Can. J. Math., Vol. XXXIV, No. 4, 1982, pp. 969–988

CLASS NUMBERS AND BIQUADRATIC RECIPROCITY

KENNETH S. WILLIAMS AND JAMES D. CURRIE

0. Notation. Throughout this paper p denotes a prime congruent to 1 modulo 4. It is well known that such primes are expressible in an essentially unique manner as the sum of the squares of two integers, that is,

$$(0.1)\quad p = a^2 + b^2,\ a \equiv 1 \pmod 2,\ b \equiv 0 \pmod 2,$$

with $|a|$ and $|b|$ uniquely determined by (0.1). Since a is odd, replacing a by $-a$ if necessary, we can specify a uniquely by

$$(0.2)\quad a \equiv 1 \pmod 4.$$

Further, as $\{[(p-1)/2]!\}^2 \equiv -1 \pmod p$, we can specify b uniquely by

$$(0.3)\quad b \equiv [(p-1)/2]!a \pmod p.$$

These choices are assumed throughout.

The following notation is also used throughout the paper: $h(d)$ denotes the class number of the quadratic field $Q(\sqrt{d})$ of discriminant d, (d/n) is the Kronecker symbol of modulus $|d|$, $[x]$ denotes the greatest integer less than or equal to the real number x, and $\{x\} = x - [x]$. It is also convenient to introduce the sums

$$(0.4)\quad S(l, m) = S_p(l, m) = \sum_{(m-1)p/l<k<mp/l} \left(\frac{k}{p}\right)$$

defined for $l = 1, 2, 3, \ldots$; $m = 1, 2, \ldots, l$, and $p \nmid l$. We note the following simple properties of these sums:

$$(0.5)\quad \sum_{m=1}^{l} S(l, m) = \sum_{0<k<p} \left(\frac{k}{p}\right) = 0,$$

$$(0.6)\quad \sum_{m=1}^{l/2} S(l, m) = \sum_{0<k<p/2} \left(\frac{k}{p}\right) = 0 \quad (l \text{ even}),$$

$$(0.7)\quad S(l, m) = S(l, l-m+1),$$

$$(0.8)\quad S(l, m) \equiv \sum_{(m-1)p/l<k<mp/l} 1 \equiv [mp/l] - [(m-1)p/l] \pmod 2.$$

Received September 16, 1981. The research of the first author was supported by Natural Sciences and Engineering Research Council Canada Grant No. A-7233, while that of the second was supported by a Natural Sciences and Engineering Research Council Canada Undergraduate Summer Research Award.

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

In addition use is made of the following result which is the special case of the theorem of Johnson and Mitchell [**6**] when p is taken to be a prime congruent to 1 (mod 4):

If l, m, n are integers satisfying

$$l \not\equiv 0 (\mathrm{mod}\ p), \quad 1 \leqq m \leqq n,$$

then

$$(0.9) \quad \left(\frac{l}{p}\right) S(n, m) = \sum_{j=0}^{[(l-1)/2]} S(ln, jn + m) + \sum_{j=1}^{[l/2]} S(ln, jn - m + 1).$$

1. Introduction. If $q \equiv 3 \pmod 4$ is prime, it is known that the class number $h(-qp)$ of the imaginary quadratic field $Q(\sqrt{-qp})$ satisfies

$$(1.1) \quad h(-qp) \equiv \begin{cases} 0 (\mathrm{mod}\ 4), & \text{if } \left(\frac{p}{q}\right) = +1, \\ 2 (\mathrm{mod}\ 4), & \text{if } \left(\frac{p}{q}\right) = -1, \end{cases}$$

(see for example [**9**, p. 189]). It is the purpose of this paper to show how $h(-qp)$ is determined modulo 8 by a congruence (mod q) involving a and b. We prove

THEOREM. *Let p and q be primes with $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. Define a and b by* (0.1), (0.2) *and* (0.3). *Then*

(a) *if $(p/q) = +1$ (equivalently $(q/p) = +1$) we have*

$$h(-qp) \equiv \begin{cases} 0 (\mathrm{mod}\ 8), & \text{if } \left(\frac{a - bi}{a + bi}\right)^{(q+1)/4} \equiv 1 (\mathrm{mod}\ q), \\ 4 (\mathrm{mod}\ 8), & \text{if } \left(\frac{a - bi}{a + bi}\right)^{(q+1)/4} \equiv -1 (\mathrm{mod}\ q); \end{cases}$$

(b) *if $(p/q) = -1$ (equivalently $(q/p) = -1$) we have* (i) *if $q > 3$ and $h(-q) \equiv 1 \pmod 4$*

$$h(-qp) \equiv \begin{cases} 2 (\mathrm{mod}\ 8), & \text{if } \left(\frac{a - bi}{a + bi}\right)^{(q+1)/4} \equiv -i (\mathrm{mod}\ q), \\ 6 (\mathrm{mod}\ 8), & \text{if } \left(\frac{a - bi}{a + bi}\right)^{(q+1)/4} \equiv i (\mathrm{mod}\ q), \end{cases}$$

(ii) *if $q > 3$ and $h(-q) \equiv 3 \pmod 4$*

$$h(-qp) \equiv \begin{cases} 2 (\mathrm{mod}\ 8), & \text{if } \left(\frac{a - bi}{a + bi}\right)^{(q+1)/4} \equiv i (\mathrm{mod}\ q), \\ 6 (\mathrm{mod}\ 8), & \text{if } \left(\frac{a - bi}{a + bi}\right)^{(q+1)/4} \equiv -i (\mathrm{mod}\ q), \end{cases}$$

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

(iii) *if* $q = 3$

$$h(-3p) \equiv \begin{cases} 2 \pmod 8, & \text{if } a \equiv -b \pmod 3, \\ 6 \pmod 8, & \text{if } a \equiv b \pmod 3. \end{cases}$$

We state the special cases $q = 3$, 7 and 11 of the theorem as corollaries.

COROLLARY 1. *Let* $p \equiv 1 \pmod 4$ *be a prime.*
If $p \equiv 1 \pmod 3$ *then*

$$h(-3p) \equiv \begin{cases} 0 \pmod 8, & \text{if } b \equiv 0 \pmod 3, \\ 4 \pmod 8, & \text{if } a \equiv 0 \pmod 3. \end{cases}$$

If $p \equiv 2 \pmod 3$ *then*

$$h(-3p) \equiv \begin{cases} 2 \pmod 8, & \text{if } a \equiv -b \pmod 3, \\ 6 \pmod 8, & \text{if } a \equiv b \pmod 3. \end{cases}$$

COROLLARY 2. *Let* $p \equiv 1 \pmod 4$ *be a prime.*
If $p \equiv 1, 2, 4 \pmod 7$ *then*

$$h(-7p) = \begin{cases} 0 \pmod 8, & \text{if } ab \equiv 0 \pmod 7, \\ 4 \pmod 8, & \text{if } ab \not\equiv 0 \pmod 7. \end{cases}$$

If $p \equiv 3, 5, 6 \pmod 7$ *then*

$$h(-7p) \equiv \begin{cases} 2 \pmod 8, & \text{if } a \equiv -2b, -3b \pmod 7, \\ 6 \pmod 8, & \text{if } a \equiv 2b, 3b \pmod 7. \end{cases}$$

COROLLARY 3. *Let* $p \equiv 1 \pmod 4$ *be a prime.*
If $p \equiv 1, 3, 4, 5, 9 \pmod{11}$ *then*

$$h(-11p) \equiv \begin{cases} 0 \pmod 8, & \text{if } b \equiv 0 \pmod{11} \text{ or } a \equiv \pm 2b \pmod{11}, \\ 4 \pmod 8, & \text{if } a \equiv 0 \pmod{11} \text{ or } a \equiv \pm 5b \pmod{11}. \end{cases}$$

If $p \equiv 2, 6, 7, 8, 10 \pmod{11}$ *then*

$$h(-11p) \equiv \begin{cases} 2 \pmod 8, & \text{if } a \equiv -b, -3b, -4b \pmod{11}, \\ 6 \pmod 8, & \text{if } a \equiv b, 3b, 4b \pmod{11}. \end{cases}$$

The congruence modulo 8 for $h(-4p)$ analogous to those in the theorem for $h(-qp)$ was given by Gauss [**4**] in a letter to Dirichlet dated 30 May, 1828. A sketch of a proof of Gauss's congruence will now be given as it serves as the model for the proof of our theorem. However, the details in the proof of our theorem are much more complicated.

The starting point of the proof is Dirichlet's class number formula [**3**, p. 152]

$$(1.2) \quad h(-4p) = 2S(4, 1).$$

(The corresponding formula in our proof is given in Lemma 2 as a special

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

case of Lemma 1.) Formula (1.2) is trivially transformed into

$$(1.3)\quad h(-4p) = \tfrac{1}{2}(p-1) - 4N,$$

where N denotes the number of quadratic non residues (mod p) in the interval $(0, p/4)$. (In our proof the derivation of the corresponding result (Lemma 12), though elementary, is highly technical in nature and requires Lemmas 3 to 11.) Next, modifying the argument given in [**10**, Lemma 3] slightly, it can be shown that

$$(1.4)\quad 2^{(p-1)/4} \equiv \begin{cases} (-1)^N (\text{mod } p), & \text{if } p \equiv 1 (\text{mod } 8), \\ (-1)^N \left(\dfrac{p-1}{2}\right)! \ (\text{mod } p), & \text{if } p \equiv 5 (\text{mod } 8). \end{cases}$$

(The corresponding result in our proof is Lemma 13.) Putting (1.3) and (1.4) together gives

$$(1.5)\quad 2^{(p-1)/4} \equiv \begin{cases} (-1)^{(p-1)/8 + h(-4p)/4} (\text{mod } p), & \text{if } p \equiv 1 (\text{mod } 8), \\ (-1)^{(p-5)/8 + (h(-4p)-2)/4} \left(\dfrac{p-1}{2}\right)! \ (\text{mod } p), & \\ & \text{if } p \equiv 5 (\text{mod } 8). \end{cases}$$

(The corresponding result in our proof is Lemma 14.) Then using the supplement to the law of biquadratic reciprocity in the form (see for example [**7**])

$$(1.6)\quad 2^{(p-1)/4} \equiv \begin{cases} 1 (\text{mod } p), & \text{if } b \equiv 0 (\text{mod } 8), \\ b/a (\text{mod } p), & \text{if } b \equiv 2 (\text{mod } 8), \\ -1 (\text{mod } p), & \text{if } b \equiv 4 (\text{mod } 8), \\ -b/a (\text{mod } p), & \text{if } b \equiv 6 (\text{mod } 8), \end{cases}$$

in (1.5), and recalling that

$$(1.7)\quad p \equiv \begin{cases} 2a - 1 (\text{mod } 16), & \text{if } p \equiv 1 (\text{mod } 8), \\ 2a + 3 (\text{mod } 16), & \text{if } p \equiv 5 (\text{mod } 8), \end{cases}$$

one obtains Gauss's congruence

$$(1.8)\quad h(-4p) \equiv -a + b + 1 \ (\text{mod } 8).$$

(The last steps in our proof are exactly analogous to the above except that we use the law of biquadratic reciprocity in the form given in [**5**] rather than its supplement.)

2. Proof of theorem. We begin the proof of the theorem by obtaining a general formula for the class number $h(dp)$ of the imaginary quadratic field $Q(\sqrt{dp})$, where $d \not\equiv 0$ (mod p) is the discriminant of an imaginary quadratic field, in terms of the sums $S(|d|, k)$, $k = 1, 2, \ldots, |d|$.

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

LEMMA 1. *If* $p \equiv 1 \pmod 4$ *is prime and* $d \not\equiv 0 \pmod p$ *is the discriminant of an imaginary quadratic field, then*

$$h(dp) = \sum_{k=1}^{|d|} \left(\sum_{j=k}^{|d|} \left(\frac{d}{j}\right)\right) S(|d|, k).$$

Proof. By Dirichlet's class number formula (see for example [**2**, p. 343], we have

$$h(dp) = \frac{\sqrt{|d|p}}{\pi} \sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{dp}{n}\right) = \frac{\sqrt{p}}{\pi} \sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{n}{p}\right) \left(\frac{d}{n}\right) \sqrt{|d|}.$$

Using the well-known Gaussian sum (see for example [**1**, p. 265])

$$\sum_{j=1}^{|d|} \left(\frac{d}{j}\right) \exp (2\pi inj/|d|) = i\left(\frac{d}{n}\right)\sqrt{|d|}, \quad (d < 0)$$

we obtain

$$\begin{aligned} h(dp) &= \frac{\sqrt{p}}{\pi} \sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{n}{p}\right) \sum_{j=1}^{|d|} \left(\frac{d}{j}\right) \sin (2\pi nj/|d|) \\ &= \frac{\sqrt{p}}{\pi} \sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{n}{p}\right) \sum_{j=1}^{|d|} \left(\frac{d}{j}\right) \sum_{k=1}^{j} (\sin (2\pi nk/|d|) \\ &\qquad - \sin (2\pi n(k - 1)/|d|). \end{aligned}$$

First interchanging the orders of summation of j and k and then of k, j and n, we obtain

$$\begin{aligned} h(dp) &= \frac{\sqrt{p}}{\pi} \sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{n}{p}\right) \sum_{k=1}^{|d|} \sum_{j=k}^{|d|} \left(\frac{d}{j}\right) (\sin (2\pi nk/|d|) \\ &\qquad - \sin (2\pi n(k - 1)/|d|)) \\ &= \frac{\sqrt{p}}{\pi} \sum_{k=1}^{|d|} \sum_{j=k}^{|d|} \left(\frac{d}{j}\right) \sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{n}{p}\right) (\sin (2\pi nk/|d|) \\ &\qquad - \sin (2\pi n(k - 1)/|d|)). \end{aligned}$$

We now make use of a form of the Poisson summation formula given by Berndt [**1**, p. 293], namely, if f is continuous and of bounded variation on $[a, b]$ and χ is a primitive even character of modulus m then

$$\sum_{a<n<b}{}' \chi(n)f(n) = \frac{2G(\chi)}{m} \sum_{n=1}^{\infty} \bar{\chi}(n) \int_a^b f(x) \cos (2\pi nx/m)dx,$$

where

$$G(\chi) = \sum_{j=1}^{m} \chi(j) \exp (2\pi ij/m).$$

The prime on the summation symbol indicates that if a or b is an integer, then the associated summand must be halved. Choosing $f(x) \equiv 1$, $\chi(n) = (p/n) = (n/p)$ so that $m = p$ and $G(\chi) = \sqrt{p}$, $a = (k - 1)p/$

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

$d|$, and $b = kp/|d|$, we have

$$\sum_{(k-1)p/|d|<n<kp/|d|} \left(\frac{n}{p}\right) = \frac{\sqrt{p}}{\pi} \sum_{n=1}^{\infty} \frac{1}{n} \left(\frac{n}{p}\right) (\sin(2\pi nk/|d|) - \sin(2\pi n(k-1)/|d|))$$

and the required result follows.

Taking $d = -q$, where $q \equiv 3 \pmod 4$ is prime, in Lemma 1, we obtain

LEMMA 2. *If $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ are primes then*

$$h(-qp) = \sum_{k=1}^{q} \left(\sum_{j=k}^{q} \left(\frac{j}{q}\right)\right) S(q, k).$$

Our next step is to express the right-hand-side of the equality in Lemma 2 as a multiple of 2. We prove

LEMMA 3. *If $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ are primes then*

$$h(-qp) = 2\left(\sum_{k=1}^{(q-1)/2} \left(1 + \sum_{j=k}^{q-1} \left(\frac{j}{q}\right)\right) S(q, k) + \left(\frac{2}{p}\right)(1 - w(q)h(-q))S\left(2q, \frac{q+1}{2}\right)\right),$$

where

$$w(q) = \begin{cases} 2 - \left(\frac{2}{q}\right), & \text{if } q > 3, \\ 1, & \text{if } q = 3. \end{cases}$$

Proof. By (0.5) we have

$$\sum_{k=1}^{q} S(q, k) = 0.$$

Using this together with Lemma 2 gives

$$h(-qp) = \sum_{k=1}^{q} \left(1 + \sum_{j=k}^{q} \left(\frac{j}{q}\right)\right) S(q, k).$$

Next, mapping k to $q - k + 1$, we obtain

$$\sum_{k=(q+3)/2}^{q} \left(1 + \sum_{j=k}^{q} \left(\frac{j}{q}\right)\right) S(q, k) = \sum_{k=1}^{(q-1)/2} \left(1 + \sum_{j=q-k+1}^{q} \left(\frac{j}{q}\right)\right) S(q, q-k+1).$$

Since (by (0.7))

$$S(q, q-k+1) = S(q, k)$$

and

$$\sum_{j=q-k+1}^{q} \left(\frac{j}{q}\right) = -\sum_{j=1}^{q-k} \left(\frac{j}{q}\right) = \sum_{j=k}^{q-1} \left(\frac{j}{q}\right),$$

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

we have

$$\sum_{k=(q+3)/2}^{q}\left(1+\sum_{j=k}^{q}\left(\frac{j}{q}\right)\right)S(q,k)=\sum_{k=1}^{(q-1)/2}\left(1+\sum_{j=k}^{q-1}\left(\frac{j}{q}\right)\right)S(q,k),$$

and so

$$h(-qp)=2\sum_{k=1}^{(q-1)/2}\left(1+\sum_{j=k}^{q-1}\left(\frac{j}{q}\right)\right)S(q,k)$$
$$+\left(1+\sum_{j=(q+1)/2}^{q-1}\left(\frac{j}{q}\right)\right)S\left(q,\frac{q+1}{2}\right).$$

Now, appealing to (0.9) with $l = 2$, $m = (q + 1)/2$, $n = q$, we have

$$\left(\frac{2}{p}\right)S\left(q,\frac{q+1}{2}\right)=2S\left(2q,\frac{q+1}{2}\right),$$

and, by a result of Dirichlet [**3**, p. 151],

$$\sum_{j=(q+1)/2}^{q-1}\left(\frac{j}{q}\right)=-\sum_{j=1}^{(q-1)/2}\left(\frac{j}{q}\right)=-w(q)h(-q),$$

where $w(q)$ is defined in the statement of Lemma 3, so that

$$\left(1+\sum_{j=(q+1)/2}^{q-1}\left(\frac{j}{q}\right)\right)S\left(q,\frac{q+1}{q}\right)$$
$$=2\left(\frac{2}{p}\right)(1-w(q)h(-q))S\left(2q,\frac{q+1}{2}\right),$$

completing the proof of the lemma.

The quantity

$$\left(\frac{2}{p}\right)(1-w(q)h(-q))S\left(2q,\frac{q+1}{2}\right)$$

appearing in Lemma 3 is determined modulo 4 in the next lemma.

LEMMA 4. *If* $p \equiv 1 \pmod 4$ *and* $q \equiv 3 \pmod 4$ *are primes then*

$$\left(\frac{2}{p}\right)(1-w(q)h(-q))S\left(2q,\frac{q+1}{2}\right)$$
$$\equiv (1-w(q)h(-q))[(q-1)p/2q] \pmod 4.$$

Proof. As $h(-q) \equiv 1 \pmod 2$ for $q \equiv 3 \pmod 4$ (see for example [**1**, Corollary 3.6] or [**9**, Proposition 1]) $1 - w(q)h(-q)$ is even and it suffices to consider the parity of $S(2q, (q + 1)/2))$. By (0.8) we have

$$S(2q,(q+1)/2) \equiv [(q+1)p/4q]-[(q-1)p/4q] \pmod 2.$$

Since

$$[(q+1)p/4q]-[(q-1)p/4q]+[(q-1)p/2q]=\tfrac{1}{2}(p-1),$$

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

we have

$$S\left(2q, \frac{q+1}{2}\right) \equiv [(q-1)p/2q] (\text{mod } 2),$$

which completes the proof.

We now begin our consideration of the quantity

$$\sum_{k=1}^{(q-1)/2} \left(1 + \sum_{j=k}^{q-1} \left(\frac{j}{q}\right)\right) S(q, k)$$

appearing in Lemma 3.

LEMMA 5. *If $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ are primes then*

$$\sum_{k=1}^{(q-1)/2} \left(1 + \sum_{j=k}^{q-1} \left(\frac{j}{q}\right)\right) S(q, k)$$
$$= \left(\frac{2}{p}\right) \sum_{k=1}^{(q-1)/2} S(2q, 2k) + 2 \sum_{k=1}^{(q-3)/4} A(k) S(q, 2k)$$
$$+ 2 \sum_{k=1}^{(q+1)/4} B(k) S(q, 2k-1),$$

where $A(k)$ and $B(k)$ are integers given by

$$A(k) = \frac{1}{2}\left(1 + \sum_{j=2k}^{q-1} \left(\frac{j}{q}\right)\right), \quad B(k) = 1 + \frac{1}{2} \sum_{j=2k-1}^{q=1} \left(\frac{j}{q}\right).$$

Proof. We make use of the following result (valid for $1 \leqq k \leqq q$)

$$S(q, k) = \left(\frac{2}{p}\right)(S(2q, k) + S(2q, q-k+1)),$$

which follows from (0.9) with $l = 2$, $m = k$, $n = q$.

We have

$$\sum_{k=1}^{(q-1)/2} \left(1 + \sum_{j=k}^{q-1} \left(\frac{j}{q}\right)\right) S(q, k) - 2 \sum_{k=1}^{(q-3)/4} A(k) S(q, 2k)$$
$$- 2 \sum_{k=1}^{(q+1)/4} B(k) S(q, 2k-1)$$
$$= \sum_{\substack{k=1 \\ k \text{ odd}}}^{(q-1)/2} \left(1 + \sum_{j=k}^{q-1} \left(\frac{j}{q}\right)\right) S(q, k) - \sum_{\substack{k=1 \\ k \text{ odd}}}^{(q-1)/2} \left(2 + \sum_{j=k}^{q-1} \left(\frac{j}{q}\right)\right) S(q, k)$$
$$= - \sum_{\substack{k=1 \\ k \text{ odd}}}^{(q-1)/2} S(q, k) = - \left(\frac{2}{p}\right) \sum_{\substack{k=1 \\ k \text{ odd}}}^{(q-1)/2} (S(2q, k) + S(2q, q-k+1))$$
$$= - \left(\frac{2}{p}\right) \sum_{\substack{k=1 \\ k \text{ odd}}}^{q} S(2q, k) = \left(\frac{2}{p}\right) \sum_{\substack{k=1 \\ k \text{ even}}}^{q} S(2q, k) \quad \text{(by (0.6))}$$
$$= \left(\frac{2}{p}\right) \sum_{k=1}^{(q-1)/2} S(2q, 2k),$$

as required.

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

Next we determine

$$\sum_{k=1}^{(q-3)/4} A(k)S(q, 2k) \quad \text{and} \quad \sum_{k=1}^{(q+1)/4} B(k)S(q, 2k - 1) \text{ modulo } 2.$$

LEMMA 6. *If* $p \equiv 1 \pmod 4$ *and* $q \equiv 3 \pmod 4$ *are primes then*

$$\sum_{k=1}^{(q-3)/4} A(k)S(q, 2k) \equiv \frac{1}{2} \sum_{k=1}^{(q-3)/2} (-1)^k [kp/q]$$
$$- \frac{1}{2} \sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right) \sum_{k=2[j/2]+1}^{(q-3)/2} (-1)^k [kp/q] \pmod 2$$

and

$$\sum_{k=1}^{(q+1)/4} B(k)S(q, 2k - 1) \equiv \sum_{k=1}^{(q-1)/2} (-1)^{k-1} [kp/q]$$
$$- \frac{1}{2} \sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right) \sum_{k=2[(j+1)/2]}^{(q-1)/2} (-1)^{k-1} [kp/q] \pmod 2.$$

Proof. We just give the details of the proof for the first of these as the other can be proved similarly. We have by (0.8)

$$\sum_{k=1}^{(q-3)/4} A(k)S(q, 2k)$$
$$\equiv \frac{1}{2} \sum_{k=1}^{(q-3)/4} \left(1 + \sum_{j=2k}^{q-1} \left(\frac{j}{q}\right)\right) ([2kp/q] - [(2k - 1)p/q]) \pmod 2$$
$$\equiv \frac{1}{2} \sum_{k=1}^{(q-3)/2} (-1)^k [kp/q]$$
$$+ \frac{1}{2} \sum_{k=1}^{(q-3)/4} \sum_{j=2k}^{q-1} \left(\frac{j}{q}\right) ([2kp/q] - [(2k - 1)p/q]) \pmod 2.$$

Interchanging the order of summation in the double sum we obtain

$$\sum_{k=1}^{(q-3)/4} \sum_{j=2k}^{q-1} \left(\frac{j}{q}\right) ([2kp/q] - [(2k - 1)p/q])$$
$$= \sum_{j=1}^{(q-3)/2} \left(\frac{j}{q}\right) \sum_{k=1}^{[j/2]} ([2kp/q] - [(2k - 1)p/q])$$
$$+ \sum_{j=(q-1)/2}^{q-1} \left(\frac{j}{q}\right) \sum_{k=1}^{(q-3)/4} ([2kp/q] - [(2k - 1)p/q])$$
$$= - \sum_{j=1}^{(q-3)/2} \left(\frac{j}{q}\right) \sum_{k=[j/2]+1}^{(q-3)/4} ([2kp/q] - [(2k - 1)p/q])$$
$$= - \sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right) \sum_{k=[j/2]+1}^{(q-3)/4} ([2kp/q] - [(2k - 1)p/q]),$$

which completes the proof.

The next lemma simplifies the sum of the congruences in Lemma 6.

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

LEMMA 7. *If* $p \equiv 1 \pmod 4$ *and* $q \equiv 3 \pmod 4$ *are primes then*

$$\sum_{k=1}^{(q-3)/4} A(k)S(q, 2k) + \sum_{k=1}^{(q+1)/4} B(k)S(q, 2k-1)$$
$$\equiv \frac{1}{2}\sum_{k=1}^{(q-1)/2} (-1)^{k-1}[kp/q] + \frac{1}{2}(1 - w(q)h(-q))[(q-1)p/2q]$$
$$+ \frac{1}{2}\sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right)[jp/q] \pmod 2.$$

Proof. We have

$$\frac{1}{2}\sum_{k=1}^{(q-3)/2} (-1)^{k}[kp/q] + \sum_{k=1}^{(q-1)/2} (-1)^{k-1}[kp/q]$$
$$= \frac{1}{2}\sum_{k=1}^{(q-1)/2} ((-1)^k + 2(-1)^{k-1})[kp/q]$$
$$- \frac{1}{2}(-1)^{(q-1)/2}[(q-1)p/2q]$$
$$= \frac{1}{2}\sum_{k=1}^{(q-1)/2} (-1)^{k-1}[kp/q + \frac{1}{2}[(q-1)p/2q]$$

and

$$\sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right) \sum_{k=2[j/2]+1}^{(q-3)/2} (-1)^{k}[kp/q]$$
$$+ \sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right) \sum_{k=2[(j+1)/2]}^{(q-1)/2} (-1)^{k-1}[kp/q]$$
$$= \sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right)([(q-1)p/2q] - [jp/q])$$
$$= w(q)h(-q)[(q-1)p/2q] - \sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right)[jp/q],$$

and the result follows from Lemma 6.

The next lemma evaluates the sum

$$\sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right)[jp/q]$$

appearing in Lemma 7.

LEMMA 8. *If* $p \equiv 1 \pmod 4$ *and* $q \equiv 3 \pmod 4$ *are primes then*

$$\sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right)[jp/q] = \frac{h(-q)}{2}\left((p-1)w(q) - \left(p - \left(\frac{p}{q}\right)\right)v(q)\right),$$

where

$$v(q) = \begin{cases} 1, & \textit{if } q > 3, \\ 1/3, & \textit{if } q = 3. \end{cases}$$

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

Proof. We have

$$\sum_{j=(q+1)/2}^{q-1} \left(\frac{j}{q}\right)[jp/q] = -\sum_{j=1}^{(q-1)/2} \left(\frac{q-j}{q}\right)\left[p - \frac{jp}{q}\right]$$

$$= -\sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right)(p - 1 - [jp/q])$$

$$= -(p-1)w(q)h(-q) + \sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right)[jp/q],$$

so

$$\sum_{j=1}^{q-1} \left(\frac{j}{q}\right)[jp/q] = -(p-1)w(q)h(-q) + 2\sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right)[jp/q].$$

Now we have

$$\sum_{j=1}^{q-1} \left(\frac{j}{q}\right)[jp/q] = \frac{p}{q}\sum_{j=1}^{q-1} \left(\frac{j}{q}\right)j - \sum_{j=1}^{q-1} \left(\frac{j}{q}\right)\{jp/q\}.$$

Since (j/q) and $\{jp/q\}$ are periodic functions of j with period q, we have

$$\sum_{j=1}^{q-1} \left(\frac{j}{q}\right)\{jp/q\} = \left(\frac{p}{q}\right)\sum_{j=1}^{q-1} \left(\frac{j}{q}\right)\{j/q\} = \frac{1}{q}\left(\frac{p}{q}\right)\sum_{j=1}^{q-1} \left(\frac{j}{q}\right)j,$$

and so

$$\sum_{j=1}^{q-1} \left(\frac{j}{q}\right)[jp/q] = \frac{1}{q}\left(p - \left(\frac{p}{q}\right)\right)\sum_{j=1}^{q-1} \left(\frac{j}{q}\right)j.$$

As (see for example [**2**, p. 344])

$$\sum_{j=1}^{q-1} \left(\frac{j}{q}\right)j = -qv(q)h(-q),$$

where $v(q)$ is defined in the statement of Lemma 8, we have

$$\sum_{j=1}^{q-1} \left(\frac{j}{q}\right)[jp/q] = -\left(p - \left(\frac{p}{q}\right)\right)v(q)h(-q),$$

and thus

$$\sum_{j=1}^{(q-1)/2} \left(\frac{j}{q}\right)[jp/q] = \frac{h(-q)}{2}\left((p-1)w(q) - \left(p - \left(\frac{p}{q}\right)\right)v(q)\right),$$

as required.

The next lemma gives an alternative expression for the sum

$$\sum_{k=1}^{(q-1)/2} (-1)^{k-1}[kp/q]$$

appearing in Lemma 7.

LEMMA 9. *If $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ are primes then*

$$\sum_{j=1}^{(q-1)/2} (-1)^{j-1}[jp/q] = \frac{1}{2}(p-1) - \sum_{j=1}^{q-1} (-1)^j [jp/2q].$$

Proof. We have

$$\begin{aligned}\sum_{j=(q+1)/2}^{q-1} (-1)^{j-1}[jp/q] &= \sum_{j=1}^{(q-1)/2} (-1)^{q-j-1}[(q-j)p/q] \\ &= \sum_{j=1}^{(q-1)/2} (-1)^j \left[p - \frac{jp}{q}\right] = \sum_{j=1}^{(q-1)/2} (-1)^j (p - 1 - [jp/q]) \\ &= -(p-1) + \sum_{j=1}^{(q-1)/2} (-1)^{j-1}[jp/q]\end{aligned}$$

so that

$$\sum_{j=1}^{q-1} (-1)^{j-1}[jp/q] = -(p-1) + 2\sum_{j=1}^{(q-1)/2} (-1)^{j-1}[jp/q].$$

Hence

$$\sum_{j=1}^{(q-1)/2} (-1)^{j-1}[jp/q] = \frac{1}{2}(p-1) + \frac{1}{2}\sum_{j=1}^{q-1} (-1)^{j-1}[jp/q]$$

and it suffices to prove that

$$\sum_{j=1}^{q-1} (-1)^{j-1}[jp/q] + 2\sum_{j=1}^{q-1} (-1)^j [jp/2q] = 0.$$

Using the simple result

$$2[x/2] = \begin{cases} [x], & \text{if } \{x/2\} < 1/2, \\ [x] - 1, & \text{if } \{x/2\} \geqq 1/2, \end{cases}$$

we have

$$\begin{aligned}&\sum_{j=1}^{q-1} (-1)^{j-1}[jp/q] + 2\sum_{j=1}^{q-1} (-1)^j [jp/2q] \\ &= \sum_{\substack{j=1 \\ \{jp/2q\}<1/2}}^{q-1} (-1)^{j-1}[jp/q] + \sum_{\substack{j=1 \\ \{jp/2q\}\geqq 1/2}}^{q-1} (-1)^{j-1}[jp/q] \\ &\quad + \sum_{\substack{j=1 \\ \{jp/2q\}<1/2}}^{q-1} (-1)^j [jp/q] + \sum_{\substack{j=1 \\ \{jp/2q\}\geqq 1/2}}^{q-1} (-1)^j ([jp/q] - 1) \\ &= \sum_{\substack{j=1 \\ [jp/2q]\geqq 1/2}}^{q-1} (-1)^{j-1}.\end{aligned}$$

The last sum is clearly seen to vanish by pairing the terms j and $q - j$. This completes the proof.

Using the expressions given in Lemmas 8 and 9 in Lemma 7 we obtain

LEMMA 10. *For primes* $p \equiv 1 \pmod 4$ *and* $q \equiv 3 \pmod 4$

$$\sum_{k=1}^{(q-3)/4} A(k)S(q, 2k) + \sum_{k=1}^{(q+1)/4} B(k)S(q, 2k-1)$$

$$\equiv \frac{p-1}{4} - \frac{1}{2}\sum_{j=1}^{q-1} (-1)^j[jp/2q]$$

$$+ \frac{1}{2}(1 - w(q)h(-q))[(q-1)p/2q]$$

$$+ \frac{h(-q)}{4}\left((p-1)w(q) - \left(p - \left(\frac{p}{q}\right)\right)v(q)\right) \pmod 2.$$

Using this in Lemma 5 gives

LEMMA 11. *For primes* $p \equiv 1 \pmod 4$ *and* $q \equiv 3 \pmod 4$

$$\sum_{k=1}^{(q-1)/2} \left(1 + \sum_{j=k}^{q-1}\left(\frac{j}{q}\right)\right) S(q, k)$$

$$\equiv \left(\frac{2}{p}\right)\sum_{k=1}^{(q-1)/2} S(2q, 2k) + \frac{p-1}{2} - \sum_{j=1}^{q-1} (-1)^j[jp/2q]$$

$$+ (1 - w(q)h(-q))[(q-1)p/2q]$$

$$+ \frac{h(-q)}{2}\left((p-1)w(q) - \left(p - \left(\frac{p}{q}\right)\right)v(q)\right) \pmod 4.$$

Appealing to Lemmas 3, 4 and 11 gives

LEMMA 12. *Let* $p \equiv 1 \pmod 4$ *and* $q \equiv 3 \pmod 4$ *be primes, and let* $N(p, q, j)$ *denote the number of quadratic nonresidues* (mod p) *in the interval* $((2j-1)p/2q, 2jp/2q)$. *Then if* $(p/q) = 1$ *we have*

$$h(-qp) \equiv 4\sum_{j=1}^{(q-1)/2} N(p, q, j) + p - 1 \pmod 8.$$

and if $(p/q) = -1$ *we have*

$$h(-qp) \equiv \begin{cases} 4\displaystyle\sum_{j=1}^{(q-1)/2} N(p, q, j) + 2 \pmod 8. & \text{if } q = 3, \\ 4\displaystyle\sum_{j=1}^{(q-1)/2} N(p, q, j) - 2h(-q) \pmod 8, & \text{if } q > 3. \end{cases}$$

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

Proof. By Lemmas 3, 4 and 11 we have

$$h(-qp) \equiv 2\left(\frac{2}{p}\right) \sum_{k=1}^{(q-1)/2} S(2q, 2k) + p - 1 - 2 \sum_{j=1}^{q-1} (-1)^j [jp/2q] + h(-q) \times \left((p-1)w(q) - \left(p - \left(\frac{p}{q}\right)\right)v(q)\right) \pmod 8.$$

Next we determine

$$\sum_{k=1}^{(q-1)/2} S(2q, 2k)$$

modulo 2. We have by (0.8)

$$\sum_{k=1}^{(q-1)/2} S(2q, 2k) \equiv \sum_{k=1}^{(q-1)/2} ([2kp/2q] - [(2k-1)p/2q]) \pmod 2$$
$$\equiv \sum_{k=1}^{q-1} (-1)^k [kp/2q] \pmod 2.$$

Appealing to Lemma 9 we obtain

$$\sum_{k=1}^{(q-1)/2} S(2q, 2k) \equiv \frac{1}{2}(p-1) - \sum_{k=1}^{(q-1)/2} (-1)^{k-1}[kp/q] \pmod 2$$
$$\equiv \sum_{k=1}^{(q-1)/2} [kp/q] \equiv \begin{cases} 0 \pmod 2, & \text{if } \left(\frac{p}{q}\right) = +1, \\ 1 \pmod 2, & \text{if } \left(\frac{p}{q}\right) = -1. \end{cases}$$

(The last congruence follows from a form of Gauss's lemma.) Then if $(p/q) = -1$ we have

$$h(-qp) \equiv 2 \sum_{k=1}^{(q-1)/2} S(2q, 2k) - 2 \sum_{j=1}^{q-1} (-1)^j [jp/2q] + h(-q)((p-1)w(q) - (p+1)v(q)) \pmod 8.$$

Since

$$N(p, q, j) = \frac{1}{2} \sum_{(2j-1)p/2q<k<2jp/2q} \left(1 - \left(\frac{k}{p}\right)\right)$$
$$= \frac{1}{2}([2jp/2q] - [(2j-1)p/2q] - S(2q, 2j))$$

we have

$$\sum_{j=1}^{(q-1)/2} N(p, q, j) = \frac{1}{2} \sum_{j=1}^{q-1} (-1)^j [jp/2q] - \frac{1}{2} \sum_{j=1}^{(q-1)/2} S(2q, 2j),$$

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

that is

$$\sum_{j=1}^{(q-1)/2} S(2q, 2j) = \sum_{j=1}^{q-1} (-1)^j [jp/2q] - 2 \sum_{j=1}^{(q-1)/2} N(p, q, j).$$

Hence we have

$$h(-qp) \equiv 4 \sum_{j=1}^{(q-1)/2} N(p, q, j)$$
$$+ h(-q)((p-1)w(q) - (p+1)v(q)) \pmod 8.$$

The required result now follows as $h(-3) = 1$ and

$$(p-1)w(q) - (p+1)v(q)$$
$$= \begin{cases} \frac{2}{3}(p-2) \equiv 2 \pmod 8, & \text{if } q = 3, \\ (p-1)\left(2 - \left(\frac{2}{q}\right)\right) - (p+1) \equiv -2 \pmod 8, & \text{if } q > 3. \end{cases}$$

If $(p/q) = +1$ we have

$$h(-qp) \equiv 2 \sum_{k=1}^{(q-1)/2} S(2q, 2k) + p - 1 - 2 \sum_{j=1}^{q-1} (-1)^j [jp/2q]$$
$$+ h(-q)(p-1)(w(q) - v(q)) \pmod 8 \equiv 4 \sum_{j=1}^{(q-1)/2} N(p, q, j)$$
$$+ p - 1 + h(-q)(p-1)(w(q) - v(q)) \pmod 8.$$

The result now follows as

$$(p-1)(w(q) - v(q)) \equiv 0 \pmod 8.$$

LEMMA 13. *Let p and q be odd distinct primes with $p \equiv 1 \pmod 4$. (We do not need to assume $q \equiv 3 \pmod 4$ for this lemma.) Then if $(p/q) = +1$ we have*

$$q^{(p-1)/4} \equiv (-1)^{\sum_{j=1}^{(q-1)/2} N(p,q,j)} \pmod p,$$

and if $(p/q) = -1$ we have

$$(-q)^{(p-1)/4} \equiv (-1)^{\sum_{j=1}^{(q-1)/2} N(p,q,j)} \left(\frac{p-1}{2}\right)! \pmod p.$$

Proof. Let s be the least positive integer such that

$$sp \equiv -1 \pmod q,$$

and define a positive integer t by

$$t = (sp + 1)/q.$$

We begin by treating the case $(p/q) = +1$. For each $j = 0, 1, \ldots, q - 1$ it is easy to check that as n runs through the quadratic non residues of p in $(0, p/2)$ which are congruent to $-pj \pmod q$, then nt runs through the quadratic non residues of p in $(2jp/2q, (2j + 1)p/2q)$. Hence for $j = 0, 1, \ldots, q - 1$ we have

$$\prod_{\substack{0<n<p/2 \\ n\equiv -pj (\mathrm{mod}\ q)}} nt \equiv \prod_{2jp/2q<n<(2j+1)p/2q} n \pmod p.$$

Multiplying these congruences together we obtain (as $qt \equiv 1 \pmod p$)

$$q^{-(p-1)/4} \prod_{0<n<p/2} n \equiv \prod_1 \prod_2 \pmod p,$$

where

$$\prod_1 = \prod_{j=0}^{(q-1)/2} \prod_{2jp/2q<n<(2j+1)p/2q} n,$$

$$\prod_2 = \prod_{j=(q+1)/2}^{q-1} \prod_{2jp/2q<n<(2j+1)p/2q} n.$$

Replacing j by $q - j$ in $\prod_2$ we obtain

$$\prod_2 = \prod_{j=1}^{(q-1)/2} \prod_{(2j-1)p/2q<p-n<2jp/2q} n.$$

Next replacing n by $p - n$ we get

$$\prod_2 \equiv (-1)^{\sum_{j=1}^{(q-1)/2} N(p,q,j)} \prod_{j=1}^{(q-1)/2} \prod_{(2j-1)p/2q<n<2jp/2q} n \pmod p,$$

where $N(p, q, j)$ denotes the number of quadratic non residues of p in $((2j - 1)p/2q, 2jp/2q)$. Hence

$$\prod_1 \prod_2 \equiv (-1)^{\sum_{j=1}^{(q-1)/2} N(p,q,j)} \prod_{0<n<p/2} n \pmod p,$$

and so

$$q^{(p-1)/4} \equiv (-1)^{\sum_{j=1}^{(q-1)/2} N(p,q,j)} \pmod p,$$

as required.

Next we treat the case $(p/q) = -1$. For each $j = 0, 1, \ldots, q - 1$ it is easy to check that as r runs through the quadratic residues of p in $(0, p/2)$ which are congruent to $-pj \pmod q$, then rt runs through the quadratic non residues n of p in $(2jp/2q, (2j + 1)p/2q)$. Hence for $j = 0, 1, \ldots, q - 1$ we have

$$\prod_{\substack{0<r<p/2 \\ r\equiv -pj (\mathrm{mod}\ q)}} rt \equiv \prod_{2jp/2q<n<(2j+1)p/2q} n \pmod p,$$

Multiplying these congruences together we obtain (as $qt \equiv 1 \pmod{p}$)

$$q^{-(p-1)/4} \prod_{0<r<p/2} r \equiv \prod_1 \prod_2 \pmod{p},$$

where

$$\prod_1 = \prod_{j=0}^{(q-1)/2} \prod_{2jp/2q<n<(2j+1)p/2q} n,$$

$$\prod_2 = \prod_{j=(q+1)/2}^{q-1} \prod_{2jp/2q<n<(2j+1)p/2q} n.$$

Replacing j by $q - j$ in $\prod_2$ we obtain

$$\prod_2 = \prod_{j=1}^{(q-1)/2} \prod_{(2j-1)p/2q<p-n<2jp/2q} n.$$

Next replacing n by $p - n$ we get

$$\prod_2 \equiv (-1)^{\sum_{j=1}^{(q-1)/2} N(p,q,j)} \prod_{j=1}^{(q-1)/2} \prod_{(2j-1)p/2q<n<2jp/2q} n \pmod{p},$$

where $N(p, q, j)$ denotes the number of quadratic non residues of p in $((2j - 1)p/2q, 2jp/2q)$. Hence we have

$$\prod_1 \prod_2 \equiv (-1)^{\sum_{j=1}^{(q-1)/2} N(p,q,j)} \prod_{0<n<p/2} n \pmod{p},$$

and so

$$q^{-(p-1)/4} \prod_{0<r<p/2} r \equiv (-1)^{\sum_{j=1}^{(q-1)/2} N(p,q,j)} \prod_{0<n<p/2} n \pmod{p}.$$

Multiplying both sides of this congruence by

$$\prod_{0<n<p/2} n \equiv (-1)^{(p-1)/4} \prod_{p/2<n<p} n \pmod{p},$$

we obtain

$$(-q)^{-(p-1)/4}\left(\frac{p-1}{2}\right)! \equiv (-1)^{\sum_{j=1}^{(q-1)/2} N(p,q,j)} \prod_{0<n<p} n \pmod{p}.$$

Next, letting g denote a primitive root $\pmod{p}$, we have

$$\prod_{0<n<p} n \equiv \prod_{j=0}^{(p-3)/2} g^{2j+1} \equiv g^{\sum_{j=0}^{(p-3)/2} (2j+1)} \equiv g^{((p-1)/2)^2}$$
$$\equiv (g^{(p-1)/2})^{(p-1)/2} \equiv (-1)^{(p-1)/2} \equiv 1 \pmod{p},$$

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

so

$$(-q)^{-(p-1)/4}\left(\frac{p-1}{2}\right)! \equiv (-1)^{\sum_{j=1}^{(q-1)/2} N(p,q,j)} \pmod{p},$$

which completes the proof of Lemma 13.

Putting Lemmas 12 and 13 together we obtain

LEMMA 14. *For primes* $p \equiv 1 \pmod 4$ *and* $q \equiv 3 \pmod 4$ *we have*

(a) *if* $(p/q) = +1$,

$$(-q)^{(p-1)/4} \equiv (-1)^{h(-qp)/4} \pmod{p},$$

(b) *if* $(p/q) = -1$ *and* $q > 3$,

$$(-q)^{(p-1)/4} \equiv (-1)^{(h(-qp)+2h(-q))/4}\left(\frac{p-1}{2}\right)! \pmod{p},$$

(c) *if* $(p/3) = -1$,

$$(-3)^{(p-1)/4} \equiv (-1)^{(h(-3p)-2)/4}\left(\frac{p-1}{2}\right)! \pmod{p}.$$

Finally the theorem follows from Lemma 14 by appealing to the law of biquadratic reciprocity in the following form (see [**5**])

$$(-q)^{(p-1)/4} \equiv \begin{cases} 1 \pmod{p}, & \text{if } \left(\dfrac{a-bi}{a+bi}\right)^{(q+1)/4} \equiv 1 \pmod{q}, \\ -1 \pmod{p}, & \text{if } \left(\dfrac{a-bi}{a+bi}\right)^{(q+1)/4} \equiv -1 \pmod{q}, \\ b/a \pmod{p}, & \text{if } \left(\dfrac{a-bi}{a+bi}\right)^{(q+1)/4} \equiv i \pmod{q}, \\ -b/a \pmod{p}, & \text{if } \left(\dfrac{a-bi}{a+bi}\right)^{(q+1)/4} \equiv -i \pmod{q}. \end{cases}$$

3. Conclusion.

It would be interesting to extend the ideas of this paper to obtain congruences for other class numbers. We just discuss one example. For primes $p \equiv 1 \pmod 8$ and $q \equiv 5 \pmod 8$ we have

$$(3.1)\quad h(-8pq) \equiv \begin{cases} 0 \pmod{8}, & \text{if } \left(\dfrac{p}{q}\right) = +1, \\ 4 \pmod{8}, & \text{if } \left(\dfrac{p}{q}\right) = -1, \end{cases}$$

see for example [**9**, p. 191]. The following conjecture for $h(-8pq) \pmod{16}$ has been verified for all such primes $p \leqq 577$ and $q \leqq 557$.

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

Conjecture. Let p and q be primes with $p \equiv 1 \pmod 8$ and $q \equiv 5 \pmod 8$. Define a and b by (0.1), (0.2) and (0.3). Then

(a) if $(p/q) = +1$ we have

(i) if $b \equiv 0 \pmod 8$,

$$h(-8pq) \equiv \begin{cases} 0 \pmod{16}, & \text{if } \left(\dfrac{a+bi}{a-bi}\right)^{(q-1)/4} \equiv 1 \pmod q, \\ 8 \pmod{16}, & \text{if } \left(\dfrac{a+bi}{a-bi}\right)^{(q-1)/4} \equiv -1 \pmod q, \end{cases}$$

(ii) if $b \equiv 4 \pmod 8$,

$$h(-8pq) \equiv \begin{cases} 0 \pmod{16}, & \text{if } \left(\dfrac{a+bi}{a-bi}\right)^{(q-1)/4} \equiv -1 \pmod q, \\ 8 \pmod{16}, & \text{if } \left(\dfrac{a+bi}{a-bi}\right)^{(q-1)/4} \equiv 1 \pmod q; \end{cases}$$

(b) if $(p/q) = -1$ we have

(i) if $h(-8q) \equiv 2 \pmod 8$,

$$h(-8pq) \equiv \begin{cases} 4 \pmod{16}, & \text{if } \left(\dfrac{a+bi}{a-bi}\right)^{(q-1)/4} \equiv -i \pmod q, \\ 12 \pmod{16}, & \text{if } \left(\dfrac{a+bi}{a-bi}\right)^{(q-1)/4} \equiv i \pmod q, \end{cases}$$

(ii) if $h(-8q) \equiv 6 \pmod 8$,

$$h(-8pq) \equiv \begin{cases} 4 \pmod{16}, & \text{if } \left(\dfrac{a+bi}{a-bi}\right)^{(q-1)/4} \equiv i \pmod q, \\ 12 \pmod{16}, & \text{if } \left(\dfrac{a+bi}{a-bi}\right)^{(q-1)/4} \equiv -i \pmod q. \end{cases}$$

The authors have proved this conjecture for $q = 5$. Moreover part (a) of the conjecture can be deduced from (1.6) and a result of Kaplan [**7**, Proposition B_6']. More generally a proof along the lines of the proof of the theorem of this paper would require relating modulo 16 certain sums involving $S(8q, k)$ arising from Lemma 1 (with $d = -8q$) to the sum

$$\sum_{k=1}^{(q-1)/2} S(2q, 2k).$$

This seems to be quite difficult. The authors have also been able to formulate other conjectures similar to the one above.

References

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

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press

2. Z. I. Borevich and I. R. Shafarevich, *Number theory* (Academic Press, N.Y., 1966).

3. P. G. L. Dirichlet, *Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres*, J. Reine Angew. Math. *21* (1840), 134–155.

4. C. F. Gauss, Letter to P. G. L. Dirichlet dated 30 May 1828. (Reproduced in P. G. L. Dirichlet's Werke, Chelsea Publishing Company, Bronx, N.Y. Volume 2, pp. 378–380.)

5. T. Gosset, *On the law of quartic reciprocity*, Mess. Math. *41* (1911), 65–90.

6. W. Johnson and K. J. Mitchell, *Symmetries for sums of the Legendre symbol*, Pacific J. Math. *69* (1977), 117–124.

7. P. Kaplan, *Sur le* 2*-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. *283/284* (1976), 313–363.

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

9. A. Pizer, *On the* 2*-part of the class number of imaginary quadratic number fields*, J. Number Theory *8* (1976), 184–192.

10. K. Yamamoto, *On Gaussian sums with biquadratic residue characters*, J. Reine Angew. Math. *219* (1965), 200–213.

Carleton University,
Ottawa, Ontario

https://doi.org/10.4153/CJM-1982-070-x Published online by Cambridge University Press