2009

# Sun's Conjectures on Fourth Powers in the Class Group of Binary Quadratic Forms

Robert W. Fitzgerald
*Southern Illinois University Carbondale*, rfitzg@math.siu.edu

# Sun's conjectures on fourth powers in the class group of binary quadratic forms

Robert W. Fitzgerald
Southern Illinois University
Carbondale, IL 62901-4408
rfitzg@math.siu.edu

**Abstract**

We prove five of Sun's conjectures on the index of the subgroup of fourth powers in the class group of binary quadratic forms.

Sun [5] proved that of $p$ and $q$ are distinct odd primes then $(-1)^{(q-1)/2}q$ is a quartic residue modulo $p$ iff $p$ is represented by an element of $G(-16q^2)^4$, where $G(\Delta)$ is the class group of primitive binary quadratic forms of discriminant $\Delta$. In [6] Sun posed a series of conjectures, labeled (8.2) through (8.6), on the order of $G(\Delta)^4$, denoted by $h_4(\Delta)$. Liu [4] has found counterexamples to conjecture (8.4). Here we prove Sun's conjectures (8.2), (8.3), (8.5) and (8.6) are correct and prove a modified version of (8.4) is also correct. The proofs are elementary.

# 1 Background

We will write the binary quadratic form $f(x,y) = ax^2+bxy+cy^2$ more briefly as $f = (a,b,c)$. We denote the $SL_2(\mathbb{Z})$ equivalence class by $[f] = [a,b,c]$.

For an odd prime $p$ dividing $\Delta$, the associated generic character is $\chi_p(f) = \left(\frac{r}{f}\right)$, where $r$ is any value represented by $f$ that is prime to $p$. We also need:

$$\chi_{-1}(f) = \left(\frac{-1}{r}\right) \qquad \chi_2(f) = \left(\frac{2}{r}\right) \qquad \chi_{-2}(f) = \left(\frac{-2}{r}\right),$$

where $r$ is any odd number represented by $f$. [1] has a chart (page 52) that lists which generic characters go with each discriminant. We will use this frequently without further reference.

We present a classical result since it does not appear in precisely this form in most references.

**Proposition 1.1.** *Let $\Delta$ be a discriminant and let $g$ be the number of generic characters for $G(\Delta)$.*

1. *The principal genus has index $2^{g-1}$. The number of genera is $2^{g-1}$.*
2. *The elements of exponent 2 in $G(\Delta)$ form a subgroup of order $2^{g-1}$.*
3. *The number of cyclic factors in the Sylow 2-subgroup of $G(\Delta)$ is $g-1$.*
4. *Every element of the principal genus is a square.*

**Proof:** Let $\chi_1, \chi_2, \ldots \chi_g$ be the generic characters and consider $\chi = (\chi_1, \ldots, \chi_g) : G(\Delta) \to \{\pm 1\}^g$. Then [1] Theorem 7.6 gives that the image of $\chi$ has order $2^{g-1}$. This proves (1) and (2) follows from [1] Theorem 4.17. Last, (2) implies (3) which implies (4). $\square$

We need one other classical result. We denote $|G(\Delta)|$ by $h(\Delta)$.

**Proposition 1.2.** *Suppose $\Delta$ is negative, even and not $-4$. Then $h(16\Delta) = 4h(\Delta)$.*

**Proof:** This follows from the formula [2] Theorem 2 (page 217)

$$h(f^2\Delta) = f h(\Delta) \prod_{q|f} \left[1 - \left(\frac{d}{q}\right) q^{-1}\right],$$

where the product is over prime divisors $q$ of $f$. This is stated for ideal class groups, but for negative discriminants these coincide with the form class groups of the same discriminant. $\square$

Our computations depend on the following.

**Lemma 1.3.** *Let $g$ be the number of generic characters for $G(\Delta)$. Let $K$ denote the principal genus and $E$ the subgroup of elements of exponent 2 in $G(\Delta)$. Write $|K \cap E| = 2^e$. Then:*

$$h_4(\Delta) = h(\Delta)/2^{g+e-1}.$$

**Proof:** Write

$$G(\Delta) = C(2^{k_1}) \times C(2^{k_2}) \times \cdots \times C(2^{k_{g-1}}) \times H,$$

where $C(2^k)$ denotes the cyclic group of order $2^k$, $H$ has odd order and we have used Theorem 1.1 (3) for the number of factors. Let $a$ be the number of $k_i$ equal to 1 and let $b$ be the number of $k_i$ greater than 1. The element of order 2 in a $C(2^k)$ is a square (equivalently, in $K$) iff $k \geq 2$. Hence $2^e = 2^b$. Thus:

$$[G(\Delta) : G(\Delta)^4] = 2^a \cdot 4^b = 2^{g-1-b} \cdot 4^b = 2^{g+b-1} = 2^{g+e-1}.$$

□

We will use the notations $K, E$ and $e$ throughout the paper.

## 2 Proof of the conjectures

We begin by proving Conjectures (8.2), (8.3) and (8.5), in this order. The method of proof is the same in each. Find the elements of exponent 2 (that is, the subgroup $E$). This can be done by finding the possible $(a, ka, c)$ of the given discriminant and reducing each; use 1.1 (2) to check that all have been found. Evaluate the generic characters of these forms and so determine those in the principal genus, $K \cap E$, and $e$, where $2^e = |K \cap E|$.

**Theorem 2.1.** *Let $p$ be a prime with $p \equiv 1 \pmod 8$. Then*

$$h_4(-8p) = h(-8p)/4 = h_4(-128p).$$

**Proof:** For $\Delta = -8p$ there are two generic characters, $\chi_p$ and $\chi_{-2}$. The two elements of exponent two are $[1, 0, 2p]$ and $[2, 0, p]$ which are both sent to 1 by both characters (as $p \equiv 1 \pmod 8$). Hence $E$ is contained in $K$. Thus $e = 1$ and Lemma 1.3 gives $h_4(-8p) = h(-8p)/4$.

For $\Delta = -128p$ there are three generic characters, $\chi_p, \chi_{-1}$ and $\chi_2$. The elements of exponent two are:

$$[1, 0, 32p] \quad [4, 4, 32p + 1] \quad [32, 0, p] \quad [32, 32, p + 8].$$

Again, each character sends each of these forms to 1. Hence $e = 2$ and we have:

$$\begin{aligned} h_4(-128p) &= h(-128p)/16 \qquad \text{by 1.3} \\ &= h(-8p)/4 \qquad \text{by 1.2} \\ &= h_4(-8p), \end{aligned}$$

by the first paragraph. $\square$

**Theorem 2.2.** *Let $p$ be a prime with $p \equiv 1 \pmod{24}$. Then*

$$h_4(-24p) = h(-24p)/8 = h_4(-384p).$$

**Proof:** For $\Delta = -24p$, there are three generic characters: $\chi_3, \chi_p$ and $\chi_2$. The elements of exponent 2 in $G(-24p)$ are: $[1,0,6p], [2,0,3p], [3,0,2p]$ and $[6,0,p]$. The first and last are sent to 1 by each character while $\chi_3$ maps the middle two to -1 (as $\left(\frac{2}{3}\right) = -1$). Hence $e = 1$ and 1.3 gives $h_4(-24p) = h(-24p)/8$.

Next, $G(-384p) = G(-16 \cdot 24p)$ has four generic characters: $\chi_3, \chi_p, \chi_{-1}$ and $\chi_2$.The eight elements in $G(-384p)$ of exponent 2 are:

$$\begin{array}{rl} f_1 = [1,0,96p] & \qquad f_2 = [4,4,24p+1] \\ f_3 = [32,0,3p] & \qquad f_4 = [32,32,3p+8] \\ f_5 = [3,0,32p] & \qquad f_6 = [12,12,8p+3] \\ f_7 = [96,0,p] & \qquad f_8 = [96,96,p+24] \end{array}$$

A simple computation shows $f_1, f_2, f_7$ and $f_8$ are in the principal genus while $\chi_3$ sends $f_3, f_4, f_5$ and $f_6$ to -1. Thus $e = 2$ and

$$h_4(-384p) = h(-384p)/32 = h(-24p)/8 = h_4(-24p).$$

$\square$

**Theorem 2.3.** *Let $p$ and $q$ be primes with $p, q \equiv 1 \pmod{8}$. Then*

$$h_4(-8pq) = h(-128pq) = \begin{cases} h(-8pq)/16, & \text{if } \left(\frac{p}{q}\right) = 1 \\ h(-8pq)/8, & \text{if } \left(\frac{p}{q}\right) = -1. \end{cases}$$

**Proof:** $G(-8pq)$ has three generic characters: $\chi_p, \chi_q$ and $\chi_{-2}$. Let $\epsilon = \left(\frac{p}{q}\right)$. The elements of exponent 2 are: $f_1 = [1,0,2pq], f_2 = [2,0,pq], f_3 = [p,0,2q]$ and $f_4 = [2p,0,q]$. Then $f_1$ and $f_2$ are in the principal genus while $f_3$ and $f_4$ are mapped by $(\chi_p, \chi_q, \chi_{-2})$ to $(\epsilon, \epsilon, 1)$. Thus if $\epsilon = 1$ then $e = 2$ and if $\epsilon = -1$ then $e = 1$. Hence 1.3 gives the result for $h_4(-8pq)$.

$G(-128pq)$ has four generic characters: $\chi_p, \chi_q, \chi_{-1}$ and $\chi_2$. The elements of exponent 2 are:

$$\begin{array}{rr} f_1 = [1, 0, 32pq] & f_2 = [4, 4, 8pq + 1] \\ f_3 = [32, 0, pq] & f_4 = [32, 32, pq + 8] \\ f_5 = [p, 0, 32q] & f_6 = [4p, 4p, p + 8q] \\ f_7 = [32p, 0, q] & f_8 = [32p, 32p, 8p + q] \end{array}$$

Computation shows that $f_1, f_2, f_3$ and $f_4$ are in the principal genus while $f_5, f_6, f_7$ and $f_8$ are mapped by $(\chi_p, \chi_q, \chi_{-1}, \chi_2)$ to $(\epsilon, \epsilon, 1, 1)$. Say $\epsilon = 1$. Then $e = 3$ and

$$h_4(-128pq) = h(-128pq)/64 = h(-8pq)/16 = h_4(-8pq).$$

When $\epsilon = -1$ then $e = 2$ and

$$h_4(-128pq) = h(-128pq)/32 = h(-8pq)/8 = h_4(-8pq),$$

which proves the result. $\square$

Sun's conjecture (8.4) states that if $p$ and $q$ are primes with $p, q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$ then

$$h_4(-4pq) = h_4(-64pq) = h(-4pq)/8.$$

Liu [4] has shown this may fail. We identify precisely when the conjecture is valid.

**Theorem 2.4.** *Let $p$ and $q$ be primes with $p, q \equiv 1 \pmod 4$ and $\left(\frac{p}{q}\right) = 1$.*

1. *If one of $p$ or $q$ is $\equiv 5 \pmod 8$ then conjecture (8.4) holds.*
2. *If $p, q \equiv 1 \pmod 8$ then*

$$2h_4(-4pq) = h_4(-64pq) = h(-4pq)/8,$$

*contrary to conjecture (8.4).*

**Proof:** $G(-4pq)$ has three generic characters: $\chi_p, \chi_q$ and $\chi_{-1}$. The elements of exponent 2 are $f_1 = [1, 0, pq]$, $f_2 = [2, 2, \frac{1}{2}(pq + 1)]$, $f_3 = [p, 0, q]$ and $f_4 = [2p, 2p, \frac{1}{2}(p + q)]$. It is easy to check that $f_1$ and $f_3$ are in the principal genus and that $f_2$ and $f_4$ lie in the same genus. We compute the values of $f_2$.

| $(p, q) \pmod 8$ | $\chi_p(f_2)$ | $\chi_q(f_2)$ | $\chi_{-1}(f_2)$ |
|---|---|---|---|
| (1,1) | 1 | 1 | 1 |
| (5,1) | -1 | 1 | -1 |
| (1,5) | 1 | -1 | -1 |
| (5,5) | -1 | -1 | 1 |

If $p, q \equiv 1 \pmod 8$ then $e = 2$ and $h_4(-4pq) = h(-4pq)/16$, proving one half of (2). If one of $p$ or $q$ is $\equiv 5 \pmod 8$ then $e = 1$ and $h_4(-4pq) = h(-4pq)/8$, proving one half of (1).

$G(-64pq)$ has four generic characters: $\chi_p, \chi_q, \chi_{-1}$ and $\chi_2$. The eight elements of exponent 2 are listed below. One can check that $\chi_p, \chi_q$ and $\chi_{-1}$ send each of them to 1. We give the values of $\chi_2$ for each possible pair of $(p, q) \pmod 8$.

| | (1,1) | (5,1) | (1,5) | (5,5) |
|---|---|---|---|---|
| $[1, 0, 16pq]$ | 1 | 1 | 1 | 1 |
| $[4, 4, 4pq_1]$ | -1 | -1 | -1 | -1 |
| $[16, 0, pq]$ | 1 | -1 | -1 | 1 |
| $[16, 16, pq + 4]$ | -1 | 1 | 1 | -1 |
| $[p, 0, 16q]$ | 1 | -1 | 1 | -1 |
| $[4p, 4p, p + 4q]$ | -1 | 1 | -1 | 1 |
| $[16p, 0, q]$ | 1 | 1 | -1 | -1 |
| $[16p, 16p, 4p + q]$ | -1 | -1 | 1 | 1 |

In each case, there are four elements of exponent 2 in the principal genus. So $e = 2$ and

$$h_4(-64pq) = h(-64pq)/32 = h(-4pq)/8,$$

which completes the proof of (1) and (2). $\square$

The proof of Conjecture (8.6) follows a different path. We use the composition on different orders described in Section 7.3 of [1]. Given a discriminant

$\Delta$, let $I(\Delta)$ denote the identity of $G(\Delta)$. The map:

$$\begin{aligned} \psi : G(n^2\Delta) &\rightarrow G(\Delta) \\ \psi([g]) &= [I(\Delta) \circ g], \end{aligned}$$

is a homomorphism by [1] Theorem 7.9. Buell's proof shows that $\psi$ is in fact surjective. Namely, let $[f] \in G(\Delta)$. We can find $(a, b, c) \in [f]$ with $(a, n) = 1$. Then $g = (a, nb, n^2c)$ is primitive of discriminant $n^2\Delta$ and $I(\Delta) \circ g = (a, b, c)$.

**Theorem 2.5.** *Let $d > 2$ be square-free. If $h_4(-64d)$ is odd then $h_4(-64d) = h_4(-4d)$.*

**Proof:** The hypothesis means that $G(-64d)$ has no elements of order $2^k$, $k \geq 3$. Then $G(-4d)$ also has no elements of order $2^k$, $k \geq 3$. Namely, suppose $[f] \in G(-4d)$ has order $2^k$, $k \geq 3$. Consider $\psi : G(16(-4d)) \rightarrow G(-4d)$ and say $\psi([g]) = [f]$. Now the order of $[g]$ is $2^s r$ for some odd $r$ and $0 \leq s \leq 2$. Then $[f]^4 = \psi([g]^4)$ has order dividing $r$ and $2^k$ and so $[f]^4 = 1$, a contradiction.

Let $|G(-4d)| = 2^t m$ with $m$ odd. Then $|G(-64d)| = 2^{t+2}m$. We can write

$$\begin{aligned} G(-64d) &= C(2)^a \times C(4)^b \times H \\ G(-4d) &= C(2)^{a'} \times C(4)^{b'} \times H', \end{aligned}$$

where $|H| = m = |H'|$. Then $G(-64d)^4 = H$ and $G(-4d)^4 = H'$ so that $h_4(-64d) = m = h_4(-4d)$. $\square$

We note that $G(\Delta)/G(\Delta)^4 \cong S$, the spinor genera group (see [3]), and so the results here can be viewed as results on the order of certain spinor genera groups.

# References


[1] D. A. Buell, Binary Quadratic Forms.Springer, New York, 1989.

[2] H. Cohn, Advanced Number Theory. Dover, New York,1962.

[3] D. Estes and G. Pall, Spinor genera of binary quadratic forms. J. Number Theory 5 (1973) 421–432.

[4] L. Liu, Counterexamples to a conjecture concerning class number of binary quadratic forms, Sci. Magna 2 (2006) 108–110.

[5] Z. H. Sun, Supplements to the theory of quartic residues, Acta Arith. 97 (2001) 361–377.

[6] Z. H. Sun, Quartic residues and binary quadratic forms, J. Number Theory 113 (2005) 10–52.