ACTA ARITHMETICA
XLVII (1986)

A congruence relating the class numbers of complex quadratic fields

by

KENNETH HARDY* and KENNETH S. WILLIAMS** (Ottawa, Ont., Canada)

1. Introduction. Throughout this paper n denotes a positive integer, $p_1, \ldots, p_s$ are s ($\geqslant 0$) distinct primes $\equiv 1 \pmod 4$, and $q_{s+1}, \ldots, q_n$ are $n-s$ ($\geqslant 0$) distinct primes $\equiv 3 \pmod 4$. We set

(1.1) $$d = (-1)^{n-s} p_1 \ldots p_s q_{s+1} \ldots q_n \equiv 1 \pmod 4.$$

The integer d is the discriminant of the quadratic field $Q(\sqrt{d})$, which is real or complex according as $n-s$ is even or odd. Setting

(1.2) $$p_i = -q_i \equiv 1 \pmod 4, \quad i = s+1, \ldots, n,$$

we have

(1.3) $$d = p_1 p_2 \ldots p_n,$$

(1.4) $$|d| = |p_1| \ldots |p_n| = p_1 \ldots p_s q_{s+1} \ldots q_n > 0.$$

The class number of the quadratic field of discriminant D is denoted by $h(D)$. If e is a (positive or negative) divisor of d, whose sign is chosen so that $e \equiv 1 \pmod 4$, then $-4e$ (resp. $-8e$) is the discriminant of the complex quadratic field $Q(\sqrt{-e})$ (resp. $Q(\sqrt{-2e})$) if $e > 0$, and e (resp. $8e$) is the discriminant of the complex quadratic field $Q(\sqrt{e})$ (resp. $Q(\sqrt{2e})$) if $e < 0$.

In this paper, for p an odd prime, $\left(\frac{-}{p}\right)$ denotes Legendre's symbol of quadratic residuacity (mod p), and $\left(\frac{-}{2}\right)$ denotes Kronecker's symbol, that is, for D the discriminant of a quadratic field

$$\left(\frac{D}{2}\right) = \begin{cases} 1, & \text{if } D \equiv 1 \pmod 8, \\ -1, & \text{if } D \equiv 5 \pmod 8, \\ 0, & \text{if } D \equiv 0 \pmod 4. \end{cases}$$

* 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.

It is the purpose of this paper to prove the following result.

THEOREM. *For d as defined in* (1.1), *we have*

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

$$+\sum_{\substack{e\mid d\\ e<0,\, e\equiv 1 \pmod 4}} \big(c_3(d, e)h(e)+c_4(d, e)h(8e)\big)+\frac{(-1)^n}{2}\prod_{i=1}^{n}(|p_i|-1)$$

$$\equiv c_5(d)+c_6(d) \pmod{2^{n+2}},$$

where

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

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

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

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

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

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

The proof of the theorem is given in Section 2. The idea of the proof is to transform the simple congruence (2.1) into sums which can be evaluated, either by appealing to classical class number formulae (see for example [1]) or by combinatorial arguments.

When $n = 1$ the theorem reduces to well-known congruences modulo 8 involving $h(-4p)$ and $h(-8p)$, where p is an odd prime (see for example [4], Proposition 2).

When $n = 2$ the theorem provides a unified congruence for the 18 congruences proved by Pizer ([4], Proposition 5) and the 16 congruences proved by Kenku ([3], Theorems 3 and 4). Unfortunately most of Kenku's congruences are incorrect. The tables below indicate which of Kenku's congruences are correct and which are incorrect.

Theorem 3 of [3]	
Case	Status
(i)	incorrect ($p = 17$, $q = 257$)
(ii)	correct
(iii)	incorrect ($p = 17$, $q = 89$)
(iv)	incorrect ($p = 17$, $q = 97$)
(v)	incorrect ($p = 37$, $q = 17$)
(vi)	incorrect ($p = 229$, $q = 17$)
(vii)	incorrect ($p = 29$, $q = 17$)
(viii)	incorrect ($p = 37$, $q = 41$)
(ix)	correct
(x)	correct
(xi)	incorrect ($p = 5$, $q = 101$)
(xii)	incorrect ($p = 17$, $q = 5$)

We note that (xi) can be made correct by replacing $p \equiv q \pmod{16}$ by $p \not\equiv q \pmod{16}$.

Theorem 4 of [3]	
Case	Status
(i)	correct
(ii)	incorrect ($p = 23$, $q = 7$)
$(\mathrm{iii})_1$	correct
$(\mathrm{iii})_2$	incorrect ($p = 11$, $q = 31$)

We note that (ii) can be corrected by replacing $h(-q)$ by $8h(-q)$ in the congruence.

When $n = 3$, by considering cases depending upon the values of p, q, r modulo 8 and the values of the Legendre symbols $\left(\frac{p}{q}\right)$, $\left(\frac{q}{r}\right)$, $\left(\frac{r}{p}\right)$ we could obtain from the theorem congruences involving $h(-4pqr)$ and $h(-8pqr)$ modulo 32 analogous to those of Pizer relating $h(-4pq)$ and $h(-8pq)$ modulo 16. However there are too many cases to make it practical to give a complete analysis. For example in the case $p \equiv q \equiv r \equiv 1 \pmod 4$ it is necessary to consider 20 cases and in the case $p \equiv q \equiv 1 \pmod 4$, $r \equiv 3 \pmod 4$ 40 cases are required.

For illustration, we just give four examples when the congruences take on especially simple forms.

COROLLARY. *Let p, q, r be distinct odd primes.*

(A) *If* $p \equiv q \equiv r \equiv 1 \pmod 8$, $\left(\frac{p}{q}\right) = \left(\frac{q}{r}\right) = \left(\frac{r}{p}\right) = -1$, *we have*

$$h(-4pqr)+h(-8pqr) \equiv 2p+2q+2r-6 \pmod{32}.$$

(B) *If* $p \equiv 1 \pmod 8$, $q \equiv 5 \pmod 8$, $r \equiv 7 \pmod 8$, $\left(\frac{p}{q}\right) = -1$, $\left(\frac{q}{r}\right) = 1$, $\left(\frac{r}{p}\right) = -1$, *we have*

$$2h(-pqr)+h(-8pqr) \equiv 2q+2r+8 \pmod{32}.$$

(C) *If* $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$, $q > 3$, $r \equiv 7 \pmod 8$, $\left(\frac{p}{q}\right) = -1$, $\left(\frac{q}{r}\right) = 1$, $\left(\frac{r}{p}\right) = -1$, *we have*

$$h(-8pqr)-h(-4pqr) \equiv 2p+2q-2r+6 \pmod{32}.$$

(D) *If* $p \equiv q \equiv r \equiv 7 \pmod 8$, $\left(\frac{p}{q}\right) = \left(\frac{q}{r}\right) = \left(\frac{r}{p}\right) = -1$, *then*

$$4h(-pqr)-h(-8pqr) \equiv 2p+2q+2r-10 \pmod{32}.$$

We remark that the congruence (A) follows from Théorème 2, Proposition B'_{16} and Proposition B'_{17} of [2].

2. Proof of the Theorem. For any positive integer k satisfying $(k, d) = 1$, we have

$$\prod_{i=1}^{n}\left(1-\left(\frac{p_i}{k}\right)\right) \equiv 0 \pmod{2^n}. \tag{2.1}$$

Thus we have

$$\sum_{e\mid d}^{*} (-1)^{\tau(e)}\left(\frac{e}{k}\right) \equiv 0 \pmod{2^n}, \tag{2.2}$$

where the asterisk indicates that e runs through the divisors of d, both positive and negative, for which $e \equiv 1 \pmod 4$, and $\tau(e)$ denotes the number of distinct prime factors of e. Summing (2.2) for $0 < k < |d|/8$, $(k, d) = 1$, and interchanging the orders of summation, we obtain

$$\sum_{e\mid d}^{*} (-1)^{\tau(e)} \sum_{\substack{0<k<|d|/8 \\ (k,d)=1}} \left(\frac{e}{k}\right) \equiv 0 \pmod{2^n}. \tag{2.3}$$

The term in (2.3) with $e = 1$ is

$$J(d) = \sum_{\substack{0<k<|d|/8 \\ (k,d)=1}} 1 = \sum_{0<k<|d|/8} \sum_{f\mid(k,d)} \mu(f). \tag{2.4}$$

The evaluation of $J(d)$ is carried out later in the proof (see (2.32)).

We now consider the terms in (2.3) for which $e \neq 1$. For convenience we define for $e\mid d$, $e \neq 1$, $e \equiv 1 \pmod 4$

$$S(d, e) = \sum_{\substack{0<k<|d|/8 \\ (k,d)=1}} \left(\frac{e}{k}\right), \tag{2.5}$$

so that (2.3) becomes

$$\sum_{\substack{e\mid d \\ e\neq 1}}^{*} \left((-1)^{\tau(e)} S(d, e)\right)+J(d) \equiv 0 \pmod{2^n}. \tag{2.6}$$

As

$$(k, d) = 1 \Leftrightarrow (k, d/e) = (k, e) = 1,$$

we have

$$S(d, e) = \sum_{\substack{0<k<|d|/8 \\ (k,d/e)=(k,e)=1}} \left(\frac{e}{k}\right) = \sum_{\substack{0<k<|d|/8 \\ (k,d/e)=1}} \left(\frac{e}{k}\right) = \sum_{0<k<|d|/8} \left(\frac{e}{k}\right) \sum_{f\mid(k,d/e)} \mu(f). \tag{2.7}$$

Interchanging the orders of summation we obtain

$$S(d, e) = \sum_{f\mid d/e} (-1)^{\tau(f)} \sum_{\substack{0<k<|d|/8 \\ f\mid k}} \left(\frac{e}{k}\right). \tag{2.8}$$

Replacing k by lf in the inner sum of (2.8), we get

$$S(d, e) = \sum_{f\mid d/e} (-1)^{\tau(f)} \left(\frac{e}{f}\right) \sum_{0<l<|d|/8f} \left(\frac{e}{l}\right). \tag{2.9}$$

Since the Kronecker symbol $\left(\frac{e}{l}\right)$ is a character of modulus $|e|$, for any integer $u \geq 0$, we have

$$\sum_{l=u|e|+1}^{(u+1)|e|} \left(\frac{e}{l}\right) = 0. \tag{2.10}$$

Adding (2.10) for $u = 0, 1, 2, \ldots, t-1$, where $t = \left[\frac{|d/e|}{8f}\right]$ and [ ] denotes the greatest integer function, we obtain

$$\sum_{0 < l \leqslant t|e|} \left(\frac{e}{l}\right) = 0. \tag{2.11}$$

Using (2.11) in (2.9) we deduce

$$S(d, e) = \sum_{f|d/e} (-1)^{\tau(f)} \left(\frac{e}{f}\right) \sum_{l=t|e|+1}^{t'} \left(\frac{e}{l}\right), \quad \text{where} \quad t' = \left[\frac{|d|}{8f}\right]. \tag{2.12}$$

Changing the variable from l to m in the inner sum of (2.12) by means of the transformation

$$l = t|e| + m,$$

we obtain, as $\left(\frac{e}{l}\right) = \left(\frac{e}{m}\right)$,

$$S(d, e) = \sum_{f|d/e} (-1)^{\tau(f)} \left(\frac{e}{f}\right) \sum_{m=1}^{t'-|e|t} \left(\frac{e}{m}\right). \tag{2.13}$$

Next we treat the inner sum in (2.13). We define integers $r = 1, 3, 5, 7$ and $s = 1, 3, 5, 7$ by

$$\frac{|d|}{f} \equiv r \pmod 8, \qquad \frac{|d/e|}{f} \equiv s \pmod 8. \tag{2.14}$$

Appealing to (2.14) we obtain

$$\left[\frac{|d|}{8f}\right] - |e| \left[\frac{|d/e|}{8f}\right] = \frac{\left(\frac{|d|}{f} - r\right)}{8} - |e| \frac{\left(\frac{|d/e|}{f} - s\right)}{8} = \frac{s|e| - r}{8},$$

so that

$$t' - |e|\, t = \left[\frac{|d|}{8f}\right] - |e| \left[\frac{|d/e|}{8f}\right] = \left[\frac{s|e|}{8}\right].$$

Hence we have

$$\sum_{m=1}^{t'-|e|t} \left(\frac{e}{m}\right) = \sum_{0 < m < (s/8)|e|} \left(\frac{e}{m}\right) = \sum_{v=1}^{s} T(v), \tag{2.15}$$

where

$$T(v) = \sum_{\frac{1}{8}(v-1)|e| < m < \frac{1}{8}v|e|} \left(\frac{e}{m}\right), \qquad v = 1, 2, \ldots, 8. \tag{2.16}$$

The values of $T(v)$ can be deduced from the work of Berndt ([1], Cors. 3.4, 3.9, 7.3) and are given as follows: setting $\lambda(e) = 1$, if $e = -3$, $\lambda(e) = 0$, otherwise, we have

$$T(1) = \begin{cases} \frac{1}{4}\left(\frac{e}{2}\right) h(-4e) + \frac{1}{4} h(-8e), & \text{if} \quad e > 0, \\ \frac{1}{4}\left(5 - \left(\frac{e}{2}\right)\right) h(e) - \frac{1}{4} h(-8e) - \lambda(e), & \text{if} \quad e < 0, \end{cases} \tag{2.17}$$

$$T(2) = \begin{cases} \frac{1}{4}\left(2 - \left(\frac{e}{2}\right)\right) h(-4e) - \frac{1}{4} h(-8e), & \text{if} \quad e > 0, \\ \frac{3}{4}\left(-1 + \left(\frac{e}{2}\right)\right) h(e) + \frac{1}{4} h(8e) + \lambda(e), & \text{if} \quad e < 0, \end{cases} \tag{2.18}$$

$$T(3) = \begin{cases} \frac{1}{4}\left(-2 - \left(\frac{e}{2}\right)\right) h(-4e) + \frac{1}{4} h(-8e), & \text{if} \quad e > 0, \\ \frac{3}{4}\left(1 - \left(\frac{e}{2}\right)\right) h(e) + \frac{1}{4} h(8e) - \lambda(e), & \text{if} \quad e < 0, \end{cases} \tag{2.19}$$

$$T(4) = \begin{cases} \frac{1}{4}\left(\frac{e}{2}\right) h(-4e) - \frac{1}{4} h(-8e), & \text{if} \quad e > 0, \\ \frac{3}{4}\left(1 - \left(\frac{e}{2}\right)\right) h(e) - \frac{1}{4} h(8e) - \lambda(e), & \text{if} \quad e < 0, \end{cases} \tag{2.20}$$

and, for $v = 5, 6, 7, 8$,

$$T(v) = \begin{cases} T(9-v), & \text{if} \quad e > 0, \\ -T(9-v), & \text{if} \quad e < 0. \end{cases} \tag{2.21}$$

Hence for $s = 1, 3, 5, 7$ we have

$$4 \sum_{v=1}^{s} T(v) = \begin{cases} \left(\frac{-1}{s}\right)\left(\frac{e}{2}\right) h(-4e) + \left(\frac{-2}{s}\right) h(-8e), & \text{if} \quad e > 0, \\ \left(5 - \left(\frac{e}{2}\right)\right) h(e) - \left(\frac{2}{s}\right) h(8e) - 4\lambda(e), & \text{if} \quad e < 0. \end{cases} \tag{2.22}$$

Using (2.22) in (2.15), and appealing to (2.13), we obtain

(2.23) $4S(d, e)$

$$= \begin{cases} \sum_{f|d/e} (-1)^{\tau(f)} \left(\frac{e}{f}\right) \left\{ \left(\frac{-1}{|d/e|/f}\right)\left(\frac{e}{2}\right) h(-4e) + \left(\frac{-2}{|d/e|/f}\right) h(-8e) \right\}, & \text{if} \quad e > 0, \\ \sum_{f|d/e} (-1)^{\tau(f)} \left(\frac{e}{f}\right) \left\{ \left(5 - \left(\frac{e}{2}\right)\right) h(e) - \left(\frac{2}{|d/e|/f}\right) h(8e) \right\} \\ \qquad + 4(-1)^n \lambda(e) \prod_{p|d/e} \left(\left(\frac{e}{p}\right) - 1\right), & \text{if} \quad e < 0. \end{cases}$$

Hence we have with $\theta(d) = 1$, if $3|d$, $\theta(d) = 0$, if $3 \nmid d$,

$$(2.24)\quad 4\sum_{\substack{e|d\\ e\neq 1}}^{*}(-1)^{\tau(e)} S(d, e)$$
$$= \sum_{\substack{e|d\\ e>1}}^{*}(-1)^{\tau(e)}\sum_{f|d/e}(-1)^{\tau(f)}\left(\frac{e}{f}\right)\left\{\left(\frac{-1}{|d/e|/f}\right)\left(\frac{e}{2}\right)h(-4e)+\left(\frac{-2}{|d/e|/f}\right)h(-8e)\right\}$$
$$+\sum_{\substack{e|d\\ e<0}}^{*}(-1)^{\tau(e)}\sum_{f|d/e}(-1)^{\tau(f)}\left(\frac{e}{f}\right)\left\{\left(5-\left(\frac{e}{2}\right)\right)h(e)-\left(\frac{2}{|d/e|/f}\right)h(8e)\right\}$$
$$+4\theta(d)\prod_{p|d/3}\left(1-\left(\frac{-3}{p}\right)\right).$$

Next, with $\alpha(k) = 1$, $\left(\frac{-1}{k}\right)$, $\left(\frac{-2}{k}\right)$, or $\left(\frac{2}{k}\right)$, we have

$$(-1)^{\tau(d/e)}\sum_{f|d/e}(-1)^{\tau(f)}\left(\frac{e}{f}\right)\alpha\left(\frac{|d/e|}{f}\right)$$
$$= (-1)^{\tau(d/e)}\alpha(|d/e|)\sum_{f|d/e}(-1)^{\tau(f)}\left(\frac{e}{f}\right)\alpha(f)$$
$$= (-1)^{\tau(d/e)}\alpha(|d/e|)\prod_{p|d/e}\left(1-\left(\frac{e}{p}\right)\alpha(p)\right) = \prod_{p|d/e}\left(\left(\frac{e}{p}\right)-\alpha(p)\right),$$

so that

$$(2.25)\quad (-1)^{\tau(e)}\sum_{f|d/e}(-1)^{\tau(f)}\left(\frac{e}{f}\right)\alpha\left(\frac{|d/e|}{f}\right) = (-1)^{n}\prod_{p|d/e}\left(\left(\frac{e}{p}\right)-\alpha(p)\right).$$

Setting

$$(2.26)\quad c_1(d, e) = \left(\frac{e}{2}\right)\prod_{p|d/e}\left(\left(\frac{e}{p}\right)-\left(\frac{-1}{p}\right)\right),$$

$$(2.27)\quad c_2(d, e) = \prod_{p|d/e}\left(\left(\frac{e}{p}\right)-\left(\frac{-2}{p}\right)\right),$$

$$(2.28)\quad c_3(d, e) = \left(5-\left(\frac{e}{2}\right)\right)\prod_{p|d/e}\left(\left(\frac{e}{p}\right)-1\right),$$

$$(2.29)\quad c_4(d, e) = -\prod_{p|d/e}\left(\left(\frac{e}{p}\right)-\left(\frac{2}{p}\right)\right),$$

we obtain from (2.24)–(2.29)

$$(2.30)\quad 4\sum_{\substack{e|d\\ e\neq 1}}^{*}(-1)^{\tau(e)} S(d, e) = (-1)^{n}\sum_{\substack{e|d\\ e>1}}^{*}\{c_1(d, e)h(-4e)+c_2(d, e)h(-8e)\}$$
$$+(-1)^{n}\sum_{\substack{e|d\\ e<0}}^{*}\{c_3(d, e)h(e)+c_4(d, e)h(8e)\}+4\theta(d)\prod_{p|d/3}\left(1-\left(\frac{-3}{p}\right)\right),$$

and so by (2.6) we obtain

$$(2.31)\quad \sum_{\substack{e|d\\ e>1}}^{*}\{c_1(d, e)h(-4e)+c_2(d, e)h(-8e)\}$$
$$+\sum_{\substack{e|d\\ e<0}}^{*}\{c_3(d, e)h(e)+c_4(d, e)h(8e)\}+(-1)^{n}4J(d) \equiv c_6(d) \pmod{2^{n+2}},$$

as

$$4(-1)^{n}\theta(d)\prod_{p|d/3}\left(1-\left(\frac{-3}{p}\right)\right)$$
$$= \begin{cases} 0, & \text{if } 3\nmid d,\\ -4, & \text{if } d=-3,\\ 0, & \text{if } d\neq -3,\ 3|d \text{ and } \exists p\equiv 1 \pmod 3 \text{ with } p|d/3,\\ (-1)^{n}2^{n+1}, & \text{if } d\neq -3,\ 3|d \text{ and all primes dividing } d/3 \text{ are} \equiv 2 \pmod 3,\end{cases}$$
$$\equiv c_6(d) \pmod{2^{n+2}},$$

where $c_6(d)$ is defined in the theorem.

Now we turn to the evaluation of $J(d)$. Interchanging the order of summation in (2.4) we obtain

$$(2.32)\quad J(d) = \sum_{f|d}(-1)^{\tau(f)}\sum_{\substack{0<k<|d|/8\\ f|k}} 1.$$

Replacing k by fl in the inner sum, we obtain

$$(2.33)\quad J(d) = \sum_{f|d}(-1)^{\tau(f)}[|d|/8f].$$

Changing the summation variable from f to $|d|/f$ in (2.33), we obtain

$$(2.34)\quad J(d) = (-1)^{n}\sum_{f|d}(-1)^{\tau(f)}[f/8].$$

Hence we have

$$J(d) = (-1)^n \sum_{f \mid |p_1 p_2 \dots p_n|} (-1)^{\varepsilon(f)} [f/8]$$

$$= (-1)^n \sum_{r=0}^{n} (-1)^r \sum_{1 \leqslant i_1 < i_2 < \dots < i_r \leqslant n} [|p_{i_1} \dots p_{i_r}|/8]$$

$$= (-1)^n \sum_{r=0}^{n} (-1)^r \sum_{\substack{s=1 \\ s \text{ odd}}}^{7} \sum_{\substack{1 \leqslant i_1 < i_2 < \dots < i_r \leqslant n \\ |p_{i_1} \dots p_{i_r}| \equiv s \pmod 8}} \left(\frac{|p_{i_1} \dots p_{i_r}| - s}{8} \right)$$

$$= \frac{(-1)^n}{8} \sum_{r=0}^{n} (-1)^r \sum_{1 \leqslant i_1 < i_2 < \dots < i_r \leqslant n} |p_{i_1} \dots p_{i_r}|$$

$$- \frac{(-1)^n}{8} \sum_{\substack{s=1 \\ s \text{ odd}}}^{7} s \sum_{r=0}^{n} (-1)^r \sum_{\substack{1 \leqslant i_1 < i_2 < \dots < i_r \leqslant n \\ |p_{i_1} \dots p_{i_r}| \equiv s \pmod 8}} 1,$$

that is

$$J(d) = \frac{1}{8}(|p_1|-1) \dots (|p_n|-1) - \frac{(-1)^n}{8} \sum_{k,l=0}^{1} (2k+4l+1) \sum_{r=0}^{n} (-1)^r \sum_{\substack{1 \leqslant i_1 < i_2 < \dots < i_r \leqslant n \\ |p_{i_1} \dots p_{i_r}| \equiv 2k+4l+1 \pmod 8}} 1. \tag{2.35}$$

A simple counting argument shows that

$$\sum_{\substack{1 \leqslant i_1 < i_2 < \dots < i_r \leqslant n \\ |p_{i_1} \dots p_{i_r}| \equiv 2k+4l+1 \pmod 8}} 1 = \sum\nolimits^{**} \binom{N_1}{n_1} \binom{N_3}{n_3} \binom{N_5}{n_5} \binom{N_7}{n_7}, \tag{2.36}$$

where the sum $\sum^{**}$ is extended over n_1, n_3, n_5, n_7 satisfying $0 \leqslant n_j \leqslant N_j$, for $j = 1, 3, 5, 7$, $n_1 + n_3 + n_5 + n_7 = r$, $n_3 + n_7 \equiv k \pmod 2$, $n_5 + n_7 \equiv l \pmod 2$, and where, for $j = 1, 3, 5, 7$,

(2.37) $N_j =$ number of $|p_i| (1 \leqslant i \leqslant n)$ such that $|p_i| \equiv j \pmod 8$,

so that

$$N_1 + N_3 + N_5 + N_7 = n \geqslant 1. \tag{2.38}$$

Hence we have

$$J(d) = \frac{1}{8} \prod_{i=1}^{n} (|p_i| - 1) - \frac{(-1)^n}{8} \sum_{k,l=0}^{1} (2k+4l+1) \sum_{r=0}^{n} (-1)^r \sum\nolimits^{**} \binom{N_1}{n_1} \binom{N_3}{n_3} \binom{N_5}{n_5} \binom{N_7}{n_7}. \tag{2.39}$$

Next we evaluate

$$A(k, l) = \sum_{r=0}^{n} (-1)^r \sum\nolimits^{**} \binom{N_1}{n_1} \binom{N_3}{n_3} \binom{N_5}{n_5} \binom{N_7}{n_7}. \tag{2.40}$$

In order to do this, we set, for $\alpha = \pm 1$, $\beta = \pm 1$,

$$F_{\alpha,\beta}(x) = (1+x)^{N_1} (1+\alpha x)^{N_3} (1+\beta x)^{N_5} (1+\alpha\beta x)^{N_7}. \tag{2.41}$$

By the binomial theorem we obtain

$$F_{\alpha,\beta}(x) = \sum_{r=0}^{n} \left\{ \sum_{\substack{n_1, n_3, n_5, n_7 = 0 \\ n_1 + n_3 + n_5 + n_7 = r}}^{N_1, N_3, N_5, N_7} \binom{N_1}{n_1} \binom{N_3}{n_3} \binom{N_5}{n_5} \binom{N_7}{n_7} \alpha^{n_3+n_7} \beta^{n_5+n_7} \right\} x^r. \tag{2.42}$$

Taking $x = -1$ and $(\alpha, \beta) = (1, 1), (-1, 1), (1, -1), (-1, -1)$ in (2.42), and appealing to (2.40), we obtain

$$\begin{cases} A(0,0) + A(1,0) + A(0,1) + A(1,1) = F_{1,1}(-1), \\ A(0,0) - A(1,0) + A(0,1) - A(1,1) = F_{-1,1}(-1), \\ A(0,0) + A(1,0) - A(0,1) - A(1,1) = F_{1,-1}(-1), \\ A(0,0) - A(1,0) - A(0,1) + A(1,1) = F_{-1,-1}(-1). \end{cases} \tag{2.43}$$

Solving the equations in (2.43) for the $A(k, l)$, we obtain

$$\begin{cases} A(0,0) = \frac{1}{4}\{F_{1,1}(-1) + F_{-1,1}(-1) + F_{1,-1}(-1) + F_{-1,-1}(-1)\}, \\ A(1,0) = \frac{1}{4}\{F_{1,1}(-1) - F_{-1,1}(-1) + F_{1,-1}(-1) - F_{-1,-1}(-1)\}, \\ A(0,1) = \frac{1}{4}\{F_{1,1}(-1) + F_{-1,1}(-1) - F_{1,-1}(-1) - F_{-1,-1}(-1)\}, \\ A(1,1) = \frac{1}{4}\{F_{1,1}(-1) - F_{-1,1}(-1) - F_{1,-1}(-1) + F_{-1,-1}(-1)\}. \end{cases} \tag{2.44}$$

Now from (2.41) we see that

$$\begin{cases} F_{1,1}(-1) = 0 \quad (\text{as } n = N_1 + N_3 + N_5 + N_7 \geqslant 1), \\ F_{-1,1}(-1) = \begin{cases} 0, & \text{if } N_1 \text{ or } N_5 \geqslant 1, \\ 2^{N_3+N_7}, & \text{if } N_1 = N_5 = 0, \end{cases} \\ F_{1,-1}(-1) = \begin{cases} 0, & \text{if } N_1 \text{ or } N_3 \geqslant 1, \\ 2^{N_5+N_7}, & \text{if } N_1 = N_3 = 0, \end{cases} \\ F_{-1,-1}(-1) = \begin{cases} 0, & \text{if } N_1 \text{ or } N_7 \geqslant 1, \\ 2^{N_3+N_5}, & \text{if } N_1 = N_7 = 0. \end{cases} \end{cases} \tag{2.45}$$

Using the values given by (2.45) in (2.44) we obtain the following table of values of the $A(k, l)$.

N_1	N_3	N_5	N_7	$A(0, 0)$	$A(1, 0)$	$A(0, 1)$	$A(1, 1)$
$\geqslant 1$	$\geqslant 0$	$\geqslant 0$	$\geqslant 0$	0	0	0	0
0	$\geqslant 1$	$\geqslant 1$	$\geqslant 1$	0	0	0	0
0	$\geqslant 1$	$\geqslant 1$	0	2^{n-2}	-2^{n-2}	-2^{n-2}	2^{n-2}
0	$\geqslant 1$	0	$\geqslant 1$	2^{n-2}	-2^{n-2}	2^{n-2}	-2^{n-2}
0	0	$\geqslant 1$	$\geqslant 1$	2^{n-2}	2^{n-2}	-2^{n-2}	-2^{n-2}
0	$\geqslant 1$	0	0	2^{n-1}	-2^{n-1}	0	0
0	0	$\geqslant 1$	0	2^{n-1}	0	-2^{n-1}	0
0	0	0	$\geqslant 1$	2^{n-1}	0	0	-2^{n-1}

Hence setting

(2.46) $$A(d) = \sum_{k,l=0}^{1} (2k+4l+1)A(k, l),$$

we have, appealing to the table,

(2.47) $$A(d) = \begin{cases} 0, & \text{if } N_1 \geqslant 1, \\ 0, & \text{if } N_1 = 0,\ N_3 \geqslant 1,\ N_5 \geqslant 1,\ N_7 \geqslant 1, \\ 0, & \text{if } N_1 = 0,\ N_3 \geqslant 1,\ N_5 \geqslant 1,\ N_7 = 0, \\ -2^n, & \text{if } N_1 = 0,\ N_3 \geqslant 1,\ N_5 = 0,\ N_7 \geqslant 1, \\ -2^{n+1}, & \text{if } N_1 = N_3 = 0,\ N_5 \geqslant 1,\ N_7 \geqslant 1, \\ -2^n, & \text{if } N_1 = 0,\ N_3 \geqslant 1,\ N_5 = N_7 = 0, \\ -2^{n+1}, & \text{if } N_1 = N_3 = 0,\ N_5 \geqslant 1,\ N_7 = 0, \\ -3\cdot 2^n, & \text{if } N_1 = N_3 = N_5 = 0,\ N_7 \geqslant 1, \end{cases}$$

and from (2.39), (2.40), (2.46)

(2.48) $$J(d) = \frac{1}{8}\prod_{i=1}^{n}(|p_i|-1) - \frac{(-1)^n}{8}A(d).$$

Thus from (2.31) and (2.48) we obtain

(2.49) $$\sum_{\substack{e|d\\ e>1}}^{*} \{c_1(d, e)h(-4e)+c_2(d, e)h(-8e)\} + \sum_{\substack{e|d\\ e<0}}^{*} \{c_3(d, e)h(e)+c_4(d, e)h(8e)\} + \frac{(-1)^n}{2}\prod_{i=1}^{n}(|p_i|-1) \equiv \tfrac{1}{2}A(d)+c_6(d) \pmod{2^{n+2}}.$$

Next, as $h(-4) = h(-8) = 1$, we have

$$c_1(d, 1)h(-4)+c_2(d, 1)h(-8) = c_1(d, 1)+c_2(d, 1) = \prod_{p|d}\left(1-\left(\frac{-1}{p}\right)\right)+\prod_{p|d}\left(1-\left(\frac{-2}{p}\right)\right),$$

that is

(2.50) $$c_1(d, 1)h(-4)+c_2(d, 1)h(-8) = \begin{cases} 0, & \text{if } N_1 \geqslant 1, \\ 0, & \text{if } N_1 = 0,\ N_3 \geqslant 1,\ N_5 \geqslant 1,\ N_7 \geqslant 1, \\ 0, & \text{if } N_1 = 0,\ N_3 \geqslant 1,\ N_5 \geqslant 1,\ N_7 = 0, \\ 2^n, & \text{if } N_1 = 0,\ N_3 \geqslant 1,\ N_5 = 0,\ N_7 \geqslant 1, \\ 2^n, & \text{if } N_1 = N_3 = 0,\ N_5 \geqslant 1,\ N_7 \geqslant 1, \\ 2^n, & \text{if } N_1 = 0,\ N_3 \geqslant 1,\ N_5 = N_7 = 0, \\ 2^n, & \text{if } N_1 = N_3 = 0,\ N_5 \geqslant 1,\ N_7 = 0, \\ 2^{n+1}, & \text{if } N_1 = N_3 = N_5 = 0,\ N_7 \geqslant 1. \end{cases}$$

so by (2.47) and (2.50) we have

$$\{c_1(d, 1)h(-4)+c_2(d, 1)h(-8)\}+\tfrac{1}{2}A(d) = \begin{cases} 0, & \text{if } N_1 \geqslant 1, \\ 0, & \text{if } N_1 = 0,\ N_3 \geqslant 1,\ N_5 \geqslant 1,\ N_7 \geqslant 1, \\ 0, & \text{if } N_1 = 0,\ N_3 \geqslant 1,\ N_5 \geqslant 1,\ N_7 = 0, \\ 2^{n-1}, & \text{if } N_1 = 0,\ N_3 \geqslant 1,\ N_5 = 0,\ N_7 \geqslant 1, \\ 0, & \text{if } N_1 = N_3 = 0,\ N_5 \geqslant 1,\ N_7 \geqslant 1, \\ 2^{n-1}, & \text{if } N_1 = 0,\ N_3 \geqslant 1,\ N_5 = N_7 = 0, \\ 0, & \text{if } N_1 = N_3 = 0,\ N_5 \geqslant 1,\ N_7 = 0, \\ 2^{n-1}, & \text{if } N_1 = N_3 = N_5 = 0,\ N_7 \geqslant 1, \end{cases}$$

that is

(2.51) $$c_1(d, 1)h(-4)+c_2(d, 1)h(-8)+\tfrac{1}{2}A(d) = \begin{cases} 2^{n-1}, & \text{if } d \text{ is divisible only by primes} \equiv 3 \pmod 4, \\ 0, & \text{otherwise}, \end{cases} = c_5(d).$$

Adding $c_1(d, 1)h(-4)+c_2(d, 1)h(-8)$ to both sides of (2.49), we obtain, by (2.51),

$$\sum_{\substack{e|d\\ e>0}}^{*} \{c_1(d, e)h(-4e)+c_2(d, e)h(-8e)\} + \sum_{\substack{e|d\\ e<0}}^{*} \{c_3(d, e)h(e)+c_4(d, e)h(8e)\} + \frac{(-1)^n}{2}\prod_{i=1}^{n}(|p_i|-1) \equiv c_5(d)+c_6(d) \pmod{2^{n+2}}.$$

This completes the proof of the theorem.

References

[1] B. C. Berndt, *Classical theorems on quadratic residues*, L'Enseign. Math. 22 (1976), pp. 261–304.
[2] P. Kaplan, *Sur le 2-groupe des classes d'idéaux des corps quadratiques*, J. Reine Angew. Math. 283/284 (1976), pp. 313–363.
[3] M. A. Kenku, *Atkin-Lehner involutions and class number residuality*, Acta Arith. 33 (1977), pp. 1–9.
[4] A. Pizer, *On the 2-part of the class number of imaginary quadratic number fields*, J. Number Theory 8 (1976), pp. 184–192.

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
OTTAWA, ONTARIO, CANADA K1S 5B6

Received on 1.4.1985
and in revised form on 10.6.1985 (1503)

ACTA ARITHMETICA
XLVII (1986)

Reducibility of lacunary polynomials, VI

by

A. Schinzel (Warszawa)

In this paper we shall complete the study of reducibility of non-reciprocal quadrinomials begun in [3] and continued in [6], [7].

As usual in this series of papers reducibility means reducibility over the rational field Q, polynomials have integral coefficients and for a polynomial $f \in Z[x]$, $f \neq 0$, $|f|$ denotes its degree, $\|f\|$ the sum of squares of its coefficients, $Kf(x)$, called the kernel of f, the polynomial $x^{-\mathrm{ord}_x f} f$ deprived of all its cyclotomic factors. The formula

$$f(x) \stackrel{\text{can}}{=} \text{const} \prod_{\sigma=1}^{s} f_\sigma(x)^{e_\sigma}$$

means in addition to the equality that the polynomials f_σ are irreducible and relatively prime in pairs. We shall prove

Theorem 1. *Let a_j $(0 \leqslant j \leqslant 3)$ be non-zero integers. Then for any quadrinomial*

$$q(x) = a_0 + \sum_{j=1}^{3} a_j x^{n_j} \quad (0 < n_1 < n_2 < n_3),$$

that is not reciprocal, we have one of the following four possibilities:

(i) *$Kq(x)$ is irreducible.*

(ii) *$q(x)$ can be divided into two parts that have the highest common factor $d(x)$ being a non-reciprocal binomial. $K(q(x)d(x)^{-1})$ is then irreducible, unless $q(x)d(x)^{-1}$ is a binomial.*

(iii) *$q(x)$ can be represented in one of the forms*

$$k(T^2 - 4TUVW - U^2V^4 - 4U^2W^4)$$
$$= k(T - UV^2 - 2UVW - 2UW^2)(T + UV^2 - 2UVW + 2UW^2),$$

$$k(U^3 + V^3 + W^3 - 3UVW)$$
$$= k(U + V + W)(U^2 + V^2 + W^2 - UV - UW - VW),$$

$$k(U^2 + 2UV + V^2 - W^2) = k(U + V + W)(U + V - W),$$