Finite Fields and Their Applications **7,** 110–124 (2001)
doi.10.1006/ffta.2000.0289, available online at http://www.idealibrary.com on IDEAL®

Classical Congruences for Parameters in Binary Quadratic Forms

Ronald Evans

Department of Mathematics, 0112, University of California at San Diego, La Jolla, California 92093-0112
E-mail: revans@ucsd.edu

Communicated by Daqing Wan

Received January 12, 2000; revised April 19, 2000; published online November 21, 2000

Let $\mathbb{Q}(\sqrt{-k})$ be an imaginary quadratic field with discriminant $-k$ and class number h, with $k \neq 3, 4$, or 8. Let p be a prime such that $(\frac{-k}{p}) = 1$. There are integers C, D, unique up to sign, such that $4p^h = C^2 + kD^2$, $p \nmid C$. Stickelberger gave a congruence for C modulo p which extends congruences of Gauss, Jacobi, and Eisenstein. Stickelberger also gave a simultaneous congruence for C modulo k, but only for *prime* k. We prove an extension of his result that holds for all k, giving along the way an exposition of his work. © 2000 Academic Press

1. INTRODUCTION

Let $-k$ be a negative fundamental discriminant, so that $\mathbb{Q}(\sqrt{-k})$ is an imaginary quadratic field of discriminant $-k$. Let h be the class number of $\mathbb{Q}(\sqrt{-k})$. Write

$$U = \left\{0 < u < k \colon \left(\frac{-k}{u}\right) = 1\right\}, \tag{1.1}$$

where $(\frac{-k}{*})$ is the Kronecker symbol.

In 1890, Stickelberger [5] proved the following elegant theorem.

Theorem 1.1. *Let $\mathbb{Q}(\sqrt{-k})$ be an imaginary quadratic field of discriminant $-k$ and class number h. Assume that $k \neq 3, 4$, or 8. Let p be a prime such that*

$(\frac{-k}{p}) = 1$. *Then there are integers* C, D, *unique up to sign, for which*

$$4p^h = C^2 + kD^2, \quad p \nmid C. \tag{1.2}$$

Moreover, one of the two choices of C (*exactly one, if* $p > 2$) *satisfies the congruence*

$$C \equiv \prod_{u \in U} [pu/k]!^{-1} \pmod{p}, \tag{1.3}$$

where $[x]$ *denotes the greatest integer* $\leq x$ *and* U *is defined by* (1.1).

EXAMPLE 1.2. Let $k = 23$, so that $h = 3$. Choose $p = 59$. Then $(\frac{-k}{p}) = (\frac{-23}{59}) = 1$ and $4p^3 = 821516 = C^2 + 23D^2$ with $C = \pm 396$, $D = \pm 170$. We have $U = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}$, and (1.3) holds with $C = -396$.

In the special case $p \equiv 1 (\operatorname{mod} k)$, Theorem 1.1 was proved by Cauchy and Jacobi; see Smith [4, p. 271]. A proof for $k = 7$ was completed by Eisenstein; see [1, pp. 418–419; 4, p. 280]. The exceptional cases $k = 3, 4, 8$ in Theorem 1.1 had been treated earlier by Gauss, Jacobi, and Eisenstein as follows. For $k = 4$, Gauss (see [1, pp. 268–269; 4, p. 268]) proved that if $p \equiv 1 \pmod 4$, then $p = a^2 + b^2$ for some a satisfying both

$$a \equiv \frac{1}{2}\binom{[p/2]}{[p/4]} \pmod{p} \tag{1.4}$$

and

$$a \equiv 1 (\operatorname{mod} 4), \tag{1.4a}$$

where the expression on the right of (1.4) is a binomial coefficient. For $k = 3$, Jacobi (see [1, p. 269; 4, p. 269]) proved that if $p \equiv 1 \pmod 3$, then $4p = a^2 + 27b^2$ for some a satisfying both

$$a \equiv \binom{[2p/3]}{[p/3]} \pmod{p} \tag{1.5}$$

and

$$a \equiv -1 (\operatorname{mod} 3). \tag{1.5a}$$

For $k = 8$, Jacobi (see [1, p. 272; 4, p. 269]) proved that if $p \equiv 1 \pmod 8$, then $p = a^2 + 2b^2$ for some a satisfying both

$$a \equiv \frac{1}{2}\binom{[p/2]}{[p/8]} \pmod{p} \tag{1.6}$$

and

$$a \equiv (-1)^{(p-1)/8} \qquad (\bmod 4). \tag{1.6a}$$

Finally, for $k = 8$, Eisenstein (see [1, p. 417; 4, pp. 281–282]) proved that if $p \equiv 3 \pmod 8$, then $p = a^2 + 2b^2$ for some a satisfying both

$$a \equiv \frac{1}{2}\binom{[p/2]}{[p/8]} \qquad (\bmod p) \tag{1.7}$$

and

$$a \equiv (-1)^{(p+5)/8} \qquad (\bmod 4). \tag{1.7a}$$

Smith [4, p. 271] wrote: "These congruential determinations possess great interest, not only because direct methods of solution present themselves very rarely in the theory of numbers, but also on account of the singular connexion which they establish between certain binomial coefficients and certain quadratic decompositions of primes." Theorem 1.1, which extends these congruential determinations (1.4)–(1.7), deserves to be more widely known.

In Section 2, we give a complete exposition of the proof of Theorem 1.1, hopefully improving the organization and readability. The exposition makes possible a short proof of our main theorem in Section 3, since Section 3 employs a lot of notation and results developed in Section 2.

Stickelberger [5, pp. 360–361] proved that for *prime* $k \geq 7$,

$$C \equiv 2(-p)^{-R} \qquad (\bmod k), \tag{1.8}$$

where C satisfies (1.2)–(1.3) and R is defined by

$$R = \frac{1}{k} \sum_{u \in U} u.$$

(It will be shown in Lemma 2.1 that R is an integer.) The weakened version $C \equiv \pm 2p^{-R} \pmod k$ of (1.8) follows easily from (1.2) and Lemma 2.1, but the significance of (1.8) is that it also determines the correct sign of C for which (1.3) holds. In other words, (1.3) and (1.8) hold simultaneously for the same choice of C.

EXAMPLE 1.3. Let $k = 23$ and $p = 59$. Then

$$2(-p)^{-R} \equiv 2(-59)^{-4} \equiv -396 \quad (\bmod 23),$$

so (1.8) holds with $C = -396$, in agreement with Example 1.2.

We can view (1.8) as extending (1.4a)–(1.7a), just as (1.3) extends (1.4)–(1.7). The congruence (1.8) depends only on k and on the value of $p \pmod{k}$ (in contrast to (1.3), which depends on k and p). Thus, for the purpose of computing the value of C that simultaneously satisfies (1.2), (1.3), and (1.8), the congruence (1.8) may be computationally more useful than (1.3) when k is small relative to p.

The primary purpose of this paper is to provide a generalization of (1.8) that works for composite as well as prime k. This is done in Section 3 (Theorem 3.1).

Given p and k as in Theorem 1.1, let H be the smallest positive integer for which

$$4p^H = A^2 + kB^2 \tag{1.9}$$

for some integers A, B. Thus $H \leq h$, but equality need not hold. For example, when $p = 41$ and $k = 20$, we have $h = 2$, but $H = 1$ since $4p = 164 = (12)^2 + 20(1)^2$. In Section 4, we briefly discuss congruences for A related to those given for C in Theorems 1.1 and 3.1.

2. PROOF OF THEOREM 1.1

Let $\mathbb{Q}(\sqrt{-k})$ be an imaginary quadratic field of discriminant $-k$ and class number h, with $k \neq 3$, 4, or 8. By [2, p. 40], k is squarefree with $k \equiv 3 \pmod{4}$, $k/4$ is squarefree with $k \equiv 1 \pmod{4}$, or $k/8$ is squarefree with $k \equiv 1 \pmod{2}$. Let p denote a prime with $(\frac{-k}{p}) = 1$ and let r be the smallest positive integer such that

$$p^r \equiv 1 \pmod{k}. \tag{2.1}$$

Write ϕ for the Euler ϕ-function.

The following four lemmas will be used to prove Theorem 1.1.

Lemma 2.1. *Define*

$$R = \frac{1}{k} \sum_{u \in U} u \qquad \text{and} \qquad N = \frac{1}{k} \sum_{\substack{0 < v < k \\ (\frac{-k}{v}) = -1}} v. \tag{2.2}$$

Then R and N are integers,

$$R + N = \phi(k)/2 = |U|, \tag{2.3}$$

and

$$N - R = h. \tag{2.4}$$

Remark. R and N are not integers when $k = 3$, 4, or 8.

Proof. We first prove (2.3). Since U can be identified with the kernel of the group homomorphism $(\frac{-k}{*})$ from $(\mathbb{Z}/k\mathbb{Z})^*$ onto $\{1, -1\}$, we have $|U| = \phi(k)/2$. Since $(\frac{-k}{*})$ is an odd function (see [2, p. 41]),

$$N = \frac{1}{k} \sum_{u \in U} (k - u) = \phi(k)/2 - R,$$

which completes the proof of (2.3).

Equality (2.4) is Dirichlet's class number formula for imaginary quadratic fields. It remains to prove $R \in \mathbb{Z}$.

If k is a prime, then $k \equiv 3 (\operatorname{mod} 4)$, so that

$$1 = \left(\frac{-k}{u}\right) = \left(\frac{u}{k}\right) \qquad \text{for } u \in U.$$

Thus

$$\sum_{u \in U} u \equiv \sum_{j=1}^{(k-1)/2} j^2 = k(k^2 - 1)/24 \equiv 0 \qquad (\operatorname{mod} k),$$

whence $R \in \mathbb{Z}$.

Next, suppose that k is composite, and write

$$k = tw, \qquad \text{with } t > 2 \text{ prime and } w > 1.$$

For each $j \in \{1, 2, \dots, t-1\}$, define

$$U_j = \{u \in U : u \equiv j (\operatorname{mod} t)\}.$$

As $|U_1| \geq |U_j|$ for each j,

$$(t - 1)|U_1| \geq \Sigma |U_j| = |U| = \phi(k)/2.$$

Thus, to prove that $|U_j| = \phi(w)/2$ for each j, it suffices to show that $|U_1| = \phi(w)/2$. This holds because U_1 can be identified with the kernel of the homomorphism $(\frac{-k}{*})$ from the group $\{x \in (\mathbb{Z}/k\mathbb{Z})^*\colon\ x \equiv 1 \ (\operatorname{mod} t)\}$ onto $\{1, -1\}$. (The homomorphism is onto because $w > 1$ and $(\frac{-k}{*})$ is a primitive character; see [2, p. 40]). Since $|U_j| = \phi(w)/2$,

$$\sum_{u \in U} u \equiv \frac{\phi(w)}{2} \sum_{j=1}^{t-1} j \equiv 0 \pmod{t}.$$

It remains to show that $\sum_{u \in U} u$ is divisible by 4 (resp. 8) when $4 \| k$ (resp. $8 \| k$). If $4 \| k$, then for each $j \in \{1, 3\}$, there exist $\phi(k/4)/2$ elements of U congruent to $j \pmod{4}$, so

$$\sum_{u \in U} u \equiv (1+3)\phi(k/4)/2 \equiv 0 \pmod{4}.$$

If $8 \| k$, then for each $j \in \{1, 3, 5, 7\}$, there exist $\phi(k/8)/2$ elements of U congruent to $j \pmod{8}$, so

$$\sum_{u \in U} u \equiv (1+3+5+7)\phi(k/8)/2 \equiv 0 \pmod{8}. \qquad \blacksquare$$

LEMMA 2.2. *For $a \in \mathbb{Z}$, $0 < a < k$, let $d_i(a)$ denote the digits in the base p expansion*

$$\frac{a(p^r - 1)}{k} = \sum_{i=1}^{r} d_i(a) p^{r-i}, \tag{2.5}$$

where p is a prime with $(\frac{-k}{p}) = 1$ and r is defined by (2.1). *Define*

$$s(a) = \sum_{i=1}^{r} d_i(a). \tag{2.6}$$

Let $L(x)$ denote the reduction of x modulo k, i.e.,

$$L(x) = x - k[x/k].$$

Then for each i,

$$d_i(a) = [pL(ap^{i-1})/k] \tag{2.7}$$

and

$$\sum_{a \in U/\langle p \rangle} s(a) = (p-1)R. \tag{2.8}$$

(*The sum in* (2.8) *is over any choice of the* $\phi(k)/2r$ *coset representatives of* $\langle p\rangle$ *in* U.)

Proof. The right member of (2.7), which clearly lies in the interval $[0, p-1]$, equals

$$[ap^i/k] - p[ap^{i-1}/k]. \tag{2.9}$$

Using (2.9) in place of $d_i(a)$ in (2.5), we obtain a telescoping series which reduces to the left side of (2.5). This proves (2.7).

From (2.7), the left member of (2.8) equals $\sum_{u\in U}[pu/k]$. Since

$$\sum_{u\in U} u = \sum_{u\in U} L(pu) = \sum_{u\in U} pu - k\sum_{u\in U}[pu/k],$$

we have

$$\sum_{u\in U}[pu/k] = \frac{p-1}{k}\sum_{u\in U} u = (p-1)R, \tag{2.10}$$

which proves (2.8). ■

LEMMA 2.3. *For the fundamental discriminant* $-k$, *define* $\zeta_k = \exp(2\pi i/k)$. *Then* $\mathrm{Gal}(\mathbb{Q}(\zeta_k)/\mathbb{Q}(\sqrt{-k})) = \{\sigma_u : u\in U\}$, *where* σ_u *is defined by* $\sigma_u(\zeta_k) = \zeta_k^u$.

Proof. This follows from the classical evaluation of the quadratic Gauss sum

$$\sum_{j=1}^{k-1}\left(\frac{-k}{j}\right)\zeta_k^j = \sqrt{-k}; \tag{2.11}$$

see [3, p. 217]. ■

The next lemma is Stickelberger's famous congruence for Gauss sums. In order to state it, we will need the following notation.

Let P be a prime ideal of $\mathbb{Z}[\zeta_k]$ dividing $p\mathbb{Z}$, and let $\mathscr{P}$ be a prime ideal of $\mathbb{Z}[\zeta_{kp}]$ dividing P. Thus

$$P\|p\mathbb{Z} \tag{2.12}$$

(i.e., p is divisible by P but not by P^2) and we have the factorization

$$P\mathbb{Z}[\zeta_{kp}] = \mathscr{P}^{p-1}. \tag{2.13}$$

Also [1, p. 343],

$$(\zeta_p - 1)^{p-1} = -pu_p, \tag{2.14}$$

where u_p is a unit in $\mathbb{Z}[\zeta_p]$ which is $\equiv 1 \pmod{\zeta_p - 1}$. By (2.12)–(2.14),

$$\mathscr{P} \| (\zeta_p - 1)\mathbb{Z}[\zeta_{pk}]. \tag{2.15}$$

Let χ_P denote the power residue symbol of order k on the field $\mathbb{Z}[\zeta_k]/P$. Thus for $\alpha \in \mathbb{Z}[\zeta_k]$,

$$\chi_P(\alpha) = 0 \qquad \text{if } \alpha \in P,$$

while if $\alpha \notin P$, then $\chi_P(\alpha)$ is the unique complex kth root of unity for which

$$\chi_P(\alpha) \equiv \alpha^{(p^r-1)/k} \pmod{P}. \tag{2.16}$$

We identify $\mathbb{Z}[\zeta_k]/P$ with the finite field $\mathbb{F}_{p^r}$ and define the Gauss sums

$$G_r(\bar{\chi}_P^a) = \sum_{v \in \mathbb{F}_{p^r}} \bar{\chi}_P^a(v)\zeta_p^{\mathrm{Tr}(v)}, \tag{2.17}$$

where Tr is the trace from $\mathbb{F}_{p^r}$ to $\mathbb{F}_p$, and $0 < a < k$. The modulus of this Gauss sum is $p^{r/2}$ [1, p. 10]. Since $\mathrm{Tr}(v^p) = \mathrm{Tr}(v)$,

$$G_r(\bar{\chi}_P^{ap}) = G_r(\bar{\chi}_P^a). \tag{2.18}$$

LEMMA 2.4. *In* $\mathbb{Q}(\zeta_{kp})$,

$$G_r(\bar{\chi}_P^a) \equiv -\frac{(\zeta_p - 1)^{s(a)}}{d_1(a)! \cdots d_r(a)!} \pmod{\mathscr{P}^{1+s(a)}},$$

for each $a = 1, 2, \ldots, k-1$.

Proof. See [1, p. 344]. ∎

Proof of Theorem 1.1. Since $(\frac{-k}{p}) = 1$, p splits in $\mathbb{Q}(\sqrt{-k})$. Hence we may write

$$(p) = \mathfrak{P}\bar{\mathfrak{P}}, \tag{2.19}$$

where $\mathfrak{P}$ is an integral ideal of $\mathbb{Q}(\sqrt{-k})$ with $\mathfrak{P} \neq \bar{\mathfrak{P}}$ and

$$P \| \mathfrak{P}. \tag{2.20}$$

Since $\mathfrak{P}^h$ is principal,

$$\mathfrak{P}^h = \left(\frac{C - D\sqrt{-k}}{2} \right) \tag{2.21}$$

for some $C, D \in \mathbb{Z}$ with $4p^h = C^2 + kD^2$. If $p|C$, then $p|D$, in which case the ideal (p) would divide $\mathfrak{P}^h$, contradicting (2.19). Thus (1.2) holds for the choice of C, D in (2.21). The uniqueness of $|C|$ and $|D|$ follows because any principal integral ideal of $\mathbb{Q}(\sqrt{-k})$ with norm p^h must have the form $\bar{\mathfrak{P}}^j \mathfrak{P}^{h-j}$ for some j, $0 \leq j \leq h$, and such an ideal is divisible by (p) unless $j \in \{0, h\}$. It remains to prove (1.3).

If $p = 2$, then (1.3) holds because both members are odd. Assume now that $p > 2$. Define

$$\eta = \prod_{a \in U/\langle p \rangle} G_r(\bar{\chi}_P^a) \in \mathbb{Q}(\zeta_{pk}). \tag{2.22}$$

Note that η is well defined, as the choice of coset representatives is immaterial by (2.18). By Lemma 2.3, $\mathrm{Gal}(\mathbb{Q}(\zeta_{pk})/\mathbb{Q}(\sqrt{-k}))$ consists of automorphisms σ_v with $v \in (\mathbb{Z}/pk\mathbb{Z})^*$ and $(\frac{-k}{v}) = 1$. For such v,

$$\sigma_v(\eta)/\eta = \prod_{a \in U/\langle p \rangle} \chi_P^a(v).$$

Viewing v as an element of $\mathbb{F}_p^*$, we can find $\gamma \in \mathbb{F}_{p^r}^*$ such that

$$v = \gamma^{(p^r-1)/(p-1)} = \gamma^{p+p^2+\cdots+p^r}.$$

Thus, by Lemma 2.1,

$$\sigma_v(\eta)/\eta = \chi_P(\gamma)^{\sum_{u \in U} u} = \chi_P(\gamma)^{kR} = 1.$$

This shows that each σ_v fixes η, so that

$$\eta \in \mathbb{Q}(\sqrt{-k}). \tag{2.23}$$

By Lemma 2.4 and (2.15),

$$\frac{-G_r(\bar{\chi}_P^a)}{(\zeta_p - 1)^{s(a)}} \equiv \frac{1}{d_1(a)! \cdots d_r(a)!} \qquad (\operatorname{mod} \mathscr{P}). \tag{2.24}$$

Multiplying the congruences in (2.24) over all $a \in U/\langle p\rangle$, we obtain, by (2.14) and Lemma 2.2,

$$E := (-1)^{\phi(k)/2r}\eta/(-p)^R \equiv \prod_{u \in U} [pu/k]!^{-1} \qquad (\operatorname{mod} \mathfrak{P}). \tag{2.25}$$

We proceed to show that E is an *integer* of $\mathbb{Q}(\sqrt{-k})$ with $(E) = \bar{\mathfrak{P}}^h$. Since $\mathscr{P}^{s(a)} \| G_r(\bar{\chi}_P^a)$, Lemma 2.2 shows that $\mathscr{P}^{(p-1)R} \| \eta$. Thus $P^R \| \eta$ by (2.13). It then follows from (2.19)–(2.20) that

$$\mathfrak{P}^R \| \eta. \tag{2.26}$$

Since $|G(\bar{\chi}_P^a)|^2 = p^r$ for $0 < a < k$, (2.22) and Lemma 2.1 yield

$$\eta\bar{\eta} = p^{\phi(k)/2} = p^{R+N}.$$

Thus $\mathfrak{P}^N \| \bar{\eta}$, i.e.,

$$\bar{\mathfrak{P}}^N \| \eta. \tag{2.27}$$

Since $N = R + h > R$ by (2.4), it follows that $(p)^R = \mathfrak{P}^R\bar{\mathfrak{P}}^R$ divides $(\eta) = \mathfrak{P}^R\bar{\mathfrak{P}}^N$, which completes the proof that E is an integer of $\mathbb{Q}(\sqrt{-k})$ with $(E) = \bar{\mathfrak{P}}^h$.

We can now write

$$E = (-1)^{\phi(k)/(2r)}\eta/(-p)^R = (C + D\sqrt{-k})/2 \tag{2.28}$$

for some $C, D \in \mathbb{Z}$ satisfying (2.21) and (1.2). Observe that

$$C = (-1)^{\phi(k)/(2r)}(\eta + \bar{\eta})/(-p)^R. \tag{2.29}$$

By (2.25) and (2.28),

$$(C + D\sqrt{-k})/2 \equiv \prod_{u \in U} [pu/k]!^{-1} \qquad (\operatorname{mod} \mathfrak{P}). \tag{2.30}$$

On the other hand, by (2.21),

$$(C - D\sqrt{-k})/2 \equiv 0 \qquad (\mathrm{mod}\, \mathfrak{P}). \tag{2.31}$$

Adding (2.30) and (2.31), we see that C satisfies the congruence (1.3). ■

3. CONGRUENCES FOR C (mod k)

Let k, h, p, and C be as in Theorem 1.1. In Theorem 3.1, we show that the congruence (1.8) for prime k can be extended to give congruences for C that work for all k.

THEOREM 3.1. *Let k, h, and p be as in Theorem* 1.1. *Define C as in* (2.29), *so that C is determined* (*only up to sign if $p = 2$*) *by* (1.2)–(1.3). *Write*

$$k = tw, \tag{3.1}$$

where t is any fixed odd prime divisor of k. If $w = 1$, then

$$C \equiv 2(-p)^{-R} \qquad (\mathrm{mod}\, t). \tag{3.2}$$

If $w > 1$ and

$$-1 \equiv p^b \qquad (\mathrm{mod}\, w)$$

for some positive integer b (*taken minimal*), *then*

$$C \equiv \begin{cases} 2p^{-R+\phi(k)/4}(-1)^{R+\phi(k)/(4b)} \quad (\mathrm{mod}\, t), & \text{if } p = 2 \\ 2p^{-R+\phi(k)/4}(-1)^{R+\phi(k)(w+1+p^b)/(4bw)} \quad (\mathrm{mod}\, t), & \text{if } p > 2. \end{cases} \tag{3.3}$$

If -1 is not a power of p (mod w), *then*

$$C \equiv \begin{cases} 2p^{-R+\phi(k)/4}(-1)^{R} \quad (\mathrm{mod}\, t), & \text{if } p = 2 \\ 2p^{-R+\phi(k)/4}(-1)^{R+\phi(k)(p^r-1)/(4kr)} \quad (\mathrm{mod}\, t), & \text{if } p > 2. \end{cases} \tag{3.4}$$

Proof. By (2.17),

$$G_r(\bar{\chi}_P^a)^t \equiv \sum_{v \in \mathbb{F}_{p^r}^*} \bar{\chi}_P^{at}(v)\zeta_p^{\mathrm{Tr}(tv)} \equiv \chi_P^a(t^t)G_r(\bar{\chi}_P^{at}) \qquad (\mathrm{mod}\, t), \tag{3.5}$$

so that by (2.22),

$$\eta^t \equiv \prod_{a \in U/\langle p \rangle} \chi_P^a(t^t) \prod_{a \in U/\langle p \rangle} G_r(\bar{\chi}_P^{at}) \qquad (\operatorname{mod} t). \tag{3.6}$$

Viewing t^t as an element of $\mathbb{F}_p^*$, we can find $\gamma \in \mathbb{F}_{p^r}^*$ such that

$$t^t = \gamma^{(p^r-1)/(p-1)},$$

so that

$$\prod_{a \in U/\langle p \rangle} \chi_P^a(t^t) = \chi_P(\gamma)^{\sum_{u \in U} u} = \chi_P(\gamma)^{kR} = 1.$$

Therefore (3.6) becomes

$$\eta^t \equiv \prod_{a \in U/\langle p \rangle} G_r(\bar{\chi}_P^{at}) \qquad (\operatorname{mod} t). \tag{3.7}$$

Also observe that by (2.29),

$$C \equiv C^t \equiv (-1)^{\phi(k)/(2r)}(\eta^t + \bar{\eta}^t)(-p)^{-R} \qquad (\operatorname{mod} t). \tag{3.8}$$

Case 1: $w = 1$ (so that $t = k$). In this case, each Gauss sum on the right side of (3.7) equals -1, since χ_P^t is trivial. Thus (3.7) yields

$$\eta^t \equiv (-1)^{\phi(k)/(2r)} \equiv \bar{\eta}^t \qquad (\operatorname{mod} t). \tag{3.9}$$

Together, (3.8) and (3.9) give the desired congruence (3.2).

Case 2: $w > 1$ and $-1 \equiv p^b \pmod w$ for a minimal positive integer b. We appeal to [1, Theorem 11.6.3], which yields the Gauss sum evaluation

$$-G_r(\bar{\chi}_P^{at}) = \begin{cases} p^{r/2}(-1)^{r/(2b)}, & \text{if } p = 2 \\ p^{r/2}(-1)^{r(w+1+p^b)/(2bw)}, & \text{if } p > 2. \end{cases} \tag{3.10}$$

Combining (3.7) and (3.10), we obtain

$$(-1)^{\phi(k)/(2r)}\eta^t \equiv \begin{cases} p^{\phi(k)/4}(-1)^{\phi(k)/(4b)} \quad (\operatorname{mod} t), & \text{if } p = 2 \\ p^{\phi(k)/4}(-1)^{\phi(k)(w+1+p^b)/(4bw)} \quad (\operatorname{mod} t), & \text{if } p > 2. \end{cases} \tag{3.11}$$

The desired congruence (3.3) now follows from (3.11) and (3.8).

Case 3: -1 is not a power of $p \pmod w$. In the proof of Lemma 2.1, we verified the claim that $\{u \in U : u \equiv -1 \pmod t\}$ has $\phi(w)/2$ elements. Analogously, one can prove that $\{u \in U : u \equiv -1 \pmod w\}$ has $\phi(t)/2$ elements. Since $\phi(t)/2 = (t-1)/2 \geq 1$, one can choose a fixed $x \in U$ for which $x \equiv -1 \pmod w$. For each $a \in U$, we have $ax \in U$; but a and ax are in different cosets of $\langle p \rangle$ in U, for otherwise -1 would equal a power of $p \pmod w$. It follows that for each $a \in U/\langle p \rangle$, both $G_r(\bar{\chi}_P^{at})$ and $G_r(\chi_P^{at})$ occur as factors in the right member of (3.7). Since

$$\chi_P(-1) = \begin{cases} 1 & \text{if } p = 2 \\ (-1)^{(p^r-1)/k}, & \text{if } p > 2, \end{cases}$$

we have [1, p. 10]

$$G_r(\bar{\chi}_P^{at}) G_r(\chi_P^{at}) = p^r \chi_P^{at}(-1) = \begin{cases} p^r, & \text{if } p = 2 \\ p^r(-1)^{(p^r-1)/k}, & \text{if } p > 2, \end{cases} \tag{3.12}$$

because at is odd when k is even, whereas when k is odd and $p > 2$, $\chi_P(-1) = 1$. By (3.12) and (3.7),

$$\eta^t \equiv \begin{cases} p^{\phi(k)/4} \pmod t, & \text{if } p = 2 \\ p^{\phi(k)/4}(-1)^{(p^r-1)\phi(k)/(4kr)} \pmod t, & \text{if } p > 2. \end{cases} \tag{3.13}$$

The desired congruence (3.4) now follows from (3.13) and (3.8). ■

Example 3.2. Let $k = 15$, so that $\phi(k) = 8$, $h = 2$, $R = 1$, and $r = 2$. Choose $p = 19$. If we take $w = 5$, $t = 3$, then $b = 1$ and (3.3) gives $C \equiv -2 \cdot 19 \equiv 1 \pmod 3$. On the other hand, if we take $w = 3$, $t = 5$, then (3.4) gives $C \equiv -2 \cdot 19 \equiv 2 \pmod 5$. These congruences $C \equiv 1 \pmod 3$ and $C \equiv 2 \pmod 5$ are each in accord with the value $C = 22$ determined by Theorem 1.1.

4. QUADRATIC FORMS REPRESENTING $4p^H$ FOR $H < h$

Let k and p be as in Theorem 1.1, and define H to be the minimal positive integer for which

$$4p^H = A^2 + kB^2 \tag{4.1}$$

for some integers A, B. Clearly $p \nmid AB$. Defining $\mathfrak{P}$ as in (2.19), we see that

$$\mathfrak{P}^H \bar{\mathfrak{P}}^H = \left(\frac{A + B\sqrt{-k}}{2}\right)\left(\frac{A - B\sqrt{-k}}{2}\right).$$

If both $\mathfrak{P}$ and $\bar{\mathfrak{P}}$ divided $(A + B\sqrt{-k})/2$, then p would divide A and B, a contradiction. Thus, without loss of generality,

$$\mathfrak{P}^H = \left(\frac{A - B\sqrt{-k}}{2}\right), \tag{4.2}$$

and so the integers A, B satisfying (4.1) are unique up to sign.

In (2.29), we expressed C in terms of Gauss sums, which enabled us to obtain simultaneous congruences for C in Theorems 1.1 and 3.1. We do not know a formula for A in terms of Gauss sums, and so we are unable to give analogous congruences for A. However, we can give such congruences for $A^{h/H}$, as follows.

Since H is the order of $[\mathfrak{P}]$ in the class group of $\mathbb{Q}(\sqrt{-k})$, we have $H|h$, and

$$\left(\frac{A + B\sqrt{-k}}{2}\right)^{h/H} = \left(\frac{C + D\sqrt{-k}}{2}\right), \tag{4.3}$$

by (4.2) and (2.21). This equality can be viewed as an equality of integers rather than of ideals, by suitably choosing the signs of A and B. Reducing (4.3) mod $\sqrt{-k}$, we see that

$$A^{h/H} \equiv 2^{(h-H)/H} C \qquad (\operatorname{mod} k). \tag{4.4}$$

Since $C \equiv D\sqrt{-k}$ (mod $\mathfrak{P}$) by (2.31), and similarly $A \equiv B\sqrt{-k}$ (mod $\mathfrak{P}$), reduction of (4.3) (mod $\mathfrak{P}$) yields

$$A^{h/H} \equiv C \qquad (\operatorname{mod} p). \tag{4.5}$$

In view of (4.4)–(4.5), the congruences for C in Theorems 1.1 and 3.1 yield analogous congruences for $A^{h/H}$.

EXAMPLE 4.1. Let $k = 23$ and $p = 59$. Then $h = 3$, $H = 1$, and

$$4p^H = 4 \cdot 59 = 236 = A^2 + 23B^2$$

with $A = \pm 12$ and $B = \pm 2$. In view of Examples 1.2 and 1.3, (4.4) becomes

$$A^3 \equiv 4C \equiv 4(-396) \qquad (\mathrm{mod}\, 23), \tag{4.6}$$

and (4.5) becomes

$$A^3 \equiv C \equiv -396 \qquad (\mathrm{mod}\, 59). \tag{4.7}$$

Both (4.6) and (4.7) hold with $A = 12$.

ACKNOWLEDGMENT

The author thanks the referees for their valuable comments.

REFERENCES

1. B. C. Berndt, R. J. Evans, and K. S. Williams, “Gauss and Jacobi Sums,” Wiley-Interscience, New York, 1998.
2. H. Davenport, “Multiplicative Number Theory,” second ed., Springer-Verlag, New York, 1980.
3. E. Hecke, “Lectures on the Theory of Algebraic Numbers” (Translated by G. Brauer, J. Goldman, and R. Kotzen), Springer-Verlag, New York, 1981.
4. H. J. S. Smith, “Report on the Theory of Numbers,” Chelsea, New York, 1965. [Collected Mathematical Papers, Vol. 1, pp. 38–364, Chelsea, New York, 1979.]
5. L. Stickelberger, *Über eine Verallgemeinerung der Kreistheilung*, *Math. Ann.* **37**(1890), 321–367.