ACTA ARITHMETICA
C.4 (2001)

Extensions of classical congruences for parameters in binary quadratic forms

by

Ronald Evans (La Jolla, CA)

1. Introduction. Let $\mathbb{Q}(\sqrt{-k})$ be an imaginary quadratic field with (fundamental) discriminant $-k$ and class number h. Define

$$U = \left\{u \in \mathbb{Z} :\ 0 < u < k \text{ and } \left(\frac{-k}{u}\right) = 1\right\} \quad \text{and} \quad R = \frac{1}{k}\sum_{u\in U} u.$$

If $k \notin \{3,4,8\}$, R is an integer with

$$R = \phi(k)/4 - h/2$$

(see [7, Lemma 2.1]). When $k \notin \{3,4,8\}$, choose integers t, w such that

$$k = tw, \quad t \text{ prime } > 2.$$

For a prime p with $\left(\frac{-k}{p}\right) = 1$, let r denote the smallest positive integer such that

$$q := p^r \equiv 1 \pmod{k}.$$

Assume that $k \notin \{3,4,8\}$. There are integers C, D, unique up to sign, such that [10]

$$4p^h = C^2 + kD^2, \quad p \nmid C. \tag{1.1}$$

In accordance with [7, Theorem 3.1], we choose the sign of C so that C is uniquely determined by the congruences (1.2)–(1.4) below. If $w = 1$, then

$$C \equiv 2(-p)^{-R} \pmod{t}; \tag{1.2}$$

if $w > 1$ and $-1 \equiv p^b \pmod{w}$ for some positive integer b (taken minimal), then

$$C \equiv \begin{cases} 2p^{h/2}(-1)^{R+\phi(k)/(4b)} \pmod{t} & \text{if } p = 2, \\ 2p^{h/2}(-1)^{R+\phi(k)(w+1+p^b)/(4bw)} \pmod{t} & \text{if } p > 2; \end{cases} \tag{1.3}$$

2000 *Mathematics Subject Classification*: Primary 11E25, 11T24; Secondary 11B65, 11R29, 11S80.

if -1 is not a power of $p \pmod w$, then

$$C \equiv \begin{cases} 2p^{h/2}(-1)^R \pmod t & \text{if } p = 2, \\ 2p^{h/2}(-1)^{R+\phi(k)(q-1)/(4kr)} \pmod t & \text{if } p > 2. \end{cases} \tag{1.4}$$

The significance of the choice of C uniquely determined by (1.1)–(1.4) is that C simultaneously satisfies Stickelberger's [10] classical congruence

$$C \equiv \prod_{u \in U} [pu/k]!^{-1} \pmod p, \tag{1.5}$$

where $[x]$ denotes the greatest integer $\le x$. This is proved in [7].

The first object of this paper is to extend (1.5) by determining $C \pmod{p^2}$. More than just a routine application of the Gross–Koblitz formula is needed to accomplish this in a usefully explicit way. Our determination for odd p is formulated in terms of expressions B_u (defined in (2.2)) that can be computed $(\mathrm{mod}\ p^2)$ for large p relatively rapidly (as indicated near the end of this section). A fast computation of C yields in particular a fast computation of Eisenstein's binomial coefficients $(\mathrm{mod}\ p^2)$, in view of Corollaries 2.3 and 4.2.

The results for $p > 2$ are presented in Section 2 (Theorem 2.2). Those for $p = 2$ are presented in Section 3 (Theorem 3.1). We remark that in the case $p = 2$, Stickelberger's congruence (1.5) is trivial (since $C \pmod 2$ always equals 1, by (1.1)). In contrast, the determination of $C \pmod 4$ is nontrivial, and the results are rather surprising (see Theorem 3.3).

Theorem 2.2 has the following counterparts for the exceptional cases $k \in \{3, 4, 8\}$. Fix a prime p with $\left(\frac{-k}{p}\right) = 1$. For $k = 4$, there are integers a, b (with a unique) such that

$$p = a^2 + b^2, \quad a \equiv 1 \pmod 4 \tag{1.6}$$

and

$$a \equiv (2^{p-1} + 1)^{-1} \binom{[p/2]}{[p/4]} + \frac{p}{2} \binom{[p/2]}{[p/4]}^{-1} \pmod{p^2}. \tag{1.7}$$

This is proved in Chowla, Dwork and Evans [3]; for a simpler proof, see [2, Theorem 9.4.3]. For $k = 3$, there are integers a, b (with a unique) such that

$$4p = a^2 + 27b^2, \quad a \equiv -1 \pmod 3 \tag{1.8}$$

and

$$a \equiv \binom{[2p/3]}{[p/3]} + p \binom{[2p/3]}{[p/3]}^{-1} \pmod{p^2}. \tag{1.9}$$

This is proved in [2, Theorem 9.4.2]. Finally, for $k = 8$, there are integers C, D (with C unique) such that

$$4p = C^2 + 8D^2, \qquad C \equiv 2(-1)^{[p/8]+[p/2]} \pmod 8 \tag{1.10}$$

and

$$C \equiv p\binom{[p/2]}{[p/8]}^{-1} + \binom{[p/2]}{[p/8]}(2 - 2^{p-1} - y/8) \pmod{p^2}, \tag{1.11}$$

where

$$y = \sqrt{2}(2-\sqrt{2})^{q-1} - \sqrt{2}(2+\sqrt{2})^{q-1}. \tag{1.12}$$

This is proved for the case $p \equiv 1 \pmod 8$ in [2, Theorem 9.4.5]. The proof for the remaining case $p \equiv 3 \pmod 8$ is more complicated and is given in Section 4 (Theorem 4.1). The complications arise because such p does not split into first degree primes in $\mathbb{Q}(\sqrt{-k})$.

Application of the binomial theorem in (1.12) shows that $y \in \mathbb{Z}$, so that (1.11) makes sense even though $\sqrt{2}$ does not exist $\pmod p$ when $p \equiv 3 \pmod 8$. From a computational point of view, it would be too slow to use the binomial expansion to compute the integer $y \pmod{p^2}$ when p is large. It is faster to find $y \pmod{p^2}$ by computing $(2 \pm \sqrt{2})^{q-1} \pmod{p^2}$ via the method of successive squarings. Similar considerations apply to the computation of the integers B_u (defined in (2.2)) which appear in Theorem 2.2.

In Corollaries 4.2 and 2.3, we apply Theorems 4.1 and 2.2 to give congruences for Eisenstein's binomial coefficients $\binom{[p/2]}{[p/8]}$ and $\binom{[3p/7]}{[p/7]} \pmod{p^2}$ in the cases $k = 8$ and $k = 7$, respectively (cf. [2, Section 12.9]). This solves Research Problem #26 posed in [2, p. 498].

Evaluations of binomial coefficients $\pmod{p^2}$ are of more than just theoretical interest. For example, Crandall, Dilcher and Pomerance [6] have employed such evaluations to speed up computations in the search for Wilson primes.

2. Determination of $C \pmod{p^2}$ when $p > 2$. Throughout this section, p is an odd prime with $\left(\frac{-k}{p}\right) = 1$. For $\zeta_k = \exp(2\pi i/k)$ and $s \in \mathbb{Z}$, define

$$A_s = \frac{1}{k}\sum_{j=1}^{k-1} \zeta_k^{-sj}\{(1-\zeta_k^j)^{q-1} - 1\} \tag{2.1}$$

and

$$B_s = A_s - A_0. \tag{2.2}$$

The following lemma generalizes a result proved for $r = 1$ in [2, p. 280].

LEMMA 2.1. *For $1 \le s \le k$, B_s is a rational integer multiple of p satisfying*

$$B_s = B_{k-s} \equiv \frac{p}{k} \sum_{0<j<ps/k} \frac{1}{j} \pmod{p^2}. \tag{2.3}$$

Proof. For any integer s, since q is odd,

$$\begin{aligned} k(A_s - A_{s-1}) &= \sum_{j=1}^{k-1} \zeta_k^{-sj}(1-\zeta_k^j)((1-\zeta_k^j)^{q-1}-1) \\ &= \sum_{j=0}^{k-1} \zeta_k^{-sj}((1-\zeta_k^j)^q - (1-\zeta_k^j)) \\ &= \sum_{j=0}^{k-1} \zeta_k^{-sj} \sum_{m=1}^{q-1} \binom{q}{m} (-\zeta_k^j)^m \\ &= \sum_{m=1}^{q-1} \binom{q}{m} (-1)^m \sum_{j=0}^{k-1} \zeta_k^{j(m-s)}. \end{aligned}$$

Therefore,

$$A_s - A_{s-1} = \sum_{\substack{0<m<q \\ m \equiv s \,(\mathrm{mod}\, k)}} (-1)^m \binom{q}{m}. \tag{2.4}$$

Thus for $s \ge 0$,

$$B_s = \sum_{\nu=1}^{s} (A_\nu - A_{\nu-1}) \in \mathbb{Z}. \tag{2.5}$$

Since

$$(1-\zeta_k^j)^{q-1} = (\zeta_k^{-j}-1)^{q-1} = (1-\zeta_k^{-j})^{q-1},$$

we see from (2.1) that $A_{k-s} = \overline{A}_s$, so that by (2.2),

$$B_{k-s} = A_{k-s} - A_0 = \overline{A}_s - \overline{A}_0 = \overline{B}_s = B_s.$$

It remains to prove the congruence in (2.3). Since $\binom{q}{m} = (q/m)\binom{q-1}{m-1}$, it follows from (2.4) that

$$A_s - A_{s-1} \equiv \sum_{\substack{0<m<q \\ m \equiv s \,(\mathrm{mod}\, k) \\ p^{r-1} \| m}} (-1)^m \binom{q}{m} \pmod{p^2}.$$

Since

$$\binom{q-1}{m-1} = \frac{(q-1)\dots(q-(m-1))}{1\dots(m-1)} \equiv (-1)^{m-1} \pmod{p},$$

we have, writing $m = p^{r-1}n$,

$$A_s - A_{s-1} \equiv -p \sum_{\substack{0<n<p \\ n\equiv sp \,(\mathrm{mod}\, k)}} \frac{1}{n} \;(\mathrm{mod}\, p^2).$$

Thus

$$A_s - A_{s-1} \equiv -p \sum_{\substack{0<n<p \\ n\equiv sp \,(\mathrm{mod}\, k)}} \frac{1}{n-sp} = -p \sum_{\substack{-sp<i<(1-s)p \\ k|i}} \frac{1}{i} \tag{2.6}$$

$$= \frac{p}{k} \sum_{(s-1)p/k<j<sp/k} \frac{1}{j} \;(\mathrm{mod}\, p^2),$$

where we have written $n - sp = i = -kj$. The congruence in (2.3) with $1 \le s \le k$ now follows from (2.5) and (2.6). ∎

The following theorem generalizes (1.5).

THEOREM 2.2. *If* $k \notin \{3, 4, 8\}$ *and* $p > 2$, *then*

$$C \equiv p^h \prod_{u\in U} [pu/k]! + (-(p-1)!)^R \prod_{u\in U} [pu/k]!^{-1} \Big(1 + \sum_{u\in U} uB_u\Big) \;(\mathrm{mod}\, p^2). \tag{2.7}$$

Proof. In [7, (2.28)], we wrote $(C + D\sqrt{-k})/2$ as a product of Gauss sums. The Gross–Koblitz formula [8], [2, (11.2.12)] expresses these Gauss sums in terms of p-adic gamma functions. Specifically, it shows that there is an embedding of $\mathbb{Q}(\sqrt{-k})$ into the field $\mathbb{Q}_p$ of p-adic rationals which maps $(C + D\sqrt{-k})/2$ to a product of p-adic gamma functions, viz.,

$$(C + D\sqrt{-k})/2 = \prod_{u\in U} \Gamma_p(u/k) \quad (\text{in } \mathbb{Q}_p). \tag{2.8}$$

Here $\Gamma_p(z)$ is the p-adic gamma function, defined as in [2, (9.3.3)] to be the limit of

$$(-1)^N \prod_{\substack{0<j<N \\ p\nmid j}} j$$

as the positive integer N p-adically approaches the p-adic integer z. By (1.1) and (2.8),

$$(C - D\sqrt{-k})/2 = p^h \prod_{u\in U} \Gamma_p(u/k)^{-1}. \tag{2.9}$$

Adding (2.8) and (2.9), we obtain

$$C = p^h \prod_{u\in U} \Gamma_p(u/k)^{-1} + \prod_{u\in U} \Gamma_p(u/k). \tag{2.10}$$

By (2.10) and (1.5),

$$\prod_{u\in U} \Gamma_p(u/k) \equiv \prod_{u\in U} [pu/k]!^{-1} \pmod p, \tag{2.11}$$

so that (2.10) becomes

$$C \equiv p^h \prod_{u\in U} [pu/k]! + \prod_{u\in U} \Gamma_p(u/k) \pmod{p^2}. \tag{2.12}$$

It remains to show that

$$\prod_{u\in U} \Gamma_p(u/k) \equiv (-(p-1)!)^R \prod_{u\in U} [pu/k]!^{-1}\Big(1 + \sum_{u\in U} uB_u\Big) \pmod{p^2},$$

which is equivalent, by Lemma 2.1, to

$$\prod_{u\in U} \Gamma_p(u/k)^{-1} \equiv (-(p-1)!)^{-R} \prod_{u\in U} [pu/k]!\Big(1 - \sum_{u\in U} uB_u\Big) \pmod{p^2}. \tag{2.13}$$

Define

$$c = \max(r, 2). \tag{2.14}$$

Note that $k \mid (p^c - 1)$. By [2, (9.3.8)],

$$\Gamma_p(1 - u/k) \equiv \Gamma_p(1 + (p^c - 1)u/k) \pmod{p^2}. \tag{2.15}$$

Since $1 + (p^c - 1)u/k$ is a positive integer,

$$\Gamma_p(1 + (p^c - 1)u/k) = \pm \prod_{\substack{1\le j\le (p^c-1)u/k \\ p\nmid j}} j, \tag{2.16}$$

by definition of Γ_p.

For $x \in \mathbb{R}$, define

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

Since $pL(u/p) = k[L(u/p)p/k] + u$, we have

$$u(p^c - 1) = k[L(u/p)p/k] + p^c u - pL(u/p),$$

which yields

$$(p^c - 1)u/k = [L(u/p)p/k] + p(up^{c-1} - L(u/p))/k. \tag{2.17}$$

For each nonnegative integer x,

$$(xp + 1)\dots(xp + p - 1) \equiv (p - 1)! \pmod{p^2},$$

so it follows from (2.17) that

$$(2.18)\qquad \prod_{\substack{1\le j\le (p^c-1)u/k\\ p\nmid j}} j \equiv (p-1)!^{(up^{c-1}-L(u/p))/k} \times \prod_{j=1}^{[L(u/p)p/k]} (j+(up^c-pL(u/p))/k) \pmod{p^2}.$$

The rightmost product on j in (2.18) is congruent to

$$[L(u/p)p/k]!\Big(1+\frac{up^c-pL(u/p)}{k}\sum_{j=1}^{[L(u/p)p/k]}\frac{1}{j}\Big) \equiv [L(u/p)p/k]!\Big(1-\frac{pL(u/p)}{k}\sum_{j=1}^{[L(u/p)p/k]}\frac{1}{j}\Big) \pmod{p^2}.$$

Taking the product over all $u \in U$ in (2.15), (2.16), and (2.18), we thus obtain

$$(2.19)\qquad \pm\prod_{u\in U}\Gamma_p(1-u/k) \equiv (p-1)!^{R(p^{c-1}-1)}\prod_{u\in U}[pu/k]!\Big(1-\sum_{u\in U}uB_u\Big) \pmod{p^2}.$$

By the reflection formula for Γ_p [2, (9.3.5)], the left member of (2.19) equals $\pm\prod_{u\in U}\Gamma_p(u/k)^{-1}$. Thus (2.19) becomes

$$(2.20)\qquad \pm\prod_{u\in U}\Gamma_p(u/k)^{-1} \equiv (p-1)!^{R(p^{c-1}-1)}\prod_{u\in U}[pu/k]!\Big(1-\sum_{u\in U}uB_u\Big) \pmod{p^2}.$$

The ambiguous sign on the left of (2.20) must be + by (2.11). Finally, the power of $(p-1)!$ in (2.20) can be simplified to $(-(p-1)!)^{-R}$, since $(p-1)!^p \equiv -1 \pmod{p^2}$. This completes the proof of (2.13). ∎

The following corollary gives a congruence $(\mathrm{mod}\, p^2)$ for Eisenstein's binomial coefficient $\binom{[3p/7]}{[p/7]}$ in the case $k=7$.

COROLLARY 2.3. *Let $k=7$ and let p be an odd prime with $\left(\frac{-7}{p}\right)=1$, i.e., with $p\equiv 1,2,$ or $4 \pmod 7$. Then*

$$(2.21)\qquad Z := \binom{[3p/7]}{[p/7]} \equiv (-1)^{[3p/7]}(p/C + C(B_1+2B_2-3B_3-1)) \pmod{p^2}.$$

Proof. For brevity, write $p_i = [ip/7],\ i=1,2,3,4$. Since $p\equiv 1,2,$ or 4 modulo 7, it follows that $Z = p_3!/(p_1!p_2!)$. For $k=7$, we have $h=1$, $U=$

$\{1,2,4\}$, and $R=1$. By (2.7),

$$C \equiv p_1!p_2!p_4!p - \frac{(p-1)!(1+B_1+2B_2+4B_4)}{p_1!p_2!p_4!} \pmod{p^2}. \tag{2.22}$$

Since $p_3+p_4=p-1$, we have

$$p_3!p_4! \equiv -(-1)^{p_3} \pmod{p}. \tag{2.23}$$

By (2.22) and (2.23),

$$C \equiv -(-1)^{p_3}p/Z \ - \frac{(p-1)!Z(1+B_1+2B_2+4B_4)}{p_3!p_4!} \pmod{p^2}. \tag{2.24}$$

By (2.23) and (2.24),

$$C \equiv -Z(-1)^{p_3} \pmod{p}. \tag{2.25}$$

Combining (2.24) and (2.25), we obtain

$$C \equiv p/C \ - \frac{(p-1)!Z(1+B_1+2B_2+4B_4)}{p_3!p_4!} \pmod{p^2}. \tag{2.26}$$

Solving (2.26) for Z and using the equality $B_4=B_3$, we obtain

$$Z \equiv (p/C-C)(1-B_1-2B_2-4B_3)Y \pmod{p^2}, \tag{2.27}$$

where

$$Y = \frac{p_3!p_4!}{(p-1)!}\ . \tag{2.28}$$

We proceed to compute $Y \pmod{p^2}$. Since

$$\begin{aligned}(p-1)! &= (p-1)\dots(p-p_3)\cdot p_4! \equiv (-1)^{p_3}p_3!p_4!\Big(1-p\sum_{j=1}^{p_3}1/j\Big)\\ &\equiv (-1)^{p_3}p_3!p_4!(1-7B_3) \pmod{p^2},\end{aligned}$$

we see that

$$Y \equiv (-1)^{p_3}(1+7B_3) \pmod{p^2}. \tag{2.29}$$

By (2.27) and (2.29),

$$Z \equiv (p/C-C)(-1)^{p_3}(1+3B_3-B_1-2B_2) \pmod{p^2},$$

which proves (2.21). ∎

Example 2.4. Let $k=7$ and $p=37$. Then $R=h=1$, $p_1=5$, $p_2=10$, $p_3=15$, $p_4=21$, $-B_2 \equiv B_1 \equiv 74 \pmod{37^2}$, $B_3=B_4 \equiv 814 \pmod{37^2}$, and

$$4p = 148 = C^2+7D^2 \quad \text{with} \quad C=\pm 6,\ D=\pm 4.$$

Congruence (1.2) becomes

$$C \equiv 2(-37)^{-1} \equiv -1 \pmod{7}$$

and congruence (2.7) becomes

$$C \equiv 37p_1!p_2!p_4! - \frac{36!(1+B_1+2B_2+4B_4)}{p_1!p_2!p_4!} \equiv 6 \pmod{37^2}.$$

Both of these congruences must hold for the same choice of $C = \pm 6$, which in this case is $C = 6$. With $C = 6$, congruence (2.21) becomes

$$Z \equiv -37/6 - 6(B_1 + 2B_2 - 3B_3 - 1) \equiv 265 \pmod{37^2}.$$

To verify this, note that

$$Z = \binom{15}{5} = 3003 = 2(37^2) + 265.$$

3. Determination of $C \pmod{p^2}$ when $p = 2$. We begin by discussing properties of the 2-adic gamma function Γ_2, which can be defined just as we defined Γ_p below (2.8), with p replaced by 2. (Although Γ_p is defined in [2, (9.3.3)] for $p > 2$ only, this definition is also valid for $p = 2$, because the congruence [2, (9.3.2)] holds for $p = 2$ whenever the modulus exceeds 4.)

Given a 2-adic integer

$$z = z_0 + z_1 2 + z_2 4 + z_3 8 + \ldots, \qquad z_i \in \{0, 1\},$$

we have the reflection formula

$$\Gamma_2(z)\Gamma_2(1-z) = (-1)^{M(z)}, \tag{3.1}$$

where

$$M(z) = z_1 + 1.$$

(The reflection formula [2, (9.3.5)] for Γ_p, which was used below (2.19), does not reduce to (3.1) when $p = 2$; it holds only for $p > 2$.) To verify (3.1), note that for integers n, N with $n > 2$ and $0 < N < 2^n$,

$$\prod_{\substack{0<j<N \\ j \text{ odd}}} j \prod_{\substack{0<j<2^n+1-N \\ j \text{ odd}}} j \equiv (-1)^{M(N)} \pmod{2^n}, \tag{3.2}$$

and when N approaches z (2-adically) in (3.2), we obtain (3.1) by the continuity of $\Gamma_2(z)$ and $M(z)$.

We shall need the Gross–Koblitz formula [2, (11.2.12)] for $p = 2$. This formula was originally presented [8] for $p > 2$, but it has been proved for $p = 2$ as well (see Coleman [4], [5]).

THEOREM 3.1. *Suppose that $p = 2$ and $\left(\frac{-k}{p}\right) = 1$, so that $k \equiv 7 \pmod 8$ (with k squarefree). Let H denote the class number of $\mathbb{Q}(\sqrt{-8k})$. Then*

$$C \equiv 2^h + (-1)^{R+H/4} \pmod 4. \tag{3.3}$$

In particular, $C \equiv -1 \pmod 4$ when $k = 7$, while for $k > 7$,

$$C \equiv (-1)^{R+H/4} \pmod 4. \tag{3.4}$$

Proof. We need only prove (3.3), since (3.4) follows from (3.3) and the fact that $h > 1$ when $k > 7$, $k \equiv 7 \pmod 8$.

In light of the proof of Theorem 2.2 and the remarks preceding Theorem 3.1, we see that (2.12) is valid for $p = 2$ as well as for $p > 2$. Thus,

$$C \equiv 2^h + \prod_{u \in U} \Gamma_2(u/k) \pmod 4.$$

It remains to prove that

$$\prod_{u \in U} \Gamma_2(u/k) \equiv (-1)^{R+H/4} \pmod 4. \tag{3.5}$$

By (3.1),

$$\prod_{u \in U} \Gamma_2(u/k)\Gamma_2(1-u/k) = (-1)^{\sum_{u \in U} M(u/k)}. \tag{3.6}$$

Since $k \equiv 7 \pmod 8$, it is easily checked that $M(u/k)$ is odd if and only if $u \equiv 0$ or $3 \pmod 4$. Thus

$$\sum_{u \in U} M(u/k) \equiv N(0,3,4,7) \pmod 2, \tag{3.7}$$

where $N(a,b,c,d)$ denotes the number of elements in U congruent to one of a, b, c, d modulo 8. Combining (3.5)–(3.7), we see that it remains to prove

$$\prod_{u \in U} \Gamma_2(1-u/k) \equiv (-1)^{R+H/4+N(0,3,4,7)} \pmod 4. \tag{3.8}$$

Since the congruence [2, (9.3.8)] holds for $p = 2$ (as well as for $p > 2$) when the modulus exceeds 4, it can be proved, analogous to the proof of (2.15)–(2.16), that

$$\Gamma_2(1-u/k) \equiv \Gamma_2(1+(2^r-1)u/k) = (-1)^{u+1} \prod_{\substack{1 \le j \le (2^r-1)u/k \\ j \text{ odd}}} j \pmod 4. \tag{3.9}$$

It follows that $\Gamma_2(1-u/k) \equiv \pm 1 \pmod 4$, with $\Gamma_2(1-u/k) \equiv -1 \pmod 4$ if and only if $(2^r-1)u/k \equiv 3, 4, 5, \text{or } 6 \pmod 8$. Thus $\Gamma_2(1-u/k) \equiv -1 \pmod 4$ if and only if $u \equiv 3, 4, 5, \text{or } 6 \pmod 8$, and so

$$\begin{aligned} \prod_{u \in U} \Gamma_2(1-u/k) &\equiv (-1)^{\sum_{u \in U} u + \sum_{u \in U} 1 + N(3,4,5,6)} \\ &= (-1)^{R+N(7,0,1,2)} \pmod 4. \end{aligned} \tag{3.10}$$

By (3.8) and (3.10), it remains to prove that

$$\sum_{\substack{u \in U \\ u \equiv 1,2,3,4 \pmod 8}} 1 \equiv H/4 \pmod 2. \tag{3.11}$$

We have

$$2 \sum_{\substack{u\in U\\ u\equiv 1,2,3,4 \pmod 8}} 1 = A + B, \tag{3.12}$$

where

$$A = \sum_{\substack{j=1\\(j,k)=1\\ j\equiv 1,2,3,4 \pmod 8}}^{k-1} 1, \quad B = \sum_{\substack{j=1\\ j\equiv 1,2,3,4 \pmod 8}}^{k-1} \left(\frac{j}{k}\right). \tag{3.13}$$

We proceed to prove that 4 divides A. For the Möbius function μ,

$$A = \sum_{\substack{j=1\\ j\equiv 1,2,3,4 \pmod 8}}^{k-1} \sum_{\substack{d|k\\ d|j}} \mu(d) = \sum_{d|k} \mu(d) \sum_{\substack{n=1\\ n\equiv d,2d,3d,4d \pmod 8}}^{k/d-1} 1, \tag{3.14}$$

where we have written $j = dn$. The inner sum on n in (3.14) is congruent to $0, 3, 1$, or $0 \pmod 4$ according as $d \equiv 1, 3, 5$, or $7 \pmod 8$. Thus,

$$A \equiv \sum_{\substack{d|k\\ d\equiv 5 \pmod 8}} \mu(d) - \sum_{\substack{d|k\\ d\equiv 3 \pmod 8}} \mu(d) \pmod 4. \tag{3.15}$$

Write $k = p_1 \dots p_\nu$, where the p_i are distinct primes. By (3.15),

$$A \equiv \sum_{\substack{d|k\\ d\equiv 5 \pmod 8}} \mu(d)(1 - (-1)^\nu) \pmod 4. \tag{3.16}$$

If ν is even, then (3.16) shows that $4 \mid A$, so suppose that ν is odd. If $\nu = 1$, then $4 \mid A$ because there are no terms in the sum in (3.16) (since $k \equiv 7 \pmod 8$). Thus suppose that ν is odd ≥ 3. By (3.16),

$$\begin{aligned} A &\equiv 2 \sum_{\substack{d|k\\ d\equiv 5 \pmod 8}} \mu(d) \equiv 2 \sum_{\substack{d|k\\ d\equiv 5 \pmod 8}} 1 \\ &= \frac{1}{2} \sum_{d|k} \sum_{\chi \pmod 8} \chi(5d) = \frac{1}{2} \sum_{\chi \pmod 8} \chi(5) \sum_{d|k} \chi(d) \\ &= \frac{1}{2} \sum_{\chi \pmod 8} \chi(5) \prod_{i=1}^{\nu} (1 + \chi(p_i)) \pmod 4. \end{aligned} \tag{3.17}$$

Each product on i above is divisible by 8, since

$$\prod_{i=1}^{\nu} (1 + \chi(p_i)) = 0 \text{ or } 2^\nu.$$

By (3.17), this completes the proof that $4 \mid A$.

In view of (3.11)–(3.12), it now suffices to prove that

$$B = H/2. \tag{3.18}$$

Since

$$\sum_{\substack{j=1\\ j\equiv 3,4 \pmod 8}}^{k-1} \left(\frac{j}{k}\right) = \sum_{\substack{j=1\\ j\equiv 3 \pmod 8}}^{k-1} \left\{\left(\frac{j}{k}\right) + \left(\frac{k-j}{k}\right)\right\} = 0,$$

$$B = \sum_{\substack{j=1\\ j\equiv 1,2 \pmod 8}}^{k-1} \left(\frac{j}{k}\right). \tag{3.19}$$

Write $k = 8f + 7$. Since $\left(\frac{2}{k}\right) = 1$, (3.19) yields

$$\begin{aligned} B &= \sum_{m=0}^{f} \left(\frac{8m+1}{k}\right) + \sum_{m=0}^{f} \left(\frac{8m+2}{k}\right) \\ &= \sum_{m=0}^{f} \left(\frac{m+f+1}{k}\right) + \sum_{m=0}^{f} \left(\frac{m+2f+2}{k}\right) \\ &= \sum_{m=f+1}^{3f+2} \left(\frac{m}{k}\right) = \sum_{k/8<j<3k/8} \left(\frac{j}{k}\right) = 2 \sum_{k/4<j<3k/8} \left(\frac{j}{k}\right), \end{aligned} \tag{3.20}$$

where the last equality follows from the last statement in Berndt [1, Cor. 7.2, p. 281]. On the other hand, by [1, (7.6), p. 282],

$$\sum_{k/4<j<3k/8} \left(\frac{j}{k}\right) = H/4. \tag{3.21}$$

Combining (3.20) and (3.21), we obtain (3.18). ∎

Example 3.2. Let $k = 143$ and $p = 2$. Then $h = 10$, $R = \phi(k)/4 - h/2 = 115$, $H = 12$, and

$$4p^h = 4096 = C^2 + 143D^2 \quad \text{with} \quad C = \pm 53,\ D = \pm 3.$$

By (1.3) with $w = 11,\ t = 13,$ and $b = 5$,

$$C \equiv 2^6(-1)^{115+120/20} = -64 \pmod{13}.$$

By (3.4)

$$C \equiv (-1)^{115+12/4} = 1 \pmod 4.$$

Both of these congruences must hold for the same choice of $C = \pm 53$, which in this case is $C = 53$.

The following theorem expresses the results of Theorem 3.1 in a form independent of class numbers.

THEOREM 3.3. *Suppose that* $p = 2$ *and* $\left(\frac{-k}{p}\right) = 1$, *so that* $k \equiv 7 \pmod 8$ (*with* k *squarefree*). *Then* $C \equiv -1 \pmod 4$, *if* $k = 7$; $C \equiv \delta \pmod 4$, *if* k *is a prime* > 7, *where* $\delta = \pm 1$ *is defined by*

$$\delta \equiv ((k-1)/2)!(-1)^{(k+1)/8} \pmod k;$$

$C \equiv \left(\frac{2Q}{P}\right) \pmod 4$, *if* $k = PQ$ *for primes* P, Q; *and* $C \equiv 1 \pmod 4$, *if* k *has more than two prime factors.*

Proof. Theorem 3.3 can be deduced from (3.3) by applying known congruences for class numbers modulo powers of 2. Such congruences are discussed in the second chapter of the book of Urbanowicz and Williams [11]. Specifically, for prime $k > 7$, one uses a theorem of Mordell [9], [11, Theorem 8, p. 52] together with a result of Berndt [1, Corollary 7.4], [11, p. 59]. For $k = PQ$, one uses the results in [11, p. 60] and [11, Theorem 13, p. 62]. Finally, when k has more than two prime factors, one uses the facts that $H/4$ and $R = \phi(k)/4 - h/2$ are both even; this is a consequence of Gauss's theory of genera [11, (1), p. 51]. ∎

4. Determination of $C \pmod{p^2}$ when $k = 8$

THEOREM 4.1. *Let* $k = 8$ *and let* p *be a prime with* $\left(\frac{-8}{p}\right) = 1$, *i.e.*, *with* $p \equiv 1$ *or* $3 \pmod 8$. *Then there are integers* C, D (*with* C *unique*) *such that* (1.10) *and* (1.11) *hold.*

Proof. This is proved for $p \equiv 1 \pmod 8$ in [2, Theorem 9.4.5], so assume that $p \equiv 3 \pmod 8$. In [2, Theorem 12.9.6], it is shown that there are integers C, D satisfying (1.10) such that $(C + D\sqrt{-8})/2$ equals a certain octic Eisenstein sum. This Eisenstein sum can in turn be expressed as a quotient of an octic Gauss sum over a quadratic Gauss sum, by [2, Theorem 12.1.1]. Using the Gross–Koblitz formula [2, (11.2.12)] and the fact that

$$(q-1)/8 = (3p-1)/8 + p(p-3)/8,$$

we find that the analog of (2.8) is

$$(C + D\sqrt{-8})/2 = \Gamma_p\left(\frac{1}{8}\right)\Gamma_p\left(\frac{3}{8}\right)\Gamma_p\left(\frac{1}{2}\right)^{-1} \quad (\text{in } \mathbb{Q}_p). \tag{4.1}$$

Therefore,

$$(C - D\sqrt{-8})/2 = p\Gamma_p\left(\frac{1}{8}\right)^{-1}\Gamma_p\left(\frac{3}{8}\right)^{-1}\Gamma_p\left(\frac{1}{2}\right),$$

and addition of these equalities yields

$$\pm C = p\Gamma_p\left(\frac{1}{8}\right)^{-1}\Gamma_p\left(\frac{3}{8}\right)^{-1} + \Gamma_p\left(\frac{1}{8}\right)\Gamma_p\left(\frac{3}{8}\right), \tag{4.2}$$

since $\Gamma_p\left(\frac{1}{2}\right) = \pm 1$ by the reflection formula. The proof of (2.20) works for $k = 8$, and shows that the analog of (2.20) is

$$\pm\,\Gamma_p\left(\frac{1}{8}\right)^{-1}\Gamma_p\left(\frac{3}{8}\right)^{-1} \equiv (p-1)!^{(p-1)/2}\left[\frac{p}{8}\right]!\left[\frac{3p}{8}\right]!(1 - B_1 - 3B_3) \pmod{p^2}. \tag{4.3}$$

Equivalently,

$$\pm\,\Gamma_p\left(\frac{1}{8}\right)\Gamma_p\left(\frac{3}{8}\right) \equiv (p-1)!^{(1-p)/2}\left[\frac{p}{8}\right]!^{-1}\left[\frac{3p}{8}\right]!^{-1}(1 + B_1 + 3B_3) \pmod{p^2}. \tag{4.4}$$

Write $\tau = (p-1)/2$. We proceed to examine the factor $(p-1)!^{-\tau}$ in (4.4). Since $\tau!^2 \equiv 1 \pmod{p}$,

$$(p-1)! = (p-1)\dots(p-\tau)\cdot\tau! \equiv -\tau!^2 + p\sum_{j=1}^{\tau} 1/j \equiv -\tau!^2 + 8B_4 \pmod{p^2}. \tag{4.5}$$

Write

$$\tau! = \varepsilon + xp, \quad \text{where} \quad x \in \mathbb{Z},\ \varepsilon = \pm 1. \tag{4.6}$$

Then $\tau!^2 \equiv 1 + 2\varepsilon xp \pmod{p^2}$, so that by (4.5),

$$(p-1)! \equiv -1 - 2\varepsilon xp + 8B_4 \pmod{p^2}. \tag{4.7}$$

Since τ is odd, the binomial theorem and (4.7) yield

$$(p-1)!^{\tau} \equiv -1 - 4B_4 + \varepsilon xp \pmod{p^2},$$

so by (4.6),

$$(p-1)!^{-\tau} \equiv -1 + 4B_4 - \varepsilon xp \equiv 4B_4 - \varepsilon\tau! \pmod{p^2}. \tag{4.8}$$

By (4.8) and (4.6),

$$(p-1)!^{-\tau}/\tau! \equiv \varepsilon(4B_4 - 1) \pmod{p^2}. \tag{4.9}$$

Therefore (4.4) becomes

$$\pm\Gamma_p\left(\frac{1}{8}\right)\Gamma_p\left(\frac{3}{8}\right) \equiv \binom{[p/2]}{[p/8]}(1 - 4B_4)(1 + B_1 + 3B_3) \equiv \binom{[p/2]}{[p/8]}(1 + B_1 + 3B_3 - 4B_4) \pmod{p^2}. \tag{4.10}$$

Consequently, (4.2) becomes

$$\pm C \equiv p\binom{[p/2]}{[p/8]}^{-1} + \binom{[p/2]}{[p/8]}(1 + B_1 + 3B_3 - 4B_4) \pmod{p^2}. \tag{4.11}$$

The congruence for $C \pmod p$ in [2, Theorem 12.9.7] shows that the + sign in (4.11) is correct. To complete the proof of (1.11), it remains to show that

$$1 + B_1 + 3B_3 - 4B_4 \equiv 2 - 2^{p-1} - y/8 \pmod{p^2}, \tag{4.12}$$

where y is the integer defined by (1.12). The proof of (4.12) proceeds just as the analogous proof in [2, Theorem 9.4.5] (with $q = p^2$ in place of p). ∎

The following corollary gives a congruence $(\mathrm{mod}\, p^2)$ for Eisenstein's binomial coefficient $\binom{[p/2]}{[p/8]}$ when $k = 8$.

Corollary 4.2. *Let $k = 8$, and let p be a prime with $\left(\frac{-8}{p}\right) = 1$, i.e., with $p \equiv 1$ or $3 \pmod 8$. Then*

$$W := \binom{[p/2]}{[p/8]} \equiv (C - p/C)(2^{p-1} + y/8) \pmod{p^2}, \tag{4.13}$$

where y is defined in (1.12).

Proof. By (1.11),

$$C \equiv p/W + W(2 - 2^{p-1} - y/8) \pmod{p^2}. \tag{4.14}$$

In particular, since p divides y by (4.12),

$$C \equiv W \pmod p. \tag{4.15}$$

By (4.14) and (4.15),

$$C \equiv p/C + W(2 - 2^{p-1} - y/8) \pmod{p^2}. \tag{4.16}$$

Solving (4.16) for W yields

$$W \equiv (C - p/C)(2 - 2^{p-1} - y/8)^{-1} \pmod{p^2},$$

and (4.13) follows. ∎

Example 4.3. Let $k = 8$ and $p = 43$. Then $h = 1$, $y \equiv 1462 \pmod{43^2}$, $\binom{[p/2]}{[p/8]} = \binom{21}{5} = 20349$, and

$$4p = 172 = C^2 + 8D^2 \quad \text{with} \quad C = \pm 10,\ D = \pm 3.$$

The congruence in (1.10) becomes

$$C \equiv 2(-1)^{5+21} = 2 \pmod 8$$

and the congruence (1.11) becomes

$$C \equiv \frac{43}{20349} + 20349\left(2 - 2^{42} - \frac{1462}{8}\right) \equiv 10 \pmod{43^2}.$$

Both of these congruences must hold for the same choice of $C = \pm 10$, which in this case is $C = 10$. With $C = 10$, (4.13) becomes

$$W \equiv \left(10 - \frac{43}{10}\right)\left(2^{42} + \frac{1462}{8}\right) \equiv 10 \pmod{43^2}.$$

To verify this, observe that

$$W = 20349 = 11(43^2) + 10.$$

References

[1] B. C. Berndt, *Classical theorems on quadratic residues*, Enseign. Math. 22 (1976), 261–304.

[2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Wiley, 1998.

[3] S. Chowla, B. Dwork and R. J. Evans, *On the mod p^2 determination of $\binom{(p-1)/2}{(p-1)/4}$*, J. Number Theory 24 (1986), 188–196.

[4] R. F. Coleman, *The Gross–Koblitz formula*, in: Galois Representations and Arithmetic Algebraic Geometry, Y. Ihara (ed.), Adv. Stud. Pure Math. 12, North-Holland, Amsterdam, 1987, 21–52.

[5] —, *p-adic Analysis*, Lecture Notes in Math. 1454, Springer, Berlin, 1990, p. 193 (Corrigenda to reference #4).

[6] R. Crandall, K. Dilcher and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. 66 (1997), 433–449.

[7] R. J. Evans, *Classical congruences for parameters in binary quadratic forms*, Finite Fields Appl. 7 (2001), 110–124.

[8] B. Gross and N. Koblitz, *Gauss sums and the p-adic Γ-function*, Ann. of Math. (2) 109 (1979), 569–581.

[9] L. J. Mordell, *The congruence* $((p-1)/2)! \equiv \pm 1 \pmod{p}$, Amer. Math. Monthly 68 (1961), 145–146.

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

[11] J. Urbanowicz and K. S. Williams, *Congruences for L-functions*, Math. Appl. 511, Kluwer, Dordrecht, 2000.

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

Received on 21.3.2000 (3781)