$+11$	$+1$	$\frac{1}{2}(11+3\sqrt{-3})$

TABLE 3

$m=3$: $f=4$: $p\equiv 1 \pmod 3$ $(\alpha=\beta=1)$							
$p\equiv 1 \pmod 3$	$F_{p^4}^* = \langle\gamma\rangle$	$E_{p^4}(\omega_3)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{3}}$	$L\equiv -1 \pmod 3$	M	$p\left(\frac{1}{2}(L+3M\sqrt{-3})\right)$
7	$\gamma = 3+2x$ $x^4 = -3-2x^2$	$\frac{1}{2}(-7-21\sqrt{-3})$	5	4	-1	-1	$\frac{1}{2}(-7-21\sqrt{-3})$
13	$\gamma = 4+x$ $x^4 = -2$	$\frac{1}{2}(65+39\sqrt{-3})$	11	3	$+5$	$+1$	$\frac{1}{2}(65+39\sqrt{-3})$
19	$\gamma = 1+2x$ $x^4 = -2-2x^2$	$\frac{1}{2}(-133+57\sqrt{-3})$	3	7	-7	$+1$	$\frac{1}{2}(-133+57\sqrt{-3})$

TABLE 4

$m=3$: $f=5$: $p\equiv 1 \pmod 3$ $(\alpha=1,\ \beta=2)$							
$p\equiv 1 \pmod 3$	$F_{p^5}^* = \langle\gamma\rangle$	$E_{p^5}(\omega_3)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{3}}$	L	M	$p\left(\frac{1}{2}(L+3M\sqrt{-3})\right)^2$
7	$\gamma = 1+x$ $x^5 = -5-x-x^2$	$\frac{1}{2}(-91-21\sqrt{-3})$	3	2	-1	$+1$	$\frac{1}{2}(-91-21\sqrt{-3})$
13	$\gamma = x$ $x^5 = -6-x-x^2$	$\frac{1}{2}(-13-195\sqrt{-3})$	7	9	$+5$	-1	$\frac{1}{2}(-13-195\sqrt{-3})$

TABLE 5

$m=3$: $f=6$: $p\equiv 1 \pmod 3$ $(\alpha=1,\ \beta=2)$							
$p\equiv 1 \pmod 3$	$F_{p^6}^* = \langle\gamma\rangle$	$E_{p^6}(\omega_3)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{3}}$	L	M	$p\left(\frac{1}{2}(L+3M\sqrt{-3})\right)^2$
7	$\gamma = 2+x$ $x^6 = -2-2x-x^2$	$\frac{1}{2}(-91-21\sqrt{-3})$	3	2	-1	$+1$	$\frac{1}{2}(-91-21\sqrt{-3})$

TABLE 6

$m=4$: $f=2$: $p\equiv 1 \pmod 4$ $(\alpha=0, \beta=1, \varepsilon=1)$							
$p\equiv 1 \pmod 4$	$F_{p^2}^{*}=\langle\gamma\rangle$	$E_{p^2}(\omega_4)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{4}}$	A	B	$A+Bi$
5	$\gamma=2+x$ $x^2=2$	$1+2i$	2	2	+1	+2	$1+2i$
13	$\gamma=2+x$ $x^2=2$	$-3+2i$	2	8	−3	+2	$-3+2i$
17	$\gamma=2+x$ $x^2=-3$	$1+4i$	7	4	+1	+4	$1+4i$
29	$\gamma=4+x$ $x^2=2$	$5+2i$	14	12	+5	+2	$5+2i$

TABLE 7

$m=4$: $f=3$: $p\equiv 1 \pmod 4$ $(\alpha=0, \beta=2, \varepsilon=(-1)^{(p-1)/4})$							
$p\equiv 1 \pmod 4$	$F_{p^3}^{*}=\langle\gamma\rangle$	$E_{p^3}(\omega_4)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{4}}$	A	B	$(-1)^{(p-1)/4}(A+Bi)^2$
5	$\gamma=4+x$ $x^3=-1-x$	$3-4i$	2	2	+1	+2	$3-4i$
13	$\gamma=4+x$ $x^3=-5-x$	$-5-12i$	11	5	−3	−2	$-5-12i$
17	$\gamma=x$ $x^3=-3-x$	$-15-8i$	14	13	+1	−4	$-15-8i$
29	$\gamma=1+x$ $x^3=-4-x$	$-21+20i$	27	17	+5	−2	$-21+20i$

TABLE 8

$m=4$: $f=4$: $p\equiv 1 \pmod 4$ $(\alpha=0, \beta=2, \varepsilon=1)$							
$p\equiv 1 \pmod 4$	$F_{p^4}^* = \langle\gamma\rangle$	$E_{p^4}(\omega_4)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{4}}$	A	B	$(A+Bi)^2$
5	$\gamma_4 = 1+x$ $x^4=-2$	$-3-4i$	3	3	+1	−2	$-3-4i$
13	$\gamma_4 = 4+x$ $x^4=-2$	$5+12i$	11	5	−3	−2	$5+12i$
17	$\gamma_4 = 1+x+x^2$ $x^4=-3$	$-15+8i$	7	4	+1	+4	$-15+8i$

TABLE 9

$m=4$: $f=5$: $p\equiv 1 \pmod 4$ $(\alpha=1, \beta=2, \varepsilon=1)$							
$p\equiv 1 \pmod 4$	$F_{p^5}^* = \langle\gamma\rangle$	$E_{p^5}(\omega_4)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{4}}$	A	B	$p(A+Bi)^2$
5	$\gamma_5 = 1+x$ $x^5=-4-x-x^2$	$-15+20i$	2	2	+1	+2	$-15+20i$
13	$\gamma_5 = x$ $x^5=-6-x-x^2$	$65+156i$	7	5	−3	−2	$65+156i$

TABLE 10

$m=4$: $f=6$: $p\equiv 1 \pmod 4$ $(\alpha=1, \beta=3, \varepsilon=1)$							
$p\equiv 1 \pmod 4$	$F_{p^6}^* = \langle\gamma\rangle$	$E_{p^6}(\omega_4)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{4}}$	A	B	$p(A+Bi)^3$
5	$\gamma_6 = 2+x$ $x^6=-1-x-x^2$	$-55-10i$	2	2	+1	+2	$-55-10i$

TABLE 11

$m = 5 \quad : \quad f = 2 \quad : \quad p \equiv 1 \pmod 5 \qquad (\alpha = 0, \beta = 1, \delta = 0, \varepsilon = -1)$						
$p \equiv 1 \pmod 5$	$F_{p^3}^* = \langle \gamma \rangle$	$E_{p^3}(\omega_5)$	$g = \gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{5}}$	x, u, v, w	$-\tau(x, u, v, w)$
11	$\gamma_1 = 2 + x$ $x^2 = 2$	$\frac{1}{4}(-1 - 2i\sqrt{10 + 2\sqrt{5}} + i\sqrt{10 - 2\sqrt{5}} - 5\sqrt{5})$	2	4	1, 0, 1, 1	$-\frac{1}{4}(1 + 2i\sqrt{10 + 2\sqrt{5}} - i\sqrt{10 - 2\sqrt{5}} + 5\sqrt{5})$
31	$\gamma_2 = 1 + x$ $x^2 = -2$	$\frac{1}{4}(-11 + 4i\sqrt{10 + 2\sqrt{5}} + 3i\sqrt{10 - 2\sqrt{5}} + 5\sqrt{5})$	3	16	11, −2, −1, −1	$-\frac{1}{4}(11 - 4i\sqrt{10 + 2\sqrt{5}} - 3i\sqrt{10 - 2\sqrt{5}} - 5\sqrt{5})$
41	$\gamma_2 = 2 + x$ $x^2 = -3$	$\frac{1}{4}(9 + 6i\sqrt{10 + 2\sqrt{5}} - 3i\sqrt{10 - 2\sqrt{5}} + 5\sqrt{5})$	7	37	−9, 0, −3, −1	$-\frac{1}{4}(-9 - 6i\sqrt{10 + 2\sqrt{5}} + 3i\sqrt{10 - 2\sqrt{5}} - 5\sqrt{5})$
61	$\gamma_1 = 2 + x$ $x^2 = 2$	$\frac{1}{4}(-1 + 2i\sqrt{10 + 2\sqrt{5}} + 9i\sqrt{10 - 2\sqrt{5}} - 5\sqrt{5})$	2	9	1, −4, 1, 1	$-\frac{1}{4}(1 - 2i\sqrt{10 + 2\sqrt{5}} - 9i\sqrt{10 - 2\sqrt{5}} + 5\sqrt{5})$

TABLE 12

$m = 5 \quad : \quad f = 3 \quad : \quad p \equiv 1 \pmod 5 \qquad (\alpha = 0, \beta = 1, \delta = 1, \varepsilon = 1)$						
$p \equiv 1 \pmod 5$	$F_{p^3}^* = \langle \gamma \rangle$	$E_{p^3}(\omega_5)$	$g = \gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{5}}$	x, u, v, w	$+\tau(x, u, v, w)\tau(x, v, -u, -w)$
11	$\gamma_3 = x$ $x^3 = -4 - x$	$\frac{1}{4}(-31 - 6i\sqrt{10 + 2\sqrt{5}} - 7i\sqrt{10 - 2\sqrt{5}} + 5\sqrt{5})$	7	5	1, −1, 0, −1	$\frac{1}{4}(-31 - 6i\sqrt{10 + 2\sqrt{5}} - 7i\sqrt{10 - 2\sqrt{5}} + 5\sqrt{5})$
31	$\gamma_3 = 4 + x$ $x^3 = -3 - x$	$\frac{1}{4}(-1 - 9i\sqrt{10 + 2\sqrt{5}} - 38i\sqrt{10 - 2\sqrt{5}} + 5\sqrt{5})$	3	16	11, −2, −1, −1	$\frac{1}{4}(-1 - 9i\sqrt{10 + 2\sqrt{5}} - 38i\sqrt{10 - 2\sqrt{5}} + 5\sqrt{5})$
41	$\gamma_3 = 3 + x$ $x^3 = -1 - x$	$\frac{1}{4}(-11 + 12i\sqrt{10 + 2\sqrt{5}} + 39i\sqrt{10 - 2\sqrt{5}} + 45\sqrt{5})$	29	18	−9, −3, 0, 1	$\frac{1}{4}(-11 + 12i\sqrt{10 + 2\sqrt{5}} + 39i\sqrt{10 - 2\sqrt{5}} + 45\sqrt{5})$

TABLE 13

$m=5$: $f=4$: $p\equiv 1 \pmod 5$ $(\alpha=0,\beta=2,\delta=1,\varepsilon=-1)$						
$p\equiv 1 \pmod 5$	$F_{p^4}^* = \langle\gamma\rangle$	$E_{p^4}(\omega_5)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{5}}$	x,u,v,w	$-\tau(x,u,v,w)^2\tau(x,v,-u,-w)$
11	$\gamma_4 = \frac{5+x}{x^4=-2-2x^2}$	$\frac{1}{4}(89-20i\sqrt{10+2\sqrt{5}}+25i\sqrt{10-2\sqrt{5}}+25\sqrt{5})$	6	3	1,0,−1,1	$\frac{1}{4}(89-20i\sqrt{10+2\sqrt{5}}+25i\sqrt{10-2\sqrt{5}}+25\sqrt{5})$
31	$\gamma_4 = \frac{7+x}{x^4=-3-2x^2}$	$\frac{1}{4}(409+135i\sqrt{10+2\sqrt{5}}+70i\sqrt{10-2\sqrt{5}}-125\sqrt{5})$	22	8	11,1,−2,1	$\frac{1}{4}(409+135i\sqrt{10+2\sqrt{5}}+70i\sqrt{10-2\sqrt{5}}-125\sqrt{5})$
41	$\gamma_4 = \frac{2+x}{x^4=-3}$	$\frac{1}{4}(981+90i\sqrt{10+2\sqrt{5}}-75i\sqrt{10-2\sqrt{5}}-25\sqrt{5})$	19	37	−9,0,−3,−1	$\frac{1}{4}(981+90i\sqrt{10+2\sqrt{5}}-75i\sqrt{10-2\sqrt{5}}-25\sqrt{5})$

TABLE 14

$m=5$: $f=5$: $p\equiv 1 \pmod 5$ $(\alpha=0,\beta=2,\delta=1,\varepsilon=-1)$						
$p\equiv 1 \pmod 5$	$F_{p^5}^* = \langle\gamma\rangle$	$E_{p^5}(\omega_5)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{5}}$	x,u,v,w	$-\tau(x,u,v,w)^2\tau(x,v,-u,-w)$
11	$\gamma_5 = \frac{x}{x^5=-4-x-x^2}$	$\frac{1}{4}(89-25i\sqrt{10+2\sqrt{5}}-20i\sqrt{10-2\sqrt{5}}-25\sqrt{5})$	7	5	1,−1,0,−1	$\frac{1}{4}(89-25i\sqrt{10+2\sqrt{5}}-20i\sqrt{10-2\sqrt{5}}-25\sqrt{5})$

TABLE 15

$m=5$: $f=6$: $p\equiv 1 \pmod 5$ $(\alpha=1,\beta=2,\delta=1,\varepsilon=-1)$						
$p\equiv 1 \pmod 5$	$F_{p^6}^* = \langle\gamma\rangle$	$E_{p^6}(\omega_5)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{5}}$	x,u,v,w	$-p\tau(x,u,v,w)^2\tau(x,v,-u,-w)$
11	$\gamma_6 = \frac{4+x}{x^6=-1-x-x^2}$	$\frac{1}{4}(979-220i\sqrt{10+2\sqrt{5}}+275i\sqrt{10-2\sqrt{5}}+275\sqrt{5})$	6	3	1,0,−1,1	$\frac{1}{4}(979-220i\sqrt{10+2\sqrt{5}}+275i\sqrt{10-2\sqrt{5}}+275\sqrt{5})$

TABLE 16

$m=6$: $f=2$: $p\equiv 1 \pmod 6$ $\quad(\alpha=0, \beta=1, \varepsilon=(-1)^{\frac{p-1}{2}}\omega_3^{\mathrm{ind}_g(2)})$								
$p\equiv 1 \pmod 6$	$F_{p^3}^* = \langle\gamma\rangle$	$E_{p^3}(\omega_6)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{3}}$	L	M	$\mathrm{ind}_g(2)$	$(-1)^{\frac{p-1}{2}}\omega_3^{\mathrm{ind}_g(2)}\frac{1}{2}(L+3M\sqrt{-3})$
7	$\gamma_x{}^2 = \begin{matrix}1+x\\ =-2\end{matrix}$	$\frac{1}{2}(-5+\sqrt{-3})$	3	2	−1	+1	2	$\frac{1}{2}(-5+\sqrt{-3})$
13	$\gamma_x{}^2 = \begin{matrix}2+x\\ =2\end{matrix}$	$\frac{1}{2}(-7+\sqrt{-3})$	2	3	+5	+1	1	$\frac{1}{2}(-7+\sqrt{-3})$
19	$\gamma_x{}^2 = \begin{matrix}2+x\\ =2\end{matrix}$	$\frac{1}{2}(1+5\sqrt{-3})$	2	7	−7	+1	1	$\frac{1}{2}(1+5\sqrt{-3})$
31	$\gamma_x{}^2 = \begin{matrix}1+x\\ =-2\end{matrix}$	$2+3\sqrt{-3}$	3	25	−4	−2	24	$2+3\sqrt{-3}$
37	$\gamma_x{}^2 = \begin{matrix}2+x\\ =2\end{matrix}$	$\frac{1}{2}(-1+7\sqrt{-3})$	2	26	+11	−1	1	$\frac{1}{2}(-1+7\sqrt{-3})$

TABLE 17

$m=6$: $f=3$: $p\equiv 1 \pmod 6$ $(\alpha=0, \beta=2, \varepsilon=(-1)^{(p-1)/2})$							
$p\equiv 1 \pmod 6$	$F_{p^3}^* = \langle\gamma\rangle$	$E_{p^3}(\omega_6)$	$g=\gamma^{\frac{p-1}{p-1}}$	$g^{\frac{p-1}{3}}$	L	M	$(-1)^{\frac{p-1}{2}}\left(\frac{1}{2}(L+3M\sqrt{-3})\right)^2$
7	$\gamma_1 = 5+x$ $x^3 = -1-x$	$\frac{1}{2}(13+3\sqrt{-3})$	3	2	−1	+1	$\frac{1}{2}(13+3\sqrt{-3})$
13	$\gamma_1 = 4+x$ $x^3 = -5-x$	$\frac{1}{2}(-1+15\sqrt{-3})$	11	3	+5	+1	$\frac{1}{2}(-1+15\sqrt{-3})$
19	$\gamma_1 = 3+x$ $x^3 = -1-x$	$\frac{1}{2}(-11-21\sqrt{-3})$	10	11	−7	−1	$\frac{1}{2}(-11-21\sqrt{-3})$
31	$\gamma_1 = 4+x$ $x^3 = -3-x$	$23-12\sqrt{-3}$	3	25	−4	−2	$23-12\sqrt{-3}$
37	$\gamma_1 = 9+x$ $x^3 = -3-x$	$\frac{1}{2}(47+33\sqrt{-3})$	32	10	+11	+1	$\frac{1}{2}(47+33\sqrt{-3})$

TABLE 18

$m=6$: $f=4$: $p\equiv 1 \pmod 6$ $(\alpha=0, \beta=3, \varepsilon=\omega_3^{2\mathrm{ind}_g(2)})$								
$p\equiv 1 \pmod 6$	$F_{p^4}^* = \langle\gamma\rangle$	$E_{p^4}(\omega_6)$	$g=\gamma^{\frac{p-1}{p-1}}$	$g^{\frac{p-1}{3}}$	L	M	$\mathrm{ind}_g(2)$	$\omega_3^{2\mathrm{ind}_g(2)}\left(\frac{1}{2}(L+3M\sqrt{-3})\right)^3$
7	$\gamma_1 = 3+2x$ $x^4 = -3-2x^2$	$\frac{1}{2}(17-19\sqrt{-3})$	5	4	−1	−1	4	$\frac{1}{2}(17-19\sqrt{-3})$
13	$\gamma_1 = 4+x$ $x^4 = -2$	$\frac{1}{2}(89+17\sqrt{-3})$	11	3	+5	+1	7	$\frac{1}{2}(89+17\sqrt{-3})$
19	$\gamma_1 = 1+2x$ $x^4 = -2-2x^2$	$\frac{1}{2}(107-73\sqrt{-3})$	3	7	−7	+1	7	$\frac{1}{2}(107-73\sqrt{-3})$
31	$\gamma_1 = 7+x$ $x^4 = -3-2x^2$	$154-45\sqrt{-3}$	22	5	−4	+2	12	$154-45\sqrt{-3}$

TABLE 19

$m=6$: $f=5$: $p\equiv 1 \pmod 6$ $(\alpha=0, \beta=4, \varepsilon=+1)$							
$p\equiv 1 \pmod 6$	$F_{p^5}^* = \langle\gamma\rangle$	$E_{p^5}(\omega_6)$	$g=\gamma^{\frac{p-1}{p-1}}$	$g^{\frac{p-1}{3}}$	L	M	$\left(\frac{1}{2}(L+3M\sqrt{-3})\right)^4$
7	$\gamma_1 = 1+x$ $x^5 = -5-x-x^2$	$\frac{1}{2}(71+39\sqrt{-3})$	3	2	−1	+1	$\frac{1}{2}(71+39\sqrt{-3})$
13	$\gamma_1 = x$ $x^5 = -6-x-x^2$	$\frac{1}{2}(-337+15\sqrt{-3})$	7	9	+5	−1	$\frac{1}{2}(-337+15\sqrt{-3})$
19	$\gamma_1 = 4+x$ $x^5 = -2-x-x^2$	$\frac{1}{2}(-601-231\sqrt{-3})$	3	7	−7	+1	$\frac{1}{2}(-601-231\sqrt{-3})$

TABLE 20

$m=7$: $f=3$: $p\equiv 2$ or $4 \pmod 7$						
$p\equiv 2$ or 4 $(\bmod 7)$	$F_{p^3}^{*}=\langle\gamma\rangle$	$E_{p^3}(\omega_7)$	$S\equiv\sum_{k=1}^{6}\left(\frac{k}{7}\right)\gamma^{k\left(\frac{q-1}{7}\right)} \pmod p$	G	H	$G+H\sqrt{-7}$
11	$\gamma = x$ $x^3=-4-x$	$2-\sqrt{-7}$	2	+2	−1	$2-\sqrt{-7}$
23	$\gamma = x$ $x^3=-3-x$	$4-\sqrt{-7}$	4	+4	−1	$4-\sqrt{-7}$
37	$\gamma = 9+x$ $x^3=-3-x$	$-3-2\sqrt{-7}$	17	−3	−2	$-3-2\sqrt{-7}$
53	$\gamma = x$ $x^3=-5-x$	$-5-2\sqrt{-7}$	24	−5	−2	$-5-2\sqrt{-7}$
67	$\gamma = 2+x$ $x^3=-3-x$	$2+3\sqrt{-7}$	44	+2	+3	$2+3\sqrt{-7}$
79	$\gamma = 1+x$ $x^3=-6-x$	$4+3\sqrt{-7}$	25	+4	+3	$4+3\sqrt{-7}$

TABLE 21

$m=7$: $f=6$: $p\equiv 2$ or $4 \pmod 7$						
$p\equiv 2$ or 4 $(\bmod 7)$	$F_{p^6}^{*}=\langle\gamma\rangle$	$E_{p^6}(\omega_7)$	$S\equiv\sum_{k=1}^{6}\left(\frac{k}{7}\right)\gamma^{k\left(\frac{q-1}{7}\right)} \pmod p$	G	H	$p\left(G+H\sqrt{-7}\right)^2$
11	$\gamma = 4+x$ $x^6=-1-x-x^2$	$-33+44\sqrt{-7}$	9	+2	+1	$-33+44\sqrt{-7}$

TABLE 22

$m=8$: $f=2$: $p\equiv 1 \pmod 8$ $\quad(\alpha=0,\ \beta=0,\ \delta=1,\ \varepsilon=i^{3\mathrm{ind}_g(2)})$									
$p\equiv 1 \pmod 8$	$F_{p^3}^* = \langle\gamma\rangle$	$E_{p^3}(\omega_8)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{8}}$	$g^{\frac{p-1}{8}}+g^{3\left(\frac{p-1}{8}\right)}$	C	D	$\mathrm{ind}_g(2)$	$i^{3\mathrm{ind}_g(2)}(C+D\sqrt{-2})$
17	$\gamma_2 = \frac{2+x}{x^2=-3}$	$3+2\sqrt{-2}$	7	15	7	−3	−2	10	$3+2\sqrt{-2}$
41	$\gamma_2 = \frac{2+x}{x^2=-3}$	$3-4\sqrt{-2}$	7	38	11	−3	+4	14	$3-4\sqrt{-2}$
73	$\gamma_2 = \frac{3+x}{x^2=-5}$	$1-6\sqrt{-2}$	14	10	61	+1	−6	16	$1-6\sqrt{-2}$

TABLE 23

$m=8$: $f=3$: $p\equiv 1 \pmod 8$ $\quad(\alpha=0,\ \beta=1,\ \delta=1,\ \varepsilon=(-1)^{(p-1)/8})$											
$p\equiv 1 \pmod 8$	$F_{p^3}^* = \langle\gamma\rangle$	$E_{p^3}(\omega_8)$	$g=\gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{8}}$	$g^{\frac{p-1}{4}}$	$g^{\frac{p-1}{8}}+g^{3\left(\frac{p-1}{8}\right)}$	A	B	C	D	$(-1)^{(p-1)/8}(A+Bi)(C+D\sqrt{-2})$
17	$\gamma_3 = \frac{x}{x^3=-3-x}$	$-3-8\sqrt{2}$ $+12i-2i\sqrt{2}$	14	9	13	7	+1	−4	−3	−2	$-3-8\sqrt{2}$ $+12i-2i\sqrt{2}$
41	$\gamma_3 = \frac{3+x}{x^3=-1-x}$	$15+16\sqrt{2}$ $+12i-20i\sqrt{2}$	29	38	9	11	+5	+4	−3	+4	$15+16\sqrt{2}$ $+12i-20i\sqrt{2}$
73	$\gamma_3 = \frac{3+x}{x^3=-4-x}$	$3-48\sqrt{2}$ $-8i-18i\sqrt{2}$	26	51	46	61	−3	+8	+1	−6	$3-48\sqrt{2}$ $-8i-18i\sqrt{2}$

TABLE 24

$m = 8$: $f = 4$: $p \equiv 1 \pmod 8$ $(\alpha = 0, \beta = 1, \delta = 2, \epsilon = 1)$										
$p \equiv 1 \pmod 8$	$F_{p^4}^* = \langle \gamma \rangle$	$E_{p^4}(\omega_8)$	$g = \gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{4}}$	$g^{\frac{p-1}{8}} + g^{3\left(\frac{p-1}{8}\right)}$	A	B	C	D	$(A+Bi)(C+D\sqrt{-2})^2$
17	$\gamma = 1+x+x^2$ $x^4 = -3$	$1-48\sqrt{2}$ $+4i+12i\sqrt{2}$	7	4	7	+1	+4	−3	−2	$1-48\sqrt{2}$ $+4i+12i\sqrt{2}$
41	$\gamma = 2+x$ $x^4 = -3$	$-115+96\sqrt{2}$ $+92i+120i\sqrt{2}$	19	32	30	+5	−4	−3	−4	$-115+96\sqrt{2}$ $+92i+120i\sqrt{2}$
73	$\gamma = 3+x$ $x^4 = -5$	$213+96\sqrt{2}$ $-568i+36i\sqrt{2}$	13	46	61	−3	+8	+1	−6	$213+96\sqrt{2}$ $-568i+36i\sqrt{2}$

TABLE 25

$m = 8$: $f = 5$: $p \equiv 1 \pmod 8$ $(\alpha = 0, \beta = 1, \delta = 3, \epsilon = 1)$										
$p \equiv 1 \pmod 8$	$F_{p^5}^* = \langle \gamma \rangle$	$E_{p^5}(\omega_8)$	$g = \gamma^{\frac{q-1}{p-1}}$	$g^{\frac{p-1}{4}}$	$g^{\frac{p-1}{8}} + g^{3\left(\frac{p-1}{8}\right)}$	A	B	C	D	$(A+Bi)(C+D\sqrt{-2})^3$
17	$\gamma = x$ $x^5 = -6-x-x^2$	$45-152\sqrt{2}$ $+180i+38i\sqrt{2}$	11	4	10	+1	+4	−3	+2	$45-152\sqrt{2}$ $+180i+38\sqrt{2}$

TABLE 26

$m = 8 \quad : \quad f = 2 \quad : \quad p \equiv 3 \pmod 8$						
$p \equiv 3 \pmod 8$	$F_{p^2}^{*} = \langle \gamma \rangle$	$E_{p^2}(\omega_8)$	$K \equiv \gamma^{\frac{q-1}{8}} + \gamma^{3\left(\frac{q-1}{8}\right)} \pmod p$	C	D	$(-1)^{\frac{p+5}{8}}(C + D\sqrt{-2})$
3	$\gamma_x = 1 + x$ $x^2 = 2$	$-1 - \sqrt{-2}$	2	+1	+1	$-1 - \sqrt{-2}$
11	$\gamma_x = 2 + x$ $x^2 = 2$	$-3 + \sqrt{-2}$	3	−3	+1	$-3 + \sqrt{-2}$
19	$\gamma_x = 2 + x$ $x^2 = 2$	$-1 + 3\sqrt{-2}$	13	+1	−3	$-1 + 3\sqrt{-2}$
43	$\gamma_x = 6 + x$ $x^2 = 2$	$5 + 3\sqrt{-2}$	27	+5	+3	$5 + 3\sqrt{-2}$

TABLE 27

$m = 8 \quad : \quad f = 4 \quad : \quad p \equiv 3 \pmod 8$						
$p \equiv 3 \pmod 8$	$F_{p^4}^{*} = \langle \gamma \rangle$	$E_{p^4}(\omega_8)$	$K \equiv \gamma^{\frac{q-1}{8}} + \gamma^{3\left(\frac{q-1}{8}\right)} \pmod p$	C	D	$-(C + D\sqrt{-2})^2$
3	$\gamma_x = 1 + x$ $x^4 = -2 - 2x^2$	$1 + 2\sqrt{-2}$	1	+1	−1	$1 + 2\sqrt{-2}$
11	$\gamma_x = 5 + x$ $x^4 = -2 - 2x^2$	$-7 - 6\sqrt{-2}$	8	−3	−1	$-7 - 6\sqrt{-2}$
19	$\gamma_x = 1 + 2x$ $x^4 = -2 - 2x^2$	$17 - 6\sqrt{-2}$	6	+1	+3	$17 - 6\sqrt{-2}$
43	$\gamma_x = 1 + x$ $x^4 = -2 - 2x^2$	$-7 - 30\sqrt{-2}$	27	+5	+3	$-7 - 30\sqrt{-2}$

TABLE 28

$m = 8$: $f = 6$: $p \equiv 3 \pmod 8$						
$p \equiv 3 \pmod 8$	$F_{p^6}^* = \langle \gamma \rangle$	$E_{p^6}(\omega_8)$	$K \equiv \gamma^{\frac{q-1}{8}} + \gamma^{3\left(\frac{q-1}{8}\right)} \pmod p$	C	D	$(-1)^{\frac{p-3}{8}} p(C + D\sqrt{-2})^3$
3	$\gamma_6 = 2 + x^2$ $x^6 = -1 - x - x^2$	$-15 - 3\sqrt{-2}$	1	+1	−1	$-15 - 3\sqrt{-2}$
11	$\gamma_6 = 4 + x$ $x^6 = -1 - x - x^2$	$99 + 275\sqrt{-2}$	8	−3	−1	$99 + 275\sqrt{-2}$

TABLE 29

$m = 8$: $f = 2$: $p \equiv 5 \pmod 8$								
$p \equiv 5 \pmod 8$	$F_{p^2}^* = \langle \gamma \rangle$	$E_{p^2}(\omega_8)$	g	$g^{\frac{p-1}{4}}$	A	B	$\mathrm{ind}_g 2$	$(-1)^{(\mathrm{ind}_g 2 - 1)/2}\, i(A + Bi)$
5	$\gamma_2 = 2 + x$ $x^2 = 2$	$-2 + i$	2	2	+1	+2	1	$-2 + i$
13	$\gamma_2 = 2 + x$ $x^2 = 2$	$-2 - 3i$	2	8	−3	+2	1	$-2 - 3i$
29	$\gamma_2 = 4 + x$ $x^2 = 2$	$-2 + 5i$	14	12	+5	+2	13	$-2 + 5i$
37	$\gamma_2 = 2 + x$ $x^2 = 2$	$6 + i$	2	31	+1	−6	1	$6 + i$
53	$\gamma_2 = 2 + x$ $x^2 = 2$	$-2 - 7i$	2	30	−7	+2	1	$-2 - 7i$

References

[1] *B. C Berndt* and *R.J. Evans*, Sums of Gauss, Jacobi, and Jacobsthal. J. Number Theory, **11** (1979), 349–398.

[2] *B.C. Berndt* and *R.J. Evans*, Sums of Gauss, Eisenstein, Jacobi, Jacobsthal, and Brewer. Illinois J. Math. **23** (1979), 374–437.

[3] *A. Cauchy*, Mémoire sur la théorie des nombres. Mém. Inst. France, **17** (1840), 249–768. (Oeuvres Completes (I) Vol. 3, 1911, pp. 5–83.)

[4] *H. Davenport* and *H. Hasse*, Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklishchen Fällen. J. Reine Angew. Math. **172** (1934), 151–182.

[5] *L.E. Dickson*, Cyclotomy, higher congruences, and Waring's problem. Amer. J. Math. **57** (1935), 391–424.

[6] *P.G.L. Dirichlet*, Ueber den biquadratischen Charakter der Zahl "Zwei". J. Reine Angew. Math. **57** (1860), 187–188.

[7] *G. Eisenstein*, Zur Theorie der quadratischen Zerfällung der Primzahlen $8n + 3$, $7n + 2$ und $7n + 4$. J. Reine Angew. Math. **37** (1848), 97–126.

[8] *C.F. Gauss*, Untersuchungen über Höhere Arithmetrik. Chelsea Publishing Company, Bronx, New York (reprinted 1965), 511–586.

[9] *A. Genocchi*, Solution de la question 293 (J.A. Serret) voir t. XIII, p. 314. Nouvelles Annales de Mathematiques, **14** (1855), 241–243.

[10] *H. Hasse*, Vorlesungen über Zahlentheorie. Springer–Verlag, Berlin–Heidelberg, New York, 1950.

[11] *R.H. Hudson* and *K.S. Williams*, Extensions of Theorems of Cunningham–Aigner and Hasse–Evans. Pacific J. Math. **104** (1983), 111–132.

[12] *K. Ireland* and *M. Rosen*, A Classical Introduction to Modern Number Theory, Graduate Texts in Mathematics No. 84. Springer–Verlag, New York (1982).

[13] *C.G.J. Jacobi*, Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie. J. Reine Angew. Math. **30** (1846), 166–182.

[14] *S.A. Katre* and *A.R. Rajwade*, Unique determination of cyclotomic numbers of order five. Manuscripta Math. **53** (1985), 65–75.

[15] *E. Lehmer*, On Euler's criterion. J. Austral. Math. Soc. **1** (1959), 64–70.

[16] *P.A. Leonard* and *K.S. Williams*, The cyclotomic numbers of order seven. Proc. Amer. Math. Soc. **51** (1975), 295–300.

[17] *R. Lidl* and *H. Niederreiter*, Finite Fields. Addison–Wesley Publishing Co., Reading. Mass., U.S.A. (1983).

[18] *M.A. Stern*, Eine Bermerkung zur Zahlentheorie. J. Reine Angew. Math. **32** (1846), 89–90.

[19] *L. Stickelberger*, Ueber eine Verallgemeinerung der Kreistheilung. Math. Ann. **37** (1890), 321–367.

[20] *A.L. Whiteman*, The sixteenth power residue character of 2. Canad. J. Math. **6** (1954), 364–373.

Department of Mathematics and Statistics, Carleton University,
Ottawa, Ontario, CANADA K1S 5B6

Department of Mathematics, Okanagan College, Vernon, British Columbia
CANADA V1B 2N5