JOURNAL OF NUMBER THEORY 19, 309–340 (1984)

Extension of a Theorem of Cauchy and Jacobi

DUNCAN A. BUELL

Department of Computer Science, Louisiana State University, Baton Rouge, Louisiana 70803

RICHARD H. HUDSON

Department of Mathematics and Statistics, University of South Carolina, Columbia, South Carolina 29208

AND

KENNETH S. WILLIAMS*

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

Communicated by H. Zassenhaus

Received December 21, 1982

Let q and p be prime with $q = a^2 + b^2 \equiv 1 \pmod 4$, $a \equiv 1 \pmod 4$, and $p = qf + 1$. In the nineteenth century Cauchy (*Mém. Inst. France* **17** (1840), 249–768) and Jacobi (*J. für Math.* **30** (1846), 166–182) generalized the work of earlier authors, who had determined certain binomial coefficients $(\bmod\, p)$ (see H. J. S. Smith, "Report on the Theory of Numbers," Chelsea, 1964), by determining two products of factorials given by $\prod_k kf! \pmod{p = qf + 1}$ where k runs through the quadratic residues and the quadratic non-residues $(\bmod\, q)$, respectively. These determinations are given in terms of parameters in representations of p^h or of $4p^h$ by binary quadratic forms. A remarkable feature of these results is the fact that the exponent h coincides with the class number of the related quadratic field. In this paper C. R. Mathews' (*Invent. Math.* **54** (1979), 23–52) recent explicit evaluation of the quartic Gauss sum is used to determine four products of factorials $(\bmod\, p = qf + 1,\ q \equiv 5 \pmod 8 > 5)$, given by $\prod_k kf!$ where k runs through the quartic residues $(\bmod\, q)$ and the three cosets which may be formed with respect to this subgroup. These determinations appear to be considerably more difficult. They are given in terms of parameters in representations of $16p^h$ by quaternary quadratic

* Research supported by grant A-7233 of the Natural Sciences and Engineering Research Council Canada.

0022-314X/84 $3.00

forms. Stickelberger's theorem is required to determine the exponent h which is shown to be closely related to the class number of the imaginary quartic field $Q(i\sqrt{2q+2a\sqrt{q}})$, $q=a^2+b^2 \equiv 5 \pmod 8$, a odd.

1. Introduction

Throughout this paper $q \equiv 5 \pmod 8$ is a prime greater than 5, and a and b are the unique integers satisfying

$$q=a^2+b^2, \qquad a \equiv 1 \pmod 4, b \equiv -\left(\frac{q-1}{2}\right)!\, a \pmod q. \tag{1.1}$$

The subgroup of the multiplicative group of residues $\pmod q$ consisting of quartic residues is denoted by A. The four cosets of A are given by $C_j = 2^j A$ $(j=0,1,2,3)$, where we adopt the convention that $C_{j+4}=C_j$. This convention is also used for other quantities which appear later in the paper, namely, s_j, α_j, and u_j.

Let $p=qf+1$ be prime. In this paper we determine the quantities

$$\prod_{k \in C_j} kf! \qquad (j=0,1,2,3) \tag{1.2}$$

modulo p. The corresponding quantities for quadratic residues were treated by Cauchy [3] and Jacobi [7] in the nineteenth century (see also [13]). The products (1.2) appear to be much more difficult to treat than those considered by Cauchy and Jacobi. We make use of a recent deep result of Matthews [10] giving the evaluation of the quartic Gauss sum (see Section 3).

The products (1.2) are determined $(\mathrm{mod}\, p)$ in terms of a solution (x,u,v,w) of the quaternary diophantine system

$$\begin{aligned} 16p^h &= x^2+2qu^2+2qv^2+qw^2, \\ xw &= av^2-2\,|b|\,uv-au^2, \\ \text{G.C.D.}\ (x,u,v,w,p) &= 1, \end{aligned} \tag{1.3}$$

satisfying

$$x \equiv -4 \pmod q, \tag{1.4}$$

which arises from the arithmetic of the quartic field $K=Q(i\sqrt{2q+2a\sqrt{q}})$. The exponent h in (1.3) is the positive odd integer given by

$$h=\max\left(|s_0-s_2|, |s_1-s_3|\right), \tag{1.5}$$

where

$$s_j = \frac{1}{q} \sum_{k \in C_j} k \qquad (j = 0, 1, 2, 3). \tag{1.6}$$

We note that K contains the real quadratic field $Q(\sqrt{q})$ as a subfield, and that K is a subfield of the cyclotomic field $Q(\rho_q)$, where $\rho_q = \exp(2\pi i/q)$, as (see, for example, [1, 2])

$$\pm i \sqrt{2q + 2a\sqrt{q}} = \sum_{x=0}^{q-1} (\rho_q^{x^4} - \rho_q^{x^2}).$$

The ring of integers of K will be denoted by R_K and the ring of integers of the cyclotomic field $Q(\rho_m)$ will be denoted by R_m.

2. The Exponent h

We begin by showing that the exponent h in (1.3) is a positive odd integer. Let g be a primitive root (mod q). For $j = 0, 1, 2, 3$ we have

$$\sum_{k \in C_j} k \equiv 2^j \sum_{r=0}^{(q-5)/4} g^{4r} \equiv 2^j \frac{g^{q-1} - 1}{g^4 - 1} \equiv 0 \pmod{q}, \tag{2.1}$$

as $g^4 - 1 \not\equiv 0 \pmod{q}$ since $q > 5$. This shows that each s_j is a positive integer. As the sum of the quadratic residues (mod q) is $\frac{1}{4}(q-1)\,q$, we have

$$s_0 + s_2 = s_1 + s_3 = \tfrac{1}{4}(q - 1). \tag{2.2}$$

Since $\frac{1}{4}(q-1)$ is odd, it follows from (2.1) that $s_0 \neq s_2$, $s_1 \neq s_3$, and that $h = \max(|s_0 - s_2|, |s_1 - s_3|)$ is a positive odd integer.

Next we give some alternative expressions for h. We have

$$h = \begin{cases} s_2 - s_0, & \text{if } \min\limits_{0 \leqslant j \leqslant 3} s_j = s_0, \\ s_3 - s_1, & \text{if } \min\limits_{0 \leqslant j \leqslant 3} s_j = s_1, \\ s_0 - s_2, & \text{if } \min\limits_{0 \leqslant j \leqslant 3} s_j = s_2, \\ s_1 - s_3, & \text{if } \min\limits_{0 \leqslant j \leqslant 3} s_j = s_3, \end{cases}$$

so that

$$\begin{cases} h = \frac{1}{4}(q-1) - 2 \min\limits_{0 \leqslant j \leqslant 3} s_j, \\ h = 2 \max\limits_{0 \leqslant j \leqslant 3} s_j - \frac{1}{4}(q-1). \end{cases} \tag{2.3}$$

Throughout the paper we let s_m denote the smallest value of the s_j ($j=0, 1, 2, 3$), and let s_n denote the smallest value of the s_j with $j \neq m$. Since, by (2.2), $s_m \leqslant s_n < (q-1)/8 < s_{n+2} \leqslant s_{m+2}$ we have

$$s_n - s_m < h/2. \tag{2.4}$$

This inequality is clearly trivial for $s_n = s_m$. For $s_n \neq s_m$, we have $s_m = \min\{s_{n+1}, s_{n+3}\}$ and $s_{m+2} = \max\{s_{n+1}, s_{n+3}\}$. Assume that (2.4) is false. Then we have

$$2(s_n - s_m) \geqslant h = s_{m+2} - s_m \Rightarrow 2s_n \geqslant s_{m+2} + s_m = (q-1)/4,$$

contradicting $s_n + s_{n+2} = (q-1)/4$ as $s_n < s_{n+2}$.

We also note that h is related to the class numbers $h(K)$ and $h(Q(\sqrt{q}))$ of K and $Q(\sqrt{q})$, respectively, in view of the class number formula [5, 12],

$$\frac{h(K)}{h(Q\sqrt{q}))} = \frac{1}{2}((s_0 - s_2)^2 + (s_1 - s_3)^2). \tag{2.5}$$

Clearly the right-hand side of (2.5) is an integer so that $h(Q(\sqrt{q})) \mid h(K)$. Thus we have

$$h = 1 \Leftrightarrow |s_0 - s_2| = |s_1 - s_3| = 1 \Leftrightarrow h(K) = h(Q(\sqrt{q})). \tag{2.6}$$

It is known [12] that $h(K) = 1$ for exactly $q = 13, 29, 37, 53, 61$ (as $q > 5$), so that $h = 1$ for these values of q.

3. Gauss Sums

Let σ_j denote the automorphism of $Q(\rho_q)$ such that $\sigma_j(\rho_q) = \rho_q^j$. We use Matthews' recent deep evaluation [10] of the quartic Gauss sum to prove the following lemma which will be needed later in the proof of our main result.

Lemma 1. *For $j \in C_1$ we have*

$$\sigma_j(i\sqrt{2q \pm 2a\sqrt{q}}) = \pm(-1)^{(b-2)/4} \frac{b}{|b|} i\sqrt{2q \mp 2a\sqrt{q}},$$

$$\sigma_j(\sqrt{q}) = -\sqrt{q}.$$

Proof. It is understood throughout this paper that fractional powers take their principal values. We set $\theta = \arg(\omega)$ $(-\pi < \theta \leqslant \pi)$, where $\omega = a + bi$ is one of the prime divisors of q in the ring of Gaussian integers. As $b \neq 0$ we have $\theta \neq \pi$. Clearly we have

$$\omega = q^{1/2} e^{i\theta}, \qquad a = q^{1/2} \cos\theta, \qquad b = q^{1/2} \sin\theta.$$

Now

$$\begin{aligned}\omega^{1/2}+\overline{\omega^{1/2}} &= q^{1/4}e^{i\theta/2}+q^{1/4}e^{-i\theta/2}\\ &= 2q^{1/4}\cos\theta/2\\ &= 2q^{1/4}\,|\cos\theta/2| \qquad \left(\text{as} -\frac{\pi}{2}<\frac{\theta}{2}<\frac{\pi}{2}\right)\\ &= 2q^{1/4}\left(\frac{1}{2}+\frac{1}{2}\cos\theta\right)^{1/2}\\ &= 2q^{1/4}\left(\frac{1}{2}+\frac{a}{2q^{1/2}}\right)^{1/2},\end{aligned}$$

that is,

$$\omega^{1/2}+\overline{\omega^{1/2}}=(2q^{1/2}+2a)^{1/2}. \tag{3.1}$$

Also

$$\begin{aligned}\omega^{1/2}-\overline{\omega^{1/2}} &= q^{1/4}e^{i\theta/2}-q^{1/4}e^{-i\theta/2}\\ &= 2iq^{1/4}\sin\theta/2\\ &= 2iq^{1/4}\frac{b}{|b|}\frac{|\sin\theta|}{\sin\theta}\sin\theta/2\\ &= 2iq^{1/4}\frac{b}{|b|}\,|\sin\theta/2|\\ &= 2iq^{1/4}\frac{b}{|b|}\left(\frac{1}{2}-\frac{1}{2}\cos\theta\right)^{1/2}\\ &= 2iq^{1/4}\frac{b}{|b|}\left(\frac{1}{2}-\frac{1}{2}\frac{a}{q^{1/2}}\right)^{1/2},\end{aligned}$$

giving

$$\omega^{1/2}-\overline{\omega^{1/2}}=i\frac{b}{|b|}(2q^{1/2}-2a)^{1/2}. \tag{3.2}$$

We now define a quartic character $\chi_\omega \pmod{\omega}$ as follows: for α a Gaussian integer not divisible by ω we set

$$\chi_\omega(\alpha)=i^k, \qquad \text{if } \alpha^{(q-1)/4}\equiv i^k \pmod{\omega}, \tag{3.3}$$

so that

$$\chi_\omega(\alpha)\equiv\alpha^{(q-1)/4} \pmod{\omega}. \tag{3.4}$$

Recently Matthews [10] proved Loxton's conjecture [9] for the value of the quartic Gauss sum, namely,

$$g(\chi_\omega) = \sum_{k=1}^{q-1} \chi_\omega(k)\,\rho_q^k = i(-1)^{(b+2)/4} \left(\frac{|b|}{|a|}\right) q^{1/4}\omega^{1/2}, \tag{3.5}$$

where $(|b|/|a|)$ denotes the usual Jacobi symbol. Next we have

$$g(\chi_\omega^3) = g(\bar{\chi}_\omega) = \bar{\chi}_\omega(-1)\,\overline{g(\chi_\omega)} = -\overline{g(\chi_\omega)}, \tag{3.6}$$

so that from (3.5) we obtain

$$g(\chi_\omega^3) = i(-1)^{(b+2)/4} \left(\frac{|b|}{|a|}\right) q^{1/4}\overline{\omega^{1/2}}. \tag{3.7}$$

Appealing to (3.1), (3.2), (3.5), and (3.7) we obtain

$$g(\chi_\omega) + g(\chi_\omega^3) = i(-1)^{(b+2)/4} \left(\frac{|b|}{|a|}\right) \sqrt{2q + 2a\sqrt{q}} \tag{3.8}$$

and

$$g(\chi_\omega) - g(\chi_\omega^3) = (-1)^{(b-2)/4} \frac{b}{|b|} \left(\frac{|b|}{|a|}\right) \sqrt{2q - 2a\sqrt{q}}\,. \tag{3.9}$$

Now we set $G_k(m, q) = \sum_{x=0}^{q-1} \rho_q^{mx^k}$, where k is a positive integer and m is an integer not divisible by q. It is well known that $G_2(m, q) = (m/q)\sqrt{q}$. We now consider $G_4(m, q)$. We have

$$\begin{aligned} G_4(m, q) &= \sum_{y=0}^{q-1} \{1 + \chi_\omega(y) + \chi_\omega^2(y) + \chi_\omega^3(y)\}\,\rho_q^{my} \\ &= \chi_\omega^3(m)\,g(\chi_\omega) + \left(\frac{m}{q}\right)\sqrt{q} + \chi_\omega(m)\,g(\chi_\omega^3), \end{aligned}$$

that is,

$$G_4(m, q) = \begin{cases} \sqrt{q} + i\chi_\omega(m)(-1)^{(b+2)/4} \left(\dfrac{|b|}{|a|}\right) \sqrt{2q + 2a\sqrt{q}}, & \\ & \text{if } \chi_\omega(m) = \pm 1, \\ -\sqrt{q} + \chi_\omega(m)(-1)^{(b+2)/4} \dfrac{b}{|b|} \left(\dfrac{|b|}{|a|}\right) \sqrt{2q - 2a\sqrt{q}}\,, & \\ & \text{if } \chi_\omega(m) = \pm i. \end{cases} \tag{3.10}$$

Finally, for $m \in C_1$, we have by (3.10)

$$\begin{aligned}
&\sigma_m(i\sqrt{2q+2a\sqrt{q}}) \\
&\quad = \sigma_m\left((-1)^{(b+2)/4}\left(\frac{|b|}{|a|}\right)(G_4(1,q)-G_2(1,q))\right) \\
&\quad = (-1)^{(b+2)/4}\left(\frac{|b|}{|a|}\right)(G_4(m,q)-G_2(m,q)) \\
&\quad = (-1)^{(b+2)/4}\left(\frac{|b|}{|a|}\right)\chi_\omega(m)(-1)^{(b+2)/4} \\
&\qquad \times \frac{b}{|b|}\left(\frac{|b|}{|a|}\right)\sqrt{2q-2a\sqrt{q}} \\
&\quad = \chi_\omega(m)\frac{b}{|b|}\sqrt{2q-2a\sqrt{q}} \\
&\quad = (-1)^{(b-2)/4}\frac{b}{|b|}i\sqrt{2q-2a\sqrt{q}},
\end{aligned}$$

as required. Squaring this result we obtain $\sigma_m(\sqrt{q}) = -\sqrt{q}$ and so

$$\begin{aligned}
\sigma_m(i\sqrt{2q-2a\sqrt{q}}) &= \sigma_m\left(\frac{-2|b|\sqrt{q}}{i\sqrt{2q+2a\sqrt{q}}}\right) \\
&= \frac{2|b|\sqrt{q}}{(-1)^{(b-2)/4}\dfrac{b}{|b|}i\sqrt{2q-2a\sqrt{q}}} \\
&= 2b\sqrt{q}\,(-1)^{(b-2/4)}\frac{i\sqrt{2q+2a\sqrt{q}}}{-2|b|\sqrt{q}} \\
&= -(-1)^{(b-2)/4}\frac{b}{|b|}i\sqrt{2q+2a\sqrt{q}},
\end{aligned}$$

as required.

4. Products of Gauss Sums

We let P be a prime ideal divisor of p in the ring R_q of integers of $Q(\rho_q)$. The conjugates of P are given by $P_l = \sigma_l(P)$, $l = 1, 2, \ldots, q-1$. The factorization of p in R_q into prime ideals is given by

$$pR_q = P_1 P_2 \cdots P_{q-1}. \tag{4.1}$$

We next define a qth-order character χ_P (mod p) as follows: for any integer x not divisible by p we set

$$\chi_P(x) = \rho_q^k, \qquad \text{if } x^{(p-1)/q} \equiv \rho_q^k \pmod{P}, \tag{4.2}$$

so that

$$\chi_P(x) \equiv x^{(p-1)/q} \pmod{P}. \tag{4.3}$$

Corresponding to this character we have the Gauss sum

$$g(\chi_P^n) = \sum_{x=1}^{p-1} \chi_P^n(x)\, \rho_p^x \qquad (\rho_p = \exp(2\pi i/p)), \tag{4.4}$$

where n is an integer not divisible by q. Clearly $g(\chi_P^n)$ is an integer of $Q(\rho_{pq})$, $\rho_{pq} = \exp(2\pi i/pq)$, that is, $g(\chi_P^n) \in R_{pq}$.

We begin by determining the effect of the automorphism (of $Q(\rho_{pq})$) $\theta_l: \rho_{pq} \to \rho_{pq}^l$, $1 \leqslant l \leqslant pq$, $(l, pq) = 1$, on $g(\chi_P^n)$. We have

$$\begin{aligned} \theta_l(g(\chi_P^n)) &= \sum_{x=1}^{p-1} \chi_P^{ln}(x)\, \rho_p^{lx} \\ &= \sum_{y=1}^{p-1} \chi_P^{ln}(l^{-1}y)\, \rho_p^y \qquad (ll^{-1} \equiv 1 \pmod{p}) \\ &= \chi_P^{-ln}(l) \sum_{y=1}^{p-1} \chi_P^{ln}(y)\, \rho_p^y, \end{aligned}$$

that is, by (4.4),

$$\theta_l(g(\chi_P^n)) = \chi_P^{-ln}(l)\, g(\chi_P^{ln}). \tag{4.5}$$

We now introduce certain products of the Gauss sums $g(\chi_P^n)$ which are central to the proof of our theorem. We define

$$\alpha_j = \prod_{k \in C_j} g(\chi_P^k), \qquad j = 0, 1, 2, 3. \tag{4.6}$$

Clearly each $\alpha_j \in R_{pq}$. We will show that in fact each α_j is actually an integer of the subfield $Q(\sum_{k \in C_0} \rho_q^k)$ of $Q(\rho_q)$, that is, of K.

First we determine the effect of θ_l on α_j. We have by (4.5) and (4.6)

$$\begin{aligned} \theta_l(\alpha_j) &= \prod_{k \in C_j} \chi_P^{-lk}(l)\, g(\chi_P^{lk}) \\ &= \{\chi_P(l)\}^{-l \sum_{k \in C_j} k} \prod_{k \in C_{j+m}} g(\chi_P^k), \end{aligned}$$

if $l \in C_m$. Thus by (2.1) we have

$$\theta_l(\alpha_j) = \alpha_{j+m}, \qquad \text{if} \quad l \in C_m. \tag{4.7}$$

Hence, in particular, for all $l \equiv 1 \pmod q$, we have $\theta_l(\alpha_j) = \alpha_j$ so each $\alpha_j \in R_q$.

Next, as $\sigma_r(\alpha_j) = \alpha_j$ for all $r \in C_0$, each α_j is in fact an integer of the subfield K of $Q(\rho_q)$. Thus there are rational integers X, U, V, W such that

$$\alpha_0 = \tfrac{1}{4}(X + Ui\sqrt{2q + 2a\sqrt{q}} + Vi\sqrt{2q - 2a\sqrt{q}} + W\sqrt{q}). \tag{4.8}$$

Then applying Lemma 1 and the result $\sigma_r(\alpha_j) = \alpha_{j+s}$ ($r \in C_s$), we obtain

$$\alpha_1 = \frac{1}{4}\left(X - V(-1)^{(b-2)/4}\frac{b}{|b|}i\sqrt{2q+2a\sqrt{q}} + U(-1)^{(b-2)/4}\right.$$
$$\left.\times \frac{b}{|b|}i\sqrt{2q - 2a\sqrt{q}} - W\sqrt{q}\right), \tag{4.9}$$

$$\alpha_2 = \frac{1}{4}(X - Ui\sqrt{2q+2a\sqrt{q}} - Vi\sqrt{2q-2a\sqrt{q}} + W\sqrt{q}), \tag{4.10}$$

$$\alpha_3 = \frac{1}{4}\left(X + V(-1)^{(b-2)/4}\frac{b}{|b|}i\sqrt{2q+2a\sqrt{q}} - U(-1)^{(b-2)/4}\right.$$
$$\left.\times \frac{b}{|b|}i\sqrt{2q - 2a\sqrt{q}} - W\sqrt{q}\right). \tag{4.11}$$

The prime ideal factorization of $g(\chi_P^k)$ in R_{pq} is given by Stickelberger's theorem [14], namely,

$$g(\chi_P^k)\, R_{pq} = \prod_{r=1}^{q-1} \mathscr{P}_r^{(p-1)(1-\{r^{-1}k/q\})},$$

where $\mathscr{P}_r$ is the unique prime ideal in R_{pq} lying above P_r, r^{-1} is the unique integer such that $rr^{-1} \equiv 1 \pmod q$, $0 < r < q$, and $\{y\}$ denotes the fractional part of the real number y. Hence

$$\begin{aligned}
\alpha_j R_{pq} &= \prod_{k \in C_j} \prod_{r=1}^{q-1} \mathscr{P}_r^{(p-1)(1-\{r^{-1}k/q\})} \\
&= \prod_{r=1}^{q-1} \mathscr{P}_r^{(p-1)((q-1)/4 - \sum_{k\in C_j}\{r^{-1}k/q\})} \\
&= \prod_{t=0}^{3} \prod_{r \in C_t} \mathscr{P}_r^{(p-1)((q-1)/4 - \sum_{k\in C_j}\{r^{-1}k/q\})}
\end{aligned}$$

$$= \prod_{t=0}^{3} \prod_{r \in C_t} \mathscr{P}_r^{(p-1)((q-1)/4 - \sum_{k \in C_{j-t}} \{k/q\})}$$

$$= \prod_{t=0}^{3} \prod_{r \in C_t} \mathscr{P}_r^{(p-1)((q-1)/4 - s_{j-t})}$$

$$= \prod_{t=0}^{3} \prod_{r \in C_t} \mathscr{P}_r^{(p-1)s_{j-t+2}},$$

so

$$\alpha_j R_q = \prod_{t=0}^{3} \prod_{r \in C_t} P_r^{s_{j-t+2}} = \prod_{t=0}^{3} Q_t^{s_{j-t+2}}, \tag{4.12}$$

where

$$Q_t = \prod_{r \in C_t} P_r. \tag{4.13}$$

From (4.1) and (4.12) we see that

$$p^{\min_{0 \leqslant t \leqslant 3} s_{j-t+2}} \| \alpha_j,$$

that is,

$$p^{\min_{0 \leqslant k \leqslant 3} s_k} \| \alpha_j,$$

and so by (2.3) we have

$$p^{(q-4h-1)/8} \| \alpha_j \qquad (j = 0, 1, 2, 3). \tag{4.14}$$

Hence there are rational integers x, u, v, w such that

$$X = p^{(q-4h-1)/8} x, \qquad U = p^{(q-4h-1)/8} u, \qquad V = p^{(q-4h-1)/8} v,$$
$$W = p^{(q-4h-1)/8} w, \tag{4.15}$$
$$\text{G.C.D.}\ (x, u, v, w, p) = 1,$$

and so

$$\alpha_0 = \frac{1}{4} p^{(q-4h-1)/8} (x + iu\sqrt{2q + 2a\sqrt{q}} + vi\sqrt{2q - 2a\sqrt{q}}$$
$$+ w\sqrt{q}), \tag{4.16}$$

$$\alpha_1 = \frac{1}{4} p^{(q-4h-1)/8} \left(x - v(-1)^{(b-2)/4} \frac{b}{|b|} i\sqrt{2q + 2a\sqrt{q}} \right.$$
$$\left. + u(-1)^{(b-2)/4} \frac{b}{|b|} i\sqrt{2q - 2a\sqrt{q}} - w\sqrt{q} \right), \tag{4.17}$$

$$\alpha_2 = \frac{1}{4} p^{(q-4h-1)/8} (x - ui\sqrt{2q + 2a\sqrt{q}} - vi\sqrt{2q - 2a\sqrt{q}}$$

$$+ w\sqrt{q}), \tag{4.18}$$

$$\alpha_3 = \frac{1}{4} p^{(q-4h-1)/8} \left(x + v(-1)^{(b-2)/4} \frac{b}{|b|} i\sqrt{2q + 2a\sqrt{q}} \right.$$

$$\left. - u(-1)^{(b-2)/4} \frac{b}{|b|} i\sqrt{2q - 2a\sqrt{q}} - w\sqrt{q} \right). \tag{4.19}$$

Finally, in view of the fundamental property

$$g(\chi_P^k)\,\overline{g(\chi_P^k)} = p \qquad (1 \leqslant k \leqslant q-1),$$

we have by (4.6)

$$\alpha_j \overline{\alpha_j} = p^{(q-1)/4} \qquad (j = 0, 1, 2, 3), \tag{4.20}$$

and so

$$\begin{cases} 16p^h = x^2 + 2qu^2 + 2qv^2 + qw^2, \\ xw = av^2 - 2\,|b|\,uv - au^2, \\ \text{G.C.D. } (x, u, v, w, p) = 1, \end{cases}$$

which is (1.3).

We conclude this section by noting that x satisfies the congruence (1.4). This is clear as, by (4.4), we have

$$g(\chi_P^k) \equiv \sum_{x=1}^{p-1} \rho_p^x \equiv -1 \pmod{1 - \rho_q},$$

and so, by (4.6), for $j = 0, 1, 2, 3$, we have

$$\alpha_j \equiv -1 \pmod{1 - \rho_q}$$

giving (by (4.8)–(4.11))

$$X = \alpha_0 + \alpha_1 + \alpha_2 + \alpha_3 \equiv -4 \pmod{1 - \rho_q}.$$

that is, (by 4.15),

$$x \equiv -4 \pmod{1 - \rho_q},$$

from which (1.4) follows, as the norm of the integer $1 - \rho_q$ of $Q(\rho_q)$ is q.

5. Statement and Proof of Main Theorem

We now state and prove the main result of our paper.

THEOREM. *Let $q > 5$ be a prime such that $q \equiv 5 \pmod 8$. Set $q = a^2 + b^2$ with a and b defined as in* (1.1). *Let $p = qf + 1$ be prime.*

Let s_j, $j = 0, 1, 2, 3$, be defined as in (1.6). It is convenient to distinguish two cases:

Case A. *s_0, s_1, s_2, s_3 not all distinct.* If s_0, s_1, s_2, s_3 are not all distinct then they occur as two pairs of equal values. The smaller of these pairs of values is denoted by $s_m = s_n$, $m \neq n$.

Case B. *s_0, s_1, s_2, s_3 all distinct.* In this case we let s_m denote the smallest value of s_j and let s_n denote the next smallest.

In Case A there exist four solutions, (x, u, v, w), $(x, -u, -v, w)$, $(x, v, -u, -w)$, $(x, -v, u, -w)$, of (1.3) satisfying (1.4) with the properties that $p \nmid (x^2 - qw^2)$, $p \nmid (|b|\, xw + 2quv)$, and that for any of these four solutions we have

$$\prod_{k \in C_m} kf! \equiv \frac{4(-1)^{s_m+1}}{2x + \dfrac{(-1)^{(b-2(n-m))/4}\, abw(x^2 - qw^2)}{(b^2xw + 2\,|b|\, quv)}} \pmod p, \tag{5.1}$$

$$\prod_{k \in C_n} kf! \equiv \frac{4(-1)^{s_m+1}}{2x + \dfrac{(-1)^{(b-2(m-n))/4}\, abw(x^2 - qw^2)}{(b^2xw + 2\,|b|\, quv)}} \pmod p, \tag{5.2}$$

$$\prod_{k \in C_{m+2}} kf! \equiv \frac{(-1)^{s_m}}{4} \left(2x + \frac{(-1)^{(b-2(n-m))/4}\, abw(x^2 - qw^2)}{(b^2xw + 2\,|b|\, quv)}\right) \pmod p, \tag{5.3}$$

$$\prod_{k \in C_{n+2}} kf! \equiv \frac{(-1)^{s_m}}{4} \left(2x + \frac{(-1)^{(b-2(m-n))/4}\, abw(x^2 - qw^2)}{(b^2xw + 2\,|b|\, quv)}\right) \pmod p. \tag{5.4}$$

In Case B there exist four solutions of (1.3) satisfying (1.4) with the properties that $p^{s_n - s_m} \,\|\, (x^2 - qw^2)$, $p^{s_n - s_m} \,\|\, (|b|\, xw + 2quv)$, and that for any of these four solutions we have

$$\prod_{k \in C_m} kf! \equiv \frac{(-1)^{s_m+1}}{x} \pmod p, \tag{5.5}$$

$$\prod_{k \in C_n} kf! \equiv \frac{4(-1)^{s_n+1}}{\left(2x + \dfrac{(-1)^{(b-2(m-n))/4}\, abw(x^2 - qw^2)}{(b^2xw + 2\,|b|\, quv)}\right)\Big/ p^{s_n - s_m}} \pmod p, \tag{5.6}$$

$$\prod_{k \in C_{m+2}} kf! \equiv (-1)^{s_m} x \pmod p, \tag{5.7}$$

$$\prod_{k \in C_{n+2}} kf! \equiv \frac{(-1)^{s_n}}{4p^{s_n - s_m}} \left(2x + \frac{(-1)^{(b-2(m-n))/4}\, abw(x^2 - qw^2)}{(b^2xw + 2\,|b|\, quv)} \right) \pmod p. \tag{5.8}$$

We begin by proving the following congruence: if k is an integer not divisible by q, r is an integer satisfying $1 \leqslant r \leqslant q-1$, and

$$\beta = (p-1)(1 - \{r^{-1}k/q\}), \tag{5.9}$$

then (compare [15, p. 489])

$$\frac{g(\chi_P^k)}{(\rho_p - 1)^{\beta}} \equiv \frac{-1}{\beta!} \pmod{\mathscr{P}_r}. \tag{5.10}$$

Setting $f = (p-1)/q$ we have from (4.3)

$$\chi_P(x) \equiv x^f \pmod{P_1}$$

and so

$$\chi_P(x) \equiv x^{r^{-1}f} \pmod{P_r}, \tag{5.11}$$

where r^{-1} is the unique integer satisfying $rr^{-1} \equiv 1 \pmod q$, $1 \leqslant r^{-1} \leqslant q-1$. Then we have by (4.4) and (5.11)

$$g(\chi_P^k) \equiv \sum_{x=1}^{p-1} x^{r^{-1}kf} \rho_p^x \pmod{\mathscr{P}_r^{p-1}}. \tag{5.12}$$

Next by the binomial theorem we have

$$\rho_p^x = (1 + (\rho_p - 1))^x = \sum_{j=0}^{x} \binom{x}{j} (\rho_p - 1)^j, \tag{5.13}$$

so that from (5.12) and (5.13) we obtain, after interchanging the order of summation,

$$g(\chi_P^k) \equiv \sum_{j=0}^{p-1} (\rho_p - 1)^j \sum_{x=j}^{p-1} x^{r^{-1}kf} \binom{x}{j} \pmod{\mathscr{P}_r^{p-1}}. \tag{5.14}$$

We now consider

$$E(j) = \sum_{x=j}^{p-1} x^{r^{-1}kf} \binom{x}{j}. \tag{5.15}$$

We have

$$E(j) = \sum_{x=1}^{p-1} x^{r^{-1}kf} \frac{x(x-1)\cdots(x-(j-1))}{j!},$$

that is,

$$E(j) = \sum_{x=1}^{p-1} x^{r^{-1}kf} \sum_{m=1}^{j} A_m(j)\, x^m, \tag{5.16}$$

where

$$A_j(j) = \frac{1}{j!}, A_{j-1}(j) = \frac{-1}{2(j-2)!}, \ldots, A_1(j) = \frac{(-1)^{j-1}}{j}. \tag{5.17}$$

Interchanging the order of summation in (5.16), we obtain

$$E(j) = \sum_{m=1}^{j} A_m(j) \sum_{x=1}^{p-1} x^{r^{-1}kf+m}. \tag{5.18}$$

As

$$\sum_{x=1}^{p-1} x^l \equiv \begin{cases} -1 \pmod{p}, & \text{if } l \equiv 0 \pmod{p-1}, \\ 0 \pmod{p}, & \text{if } l \not\equiv 0 \pmod{p-1}, \end{cases} \tag{5.19}$$

we obtain from (5.18) that

$$\begin{aligned} E(j) &\equiv - \sum_{\substack{m=1 \\ r^{-1}kf+m \equiv 0 \pmod{p-1}}}^{j} A_m(j) \pmod{p} \\ &\equiv - \sum_{\substack{u=1 \\ r^{-1}k+u \equiv 0 \pmod{q}}}^{[j/f]} A_{fu}(j) \pmod{p} \\ &\equiv - \sum_{\substack{u=1 \\ u \equiv q(1-\{r^{-1}k/q\}) \pmod{q}}}^{[j/f]} A_{fu}(j) \pmod{p}, \end{aligned}$$

that is

$$E(j) \equiv - \sum_{t=1}^{[1/q[j/f]+\{r^{-1}k/q\}]} A_{f(tq-q\{r^{-1}k/q\})}(j) \pmod{p}. \tag{5.20}$$

Writing $j = fl + m$, with $0 \leqslant m < f$, so that $[j/f] = l$, we have

$$E(fl+m) \equiv - \sum_{t=1}^{[l/q+\{r^{-1}k/q\}]} A_{f(tq-q\{r^{-1}k/q\})}(fl+m) \pmod{p}. \tag{5.21}$$

The sum on the right-hand side of (5.21) is empty unless

$$\left[\frac{l}{q}+\{r^{-1}k/q\}\right]\geqslant 1,$$

that is,

$$\frac{l}{q}+\{r^{-1}k/q\}\geqslant 1, \qquad l\geqslant q(1-\{r^{-1}k/q\}).$$

Thus the smallest value of j for which $E(j)$ is possibly non-zero $(\operatorname{mod} p)$ is given by $l=q(1-\{r^{-1}k/q\})$, $m=0$, that is, $j=(p-1)(1-\{r^{-1}k/q\})=\beta$. Indeed using (5.21) and (5.17), we obtain

$$E(\beta)\equiv -A_\beta(\beta)\equiv -\frac{1}{\beta!}\,(\operatorname{mod} p). \tag{5.22}$$

Then, from (5.14), we obtain

$$g(\chi_P^k)\equiv -\frac{(\rho_p-1)^\beta}{\beta!}\,(\operatorname{mod} \mathscr{P}_r^{\beta+1}). \tag{5.23}$$

Next, from (5.23), we obtain

$$(\rho_p-1)^\beta\left\{\frac{g(\chi_P^k)}{(\rho_p-1)^\beta}+\frac{1}{\beta!}\right\}\equiv 0\ (\operatorname{mod} \mathscr{P}_r^{\beta+1}).$$

As $\mathscr{P}_r\,\|\,\rho_p-1$, $\mathscr{P}_r^\beta\,\|\,(\rho_p-1)^\beta$, we have

$$\mathscr{P}_r\;\Big|\;\frac{g(\chi_P^k)}{(\rho_p-1)^\beta}+\frac{1}{\beta!},$$

giving

$$\frac{g(\chi_P^k)}{(\rho_p-1)^\beta}\equiv -\frac{1}{\beta!}\,(\operatorname{mod} \mathscr{P}_r),$$

which completes the proof of (5.10).

Next we derive the following congruence: for integers j and e we prove

$$\frac{\alpha_j}{p^{s_e}}\equiv\frac{(-1)^{s_e+1}}{\prod_{k\in C_e} kf!}\,(\operatorname{mod} \mathscr{P}_r), \tag{5.24}$$

where $r\in C_{j+2-e}$. From (4.6), (5.9), and (5.10) we have

$$\frac{\alpha_j}{((\rho_p-1)^{p-1})^{(q-1)/4-\sum_{k\in C_j}\{r^{-1}k/q\}}}$$
$$\equiv\frac{-1}{\prod_{k\in C_j}((q-q\{r^{-1}k/q\})f)!}\,(\operatorname{mod} \mathscr{P}_r). \tag{5.25}$$

As $r \in C_{j+2-e}$, we have

$$\sum_{k \in C_j} \{r^{-1}k/q\} = \sum_{k \in C_{e+2}} \{k/q\} = s_{e+2}$$

and

$$\begin{aligned}\prod_{k \in C_j} ((q - q\{r^{-1}k/q\})f)! &= \prod_{k \in C_{e+2}} ((q-k)f)! \\ &= \prod_{k \in C_e} kf!,\end{aligned}$$

and so

$$\frac{\alpha_j}{((\rho_p - 1)^{p-1})^{s_e}} \equiv \frac{-1}{\prod_{k \in C_e} kf!} \pmod{\mathscr{P}_r}, \qquad r \in C_{j+2-e}. \tag{5.26}$$

From the well-known identity

$$p = (\rho_p - 1)(\rho_p^2 - 1) \cdots (\rho_p^{p-1} - 1),$$

we have (as $\rho_p \equiv 1 \pmod{\mathscr{P}_r}$)

$$\begin{aligned}\frac{p}{(\rho_p - 1)^{p-1}} &= (\rho_p + 1)(\rho_p^2 + \rho_p + 1) \cdots (\rho_p^{p-2} + \cdots + 1) \\ &\equiv 2 \cdot 3 \cdots (p-1) \pmod{\mathscr{P}_r},\end{aligned}$$

that is,

$$\frac{p}{(\rho_p - 1)^{p-1}} \equiv -1 \pmod{\mathscr{P}_r}. \tag{5.27}$$

Hence, by (5.26) and (5.27), we have

$$\frac{\alpha_j(-1)^{s_e}}{p^{s_e}} \equiv \frac{-1}{\prod_{k \in C_e} kf!} \pmod{\mathscr{P}_r}, \qquad r \in C_{j+2-e},$$

completing the proof of (5.24).

We next take $j = 0$ in (5.24), obtaining

$$\frac{\alpha_0}{p^{s_e}} \equiv \frac{(-1)^{s_e+1}}{\prod_{k \in C_e} kf!} \pmod{\mathscr{P}_r}, \qquad r \in C_{2-e}. \tag{5.28}$$

Multiplying (5.28) by $p^{s_e - s_m}$, we obtain

$$\frac{\alpha_0}{p^{s_m}} \equiv \frac{(-1)^{s_e+1} p^{s_e-s_m}}{\prod_{k \in C_e} kf!} \pmod{\mathscr{P}_r^{(p-1)(s_e-s_m)+1}}, \tag{5.29}$$

where $r \in C_{2-e}$. Appealing to (2.3), (4.16), and (5.29), we have

$$\begin{aligned} \tfrac{1}{4}(x + ui\sqrt{2q+2a\sqrt{q}} + vi\sqrt{2q-2a\sqrt{q}} + w\sqrt{q}) &= \alpha_0/p^{s_m} \\ &\equiv \frac{(-1)^{s_e+1} p^{s_e-s_m}}{\prod_{k \in C_e} kf!} \pmod{\mathscr{P}_r^{(p-1)(s_e-s_m)+1}}, \end{aligned} \tag{5.30}$$

where $r \in C_{2-e}$ and (x, u, v, w) is a solution of (1.3) satisfying (4.21). Further from (4.18) and (4.12) (with $j = 2$), we have

$$\begin{aligned} \tfrac{1}{4}(x - ui\sqrt{2q+2a\sqrt{q}} - vi\sqrt{2q-2a\sqrt{q}} + w\sqrt{q}) &= \alpha_2/p^{s_m} \\ &\equiv 0 \pmod{\mathscr{P}_r^{(p-1)(s_{e+2}-s_m)}}, \end{aligned} \tag{5.31}$$

where $r \in C_{2-e}$. From this point on, we shall assume that e is either m or n, so that

$$s_e < s_{e+2}. \tag{5.32}$$

From (5.32) we have

$$(p-1)(s_e - s_m) + 1 < (p-1)(s_{e+2} - s_m),$$

so that by (5.30) and (5.31) we obtain

$$\frac{1}{2}(x + w\sqrt{q}) \equiv \frac{(-1)^{s_e+1} p^{s_e-s_m}}{\prod_{k \in C_e} kf!} \pmod{\mathscr{P}_r^{(p-1)(s_e-s_m)+1}}, \tag{5.33}$$

where $r \in C_{2-e}$.

Appealing to (4.12), (4.17), and (4.19), we have

$$\begin{aligned} \mathscr{P}_r^{(p-1)(s_{e-1}-s_m)} \Bigg\| \frac{1}{4}\Bigg(x - v(-1)^{(b-2)/4}\frac{b}{|b|} i\sqrt{2q+2a\sqrt{q}} \\ + u(-1)^{(b-2)/4}\frac{b}{|b|}\sqrt{2q-2a\sqrt{q}} - w\sqrt{q}\Bigg), \end{aligned} \tag{5.34}$$

$$\begin{aligned} \mathscr{P}_r^{(p-1)(s_{e+3}-s_m)} \Bigg\| \frac{1}{4}\Bigg(x + v(-1)^{(b-2)/4}\frac{b}{|b|} i\sqrt{2q+2a\sqrt{q}} \\ - u(-1)^{(b-2)/4}\frac{b}{|b|} i\sqrt{2q-2a\sqrt{q}} - w\sqrt{q}\Bigg), \end{aligned} \tag{5.35}$$

where $r \in C_{2-e}$. Hence, as $s_{e+1} \neq s_{e+3}$, we have

$$\mathscr{P}_r^{(p-1)\min(s_{e+1}-s_m,\, s_{e+3}-s_m)} \| \tfrac{1}{2}(x - w\sqrt{q}), \tag{5.36}$$

where $r \in C_{2-e}$. Thus, in particular, we have:

$$\begin{cases} \textit{Case } \mathrm{A}: \mathscr{P}_r \nmid \tfrac{1}{2}(x - w\sqrt{q}), & r \in C_{2-m} \text{ or } C_{2-n}; \\ \textit{Case } \mathrm{B}: \mathscr{P}_r \nmid \tfrac{1}{2}(x - w\sqrt{q}), & r \in C_{2-n}, \\ \qquad \mathscr{P}_r^{(p-1)(s_n-s_m)} \| \tfrac{1}{2}(x - w\sqrt{q}), & r \in C_{2-m}. \end{cases} \tag{5.37}$$

From (5.33) and (5.37) we see that in Case A

$$\mathscr{P}_r \nmid \tfrac{1}{2}(x + w\sqrt{q}), \qquad \mathscr{P}_r \nmid \tfrac{1}{2}(x - w\sqrt{q}), \qquad r \in C_{2-m} \text{ or } C_{2-n};$$

and that in Case B

$$\begin{cases} \mathscr{P}_r^{(p-1)(s_n-s_m)} \| \tfrac{1}{2}(x + w\sqrt{q}), & \mathscr{P}_r \nmid \tfrac{1}{2}(x - w\sqrt{q}), & r \in C_{2-n}, \\ \mathscr{P}_r \nmid \tfrac{1}{2}(x + w\sqrt{q}), & \mathscr{P}_r^{(p-1)(s_n-s_m)} \| \tfrac{1}{2}(x - w\sqrt{q}), & r \in C_{2-m}. \end{cases}$$

Hence in both cases we have

$$\mathscr{P}_r^{(p-1)(s_n-s_m)} \| \tfrac{1}{4}(x^2 - qw^2), \qquad r \in C_{2-m} \text{ or } C_{2-n}. \tag{5.38}$$

It follows from (1.3), (2.4), and (5.38) that

$$p^{s_n-s_m} \| (x^2 - qw^2), \qquad p^{s_n-s_m} \| x^2 + qu^2 + qv^2. \tag{5.39}$$

Next we show that

$$p^{s_n-s_m} \| (|b| v^2 + 2auv - |b| u^2), \tag{5.40}$$

$$p^{s_n-s_m} \| (|b| xw + 2quv). \tag{5.41}$$

From (5.39) we have that

$$p^{2(s_n-s_m)} \| (x^2 - qw^2)^2 \tag{5.42}$$

and we note that

$$\begin{aligned} &(x^2 - qw^2)^2 \\ &\quad = (x^2 + qw^2)^2 - 4qx^2w^2 \\ &\quad = (16p^h - 2q(u^2 + v^2))^2 - 4q(av^2 - 2|b| uv - au^2)^2 \\ &\quad = 256p^{2h} - 64qp^h(u^2 + v^2) + 4q(|b| v^2 + 2auv - |b| u^2)^2. \end{aligned} \tag{5.43}$$

Appealing to (2.4), (5.42), and (5.43) we see that (5.40) holds. Then, as

$$|b|\,xw + 2quv = a(|b|\,v^2 + 2auv - |b|\,u^2),$$

we have (5.41).

From (5.34) we have

$$\frac{1}{4}\left(x - v(-1)^{(b-2)/4}\frac{b}{|b|}i\sqrt{2q+2a\sqrt{q}} + u(-1)^{(b-2)/4}\right.$$
$$\left.\times\frac{b}{|b|}i\sqrt{2q-2a\sqrt{q}} - w\sqrt{q}\right)$$
$$\equiv \begin{cases} 0 \pmod{\mathscr{P}_r^{(p-1)(s_{n+1}-s_m)}}, & \text{if } r \in C_{2-n}, \\ 0 \pmod{\mathscr{P}_r^{(p-1)(s_{m+1}-s_m)}}, & \text{if } r \in C_{2-m}, \end{cases} \tag{5.44}$$

and from (5.35) we have

$$\frac{1}{4}\left(x + v(-1)^{(b-2)/4}\frac{b}{|b|}i\sqrt{2q+2a\sqrt{q}} - u(-1)^{(b-2)/4}\right.$$
$$\left.\times\frac{b}{|b|}i\sqrt{2q-2a\sqrt{q}} - w\sqrt{q}\right)$$
$$\equiv \begin{cases} 0 \pmod{\mathscr{P}_r^{(p-1)(s_{n+3}-s_m)}}, & \text{if } r \in C_{2-n}, \\ 0 \pmod{\mathscr{P}_r^{(p-1)(s_{m+3}-s_m)}}, & \text{if } r \in C_{2-m}. \end{cases} \tag{5.45}$$

Adding (5.44) (respectively (5.45)) to (5.31) and multiplying by 4, we obtain

$$2x - \left(u + v(-1)^{(b-2)/4}\frac{b}{|b|}\right)i\sqrt{2q+2a\sqrt{q}}$$
$$+ \left(u(-1)^{(b-2)/4}\frac{b}{|b|} - v\right)i\sqrt{2q-2a\sqrt{q}}$$
$$\equiv \begin{cases} 0 \pmod{\mathscr{P}_r^{(p-1)\min(s_{n+1}-s_m,\,s_{n+2}-s_m)}}, & \text{if } r \in C_{2-n}, \\ 0 \pmod{\mathscr{P}_r^{(p-1)\min(s_{m+1}-s_m,\,s_{m+2}-s_m)}}, & \text{if } r \in C_{2-m}, \end{cases} \tag{5.46}$$

and

$$2x - \left(u - v(-1)^{(b-2)/4}\frac{b}{|b|}\right)i\sqrt{2q+2a\sqrt{q}}$$
$$- \left(u(-1)^{(b-2)/4}\frac{b}{|b|} + v\right)i\sqrt{2q-2a\sqrt{q}}$$
$$\equiv \begin{cases} 0 \pmod{\mathscr{P}_r^{(p-1)\min(s_{n+2}-s_m,\,s_{n+3}-s_m)}}, & \text{if } r \in C_{2-n}, \\ 0 \bmod \mathscr{P}_r^{(p-1)\min(s_{m+2}-s_m,\,s_{m+3}-s_m)}), & \text{if } r \in C_{2-m}. \end{cases} \tag{5.47}$$

Appealing to (5.46) we have, after taking $2x$ over to the right-hand side in (5.46) and squaring, that

$$4x^2 \equiv -\left(u + v(-1)^{(b-2)/4}\frac{b}{|b|}\right)^2(2q + 2a\sqrt{q})$$
$$-\left(u(-1)^{(b-2)/4}\frac{b}{|b|} - v\right)^2(2q - 2a\sqrt{q})$$
$$+4\left(u + v(-1)^{(b-2)/4}\frac{b}{|b|}\right)\left(u(-1)^{(b-2)/4}\frac{b}{|b|} - v\right)|b|\sqrt{q}$$
$$\begin{cases}(\operatorname{mod} \mathscr{P}_r^{(p-1)\min(S_{n+1}-S_m, S_{n+2}-S_m)}), & \text{if } r \in C_{2-n},\\ (\operatorname{mod} \mathscr{P}_r^{(p-1)\min(S_{m+1}-S_m, S_{m+2}-S_m)}), & \text{if } r \in C_{2-m}.\end{cases} \tag{5.48}$$

Similarly, appealing to (5.47), we have

$$4x^2 \equiv -\left(u - v(-1)^{(b-2)/4}\frac{b}{|b|}\right)^2(2q + 2a\sqrt{q})$$
$$-\left(u(-1)^{(b-2)/4}\frac{b}{|b|} + v\right)^2(2q - 2a\sqrt{q})$$
$$-4\left(u - v(-1)^{(b-2)/4}\frac{b}{|b|}\right)\left(u(-1)^{(b-2)/4}\frac{b}{|b|} + v\right)|b|\sqrt{q}$$
$$\begin{cases}(\operatorname{mod} \mathscr{P}_r^{(p-1)\min(S_{n+2}-S_m, S_{n+3}-S_m)}), & \text{if } r \in C_{2-n},\\ (\operatorname{mod} \mathscr{P}_r^{(p-1)\min(S_{m+2}-S_m, S_{m+3}-S_m)}), & \text{if } r \in C_{2-m}.\end{cases} \tag{5.49}$$

Simplifying the expression in (5.48) and appealing to (5.40), we have, for each solution (x, u, v, w) of (1.3) satisfying (4.21), that

$$\sqrt{q} \equiv \frac{(-1)^{(b+2/4}(x^2 + qu^2 + qv^2)}{bv^2 + 2a\dfrac{b}{|b|}uv - bu^2}$$
$$\begin{cases}(\operatorname{mod} \mathscr{P}_r^{(p-1)\min(S_{n+1}-S_n, S_{n+2}-S_n)}), & \text{if } r \in C_{2-n},\\ (\operatorname{mod} \mathscr{P}_r^{(p-1)\min(S_{m+1}-S_n, S_{m+2}-S_n)}), & \text{if } r \in C_{2-m}.\end{cases} \tag{5.50}$$

Similarly, simplifying the expression in (5.49) we have

$$\sqrt{q} \equiv \frac{(-1)^{(b-2)/4}(x^2 + qu^2 + qv^2)}{bv^2 + 2a\dfrac{b}{|b|}uv - bu^2}$$
$$\begin{cases}(\operatorname{mod} \mathscr{P}_r^{(p-1)\min(S_{n+2}-S_n, S_{n+3}-S_n)}), & \text{if } r \in C_{2-n},\\ (\operatorname{mod} \mathscr{P}_r^{(p-1)\min(S_{m+2}-S_n, S_{m+3}-S_n)}), & \text{if } r \in C_{2-m}.\end{cases} \tag{5.51}$$

From (1.3) we have

$$x^2 + qu^2 + qv^2 \equiv \tfrac{1}{2}(x^2 - qw^2) (\operatorname{mod} p^h)$$

and

$$\frac{bxw}{a} + \frac{2bquv}{|b|\,a} = bv^2 + \frac{2ab}{|b|} uv - bu^2,$$

so that (5.50) and (5.51) become

$$\sqrt{q} \equiv \frac{(-1)^{(b+2)/4}\, a(x^2 - qw^2)}{2\left(bxw + 2\dfrac{b}{|b|} quv\right)} \begin{cases} (\operatorname{mod} \mathscr{P}_r^{(p-1)\min(S_{n+1}-S_n, S_{n+2}-S_n)}), & \text{if } r \in C_{2-n}, \\ (\operatorname{mod} \mathscr{P}_r^{(p-1)\min(S_{m+1}-S_n, S_{m+2}-S_n)}), & \text{if } r \in C_{2-m}, \end{cases} \tag{5.52}$$

$$\sqrt{q} \equiv \frac{(-1)^{(b-2)/4}\, a(x^2 - qw^2)}{2\left(bxw + 2\dfrac{b}{|b|} quv\right)} \begin{cases} (\operatorname{mod} \mathscr{P}_r^{(p-1)\min(S_{n+2}-S_n, S_{n+3}-S_n)}), & \text{if } r \in C_{2-n}, \\ (\operatorname{mod} \mathscr{P}_r^{(p-1)\min(S_{m+2}-S_n, S_{m+3}-S_n)}), & \text{if } r \in C_{2-m}. \end{cases} \tag{5.53}$$

We now restrict our attention to Case A. As the values of s_j in this case appear as two equal pairs of values with s_j and s_{j+2} distinct for $j = 0, 1, 2, 3$ we deduce that $n = m + 1$ or $n = m + 3$. Hence

$$\begin{aligned} \min(s_{n+1} - s_n, s_{n+2} - s_n) &= \begin{cases} s_{n+2} - s_n \geqslant 1, & \text{if } n = m+1, \\ 0, & \text{if } n = m+3, \end{cases} \\ \min(s_{m+1} - s_n, s_{m+2} - s_n) &= \begin{cases} 0, & \text{if } n = m+1, \\ s_{n+2} - s_n \geqslant 1, & \text{if } n = m+3, \end{cases} \\ \min(s_{n+2} - s_n, s_{n+3} - s_n) &= \begin{cases} 0 & \text{if } n = m+1, \\ s_{n+2} - s_n \geqslant 1, & \text{if } n = m+3, \end{cases} \\ \min(s_{m+2} - s_n, s_{m+3} - s_n) &= \begin{cases} s_{n+2} - s_n \geqslant 1, & \text{if } n = m+1, \\ 0, & \text{if } n = m+3. \end{cases} \end{aligned} \tag{5.54}$$

From (5.52), (5.53), and (5.54), we see that

$$\sqrt{q} \equiv \begin{cases} \dfrac{(-1)^{(m-n-1)/2}\, (-1)^{(b-2)/4}\, a(x^2 - qw^2)}{2\left(bxw + 2\dfrac{b}{|b|} quv\right)} (\operatorname{mod} \mathscr{P}_r), & \text{if } r \in C_{2-n}, \\ \dfrac{(-1)^{(n-m-1)/2}\, (-1)^{(b-2)/4}\, a(x^2 - qw^2)}{2\left(bxw + 2\dfrac{b}{|b|} quv\right)} (\operatorname{mod} \mathscr{P}_r), & \text{if } r \in C_{2-m}. \end{cases} \tag{5.55}$$

Substituting (5.55) into (5.33) we obtain

$$\begin{aligned} &\frac{x}{2}+\frac{w}{4}\frac{(-1)^{(b-2(m-n))/4}\,a(x^2-qw^2)}{\left(bxw+2\dfrac{b}{|b|}quv\right)} \\ &\qquad \equiv \frac{(-1)^{s_n+1}}{\prod_{k\in C_n} kf!} \pmod{\mathscr{P}_r}, \qquad \text{if } r\in C_{2-n}, \\ &\frac{x}{2}+\frac{w}{4}\frac{(-1)^{(b-2(n-m))/4}\,a(x^2-qw^2)}{\left(bxw+2\dfrac{b}{|b|}quv\right)} \\ &\qquad \equiv \frac{(-1)^{s_m+1}}{\prod_{k\in C_m} kf!} \pmod{\mathscr{P}_r}, \qquad \text{if } r\in C_{2-m}. \end{aligned} \tag{5.56}$$

As both sides of the congruences in (5.56) are rational integers, the required congruences (5.1) and (5.2) follow immediately.

Next, a simple modificaton of Wilson's theorem yields for positive integers c and d satisfying $c+d=q$,

$$cf!\,df! \equiv (-1)^{cf-1} \equiv (-1)^{df-1} \pmod{p}, \tag{5.57}$$

so that, as $(q-1)/4$ is odd, we have

$$\frac{-1}{\prod_{k\in C_j} kf!} \equiv \prod_{k\in C_{j+2}} kf! \pmod{p} \qquad (j=0,1,2,3). \tag{5.58}$$

Using (5.58), the congruences (5.3) and (5.4) now follow from (5.1) and (5.2).

We note that the expressions on the right-hand sides of (5.1)–(5.4) are independent of the choice of solution (x, u, v, w), $(x, -u, -v, w)$, $(x, v, -u, -w)$, or $(x, -u, v, -w)$ for which our Theorem holds.

We observe that from (5.39) and (5.41) we have $p \nmid (x^2-qw^2)$ and $p \nmid |b|xw+2quv$, completing the proof of our Theorem in Case A.

Next we turn our attention to Case B. We begin by determining

$$\prod_{k\in C_m} kf! \pmod{p} \qquad \text{and} \qquad \prod_{k\in C_{m+2}} kf! \pmod{p}.$$

From (5.33), with $e=m$, we have

$$\frac{1}{2}(x+w\sqrt{q}) \equiv \frac{(-1)^{s_m+1}}{\prod_{k\in C_m} kf!} \pmod{\mathscr{P}_r}, \qquad r\in C_{2-m}. \tag{5.59}$$

From (5.37) we have (as $s_n > s_m$ in this case) that

$$\tfrac{1}{2}(x - w\sqrt{q}) \equiv 0 \pmod{\mathscr{P}_r}, \qquad r \in C_{2-m}. \tag{5.60}$$

Adding (5.59) and (5.60) we obtain

$$x \equiv \frac{(-1)^{s_m+1}}{\prod_{k\in C_m} kf!} \pmod{\mathscr{P}_r}, \qquad r \in C_{2-m}. \tag{5.61}$$

As the expressions on the left- and right-hand sides of the congruence (5.61) are rational integers (mod p), we obtain

$$\prod_{k\in C_m} kf! \equiv \frac{(-1)^{s_m+1}}{x} \pmod{p},$$

which is (5.5). In view of (5.58) we also have

$$\prod_{k\in C_{m+2}} kf! \equiv (-1)^{s_m} x \pmod{p},$$

which is (5.7). Finally, we determine

$$\prod_{k\in C_n} kf! \pmod{p} \qquad \text{and} \qquad \prod_{k\in C_{n+2}} kf! \pmod{p}.$$

To obtain this determination we use (5.33) with $e = n$, that is, with $r \in C_{2-n}$. This case is more complicated as both sides of the congruence (5.33) contain positive powers of $\mathscr{P}_r$ and it is necessary to determine the exact power of $\mathscr{P}_r$ dividing both sides of the congruence. In this case we have $s_m < s_n < s_{n+2} < s_{m+2}$ with $n = m+1$ or $n = m+3$. Hence we have

$$\begin{aligned} \min(s_{n+1} - s_n, s_{n+2} - s_n) &= s_{n+2} - s_n \geqslant 1, && \text{if } n = m+1, \\ \min(s_{n+2} - s_n, s_{n+3} - s_n) &= s_{n+2} - s_n \geqslant 1, && \text{if } n = m+3, \end{aligned} \tag{5.62}$$

and so by (5.52), (5.53), and (5.62) we have

$$\sqrt{q} \equiv \frac{(-1)^{(b-2(m-n))/4}\, a(x^2 - qw^2)}{2\left(bxw + 2\dfrac{b}{|b|}quv\right)} \pmod{\mathscr{P}_r}, \qquad r \in C_{2-n}. \tag{5.63}$$

However, we need to determine $\sqrt{q}$ modulo $\mathscr{P}_r^{(p-1)(s_n-s_m)+1}$ in order to be able to use (5.63) in (5.33).

Defining an integer E by

$$E \equiv \frac{(-1)^{(b-2(m-n))/4}\, a(x^2 - qw^2)}{2\left(bxw + 2\dfrac{b}{|b|}quv\right)} \pmod{p^h}, \tag{5.64}$$

we have from (5.43) that

$$E^2 \equiv q \pmod{p^h},$$

so that for $r \in C_{2-n}$ we have

$$\mathscr{P}_r^{(p-1)h} | (\sqrt{q} - E)(\sqrt{q} + E).$$

Moreover, in $Q(\rho_{pq})$, we have from (5.63) that $\mathscr{P}_r | \sqrt{q} - E$, and, consequently, $\mathscr{P}_r \nmid \sqrt{q} + E$.

Thus, for $r \in C_{2-n}$ we have $\sqrt{q} \equiv E \pmod{p_r^{(p-1)h}}$, and trivially $(p-1)\,h \geqslant (p-1)(s_n - s_m) + 1$ by (1.4), so that

$$\sqrt{q} \equiv \frac{(-1)^{(b-2(m-n))/4}\, a(x^2 - qw^2)}{2\left(bxw + 2\dfrac{b}{|b|}quv\right)} \pmod{\mathscr{P}_r^{(p-1)(s_n - s_m)+1}}. \tag{5.65}$$

Using this expression for $\sqrt{q}$ in (5.33) we obtain

$$\begin{aligned} &\frac{x}{2} + \frac{w}{4}\,\frac{(-1)^{(b-2(m-n))/4}\, a(x^2 - qw^2)}{\left(bxw + 2\dfrac{b}{|b|}quv\right)} \\ &\equiv \frac{(-1)^{s_n+1}\, p^{s_n - s_m}}{\prod_{k \in C_n} kf!} \pmod{\mathscr{P}_r^{(p-1)(s_n - s_m)+1}}. \end{aligned} \tag{5.66}$$

As the left- and right-hand sides of (5.66) are rational integers and the integers of $Q(\rho_{pq})$ can be factored uniquely as products of prime ideals, we obtain

$$\begin{aligned} &\frac{x}{2} + \frac{w}{4}\,\frac{(-1)^{(b-2(m-n))/4}\, a(x^2 - qw^2)}{\left(bxw + 2\dfrac{b}{|b|}quv\right)} \\ &\equiv \frac{(-1)^{s_n+1}\, p^{s_n - s_m}}{\prod\limits_{k \in C_n} kf!} \pmod{p^{s_n - s_m + 1}}. \end{aligned} \tag{5.67}$$

Now (5.6) follows immediately from (5.67), and (5.8) follows upon applying (5.57). Finally, from (5.39) and (5.41) we have

$$p^{s_n - s_m} \| (x^2 - qw^2), \qquad p^{s_n - s_m} \| (|b|xw + 2quv),$$

completing the proof of our Theorem.

6. Solution of the System (1.3)–(1.4) when $h = 1$

When $h = 1$ (this includes all $q \leqslant 61$) we show that the Diophantine system (1.3)–(1.4) has precisely four solutions. If (x, u, v, w) is one of these, the others are $(x, -u, -v, w)$, $(x, v, -u, -w)$, and $(x, -v, u, -w)$. This implies that when $h = 1$ we may use any solution of (1.3)–(1.4) when applying the Theorem in Section 5.

From Section 4 we know that (1.3)–(1.4) is solvable in integers. Let (x, u, v, w) and (x', u', v', w') be any two solutions of this system. We set

$$\begin{aligned} \gamma &= \tfrac{1}{4} p^{(q-5)/8}\left(x + iu\sqrt{2q + 2a\sqrt{q}} + iv\sqrt{2q - 2a\sqrt{q}} + w\sqrt{q}\right), \\ \gamma' &= \tfrac{1}{4} p^{(q-5)/8}\left(x' + iu'\sqrt{2q + 2a\sqrt{q}} + iv'\sqrt{2q - 2a\sqrt{q}} + w'\sqrt{q}\right), \end{aligned} \tag{6.1}$$

and note that γ and γ' are integers of K satisfying

$$\gamma\bar{\gamma} = \gamma'\bar{\gamma}' = p^{(q-1)/4}, \qquad p^{(q-5)/8} \parallel \gamma, \qquad p^{(q-5)/8} \parallel \gamma'. \tag{6.2}$$

From (6.2) we see that the only prime ideals of R_q dividing the principal ideals γR_q and $\gamma' R_q$ must divide p, so that the P_i are the only prime ideals dividing γR_q and $\gamma' R_q$. Let γ_1 denote either of γ, γ'. We have

$$\gamma_1 R_q = P_1^{c_1} \cdots P_{q-1}^{c_{q-1}}, \tag{6.3}$$

for non-negative integers c_i. As $\gamma_1 \in K$, we have

$$\sigma_r(\gamma_1 R_q) = \gamma_1 R_q, \qquad r \in C_0, \tag{6.4}$$

so from (6.3) we obtain

$$c_s = u_i \qquad \text{for all } s \in C_i \ (i = 0, 1, 2, 3), \tag{6.5}$$

that is,

$$\gamma_1 R_q = \prod_{i=0}^{3} \left(\prod_{s \in C_i} P_s \right)^{u_i}. \tag{6.6}$$

From (6.6) we have

$$\bar{\gamma}_1 R_q = \prod_{i=0}^{3} \left(\prod_{s \in C_i} P_s \right)^{u_{i+2}}. \tag{6.7}$$

Multiplying (6.6) and (6.7) together and appealing to (6.2), we obtain (as $pR_q = P_1 \cdots P_{q-1}$) that

$$u_0 + u_2 = u_1 + u_3 = (q-1)/4. \tag{6.8}$$

Also from (6.2) and (6.6) we see that

$$\min_{0 \leqslant i \leqslant 3} u_i = (q-5)/8. \tag{6.9}$$

There are exactly four 4-tuples (u_0, u_1, u_2, u_3) satisfying (6.8) and (6.9), given by

u_0	u_1	u_2	u_3
$(q-5)/8$	$(q-5)/8$	$(q+3)/8$	$(q+3)/8$
$(q-5)/8$	$(q+3)/8$	$(q+3)/8$	$(q-5)/8$
$(q+3)/8$	$(q-5)/8$	$(q-5)/8$	$(q+3)/8$
$(q+3)/8$	$(q+3)/8$	$(q-5)/8$	$(q-5)/8$

One of these four possibilities gives the exponents in the prime ideal decomposition (6.6) of γR_q. The other three give those for $\sigma_s(\gamma) R_q$ $(s \in C_1, C_2, C_3)$. Since the exponents in the prime ideal decomposition of $\gamma' R_q$ must also be given by one of the four possibilities above, we have

$$\gamma' R_q = \sigma_s(\gamma) R_q, \qquad \text{for some } s.$$

As γ' and $\sigma_s(\gamma)$ both belong in R_K we have

$$\gamma' R_K = \sigma_s(\gamma) R_K.$$

Further, as ± 1 are the only units in R_K [5, p. 4], we have $\gamma' = \pm\sigma_s(\gamma)$. Since the rational parts of both $\gamma'/\frac{1}{4}p^{(q-5)/8}$ and $\sigma_s(\gamma)/\frac{1}{4}p^{(q-5)/8}$ are congruent to -4 modulo q, we must have $\gamma' = \sigma_s(\gamma)$. This completes the proof that there are only four solutions to (1.3)–(1.4) when $h = 1$.

We note that when $q = 13$, this resolves in the affirmative a conjecture of Muskat and Zee [11, p. 19]. When $h > 1$, numerical evidence would appear to suggest that if h is the least exponent for which the system (1.3)–(1.4) is solvable then it has exactly four solutions.

7. Binomial Coefficients (mod p) and Numerical Examples

As Smith [13] has noted, the results of Cauchy [3] and Jacobi [7] greatly generalize the results of earlier authors who determined certain binomial coefficients $\binom{rf}{sf}$ $(1 \leqslant s < r \leqslant q-1)$ modulo p. For quaternary quadratic systems similar to or coinciding with (1.3) when $h = 1$, congruences (mod p) for certain binomial coefficients have been given by Emma Lehmer [8] and by Hudson and Williams [6, Theorems 16.1 and 19.3].

In this section we use (5.57) to reformulate our theorem in terms of binomial coefficients for certain small values of q. We also give three numerical examples. (See Examples 7.1, 7.2, and 7.3.)

For $5 < q \leqslant 61$ (then $h(K) = 1$; see [12]) there are, by Section 6, exactly four solutions to (1.3)–(1.4) and we have the following corollary.

COROLLARY. *Let (x, u, v, w) be any solution of the system* (1.3)–(1.4) *with $h = 1$, $q \leqslant 61$. Then we have*

$$\binom{4f}{f} \equiv -\frac{x}{2} + \frac{3(x^2 - 13w^2)\,w}{8(xw + 13uv)} \pmod{p = 13f + 1}, \tag{7.1}$$

$$\binom{7f}{2f} \equiv -\frac{x}{2} - \frac{3(x^2 - 13w^2)\,w}{8(xw + 13uv)} \pmod{p = 13f + 1}, \tag{7.2}$$

$$\frac{\binom{13f}{4f}\binom{16f}{5f}\binom{11f}{5f}}{\binom{8f}{f}\binom{13f}{5f}} \equiv -\frac{x}{2} + \frac{5(x^2 - 29w^2)\,w}{8(xw + 29uv)} \pmod{p = 29f + 1}, \tag{7.3}$$

$$\frac{\binom{5f}{2f}\binom{15f}{4f}\binom{16f}{5f}}{\binom{18f}{8f}\binom{16f}{4f}} \equiv -\frac{x}{2} - \frac{5(x^2 - 29w^2)\,w}{8(xw + 29uv)} \pmod{p = 29f + 1}, \tag{7.4}$$

$$\frac{\binom{11f}{f}\binom{21f}{9f}}{\binom{7f}{3f}} \equiv -\frac{x}{2} - \frac{(x^2 - 37w^2)\,w}{8(3xw + 37uv)} \pmod{p = 37f + 1}, \tag{7.5}$$

$$\frac{\binom{14f}{6f}\binom{18f}{5f}}{\binom{17f}{2f}} \equiv -\frac{x}{2} + \frac{(x^2 - 37w^2)\,w}{8(3xw + 37uv)} \pmod{p = 37f + 1}, \tag{7.6}$$

$$\frac{\binom{28f}{11f}\binom{16f}{7f}\binom{10f}{4f}\binom{24f}{10f}}{\binom{11f}{f}\binom{28f}{13f}\binom{25f}{11f}} \equiv -\frac{x}{2} + \frac{7(x^2 - 53w^2)\,w}{8(xw + 53uv)} \pmod{p = 53f + 1}, \tag{7.7}$$

$$\frac{\binom{13f}{5f}\binom{26f}{12f}\binom{26f}{3f}\binom{31f}{10f}\binom{27f}{13f}}{\binom{18f}{10f}\binom{5f}{2f}\binom{33f}{19f}\binom{8f}{3f}}$$

$$\equiv -\frac{x}{2} - \frac{7(x^2-53w^2)\,w}{8(xw+53uv)} \pmod{p = 53f+1}, \tag{7.8}$$

$$\frac{\binom{14f}{f}\binom{27f}{12f}\binom{36f}{16f}}{\binom{9f}{4f}\binom{22f}{3f}} \equiv -\frac{x}{2} - \frac{5(x^2-61w^2)\,w}{8(3xw+61uv)} \pmod{p = 61f+1}, \tag{7.9}$$

$$\frac{\binom{18f}{8f}\binom{23f}{6f}\binom{32f}{11f}}{\binom{28f}{2f}\binom{31f}{7f}} \equiv -\frac{x}{2} + \frac{5(x^2-61w^2)\,w}{8(3xw+61uv)} \pmod{p = 61f+1}. \tag{7.10}$$

Remarks. The congruences (7.1) and (7.2) were established in [6, Theorem 16.1]. Each binomial coefficient in (7.1)–(7.10) is selected to be a representative binomial coefficient of order q as defined in [6, Sect. 2].

The above corollary was originally proved using Jacobi sums but this method appears difficult to extend to arbitrary q. We note that this approach explains why the number of binomial coefficients in the numerator plus those in the denominator in (7.1)–(7.10) is precisely $(q-1)/12$ if and only if $q \equiv 13 \pmod{24}$. Lastly, we remark that the number of binomial coefficients in (7.7) and (7.8) differs because of cancellation of a binomial coefficient in the former congruence.

Congruences for binomial coefficients like the above may be derived when $q \geqslant 101$ although the derivation is somewhat tedious. The following three examples illustrate some of the possibilities which arise when applying the Theorem in Section 5. Examples 7.1 and 7.2, which we give both in terms of factorials and in terms of binomial coefficients $(\bmod\, p)$, illustrate Case B. In Example 7.1 the least exponent for which (1.3) is solvable is $h = 3$ and numerical data indicate that there are only four solutions of (1.3)–(1.4). In Example 7.2 the least exponent for which (1.3) is solvable is 1 (although $h = 3$). In this example there are twelve solutions of (1.3)–(1.4). The congruences (5.1)–(5.8) hold for exactly four of these twelve solutions. Finally, Example 7.3 illustrates Case A. Case A can occur only if $h(K)/h(Q(\sqrt{q}))$ is a perfect square but the converse may not be true (see, e.g., Tables I and II for $q = 181$).

TABLE I

Values of $h^*(K) = h(K)/h(Q(\sqrt{q}))$, $5 < q < 1000$

q	$h^*(K)$	q	$h^*(K)$	q	$h^*(K)$
13	1	277	17	661	9
29	1	293	9	677	25
37	1	317	13	701	25
53	1	349	5	709	61
61	1	373	5	733	45
101	5	389	41	757	125
109	17	397	13	773	29
149	9	421	25	797	37
157	5	461	25	821	17
173	5	509	13	829	145
181	25	541	61	853	17
197	5	557	13	877	37
229	17	613	25	941	41
269	13	653	25	997	25

TABLE II

Values of s_j, $j = 0, 1, 2, 3$, for $5 < q < 300$

q	s_0	s_1	s_2	s_3	q	s_0	s_1	s_2	s_3
13	1	1	2	2	157	19	18	20	21
29	4	3	3	4	173	23	22	20	21
37	4	5	5	4	181	19	22	26	23
53	7	7	6	6	197	25	26	24	23
61	7	8	8	7	229	27	26	30	31
101	14	12	11	13	269	31	34	36	33
109	11	12	16	15	277	36	32	33	37
149	17	17	20	20	293	35	38	38	35

EXAMPLE 7.1. Let $q = 101$ ($a = 1$, $b = -10$), $p = 607$, so that $p^2 = 368449$. Then $s_0 = 14$, $s_1 = 12$, $s_2 = 11$, $s_3 = 13$ so that h in (1.3) is equal to 3. We note that (1.3) is not solvable if h is replaced by any exponent less than 3, and that there are exactly four solutions when $h = 3$ and $x \equiv -4 \pmod{q}$, namely, $(x, u, v, w) = (-8185, -966, 1971, -5013)$, together with the three solutions $(x, -u, -v, w)$, $(x, v, -u, -w)$, and $(x, -u, v, -w)$.

It is easily checked that for this solution we have $p \| (x^2 - qw^2)$ and $p \| (|b|\, xw + 2quv)$. Consequently, our Theorem asserts that, with $f = 6$, we have

$$\frac{(-1)^{11}}{\prod_{k\in C_2} kf!} \equiv \frac{\binom{53f}{4f}\binom{54f}{9f}\binom{46f}{13f}\binom{44f}{14f}\binom{40f}{17f}\binom{42f}{20f}\binom{95f}{42f}\binom{94f}{40f}\binom{90f}{44f}\binom{60f}{21f}}{\binom{6f}{f}\binom{47f}{16f}\binom{43f}{19f}\binom{18f}{7f}\binom{62f}{25f}\binom{54f}{18f}\binom{60f}{6f}}$$

$$\equiv 8185 \equiv 294 \pmod{607}.$$

We have verified this congruence by direct computation.

Moreover we must have, with $f = 6$, that

$$\frac{(-1)^{12}}{\prod_{k\in C_1} kf!} \equiv \frac{\binom{12f}{2f}\binom{18f}{7f}\binom{44f}{3f}\binom{27f}{15f}\binom{39f}{7f}\binom{42f}{7f}\binom{12f}{4f}}{\binom{48f}{8f}\binom{55f}{26f}\binom{38f}{4f}\binom{50f}{22f}\binom{22f}{7f}\binom{15f}{7f}}$$

$$\equiv 302 \pmod{607},$$

$$\frac{(-1)^{12}}{\prod_{k\in C_1} kf!} \equiv \frac{1}{607}\left(\frac{8185}{2} + \frac{(34599)(-5013)}{8(299381 - 340657)}\right) \equiv \frac{183314}{607}$$

$$\equiv 302 \pmod{607}.$$

EXAMPLE 7.2. Let $q = 157$ $(a = -11,\ b = -6)$, $p = 1571$, so that $p^2 = 2468041$. Then $s_0 = 19$, $s_1 = 18$, $s_2 = 20$, $s_3 = 21$ so that $h = 3$ in (1.3). However, in this case (1.3) is solvable if h is replaced by 1. There are (as a consequence which will be discussed elsewhere) 12 solutions of (1.3) with $h = 3$. Among these is the solution $(x, u, v, w) = (-23868, -3254, -8570, -14948)$. For this solution we again have $p \,\|\, (x^2 - qw^2)$ and $p \,\|\, (|b|\, xw + 2quv)$. Thus the Theorem in Section 5 together with (5.58) yields, with $f = 10$, that

$$\frac{(-1)^{18}}{\prod_{k\in C_1} kf!} \equiv \frac{\binom{133f}{2f}\binom{98f}{18f}\binom{97f}{5f}\binom{63f}{29f}\binom{135f}{28f}\binom{88f}{43f}\binom{116f}{21f}\binom{102f}{32f}}{\binom{38f}{15f}\binom{73f}{7f}\binom{149f}{53f}\binom{85f}{6f}\binom{137f}{54f}}$$

$$\equiv 23868 \equiv 303 \pmod{1571}.$$

Moreover

$$\frac{(-1)^{19}}{\prod_{k\in C_1} kf!} \equiv \frac{\binom{145f}{f}\binom{49f}{9f}\binom{127f}{46f}\binom{110f}{17f}\binom{86f}{19f}\binom{146f}{14f}\binom{51f}{16f}}{\binom{100f}{44f}\binom{115f}{33f}\binom{135f}{48f}\binom{121f}{3f}\binom{147f}{27f}\binom{126f}{58f}}$$

$$\equiv 1090 \pmod{1571},$$

$$\frac{(-1)^{19}}{\prod_{k\in C_0} kf!} \equiv \frac{1}{1571}\left(\frac{23868}{2} - \frac{11(2031994-2237795)(-14948)}{8(1674839+2387767)}\right)$$
$$\equiv \frac{1712390}{1571} \equiv 1090 \pmod{1571}.$$

EXAMPLE 7.3. Let $q = 149$ ($a = -7$, $b = -10$), $p = 1193$. Then $s_0 = 17$, $s_1 = 17$, $s_2 = 20$, $s_3 = 20$ and (as $s_2 - s_0 = s_3 - s_1$) we are in Case A. Note that for this example (1.3) is not solvable if h is replaced by 1 or 2 and that we have four solutions with $h = 3$ and $x \equiv -4 \pmod{q}$ as in Example 7.1. Taking any one of these, say,

$$(x, u, v, w) = (2380, 2744, 8824, 3392),$$

we have

$$\frac{-2380}{2} \pm \frac{-7(36-550)(3392)}{8(838+9)}$$
$$\equiv 3 \pm \frac{26}{811} \equiv 690 \quad \text{or} \quad 509 \pmod{1193}.$$

Indeed, we have verified by direct computation that

$$\frac{(-1)^{17}}{\prod_{k\in C_1} kf!} \equiv 690 \pmod{1193} \quad \text{and} \quad \frac{(-1)^{17}}{\prod_{k\in C_0} kf!} \equiv 509 \pmod{1193}.$$

REFERENCES

1. B. C. BERNDT, Sums of Gauss, Jacobi, and Jacobsthal, *J. Number Theory* **11**(1979), 349–398.
2. B. C. BERNDT AND R. J. EVANS, The determination of Gauss sums, *Bull. Amer. Math. Soc.* **5** (1981), 107–129.
3. L'AUGUSTIN CAUCHY, Mémoire sur la théorie des nombres, *Mém. Inst. France* **17** (1840), 249–768 (Oeuvres completés (1) 3(1911), pp. 5–83).
4. L. E. DICKSON, Cyclotomy and trinomial congruences, *Trans. Amer. Math. Soc.* **37** (1935), 363–380.
5. R. H. HUDSON AND K. S. WILLIAMS, A class number formula for certain quartic fields, Carleton Mathematical Series No. 174, 1981, Carleton University, Ottawa.
6. R. H. HUDSON AND K. S. WILLIAMS, On Jacobi sums and binomial coefficients, *Trans. Amer. Math. Soc.* **281** (1984), 431–505.
7. C. G. J. JACOBI, Über die Kreistheilung und ihre Anwending auf die Zahlentheorie, *J. für Math.* **30** (1846), 166–182.
8. E. LEHMER, On Euler's criterion, *J. Austral. Math. Soc.* **1** (1959), 64–70.
9. J. H. LOXTON, Some conjectures concerning Gauss sums, *J. Reine Angew. Math.* **297**(1978), 153–158.

10. C. R. MATTHEWS, Gauss sums and elliptic functions. II. The quartic sum, *Invent. Math.* **54** (1979), 23–52.
11. J. B. MUSKAT AND YUN-CHENG ZEE, On the uniqueness of solutions of certain Diophantine equations, *Proc. Amer. Math. Soc.* **49** (1975), 13–19.
12. B. SETZER, The determination of all imaginary, quartic, Abelian number fields with class number 1, *Math. Comp.* **35** (1980), 1383–1386.
13. H. J. S. SMITH, "Report on the Theory of Numbers," Chelsea, New York, 1964.
14. L. STICKELBERGER, Ueber eine Verallemeinerung der Kreisteilung, *Math. Ann.* **37** (1890), 321–367.
15. K. YAMAMOTO, On a conjecture of Hasse concerning multiplicative relations of Gaussian sums, *J. Combin. Theory* **1** (1966), 476–489.