JOURNAL OF NUMBER THEORY 27, 178–195 (1987)

Congruences modulo 16 for the Class Numbers of Complex Quadratic Fields

KENNETH HARDY* AND KENNETH S. WILLIAMS†

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

Communicated by H. Zassenhaus

Received April 28, 1986

Let $h(d)$ denote the class number of the quadratic field $Q(\sqrt{d})$ of discriminant d. A number of new determinations of $h(d)$ modulo 16 are proved. For example, it is shown that if p and q are primes satisfying $p \equiv q \equiv 5 \pmod 8$, $(p/q) = 1$, then

$$h(-8pq) \equiv \begin{cases} 4 \pmod{16} & \text{if } \left(\dfrac{aA+bB}{p}\right) = (-1)^{(b+B+4)/4}, \\ 12 \pmod{16} & \text{if } \left(\dfrac{aA+bB}{p}\right) = (-1)^{(b+B)/4}, \end{cases}$$

where a and b are unique integers such that $p = a^2 + b^2$, $a \equiv 1 \pmod 4$, $b \equiv ((p-1)/2)!\ a \pmod p$, and A and B are the unique integers such that $q = A^2 + B^2$, $A \equiv 1 \pmod 4$, $B \equiv ((q-1)/2)!\ A \pmod q$. © 1987 Academic Press, Inc.

1. INTRODUCTION

As usual we denote the class number of the quadratic field $Q(\sqrt{d})$ of discriminant d by $h(d)$. When $d = (-1)^{n-s} p_1 \cdots p_s\, q_{s+1} \cdots q_n$, where n is a positive integer, $p_1, ..., p_s$ are s ($\geqslant 0$) distinct primes $\equiv 1 \pmod 4$, and $q_{s+1}, ..., q_n$ are $n-s$ ($\geqslant 0$) distinct primes $\equiv 3 \pmod 4$, the authors [8] have proved a congruence of the form

* Research supported by Natural Sciences and Engineering Research Council of Canada, Grant A-8049.

† Research supported by Natural Sciences and Engineering Research Council of Canada, Grant A-7233.

0022-314X/87 $3.00

$$\sum_{\substack{e \mid d \\ e>0,\ e \equiv 1 \pmod 4}} (c_1(d,e)\,h(-4e) + c_2(d,e)\,h(-8e))$$

$$+ \sum_{\substack{e \mid d \\ e<0,\ e \equiv 1 \pmod 4}} (c_3(d,e)\,h(e) + c_4(d,e)\,h(8e))$$

$$+ \frac{(-1)^n}{2} \prod_{i=1}^{n} (|p_i| - 1) \equiv c_5(d) + c_6(d) \pmod{2^{n+2}}, \qquad (1.1)$$

where

$$c_1(d,e) = \left(\frac{e}{2}\right) \prod_{p \mid d/e} \left(\left(\frac{e}{p}\right) - \left(\frac{-1}{p}\right)\right),$$

$$c_2(d,e) = \prod_{p \mid d/e} \left(\left(\frac{e}{p}\right) - \left(\frac{-2}{p}\right)\right),$$

$$c_3(d,e) = \left(5 - \left(\frac{e}{2}\right)\right) \prod_{p \mid d/e} \left(\left(\frac{e}{p}\right) - 1\right),$$

$$c_4(d,e) = -\prod_{p \mid d/e} \left(\left(\frac{e}{p}\right) - \left(\frac{2}{p}\right)\right),$$

$$c_5(d) = \begin{cases} 2^{n-1} & \text{if } d \text{ is divisible only by primes } \equiv 3 \pmod 4, \\ 0 & \text{otherwise,} \end{cases}$$

$$c_6(d) = \begin{cases} 0 & \text{if } 3 \nmid d, \\ 4 & \text{if } d = -3, \\ 0 & \text{if } d \neq -3,\ 3 \mid d, \text{ and } p \mid d/3 \\ & \quad \text{for some prime } p \equiv 1 \pmod 3, \\ 2^{n+1} & \text{if } d \neq -3,\ 3 \mid d, \text{ and all primes} \\ & \quad p \mid d/3 \text{ satisfy } p \equiv 2 \pmod 3. \end{cases}$$

This congruence contains as special cases many known congruences, for example, those of Pizer [13] and those of Kenku [11].

In this paper we analyze (1.1) in the case $n = 2$ in order to obtain new congruences modulo 16 involving $h(-8pq)$ and $h(-4pq)$, when $pq \equiv 1 \pmod 4$, and $h(-pq)$, when $pq \equiv 3 \pmod 4$, where p and q are distinct odd primes. We begin by giving a summary of references to known results (see Table I). In cases 1–3, 7, 9, 10, 13, and 18, (1.1) does not give new information. In case 4, (1.1) is used, together with the conjecture given in [16],

TABLE I

Case	p (mod 8)	q (mod 8)	$\left(\frac{p}{q}\right)$	$h(-4pq)$ (mod 16)	$h(-8pq)$ (mod 16)
1	1	1	+1	[10 : C'_1]	[10 : C'_2]
2	1	1	−1	[10 : B'_2]	[10 : B'_5]
3	1	5	+1	[10 : B'_3]	[10 : B'_6]
4	1	5	−1		[16][a]
5	5	5	+1	[10 : B'_4]	
6	5	5	−1	[10 : B'_1]	

	p (mod 8)	q (mod 8)	$\left(\frac{p}{q}\right)$	$h(-pq)$ (mod 8)	$h(-8pq)$ (mod 16)
7	1	3	+1	[9]	[10 : B'_{10}]
8	1	3	−1	[16]	
9	1	7	+1	[9]	[10 : C'_4]
10	1	7	−1	[16]	[10 : B'_9]
11	5	3	+1	[9]	
12	5	3	−1	[16]	
13	5	7	+1	[9]	[10 : B'_{11}]
14	5	7	−1	[16]	

	p (mod 8)	q (mod 8)	$\left(\frac{p}{q}\right)$	$h(-4pq)$ (mod 16)	$h(-8pq)$ (mod 16)
15	3	3	+1		[10 : B'_{15}]
16	3	7	+1		[10 : B'_{15}]
17	3	7	−1		
18	7	7	+1	[10 : B'_{12}]	[10 : B'_{14}]

[a] Conjecture only.

to conjecture the value of $h(-4pq)$ (mod 16) (see Section 2, Conjecture). In cases 5, 6, 8, 11, 12, and 14, (1.1) is used in conjunction with results specified in the table to obtain the value of $h(-8pq)$ (mod 16) (see Section 3, Theorem 1; Section 4, Theorem 2; Section 5, Theorem 3; Section 6, Theorem 4; Section 7, Theorem 5; Section 8, Theorem 6). In cases 15 and 16, as $h(-8pq)$ is known modulo 16, (1.1) gives $h(-4pq)$ (mod 16) (see Section 9, Theorem 7; Section 10, Theorem 8). In case 17, since neither $h(-4pq)$ nor $h(-8pq)$ is known individually (mod 16), (1.1) just gives $h(-4pq)+h(-8pq)$ (mod 16) (see Section 11, Theorem 9).

In proving our results we shall need the classical congruences (see, e.g., [13, Propositions 1 and 2])

$$h(-4p) \equiv \tfrac{1}{2}(p-1) \pmod 4 \qquad \text{if } p \equiv 1 \pmod 4, \tag{1.2}$$

$$h(-p) \equiv 1 \pmod 2 \qquad \text{if } p \equiv 3 \pmod 4, \tag{1.3}$$

$$h(-4p) + h(-8p) \equiv \tfrac{1}{2}(p-1) \pmod 8 \qquad \text{if } p \equiv 1 \pmod 8, \tag{1.4}$$

$$2h(-p) + h(-8p) \equiv \begin{cases} \tfrac{1}{2}(p-3) \pmod 8 & \text{if } p \equiv 3 \pmod 8,\ p > 3, \\ 4 \pmod 8 & \text{if } p = 3, \end{cases} \tag{1.5}$$

$$h(-4p) + h(-8p) \equiv \tfrac{1}{2}(p+3) \pmod 8 \qquad \text{if } p \equiv 5 \pmod 8, \tag{1.6}$$

$$h(-8p) \equiv \tfrac{1}{2}(p+1) \pmod 8 \qquad \text{if } p \equiv 7 \pmod 8. \tag{1.7}$$

We will also use the following notation. If p is a prime $\equiv 1 \pmod 4$ we let a and b be the unique integers such that

$$p = a^2 + b^2, \qquad a \equiv 1 \pmod 4, \qquad b \equiv ((p-1)/2)!\, a \pmod p. \tag{1.8}$$

Similarly if q is a prime $\equiv 1 \pmod 4$, we define integers A and B uniquely by replacing p by q, a by A, b by B in (1.8). Frequent use will be made of the congruence (and the similar one involving q and A)

$$p \equiv \begin{cases} 2a - 1 \pmod{16} & \text{if } p \equiv 1 \pmod 8, \\ 2a + 3 \pmod{16} & \text{if } p \equiv 5 \pmod 8. \end{cases} \tag{1.9}$$

This is given in [16, p. 972] and is a straightforward deduction from (1.8). We will also use the congruence

$$h(-4p) \equiv -a + b + 1 \pmod 8. \tag{1.10}$$

This congruence was given by Gauss in a letter to Dirichlet dated 30 May 1828 [5], [6, p.287]. A proof by Dedekind is given in [6, pp. 299–301; 7, pp. 692–693] (see also [1, 16, 18]).

From (1.4), (1.6), (1.8), (1.9), and (1.10) (see also [1]), we obtain

$$h(-8p) \equiv b \pmod 8. \tag{1.11}$$

In addition, if $(p/q) = +1$, Burde's rational biquadratic reciprocity law [4] asserts that

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{aA + bB}{p}\right) = \left(\frac{aA + bB}{q}\right) \tag{1.12}$$

(see also [14]).

On the other hand if $p \equiv 3 \pmod 4$ then by a result of Mordell [12] we have for $p > 3$,

$$h(-p) \equiv \begin{cases} 1 \pmod 4 & \text{if } \left(\frac{p-1}{2}\right)! \equiv -1 \pmod p, \\ 3 \pmod 4 & \text{if } \left(\frac{p-1}{2}\right)! \equiv 1 \pmod p. \end{cases} \tag{1.13}$$

Then, from (1.5) and (1.13), we obtain for $p \equiv 3 \pmod 8$ and $p > 3$,

$$h(-8p) \equiv \begin{cases} 2 \pmod 8 & \text{if } \left(\frac{p-1}{2}\right)! \equiv (-1)^{(p-3)/8} \pmod p. \\ 6 \pmod 8 & \text{if } \left(\frac{p-1}{2}\right)! \equiv (-1)^{(p+5)/8} \pmod p. \end{cases} \tag{1.14}$$

2. $p \equiv 1 \pmod 8$, $q \equiv 5 \pmod 8$, $(p/q) = -1$

In this case (1.1) gives

$$h(-8pq) + h(-4pq) + 2h(-4p) \equiv q + 3 \pmod{16} \tag{2.1}$$

(cf. [13, Proposition 5, Eq. (21)]).

Kaplan [10, Cas 1a, p. 347; Cas 2a, p. 350] gives

$$h(-4pq) \equiv h(-8pq) \equiv 4 \pmod 8. \tag{2.2}$$

Combining (2.1) with a conjecture of Williams and Currie [16] for the value of $h(-8pq)$ modulo 16, and using (1.10), we obtain a conjecture for $h(-4pq)$ modulo 16.

Conjecture. Let p and q be primes such that

$$p \equiv 1 \pmod 8, \qquad q \equiv 5 \pmod 8, \qquad \left(\frac{p}{q}\right) = -1,$$

and define integers a, b, A, B uniquely using (1.8). Then we have

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

The following table illustrates the conjecture. We write

$$X \equiv \left(\frac{a+bi}{a-bi}\right)^{(q-1)/4} \pmod{q}, \qquad Y = (-1)^{(a+A+b+B)/4}\, i.$$

p	q	a	b	A	B	X	Y	$h(-4pq)$
17	5	1	−4	1	2	i	i	4
113	5	−7	8	1	2	i	$-i$	12
193	5	−7	12	1	2	$-i$	i	44
337	5	9	16	1	2	$-i$	$-i$	52
41	13	5	4	−3	−2	i	$-i$	12
73	13	−3	−8	−3	−2	$-i$	i	12
97	13	9	4	−3	−2	i	i	20
137	13	−11	4	−3	−2	$-i$	$-i$	68

3. $p \equiv q \equiv 5 \pmod 8$, $(p/q) = 1$

In this case (1.1) gives

$$h(-8pq) + h(-4pq) + 2h(-8p) + 2h(-8q) \equiv 4 \pmod{16} \tag{3.1}$$

(cf. [13, Proposition 5, Eq. (29)]). This congruence can be used to determine $h(-8pq)$ modulo 16.

We have

THEOREM 1. *Let p and q be primes such that*

$$p \equiv q \equiv 5 \pmod 8, \qquad \left(\frac{p}{q}\right) = 1,$$

and define integers a, b, A, B uniquely using (1.8). *Then we have*

$$h(-8pq) \equiv \begin{cases} 4 \pmod{16} & \text{if } \left(\frac{aA+bB}{p}\right) = (-1)^{(b+B+4)/4}, \\ 12 \pmod{16} & \text{if } \left(\frac{aA+bB}{p}\right) = (-1)^{(b+B)/4}. \end{cases}$$

Proof. From Kaplan [10, Proposition B_4'] we have

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = (-1)^{(h(-4pq)+8)/8}. \tag{3.2}$$

Hence, from (1.12) and (3.2), we obtain

$$\left(\frac{aA+bB}{p}\right)=(-1)^{(h(-4pq)+8)/8}. \tag{3.3}$$

Next, by (1.11), we have

$$h(-8p)\equiv b \pmod 8, \qquad h(-8q)\equiv B \pmod 8,$$

so that

$$(-1)^{(b+B)/4}=(-1)^{(h(-8p)+h(-8q))/4}. \tag{3.4}$$

Multiplying (3.3) and (3.4) together, we obtain

$$\left(\frac{aA+bB}{p}\right)(-1)^{(b+B)/4}=(-1)^{(h(-4pq)+2h(-8p)+2h(-8q)+8)/8}. \tag{3.5}$$

Using $h(-8pq)\equiv 4 \pmod 8$ [10, Cas 2a, p. 350], in (3.1), we obtain

$$h(-8pq)\equiv h(-4pq)+2h(-8p)+2h(-8q)+4 \pmod{16}. \tag{3.6}$$

Putting (3.6) into (3.5), we get

$$(-1)^{(h(-8pq)+4)/8}=\left(\frac{aA+bB}{p}\right)(-1)^{(b+B)/4},$$

which is the required result.

The following table illustrates Theorem 1. We write $X=(-1)^{(b+B)/4}$, $Y=((aA+bB)/p)$.

p	q	a	b	A	B	X	Y	$h(-8pq)$
5	29	1	2	5	2	−1	1	20
5	61	1	2	5	−6	−1	−1	12
13	29	−3	−2	5	2	1	−1	20
13	61	−3	−2	5	−6	1	1	12

4. $p\equiv q\equiv 5 \pmod 8$, $(p/q)=-1$

In this case (1.1) gives

$$h(-8pq)+h(-4pq)+2h(-4p)+2h(-4q)\equiv 4 \pmod{16} \tag{4.1}$$

(cf. [13, Proposition 5, Eq. (30)]). This congruence can be used to determine $h(-8pq)$ (mod 16). We prove

THEOREM 2. *Let p and q be primes such that*

$$p \equiv q \equiv 5 \pmod 8, \qquad \left(\frac{p}{q}\right) = -1,$$

and define integers a, b, A, B uniquely using (1.8). Then we have

$$h(-8pq) \equiv \begin{cases} 4 \pmod{16} & \text{if } \left(\dfrac{aA + (-1)^{(b+B)/4}\, bB}{p}\right) = (-1)^{(b+B+4)/4}, \\ 12 \pmod{16} & \text{if } \left(\dfrac{aA + (-1)^{(b+B)/4}\, bB}{p}\right) = (-1)^{(b+B)/4}. \end{cases}$$

Proof. From Kaplan [10, Proposition B_1'] we have

$$\left(\frac{pq}{2}\right)_4 \left(\frac{2p}{q}\right)_4 \left(\frac{2q}{p}\right)_4 = (-1)^{h(-4pq)/8}. \tag{4.2}$$

Appealing to [15, Problem 323], we have

$$\left(\frac{2p}{q}\right)_4 \left(\frac{2q}{p}\right)_4 = \left(\frac{aA + (-1)^{(b+B)/4}\, bB}{p}\right). \tag{4.3}$$

Using (4.3) in (4.2), we obtain

$$(-1)^{(pq-1)/8} \left(\frac{aA + (-1)^{(b+B)/4}\, bB}{p}\right) = (-1)^{h(-4pq)/8}. \tag{4.4}$$

Next from (1.9) and (1.10) we get

$$2h(-4p) + 2h(-4q) \equiv p + q + 6 + 2b + 2B \pmod{16},$$

that is,

$$2h(-4p) + 2h(-4q) \equiv pq + 7 + 2b + 2B \pmod{16},$$

and so

$$(-1)^{(pq+7)/8 + (b+B)/4} = (-1)^{(h(-4p) + h(-4q))/4}. \tag{4.5}$$

Multiplying (4.4) and (4.5) together, we get

$$(-1)^{(h(-4pq) + 2h(-4p) + 2h(-4q))/8} = -\left(\frac{aA + (-1)^{(b+B)/4}\, bB}{p}\right)(-1)^{(b+B)/4}. \tag{4.6}$$

Now from (4.1) we have, as $h(-8pq) \equiv 4 \pmod 8$ [10, Cas 2a, p. 350],

$$h(-8pq) \equiv h(-4pq) + 2h(-4p) + 2h(-4q) + 4 \pmod{16}. \tag{4.7}$$

Using (4.7) in (4.6), we obtain

$$(-1)^{(h(-8pq)-4)/8} = -\left(\frac{aA+(-1)^{(b+B)/4}\,bB}{p}\right)(-1)^{(b+B)/4},$$

which gives the required result.

The following table illustrates Theorem 2. We write

$$X=(-1)^{(b+B)/4}, \qquad Y=((aA+XbB)/p).$$

p	q	a	b	A	B	X	Y	$h(-8pq)$
5	13	1	2	−3	−2	1	−1	4
13	53	−3	−2	−7	−2	−1	1	20
29	37	5	2	1	−6	−1	−1	28
61	101	5	−6	1	−10	1	1	44

5. $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$, $(p/q) = -1$

In this case (1.1) gives

$$h(-8pq)+2h(-pq)+2h(-4p) \equiv q-3 \pmod{16} \tag{5.1}$$

(cf. [13, Proposition 5, Eq. (19)]). This congruence can be used to determine $h(-8pq)$ modulo 16.

We prove

THEOREM 3. *Let p and q be primes such that*

$$p \equiv 1 \pmod 8, \qquad q \equiv 3 \pmod 8, \qquad \left(\frac{p}{q}\right) = -1,$$

and define a, b by (1.8). *Then, for $q > 3$, we have*

$$h(-8pq) \equiv \begin{cases} 4 \pmod{16} & \text{if } \left(\dfrac{a-bi}{a+bi}\right)^{(q+1)/4} \\ & \quad \equiv (-1)^{(2a-2b+q+3)/8}\left(\dfrac{q-1}{2}\right)!\, i \pmod q \\ 12 \pmod{16} & \text{if } \left(\dfrac{a-bi}{a+bi}\right)^{(q+1)/4} \\ & \quad \equiv (-1)^{(2a-2b+q+11)/8}\left(\dfrac{q-1}{2}\right)!\, i \pmod q, \end{cases}$$

and, for $q=3$, *we have*

$$h(-24p) \equiv \begin{cases} 2a-2b+2 \pmod{16} & \text{if } a \equiv b \pmod 3, \\ 2a-2b+10 \pmod{16} & \text{if } a \equiv -b \pmod 3. \end{cases}$$

Proof. From (1.13) and [16, Theorem (b)(i), (ii)] we have for $q>3$

$$h(-pq) \equiv \begin{cases} 2 \pmod 8 & \text{if } \left(\dfrac{a-bi}{a+bi}\right)^{(q+1)/4} \equiv \left(\dfrac{q-1}{2}\right)!\, i \pmod q, \\ 6 \pmod 8 & \text{if } \left(\dfrac{a-bi}{a+bi}\right)^{(q+1)/4} \equiv -\left(\dfrac{q-1}{2}\right)!\, i \pmod q. \end{cases} \tag{5.2}$$

The required result now follows from (1.10), (5.1), and (5.2).

For $q=3$ the result follows from (1.10), (5.1), and [16, Theorem (b)(iii)]. We remark that in this case (5.1) is equivalent to (11.9) and (11.10) of Corollary 11.4 of [2]. The following short tables illustrate Theorem 3. We write

$$X \equiv \left(\frac{a-bi}{a+bi}\right)^{(q+1)/4} \pmod q,$$

$$Y \equiv (-1)^{(2a-2b+q+3)/8} \left(\frac{q-1}{2}\right)!\, i \pmod q.$$

$q>3$:

p	q	a	b	X	Y	$h(-8pq)$
17	11	1	−4	$-i$	i	28
41	11	5	4	i	$-i$	28
193	11	−7	12	i	i	36
409	11	−3	20	$-i$	$-i$	36
41	19	5	4	$-i$	i	12
89	19	5	−8	$-i$	$-i$	20
97	19	9	4	i	$-i$	44
113	19	−7	8	i	i	36

$q=3$:

p	a	b	$a\equiv b$ (mod 3)	$2a-2b+2$ (mod 16)	$h(-24p)$
17	1	−4	No	12	4
41	5	4	No	4	12
113	−7	8	Yes	4	20
281	5	−16	Yes	12	44

6. $p \equiv 5 \pmod 8$, $q \equiv 3 \pmod 8$, $(p/q) = 1$.

In this case (1.1) gives

$$h(-8pq) + 2h(-4p) + 2h(-8q) \equiv p - 1 \pmod{16} \qquad (6.1)$$

(cf. [13, Proposition 5, Eq. (25)]). This congruence enables us to determine $h(-8pq)$ modulo 16.

THEOREM 4. *Let p and q be primes such that*

$$p \equiv 5 \pmod 8, \qquad q \equiv 3 \pmod 8, \qquad \left(\frac{p}{q}\right) = 1,$$

and define a and b by (1.8). *Then, for $q > 3$, we have*

$$h(-8pq) \equiv \begin{cases} 4 \pmod{16} & \text{if } \left(\frac{q-1}{2}\right)! \equiv (-1)^{(q+2b+1)/8} \pmod q, \\ 12 \pmod{16} & \text{if } \left(\frac{q-1}{2}\right)! \equiv (-1)^{(q+2b+9)/8} \pmod q; \end{cases}$$

and, for $q = 3$, we have

$$h(-24p) = -2b \pmod{16}.$$

Proof. For $q > 3$ the result follows from (1.9), (1.10), (1.14), and (6.1). For $q = 3$ the result follows from (1.9), (1.10), (6.1) and the fact that $h(-24) = 2$. We remark that in this case (6.1) is equivalent to (11.7) and (11.8) of Corollary 11.4 of [2].

The following tables illustrate Theorem 4. We write

$$X \equiv ((q-1)/2)! \pmod q, \qquad Y = (-1)^{(q+2b+1)/8}.$$

$q > 3$:

p	q	b	X	Y	$h(-8pq)$
5	11	2	−1	1	12
5	59	2	1	1	20
53	11	−2	−1	−1	36
53	59	−2	1	−1	140

$q=3$:

p	b	$h(-24p)$
13	-2	4
37	-6	12
61	-6	12
277	14	20

7. $p \equiv 5 \pmod 8$, $q \equiv 3 \pmod 8$, $(p/q) = -1$

In this case (1.1) gives

$$h(-8pq) + 2h(-8p) + 4h(-q) \equiv \begin{cases} p-1 \pmod{16} & \text{if } q > 3, \\ p+7 \pmod{16} & \text{if } q = 3 \end{cases} \tag{7.1}$$

(cf. [13, Proposition 5, Eq. (26)]. This congruence enables us to determine $h(-8pq)$ modulo 16.

THEOREM 5. *Let p and q be primes such that*

$$p \equiv 5 \pmod 8, \qquad q \equiv 3 \pmod 8, \qquad \left(\frac{p}{q}\right) = -1,$$

and define a and b by (1.8). *Then, for $q > 3$, we have*

$$h(-8pq) \equiv \begin{cases} 4 \pmod{16} & \text{if } \left(\frac{q-1}{2}\right)! \equiv (-1)^{(a-b+1)/4} \pmod q, \\ 12 \pmod{16} & \text{if } \left(\frac{q-1}{2}\right)! \equiv (-1)^{(a-b-3)/4} \pmod q; \end{cases}$$

and, for $q = 3$, we have

$$h(-24p) \equiv 2a - 2b + 6 \pmod{16}.$$

Proof. For $q > 3$ the result follows from (1.9), (1.11), (1.13), and (7.1). For $q = 3$ the result follows from (1.9), (1.11), and (7.1). We remark that (7.1) in this case is equivalent to (11.5) and (11.6) of Corollary 11.4 of [2].

The following tables illustrate Theorem 5. We write

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

$q > 3$:

p	q	a	b	X	Y	$h(-8pq)$
13	11	−3	−2	−1	1	12
29	11	5	2	−1	−1	20
13	59	−3	−2	1	1	20
61	59	5	−6	1	−1	28

$q = 3$:

p	a	b	$2a-2b+6$	$h(-24p)$
5	1	2	4	4
29	5	2	12	12
53	−7	−2	−4	12
197	1	−14	36	20

8. $p \equiv 5 \pmod 8$, $q \equiv 7 \pmod 8$, $(p/q) = -1$

In this case (1.1) gives

$$h(-8pq) + 2h(-pq) \equiv p + 3 \pmod{16} \tag{8.1}$$

(cf. [13, Proposition 5, Eq. (32)]). This congruence enables us to determine $h(-8pq)$ modulo 16. We have

THEOREM 6. *Let p and q be primes such that*

$$p \equiv 5 \pmod 8, \qquad q \equiv 7 \pmod 8, \qquad \left(\frac{p}{q}\right) = -1,$$

and define a and b as in (1.8). *Then we have*

$$h(-8pq) \equiv \begin{cases} 4 \pmod{16} \\ \quad \text{if } \left(\dfrac{a-bi}{a+bi}\right)^{(q+1)/4} \equiv (-1)^{(a-1)/4}\left(\dfrac{q-1}{2}\right)!\ i \pmod q, \\ 12 \pmod{16} \\ \quad \text{if } \left(\dfrac{a-bi}{a+bi}\right)^{(q+1)/4} \equiv (-1)^{(a+3)/4}\left(\dfrac{q-1}{2}\right)!\ i \pmod q. \end{cases}$$

Proof. The result follows from (1.9), (1.13), (8.1), and [16, Theorem (b) (i), (ii)].

The following table illustrates Theorem 6. We write

$$X \equiv \left(\frac{a-bi}{a+bi}\right)^{(q+1)/4} \pmod q, \qquad Y \equiv (-1)^{(a-1)/4}((q-1)/2)! \pmod q.$$

p	q	a	b	X	Y	$h(-8pq)$
5	7	1	2	$-i$	$-i$	4
13	7	-3	-2	$-i$	i	12
101	7	1	-10	i	$-i$	28
157	7	-11	-6	i	i	36
5	23	1	2	i	i	20
53	23	-7	-2	$-i$	i	28
61	23	5	-6	$-i$	$-i$	36
157	23	-11	-6	i	$-i$	44

9. $p \equiv q \equiv 3 \pmod 8$, $(p/q) = 1$

In this case (1.1) gives

$$h(-8pq) + h(-4pq) + 4h(-p) + 2h(-8q) \equiv \begin{cases} p+q-2 \pmod{16} & \text{if } p > 3, \\ q+9 \pmod{16} & \text{if } p = 3 \end{cases} \tag{9.1}$$

(cf. [13, Proposition 5, Eq. (24)]). As $h(-8pq)$ is known modulo 16 [10, Proposition B'_{15}], (9.1) allows us to determine $h(-4pq)$ modulo 16. We have

THEOREM 7. *Let p and q be distinct primes satisfying*

$$p \equiv q \equiv 3 \pmod 8, \qquad \left(\frac{p}{q}\right) = 1.$$

There exist integers x, y, k, l and m such that

$$p = l^2 - 2k^2 m, \qquad 2q = k^2x^2 + 2lxy + 2my^2$$

(*see* [10, p. 356]). *Define* $\varepsilon_p = \pm 1$ *and* $\varepsilon_q = \pm 1$ *by*

$$\left(\frac{p-1}{2}\right)! \equiv \varepsilon_p \pmod{p}, \qquad \left(\frac{q-1}{2}\right)! \equiv \varepsilon_q \pmod{q}.$$

Then, for $p > 3$ *and* $q > 3$, *we have*

$$h(-4pq) \equiv \begin{cases} 4 \pmod{16} & \text{if } \varepsilon_p \varepsilon_q = (-1)^{(p-3)/8} \left(\dfrac{-2}{|k^2x + ly|}\right), \\ 12 \pmod{16} & \text{if } \varepsilon_p \varepsilon_q = (-1)^{(p+5)/8} \left(\dfrac{-2}{|k^2x + ly|}\right). \end{cases}$$

If $p = 3$ *and* $q > 3$ *we have*

$$h(-12q) \equiv \begin{cases} 4 \pmod{16} & \text{if } \varepsilon_q = \left(\dfrac{-2}{|k^2x + ly|}\right), \\ 12 \pmod{16} & \text{if } \varepsilon_q = -\left(\dfrac{-2}{|k^2x + ly|}\right). \end{cases}$$

If $p > 3$ *and* $q = 3$ *we have*

$$h(-12p) \equiv \begin{cases} p-7 \pmod{16} & \text{if } \varepsilon_p = -\left(\dfrac{-2}{|k^2x + ly|}\right), \\ p+1 \pmod{16} & \text{if } \varepsilon_p = \left(\dfrac{-2}{|k^2x + ly|}\right). \end{cases}$$

Proof. From [10, Proposition B'_{15}] we have

$$h(-8pq) \equiv \begin{cases} 0 \pmod{16} & \text{if } \left(\dfrac{-2}{|k^2x + ly|}\right) = 1, \\ 8 \pmod{16} & \text{if } \left(\dfrac{-2}{|k^2x + ly|}\right) = -1. \end{cases} \tag{9.2}$$

For $p > 3$ and $q > 3$ the result follows from (1.13), (1.14), (9.1), and (9.2). For $p = 3$ and $q > 3$ the result follows from (1.14), (9.1), and (9.2). For $p > 3$ and $q = 3$ the result follows from (1.13), (9.1), and (9.2).

We remark that (9.1) is equivalent to the appropriate congruences of Corollary 11.6 of [2] when p or $q = 3$.

The following tables illustrate Theorem 7. We write

$$X=\left(\frac{-2}{|k^2x+ly|}\right),\qquad Y=(-1)^{(p-3)/8}.$$

$p>3,\ q>3$:

p	q	ε_p	ε_q	k	l	m	x	y	X	Y	$h(-4pq)$
11	19	−1	−1	1	1	−5	6	1	−1	−1	20
19	179	−1	−1	1	7	15	−2	−3	−1	1	92
11	107	−1	1	1	3	−1	12	1	−1	−1	12
59	11	1	−1	1	7	−5	2	1	1	−1	20
19	59	−1	1	1	5	3	2	3	1	1	44
307	43	1	−1	1	17	−9	4	7	1	1	92
107	59	1	1	1	11	7	4	1	−1	−1	36
307	59	1	1	3	1	−17	4	1	−1	1	92

$p=3,\ q>3$:

q	ε_q	k	l	m	x	y	X	$h(-12q)$
11	−1	1	3	3	2	1	−1	4
59	1	1	1	−1	−12	1	1	4
83	1	1	5	11	8	1	−1	12
131	−1	1	5	11	2	3	1	12

$p>3,\ q=3$:

p	p(mod 16)	ε_p	k	l	m	x	y	X	$h(-12p)$
19	3	−1	1	3	−5	2	1	−1	4
43	11	−1	1	5	−9	2	1	−1	12
67	3	−1	3	29	43	−2	1	1	12
139	11	1	5	17	3	0	1	1	12
211	3	1	5	19	3	0	1	1	20
379	11	1	5	−27	7	2	1	−1	20
547	3	1	7	127	159	−2	1	−1	44
571	11	−1	3	7	−29	2	1	1	36

10. $p\equiv 3 \pmod 8$, $q\equiv 7 \pmod 8$, $(p/q)=1$

In this case (1.1) gives

$$h(-8pq)+h(-4pq)\equiv 0 \pmod{16} \qquad (10.1)$$

(cf. [13, Proposition 5, Eq. (27)]). We remark that, when $p=3$, (10.1) is equivalent to the last two congruences of Corollary 11.6 of [2].

As $p \equiv 3 \pmod 8$ and $(q/p) = -1$ there exist integers x, y, k, l, and m such that

$$2q = k^2x^2 + 2lxy + 2my^2, \qquad p = l^2 - 2k^2m, \tag{10.2}$$

[10, p. 356]. Moreover, as $q \equiv 7 \pmod 8$, by [10, Proposition B'_{15}], we have

$$h(-8pq) \equiv 0 \pmod{16} \quad \Leftrightarrow \quad \left(\frac{|k^2x+ly|}{q}\right) = 1. \tag{10.3}$$

From (10.1) and (10.3) we obtain

THEOREM 8. *Let p and q be primes satisfying*

$$p \equiv 3 \pmod 8, \qquad q \equiv 7 \pmod 8, \qquad \left(\frac{p}{q}\right) = 1.$$

Then, with x, y, l, m as defined in (10.2), *we have*

$$h(-4pq) \equiv \begin{cases} 0 \pmod{16} & \text{if } \left(\dfrac{|k^2x+ly|}{q}\right) = 1, \\ 8 \pmod{16} & \text{if } \left(\dfrac{|k^2x+ly|}{q}\right) = -1. \end{cases}$$

The following table illustrates Theorem 8. We write $Z = (|k^2x+ly|/q)$.

p	q	k	l	m	x	y	$h(-4pq)$	Z
3	23	1	1	−1	6	1	8	−1
107	7	1	9	−13	2	1	32	1

11. $p \equiv 3$, $q \equiv 7 \pmod 8$, $(p/q) = -1$

In this case, from [10, Cas 5a, p. 354; Cas 7a, p. 356] (see also [3]), we have $h(-4pq) \equiv h(-8pq) \equiv 4 \pmod 8$, so that $h(-4pq) + h(-8pq) \equiv 0 \pmod 8$. However, $h(-4pq)$ and $h(-8pq)$ are not known individually modulo 16, so that (1.1) in this case just gives

THEOREM 9. [13, Proposition 5, Eq. (28)]. *Let p and q be primes satisfying*

$$p \equiv 3 \pmod 8, \qquad q \equiv 7 \pmod 8, \qquad \left(\frac{p}{q}\right) = -1.$$

Then

$$h(-8pq) + h(-4pq) \equiv p + q - 2 \pmod{16}.$$

REFERENCES

1. P. BARKAN, Une propriété de congruence de la longeur de la période d'un développement en fraction continue, *C. R. Acad. Sci. Paris Sér. A* **281** (1975), 825–828.
2. B. C. BERNDT, Classical theorems on quadratic residues, *L'Enseign. Math.* **22** (1976), 261–304.
3. E. BROWN AND C. J. PARRY, Class numbers of imaginary quadratic fields having exactly three discriminantal divisors, *J. Reine Angew. Math.* **260** (1973), 31–34.
4. K. BURDE, Ein rationales biquadratisches Reziprozitätsgesetz, *J. Reine Angew. Math.* **235** (1969), 175–184.
5. C. F. GAUSS, Letter to P. G. L. Dirichlet dated 30 May 1828, reproduced in "P. G. L. Dirichlet's Werke," Vol. 2, pp. 378–380, Chelsea, New York.
6. C. F. GAUSS, "Werke" (Zweiter Band), Koniglichen Gesellschaft der Wissenschaften, Göttingen, 1876.
7. G. F. GAUSS, Untersuchungen über höhere Arithmetik, republished by Chelsea, New York, 1965.
8. K. HARDY AND K. S. WILLIAMS, A congruence relating the class numbers of complex quadratic fields, *Acta. Arith.* **47** (1986), 263–276.
9. P. KAPLAN, Divisibilité par 8 du nombres des classes des corps quadratiques dont le 2-groupe des classes est cyclique, et reciprocité biquadratique, *J. Math. Soc. Japan* **25** (1973), 596–608.
10. P. KAPLAN, Sur le 2-groupe des classes d'idéaux des corps quadratiques *J. Reine Angew. Math.* **283–284** (1976), 313–363.
11. M. A. KENKU, Atkin-Lehner involutions and class number residuality, *Acta Arith.* **33** (1977), 1–9.
12. L. J. MORDELL, The congruence $(p-1/2)! \equiv \pm 1 \pmod p$, *Amer. Math. Monthly* **68** (1961), 145–146.
13. A. PIZER, On the 2-part of the class number of imaginary quadratic number fields, *J. Number Theory* **8** (1976), 184–192.
14. K. S. WILLIAMS, Note on Burde's rational biquadratic reciprocity law, *Canad. Math. Bull.* **20** (1977), 145–146.
15. K. S. WILLIAMS, Problem 323, *Canad. Math. Bull.* **26** (1983), 379–380.
16. K. S. WILLIAMS AND J. D. CURRIE, Class numbers and biquadratic reciprocity, *Canad. J. Math.* **34** (1982), 969–988.
17. K. S. WILLIAMS, K. HARDY AND C. FRIESEN, On the evaluation of the Legendre symbol $((A + B\sqrt{m})/p)$, *Acta Arith.* **45** (1985), 255–272.
18. K. YAMAMOTO, On Gaussian sums with biquadratic residue characters, *J. Reine Angew. Math.* **219** (1965), 200–213.

641 27 2-6