ACTA ARITHMETICA
191.4 (2019)

# Some congruences connecting quadratic class numbers with continued fractions

by

Weidong Cheng (Nanjing and Chongqing) and Xuejun Guo (Nanjing)

**1. Introduction.** In what follows, $p$ always stands for a positive prime number. Let $h(-p)$ and $h(p)$ be the ideal class numbers of the quadratic number fields $\mathbb{Q}(\sqrt{-p})$ and $\mathbb{Q}(\sqrt{p})$ respectively. It is of interest to study the relationships between $h(-p)$ and $h(p)$ modulo the powers of 2. Many results on this topic are already known. For example, if $p \equiv 3 \pmod 4$ is prime then $h(-p)$ and $h(p)$ are odd (see [1, p. 413] and [2, p. 100, §3]). More recently, motivated by a conjecture of Richard Guy, Lynn Chua, Benjamin Gunby, Soohyun Park and Allen Yuan [3] proved a congruence connecting $h(p)$ and $h(-p)$ with continued fractions modulo 16. Specifically, suppose that $\sqrt{p}$ has the negative continued fraction expansion

$$\sqrt{p} = b_0 - \cfrac{1}{b_1 - \cfrac{1}{b_2 - \ddots}}, \tag{1.1}$$

where $b_i \geq 2$ are integers for $i \geq 1$, and $b_0$ is an arbitrary integer. The sequence $\{b_i\}_{i\in\mathbb{N}}$ is periodic from $b_1$ on; let $b_1, \ldots, b_r$ be its minimal period. Define

$$m(p) := \frac{1}{3}\sum_{i=1}^{r}(b_i - 3). \tag{1.2}$$

(For a more general definition, see Definition 2.3.) In [3], the authors mainly proved the following theorem.

2010 *Mathematics Subject Classification*: Primary 11R29; Secondary 11A55, 11F20.
*Key words and phrases*: ideal class numbers, quadratic fields, continued fractions, Hirzebruch sums, Dedekind sums.
Received 23 October 2016; revised 21 March 2019.
Published online 7 October 2019.

DOI: 10.4064/aa8640-4-2019

Theorem 1.1 (Chua, Gundy, Park and Yuan [3, Theorem 1.3]). *If* $p \equiv 3 \pmod 4$, *then*

$$h(-p) \equiv h(p)m(p) \pmod{2^4}. \tag{1.3}$$

To prove Theorem 1.1, the authors used a significant result obtained by Hirzebruch [11, p. 241] and Zagier [24, 25] relating imaginary quadratic class numbers to continued fractions that will be stated in Section 2.3. Note that the congruence (1.3) does not hold modulo $2^5$: for example, if $p = 79$, then $h(-79) = 5, h(79) = 3$, $m(79) = 7$ and $h(79)m(479) - h(-79) = 2^4$.

We are going to study the same problem for $p \equiv 1 \pmod 4$. Note that Zagier's result does not work in that case. Fortunately, Hongwen Lu generalized Zagier's formula in the 1990s (see for example [14, 15, 17]), which enables us to prove some congruences between $h(p)$ and $h(-p)$ modulo powers of 2 by applying similar techniques to those in [3].

The main results of this paper are the following.

Main Theorem 1.2. *If* $p \equiv 1 \pmod 8$, *then*

$$h(-p) \equiv h(p)m(4p) \pmod{2^3}, \tag{1.4}$$

*where $m(4p)$ is an integer depending on the minimal period of the negative regular continued fraction expansion of $\sqrt{4p}$ as in Definition* 2.3.

Main Theorem 1.3. *Let* $p \equiv 5 \pmod 8$, *and suppose that* $\epsilon = (t+u\sqrt{p})/2 > 1$ *is the* (*unique*) *fundamental unit of* $\mathbb{Q}(\sqrt{p})$ *such that* $t \equiv u \equiv 0 \pmod 2$. *Then*

$$h(-p) \equiv h(p)m(4p) \pmod{2^2}, \tag{1.5}$$

*where $m(4p)$ is as above.*

According to Table 2 in Appendix, if $p = 37$, then $h(-37) = 2, h(37) = 1$, $m(4{\cdot}37) = 6$ and $h(37)m(4{\cdot}37) - h(-37) = 2^2$. This implies that the modulus $2^2$ in (1.5) is optimal.

The organization of this paper is the following. In Section 2, we give some preliminaries on continued fractions, Hirzebruch sums and Dedekind sums, and also include an overview of the results of Don Zagier and Hongwen Lu to make our exposition self-contained. In Section 3, we show some lemmas, and then our main Theorems 1.2 and 1.3 are proved.

## 2. Preliminaries

**2.1. Continued fractions and Hirzebruch sums.** For the basics about continued fraction expansions of real numbers, we refer to Hardy and Wright [9, Chapter X] and Lu [15, Chapter 1]. For any $\alpha \in \mathbb{R}$, the *regular* *continued fraction expansion* of $\alpha$ is the expression

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}},$$

where $a_i \geq 1$ are integers for $i \geq 1$, and $a_0$ is an arbitrary integer. We then write $\alpha = [a_0; a_1, a_2, \ldots]$.

Similarly, for any $\alpha \in \mathbb{R}$, the *negative continued fraction expansion* of $\alpha$ is the expression

$$\alpha = b_0 - \cfrac{1}{b_1 - \cfrac{1}{b_2 - \ddots}}$$

where $b_i \geq 2$ are integers for $i \geq 1$, and $b_0$ is an arbitrary integer. We then write $\alpha = [[b_0; b_1, b_2, \ldots]]$. Recall that we have used this kind of continued fraction expansion to define $m(p)$ in (1.2).

For irrational numbers, the transformation formula between the above two kinds of continued fraction expansions is given below.

PROPOSITION 2.1 (Zagier [24, pp. 177–178], or Lu [15, pp. 15–16, Lemma 1.8], or Eustis [6]). *Let $\theta \in \mathbb{R} \setminus \mathbb{Q}$. If $\theta = [a_0; a_1, a_2, \ldots]$, then $\theta = [[a_0 + 1; \tau^{a_1-1}, a_2+2, \tau^{a_3-1}, a_4, \tau^{a_5-1}, a_6+2, \ldots]]$, where $\tau^n$ denotes $2, \ldots, 2$ ($n$ times) for $0 \leq n \in \mathbb{Z}$.*

DEFINITION 2.2. A continued fraction with elements $\{a_i\}_{i\geq 0}$ is said to be *periodic* if there exist $k$ and $L$ such that $a_l = a_{l+k}$ for $l \geq L$. If $k$ and $L$ are minimal possible, then we call $a_L, \ldots, a_{L+k-1}$ the *minimal period*, and the corresponding continued fraction is written as

$$[a_0; a_1, \ldots, a_{L-1}, \overline{a_L, \ldots, a_{L+k-1}}] \quad \text{or} \quad [[a_0; a_1, \ldots, a_{L-1}, \overline{a_L, \ldots, a_{L+k-1}}]].$$

A *quadratic surd* is an irrational root of a quadratic equation with integeral coefficients. It is well-known that each irrational number has a unique infinite continued fraction expansion. And the Euler–Lagrange theorem [9, §10.12] says that for any irrational number $\alpha$, the continued fraction expansion of $\alpha$ is eventually periodic if and only if $\alpha$ is a quadratic surd.

DEFINITION 2.3 (Lu [15, p. 154] and Chua, Gundy, Park and Yuan [3, p. 1346, (1.2)]). Let $\alpha$ be a quadratic surd with regular continued fraction expansion $\alpha = [\hat{a}_0; \hat{a}_1, \ldots, \hat{a}_s, \overline{a_1, \ldots, a_k}]$, where $\overline{a_1, \ldots, a_k}$ is the minimal period. Define

$$\Psi(\alpha) := \begin{cases} \sum_{i=1}^{k} (-1)^{i+s} a_i & \text{if } k \text{ is even,} \\ 0 & \text{if } k \text{ is odd.} \end{cases}$$

We call $\Psi(\alpha)$ the *Hirzebruch sum* of $\alpha$. Similarly, suppose that $\alpha$ has the negative continued fraction expansion $\alpha = [[\hat{b}_0; \hat{b}_1, \dots, \hat{b}_t, \overline{b_1, \dots, b_l}]]$, where $\overline{b_1, \dots, b_l}$ is the minimal period. Define

$$m(\alpha^2) := \frac{1}{3}\sum_{j=1}^{l}(b_j - 3).$$

The relationship between $\Psi(*)$ and $m(*)$ is the following.

Proposition 2.4. *If $\alpha$ is a quadratic surd, then $\Psi(\alpha) = 3m(\alpha^2)$.*

*Proof.* Let $\alpha = [a_0; a_1, \dots, a_s, \overline{a_{s+1}, \dots, a_{s+k}}]$, where $\overline{a_{s+1}, \dots, a_{s+k}}$ is the minimal period. On the one hand, from Definition 2.3 we have

$$\Psi(\alpha) = \begin{cases} (-1)^{s+1}[(a_{s+1} + a_{s+3} + \dots + a_{s+k-1}) - (a_{s+2} + a_{s+4} + \dots + a_{s+k})] & \text{if } k \text{ is even,} \\ 0 \quad \text{if } k \text{ is odd.} \end{cases}$$

On the other hand, according to Proposition 2.1, $\alpha = [[a_0 + 1; \tau^{a_1 - 1}, a_2 + 2, \tau^{a_3 - 1}, a_4 + 2, \dots]]$.

We distinguish four cases:

(1) For $s \equiv 0 \pmod 2$ and $k \equiv 0 \pmod 2$, since $a_s \neq a_{s+k}$ implies $a_s + 2 \neq a_{s+k} + 2$, we have $\alpha = [[a_0 + 1; \tau^{a_1 - 1}, a_2 + 2, \tau^{a_3 - 1}, a_4 + 2, \dots, \tau^{a_{s-1} - 1}, a_s + 2, \overline{\tau^{a_{s+1} - 1}, a_{s+2} + 2, \dots, \tau^{a_{s+k-1} - 1}, a_{s+k} + 2}]]$. Therefore, Definition 2.3 gives

$$\begin{aligned} m(\alpha^2) &= \tfrac{1}{3}[-(a_{s+1} - 1) - (a_{s+3} - 1) - \dots - (a_{s+k-1} - 1) \\ &\qquad + (a_{s+2} - 1) + (a_{s+4} - 1) + \dots + (a_{s+k} - 1)] \\ &= \tfrac{1}{3}(-1)^{s+1}[(a_{s+1} + a_{s+3} + \dots + a_{s+k-1}) - (a_{s+2} + a_{s+4} + \dots + a_{s+k})] \\ &= \tfrac{1}{3}\Psi(\alpha). \end{aligned}$$

Here we have used the fact that $(-1)^{s+1} = -1$.

(2) For $s \equiv 1 \pmod 2$ and $k \equiv 0 \pmod 2$, if $a_s \leq a_{s+k}$ then $\alpha = [[a_0 + 1; \tau^{a_1 - 1}, a_2 + 2, \tau^{a_3 - 1}, a_4 + 2, \dots, a_{s-1} + 2, \overline{\tau^{a_s - 1}, a_{s+1} + 2, \tau^{a_{s+2} - 1}, \dots, a_{s+k-1} + 2, \tau^{a_{s+k} - a_s - 2}}]]$. It follows that

$$\begin{aligned} m(\alpha^2) &= \tfrac{1}{3}[-(a_s - 1) - (a_{s+2} - 1) - (a_{s+4} - 1) - \dots - (a_{s+k-2} - 1) \\ &\qquad - (a_{s+k} - a_s - 2) + (a_{s+1} - 1) + (a_{s+3} - 1) + \dots + (a_{s+k-1} - 1)] \\ &= \tfrac{1}{3}[(a_{s+1} + a_{s+3} + \dots + a_{s+k-1}) - (a_{s+2} + a_{s+4} + \dots + a_{s+k})] \\ &= \tfrac{1}{3}(-1)^{s+1}[(a_{s+1} + a_{s+3} + \dots + a_{s+k-1}) - (a_{s+2} + a_{s+4} + \dots + a_{s+k})] \\ &= \tfrac{1}{3}\Psi(\alpha). \end{aligned}$$

Here we have used the fact that $(-1)^{s+1} = 1$.

Similarly, if $a_s > a_{s+k}$ then $\alpha = [[a_0+1; \tau^{a_1-1}, a_2+2, \tau^{a_3-1}, a_4+2, \dots, a_{s-1}+2, \tau^{a_s-a_{s+k}}, \overline{\tau^{a_{s+k}-1}, a_{s+1}+2, \tau^{a_{s+2}-1}, \dots, a_{s+k-1}+2}]]$. Hence

$$\begin{aligned} m(\alpha^2) &= \tfrac{1}{3}[-(a_{s+k}-1)-(a_{s+2}-1)-(a_{s+4}-1)-\cdots-(a_{s+k-2}-1) \\ &\qquad +(a_{s+1}-1)+(a_{s+3}-1)+\cdots+(a_{s+k-1}-1)] \\ &= \tfrac{1}{3}[(a_{s+1}+a_{s+3}+\cdots+a_{s+k-1})-(a_{s+2}+a_{s+4}+\cdots+a_{s+k})] \\ &= \tfrac{1}{3}\Psi(\alpha). \end{aligned}$$

(3) For $s \equiv 0 \pmod 2$ and $k \equiv 1 \pmod 2$, we have $\alpha = [[a_0+1; \tau^{a_1-1}, a_2+2, \tau^{a_3-1}, a_4+2, \dots, \tau^{a_{s-1}-1}, a_s+2, \overline{\tau^{a_{s+1}-1}, a_{s+2}+2, \dots, a_{s+k-1}+2, \tau^{a_{s+k}-1}, a_{s+1}+2, \tau^{a_{s+2}-1}, \dots, \tau^{a_{s+k-1}-1}, a_{s+k}+2}]]$. Hence

$$\begin{aligned} m(\alpha^2) &= \tfrac{1}{3}[-(a_{s+1}-1)-(a_{s+3}-1)-\cdots-(a_{s+k}-1)-(a_{s+2}-1) \\ &\qquad -(a_{s+4}-1)-\cdots-(a_{s+k-1}-1)+(a_{s+2}-1)+(a_{s+4}-1)+\cdots \\ &\qquad +(a_{s+k-1}-1)+(a_{s+1}-1)+(a_{s+3}-1)+\cdots+(a_{s+k}-1)] \\ &= 0 = \tfrac{1}{3}\Psi(\alpha). \end{aligned}$$

(4) For $s \equiv 1 \pmod 2$ and $k \equiv 1 \pmod 2$, similarly to (2), if $a_s \le a_{s+k}$ then $\alpha = [[a_0+1; \tau^{a_1-1}, a_2+2, \tau^{a_3-1}, a_4+2, \dots, a_{s-1}+2, \overline{\tau^{a_s-1}, a_{s+1}+2, \tau^{a_{s+2}-1}, \dots, \tau^{a_{s+k-1}-1}, a_{s+k}+2, \tau^{a_{s+1}-1}, a_{s+2}+2, \dots, a_{s+k-1}+2, \tau^{a_{s+k}-a_s-2}}]]$; and if $a_s > a_{s+k}$ then $\alpha = [[a_0+1; \tau^{a_1-1}, a_2+2, \tau^{a_3-1}, a_4+2, \dots, a_{s-1}+2, \tau^{a_s-a_{s+k}}, \overline{\tau^{a_{s+k}-1}, a_{s+1}+2, \tau^{a_{s+2}-1}, \dots, \tau^{a_{s+k-1}-1}, a_{s+k}+2, \tau^{a_{s+1}-1}, a_{s+2}+2, \dots, a_{s+k-1}+2}]]$. As in (3), in both cases, we have $m(\alpha^2) = 0 = \frac{1}{3}\Psi(\alpha)$. ∎

In what follows, we follow the notation of [15], and use $\Psi(*)$ instead of $m(*)$ through our proof in Section 3.

Now we list some important properties of Hirzebruch sums of real quadratic surds.

Proposition 2.5. *Let $\alpha$ be a real quadratic surd and $n \in \mathbb{Z}$. Then*

$$\Psi(\alpha \pm n) = \Psi(\alpha).$$

*Proof.* This follows immediately from the definitions of regular continued fraction expansion and Hirzebruch sums. ∎

Proposition 2.6. *Let $a, b, c$ be rational integers such that $|b| \le a \le -c$, $\gcd(a,b,c) = 1$ and $d = b^2 - 4ac$ is not a perfect square. If the fundamental unit of $\mathbb{Q}(\sqrt{d})$ has norm $-1$, then $\Psi\big(\frac{b+\sqrt{d}}{2a}\big) = 0$.*

*Proof.* This follows easily from [15, Chapter 1, p. 47, Lemma 2.4]. Actually, from [15] we see that if the fundamental unit of $\mathbb{Q}(\sqrt{d})$ has norm $-1$ then the length of the minimal period of the regular continued fraction expansion of $\frac{b+\sqrt{d}}{2a}$ must be odd. This implies that $\Psi\big(\frac{b+\sqrt{d}}{2a}\big) = 0$. ∎

Proposition 2.7. *For any real quadratic surd $\alpha = (u+\sqrt{v})/w$, where $u, v, w$ are integers such that $w \neq 0$ and $v > 0$, let $\alpha' := (u-\sqrt{v})/w$ denote the algebraic conjugate of $\alpha$. Then $\Psi(\alpha) = \Psi(-\alpha')$.*

*Proof.* This follows easily from Herzog [10, Theorem 1] and Perron [19, p. 56, lines 2, 3]. In fact, we only need to verify each of the 28 cases in [10, Theorem 1, Table I]. The details are omitted. ■

**2.2. Dedekind sums.** For the basics about Dedekind sums, we refer to Rademacher and Grosswald's book [20].

Definition 2.8 ([20, p. 1]). The *Dedekind sums* are denoted by $s(h,k)$ and defined as follows: Let $h, k$ be integers with $\gcd(h,k) = 1$ and $k \geq 1$; then

$$s(h,k) := \sum_{n=1}^{k} \left(\left(\frac{hn}{k}\right)\right)\left(\left(\frac{n}{k}\right)\right),$$

where

$$((x)) := \begin{cases} x - [x] - 1/2 & \text{if } x \notin \mathbb{Z}, \\ 0 & \text{if } x \in \mathbb{Z}. \end{cases}$$

Here $[x]$ denotes the greatest integer not exceeding $x$.

The following propositions on Dedekind sums will be used in our proof.

Proposition 2.9 (Zagier [25, p. 83, i), line 7]). *Let $h, k$ be coprime integers with $k \geq 1$. Then*

$$s(h,k) = s(h \pm k, k).$$

Proposition 2.10 (Reciprocity Theorem, [20, p. 4, Theorem 1]). *Let $h, k$ be coprime integers with $k \geq 1$. Then*

$$s(h,k) + s(k,h) = -\frac{1}{4} + \frac{1}{12}\left(\frac{h}{k} + \frac{1}{hk} + \frac{k}{h}\right).$$

Proposition 2.11 ([20, p. 38, Theorem 4]). *Let $d, c$ be coprime integers with $c \geq 1$ odd. Then*

$$\left(\frac{d}{c}\right) = (-1)^{\frac{1}{2}(\frac{c-1}{2} - 6cs(d,c))}.$$

**2.3. Overview of Zagier's work.** In this subsection, we describe some of the main ideas of Zagier's work [25], which will be used in Section 3 frequently (see also [3, Section 2.2]).

A matrix $A \in \mathrm{SL}(2,\mathbb{Z})$ is called *hyperbolic* if $|\mathrm{Tr}(A)| > 2$, where Tr denotes trace. From [25, §III, p. 86], there exists a one-to-one correspondence

$$A \leftrightarrow (M, V) \tag{2.1}$$

between conjugacy classes of hyperbolic matrices $A \in \mathrm{SL}(2,\mathbb{Z})$ and equivalence classes of pairs $(M, V)$, where $M$ is a free $\mathbb{Z}$-module of rank 2 in a real quadratic field $K$, and $V$ is an abelian group of rank 1 generated by a totally positive unit $\varepsilon \in K$ such that $\varepsilon M = M$. Two pairs $(M, V)$ and $(M', V')$ are *equivalent* if $M' = \alpha M$ for some $\alpha \neq 0$ in $K$ and $V' = V$.

Namely, suppose $(M, V)$ is such a pair, and $\{\beta_1, \beta_2\}$ is an oriented basis of $M$ (i.e., $\beta_2 > 0$ and $\beta_1\beta_2' - \beta_1'\beta_2 > 0$, where $\beta_i'$ denotes the algebraic conjugate of $\beta_i$ for $i = 1, 2$). Let $\varepsilon > 1$ be a generator of $V$. Noting that $\varepsilon M = M$, we consider the linear transformation of multiplying by $\varepsilon$ on $M$, and write

$$\varepsilon\beta_1 = a\beta_1 + b\beta_2, \qquad \varepsilon\beta_2 = c\beta_1 + d\beta_2. \tag{2.2}$$

This gives a hyperbolic matrix $A := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$. Conversely, given a hyperbolic matrix $A \in \mathrm{SL}(2,\mathbb{Z})$, let $w$ and $w'$ be the roots of $A \cdot x = x$ such that $w > w'$, where $A \cdot x$ denotes the corresponding linear fractional transformation on $\mathbb{C}$. We choose $\beta_1 = w$, $\beta_2 = 1$, so $M$ is the module generated by $w$ and 1. Let $\varepsilon > 1 > \varepsilon' > 0$ be the eigenvalues of $A$, and choose $V$ to be generated by $\varepsilon$.

Each hyperbolic matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with $c > 0$ is conjugate in $\mathrm{SL}(2,\mathbb{Z})$ to a product of the form

$$\begin{pmatrix} b_1 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} b_2 & -1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} b_r & -1 \\ 1 & 0 \end{pmatrix} \tag{2.3}$$

with $b_1, \dots, b_r \in \mathbb{Z}$, $b_i \geq 2$ and at least one $b_i > 2$ (see [25, §V, pp. 91–92]). Furthermore, $r$ is unique and $b_1, \dots, b_r$ are unique up to a cyclic permutation. We call $(b_1, \dots, b_r)$ the *cycle* associated with the matrix $A$. To find these $b_i$, let $w$ be the larger solution to the equation $A \cdot x = x$, and suppose the negative continued fraction expansion of $w$ is

$$w = c_0 - \cfrac{1}{c_1 - \cfrac{1}{c_2 - \ddots}} \qquad (c_i \geq 2 \text{ for } i \geq 1). \tag{2.4}$$

The sequence $\{c_i\}_{i \in \mathbb{N}}$ will be periodic from a certain index $i_0$ on, and the cycle $(b_1, \dots, b_r)$ of $A$ is just the period of this sequence, i.e., $(b_1, \dots, b_r)$ is either the minimal period in (2.4) or $\kappa$ times the minimal period, depending on whether in the pair $(M, V)$ corresponding to $A$ the group $V$ coincides with the group of all totally positive units leaving $M$ invariant or is a subgroup of index $\kappa$ of that group.

By Dedekind's theorem [25, p. 83, Théorème], given $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{Z})$ with $c > 0$, we define an integer

$$n_A := \frac{a+d}{c} - 3 - 12s(d,c), \tag{2.5}$$

where $s(d,c)$ is the Dedekind sum defined in Definition 2.8. Note that $n_A$ was originally defined by taking the logarithm of $\Delta(A\cdot z)$, where $\Delta$ is the well-known cusp form of weight 12 on $\mathrm{SL}(2,\mathbb{Z})$. It is easy to see that $n_A$ depends only on the conjugacy class of $A$, i.e., $n_{BAB^{-1}} = n_A$ for any $A, B \in \mathrm{SL}(2,\mathbb{Z})$. If a hyperbolic matrix $A$ is written as a product (2.3), then [25, p. 90, Lemme] says that

$$n_A = \sum_{i=1}^{r} (b_i - 3). \tag{2.6}$$

By Definition 2.3 and Proposition 2.4, this is equivalent to

$$n_A = 3\kappa m(w^2) = \kappa\Psi(w), \tag{2.7}$$

where $\kappa$ is an index depending on the choice of $V$ as in the previous paragraph. In our later proof, $\kappa = 1$ always holds (see the remark at the end of this subsection).

The above analysis makes it possible to calculate $n_A$ through continuous fractions. Actually, combining this fact with the theorems of Meyer (see [18] or [25, pp. 86–87]), one can obtain remarkable identities expressing class numbers in terms of continuous fractions. For example, Zagier [24, 25] proved that if $p > 3$ is a prime congruent to 3 modulo 4, then

$$h(-p) = \frac{1}{3}\sum_{I\in C} \chi(I)n(I), \tag{2.8}$$

where $C$ is a complete set of representatives of the narrow ideal classes of $\mathbb{Q}(\sqrt{p})$, $\chi$ is the genus character [22, pp. 60–61], and $n(I) = n_A$ with $A$ the matrix corresponding to the action of the fundamental unit of $\mathbb{Q}(\sqrt{p})$ on a basis of $I$. Note that $\chi(I)n(I)$ is independent of the choice of $I \in C$. In particular, if $h(p) = 1$ in (2.8), then (2.7) gives

$$h(-p) = m(p). \tag{2.9}$$

This formula can also be found in [11, p. 241, Proposition].

Remark. We will generally let $K = \mathbb{Q}(\sqrt{p})$, $M$ will be some free $\mathbb{Z}$-module of rank 2 in the ring $\mathcal{O}_K$ of integers, and $V$ will be the full group of all totally positive units in $\mathcal{O}_K$ which leave $M$ invariant. This gives $\kappa = 1$ in (2.8). Actually, one can choose $V = \{\epsilon_+^n \mid n \in \mathbb{Z}\}$, where $\epsilon_+$ is a totally positive fundamental unit in $K$. Thus we obtain a well-defined pair $(M, V)$. Under the correspondence (2.1), one has to consider the linear transformation of multiplying by $\epsilon_+$ on the generators of $M$ as in (2.2), which gives rise to a hyperbolic matrix in $\mathrm{SL}(2,\mathbb{Z})$. Furthermore, an analogue of (2.8) will be stated in the next subsection; then the correspondence (2.1) and formula

(2.7) show how to write the Hirzebruch sums there in terms of Dedekind sums.

**2.4. Lu's theorem.** Let $d > 1$ be a fundamental discriminant and $\mathcal{O}_K$ the ring of integers of $K = \mathbb{Q}(\sqrt{d})$. For any $\alpha_1, \alpha_2 \in \mathcal{O}_K$, we denote by $[\alpha_1, \alpha_2]$ the free $\mathbb{Z}$-module of rank 2 generated by $\alpha_1$ and $\alpha_2$, say $\alpha_1\mathbb{Z} \oplus \alpha_2\mathbb{Z}$, and by $\mathrm{Cl}(K)$ the ideal class group of $K$. The elements in $\mathrm{Cl}(K)$ are called *ideal classes.* Throughout, we let id be the identity in $\mathrm{Cl}(K)$, and use capital fraktur letters to denote ideal classes in $\mathrm{Cl}(K)$, e.g., $\mathfrak{A}, \mathfrak{I}$. For any $\mathfrak{I} \in \mathrm{Cl}(K)$, one can always choose an integral ideal $I = [a, (-b + \sqrt{d})/2] \in \mathfrak{I}$, where $0 < a \in \mathbb{Z}$, $b \in \mathbb{Z}$, and there exists a $c \in \mathbb{Z}$ such that $d = b^2 - 4ac$, $\gcd(a, b, c) = 1$, and either $|b| < a \le -c$ or $b = a \le -c$. Actually $a$ can be taken to be the minimal positive integer in $\mathfrak{I}$, and $a, b$ are uniquely determined by $\mathfrak{I}$ (see for example, [15, p. 139], or [4, Chapter 5, §5.2 and §5.6]). All the $I$ chosen in this way form a complete set of representatives of ideal classes in $\mathbb{Q}(\sqrt{d})$.

In [15, Chapter 6], Lu gave a new proof for the class number formula of Hirzebruch and Zagier [24, p. 782, (9.6)]. Moreover, Lu proved three more analogous class number formulas connecting the class numbers of imaginary quadratic fields with Hirzebruch sums $\Psi(*)$. Here we list one of those formulas, which is essential to our proof in Section 3.

Theorem 2.12 (Lu [15, pp. 348–349, Theorem 3.3]). *Let both $d > 1$ and $-k < -1$ be the fundamental discriminants such that $4 \,\|\, k$ and $\gcd(d, k) = 1$, and let $K = \mathbb{Q}(\sqrt{d})$. Then*

$$24\delta_d J h(-k)h(-dk) = w_{-k}w_{-kd} \sum_{\substack{\mathfrak{I}\in\mathrm{Cl}(K)\\ I=[a,(-b+\sqrt{d})/2]\in\mathfrak{I}}} (S_1(I) + S_2(I)),$$

*where*

$$S_1(I) = \sum_{\substack{4nu=k\\ n,u\ge1}} \chi_u(a) \sum_{m \,(\mathrm{mod}\, 4n)} \chi_{4n}(am^2 + bm + c)\Psi\biggl(\frac{u}{4n}\biggl(m + \frac{b+\sqrt{d}}{2a}\biggr)\biggr),$$

$$\begin{aligned} S_2(I) = \sum_{\substack{4nu=k\\ n,u\ge1}} \chi_{4u}(a) \sum_{m \,(\mathrm{mod}\, n)} \chi_n(am^2 + bm + c)\biggl(\eta\Psi\biggl(\frac{u}{n}\biggl(m + \frac{b+\sqrt{d}}{2a}\biggr)\biggr) \\ - 3\Psi\biggl(\frac{2u}{n}\biggl(m + \frac{b+\sqrt{d}}{2a}\biggr)\biggr) + 2\Psi\biggl(\frac{4u}{n}\biggl(m + \frac{b+\sqrt{d}}{2a}\biggr)\biggr)\biggr).\end{aligned}$$

*Here $I = [a, (-b+\sqrt{d})/2] \in \mathfrak{I}$ is such that $a, b, c$ are integers satisfying $a > 0$, $d = b^2 - 4ac$, $\gcd(a, b, c) = 1$ and either $|b| < a \le -c$ or $b = a \le -c$; such $I$ runs through a complete set of representatives of ideal classes in $\mathrm{Cl}(K)$. Moreover, $\epsilon$ (resp. $\epsilon_+$) is the fundamental unit (resp. totally positive fundamental unit) of $K$; $\delta_d$ is the exponent given by $\epsilon_+ = \epsilon^{\delta_d}$; $J$ (resp. $J'$) is a* *positive integer such that* $\epsilon_+^J$ *(resp.* $\epsilon_+^{J'}$*) corresponds to the least solution of Pell's equation* $x^2 - dk^2y^2 = 4$ *(resp.* $x^2 - d(k/4)^2y^2 = 4$*) in integers;* $w_{-D}$ *is the number of roots of unity in* $\mathbb{Q}(\sqrt{-D})$*;*

$$\eta = \frac{J}{J'} = \begin{cases} 1 & \textit{if } d \equiv 1 \pmod 8, \\ 1 \textit{ or } 3 & \textit{if } d \equiv 5 \pmod 8; \end{cases}$$

$\chi_u$ *and* $\chi_n$ *are real primitive characters modulo* $u$ *and* $n$ *respectively; and finally* $\Psi(*)$ *is a Hirzebruch sum.*

Theorem 2.12 can be proved by applying the Kronecker limit formula for real quadratic number fields with respect to the $L$-functions defined by

$$\tilde{L}(s,\chi,I) := \sum_{\lambda \in I/\epsilon_+,\, \lambda \gg 0} \frac{\chi(N(\lambda)/N(I))}{(N(\lambda)/N(I))^s}, \quad \mathrm{Re}(s) > 1, \tag{2.10}$$

and

$$\tilde{L}(s,\chi) := \sum_{I} \tilde{L}(s,\chi,I), \quad \mathrm{Re}(s) > 1, \tag{2.11}$$

where $I = [a, (-b+\sqrt{d})/2]$ is an integral ideal as above, and it runs over a complete set of representatives of the ideal class group (in a narrower sense) of $K$ in (2.11); $\chi$ is a Dirichlet character; $\lambda$ runs over all algebraic integers in $I$, and $\lambda \gg 0$ means that $\lambda$ is totally positive; and $N(*)$ denotes the norm over $\mathbb{Q}$. Such Kronecker limit formulas were studied by Lu and his students in the 1980s–1990s: see for example [13, 17, 16] and [15, Chapter 3].

For the complete proof of the above theorem, we refer the reader to [15, pp. 358–367, Chapter 6, Section 3.4]. Two references in English are [17, p. 1413, Theorem 8] and [14, p. 1146, Theorem 2], but there are some differences in formulas appearing in those earlier references.

## 3. Proofs of main results

**3.1. Some lemmas.** In this subsection, we give some lemmas which will be essential to the proof of Theorems 1.2 and 1.3.

Lemma 3.1. *Let* $p \equiv 1 \pmod 4$ *and* $K = \mathbb{Q}(\sqrt{p})$*. Suppose one of the following conditions is satisfied:*

(1) $p \equiv 1 \pmod 8$*;*

(2) $p \equiv 5 \pmod 8$*, and the fundamental unit of* $K$*, say* $\epsilon := (t+u\sqrt{p})/2 > 1$*, satisfies* $t \equiv u \equiv 0 \pmod 2$*.*

*Then*

$$h(-p) = \frac{1}{6} \sum_{\substack{\mathfrak{I} \in \mathrm{Cl}(K) \\ I = [a, (-b+\sqrt{p})/2] \in \mathfrak{I}}} \left(S_1(I) + S_2(I)\right), \tag{3.1}$$

*where*

$$\begin{aligned} S_1(I) &= \chi_4(c)\biggl(\varPsi\biggl(\frac{b+\sqrt{p}}{8a}\biggr)-\varPsi\biggl(\frac{4a+b+\sqrt{p}}{8a}\biggr)\biggr)\\ &\quad+\chi_4(a+b+c)\biggl(\varPsi\biggl(\frac{2a+b+\sqrt{p}}{8a}\biggr)-\varPsi\biggl(\frac{-2a+b+\sqrt{p}}{8a}\biggr)\biggr),\\ S_2(I) &= \chi_4(a)\biggl(-3\varPsi\biggl(\frac{b+\sqrt{p}}{a}\biggr)+2\varPsi\biggl(\frac{2b+2\sqrt{p}}{a}\biggr)\biggr), \end{aligned}$$

*where the notations are as in Theorem* 2.12.

*Proof.* This is a special case of Theorem 2.12. In fact, if we take $k=4$, $d=p$ in Theorem 2.12, then $h(-k)=1$, $h(-dk)=h(-p)$, $w_{-k}=4$ and $w_{-kd}=2$.

Under the assumptions (1) and (2), the fundamental unit of $\mathbb{Q}(\sqrt{p})$ has norm $-1$ (see for example [8, p. 182, Corollary 2]), which implies $\delta_d=2$, $J=J'=1$, and thus $\eta=1$ in Theorem 2.12 by [7, p. 120, Lemma 11].

Note that the real primitive character $\chi_4$ is defined by $\chi_4(\overline{0})=\chi_4(\overline{2})=0$, $\chi_4(\overline{1})=1, \chi_4(\overline{3})=-1$, where $\overline{s}$ $(s=0,1,2,3)$ denote the congruent residues modulo 4. Since $b$ is odd, it is easy to see that $\chi_4(2b+c)=\chi_4(2+c)=-\chi_4(c)$ and $\chi_4(a-b+c)=-\chi_4(a+b+c)$ by splitting into cases depending on the parity of $a$ and $c$. Finally, by Propositions 2.5 and 2.6, we have $\varPsi\bigl(\frac{6a+b+\sqrt{p}}{8a}\bigr)=\varPsi\bigl(\frac{-2a+b+\sqrt{p}}{8a}\bigr)$ and $\varPsi\bigl(\frac{b+\sqrt{p}}{2a}\bigr)=0$. ∎

For the remainder of this paper, for any $\mathfrak{I}\in \mathrm{Cl}(K)$, we always choose $I=[a,(-b+\sqrt{p})/2]\in\mathfrak{I}$ such that $a>0$, $p=b^2-4ac$ for some $c\in\mathbb{Z}$, $\gcd(a,b,c)=1$ and either $|b|<a\le -c$ or $b=a\le -c$. Such an $I$ is uniquely determined by $\mathfrak{I}$ if we choose $a$ to be the minimal positive integer in $\mathfrak{I}$, and thus $a,b$ are uniquely determined by $\mathfrak{I}$. Note that $I$ is different from the ideals in $\mathfrak{I}$ corresponding to the "reduced forms" with respect to real quadratic number fields. Therefore, for any $\mathfrak{I}\in\mathrm{Cl}(K)$, we may define

$$t_{\mathfrak{I}}=t_I:=S_1(I)+S_2(I), \tag{3.2}$$

where $S_1(I), S_2(I)$ are as in Lemma 3.1.

Lemma 3.2. *In the notation above, if* $p\equiv 1 \pmod 4$, *then* $t_{\mathfrak{I}}=t_{\mathfrak{I}^{-1}}$ *for any* $\mathfrak{I}\in\mathrm{Cl}(K)$, *where* $\mathfrak{I}^{-1}$ *is the inverse of* $\mathfrak{I}$ *in* $\mathrm{Cl}(K)$.

*Proof.* For any $\mathfrak{I}\in\mathrm{Cl}(K)$, choose $I=[a,(-b+\sqrt{p})/2]\in\mathfrak{I}$ as before. Then $J=[a,(b+\sqrt{p})/2]\in\mathfrak{I}^{-1}$ [4, p. 227, Proposition 5.2.5]. By (3.2), $t_{\mathfrak{I}}=t_I$, $t_{\mathfrak{I}^{-1}}=t_J$. So it suffices to show that $t_I=t_J$.

Lemma 3.1 shows that

$$\begin{aligned} S_1(J) &= \chi_4(c)\biggl(\varPsi\biggl(\frac{-b+\sqrt{p}}{8a}\biggr)-\varPsi\biggl(\frac{4a-b+\sqrt{p}}{8a}\biggr)\biggr)\\ &\quad+\chi_4(a-b+c)\biggl(\varPsi\biggl(\frac{2a-b+\sqrt{p}}{8a}\biggr)-\varPsi\biggl(\frac{-2a-b+\sqrt{p}}{8a}\biggr)\biggr). \end{aligned}$$

From Propositions 2.5 and 2.7 we have $\Psi\big(\frac{-b+\sqrt{p}}{8a}\big) = \Psi\big(\frac{b+\sqrt{p}}{8a}\big)$, $\Psi\big(\frac{4a-b+\sqrt{p}}{8a}\big)$ $=\Psi\big(\frac{4a-b+\sqrt{p}}{8a}-1\big)=\Psi\big(\frac{-4a-b+\sqrt{p}}{8a}\big)=\Psi\big(\frac{4a+b+\sqrt{p}}{8a}\big)$, $\Psi\big(\frac{2a-b+\sqrt{p}}{8a}\big)=\Psi\big(\frac{-2a+b+\sqrt{p}}{8a}\big)$, $\Psi\big(\frac{-2a-b+\sqrt{p}}{8a}\big) = \Psi\big(\frac{2a+b+\sqrt{p}}{8a}\big)$. Recalling that $\chi_4(a-b+c) = -\chi_4(a+b+c)$ from the proof of Lemma 3.1, we get $S_1(J) = S_1(I)$.

Similarly, we obtain $S_2(J) = S_2(I)$. Then substituting $S_1(J)$ and $S_2(J)$ into (3.2) gives $t_J = S_1(J) + S_2(J) = S_1(I) + S_2(I) = t_I$. ■

In what follows in this subsection, unless otherwise specified, $p$ denotes a prime number satisfying $p \equiv 1 \pmod 8$.

Lemma 3.3. *In the notation above, if* $p \equiv 1 \pmod 8$, *then* $t_{\mathrm{id}} = 2\Psi(2\sqrt{p})$, *where* id *denotes the identity element in* $\mathrm{Cl}(K)$.

*Proof.* For $K = \mathbb{Q}(\sqrt{p})$ with $p \equiv 1 \pmod 8$, the ring $\mathcal{O}_K$ has a $\mathbb{Z}$-basis consisting of 1 and $\frac{-1+\sqrt{p}}{2}$. Choose $\mathcal{O}_K$ for the representative of $\mathrm{id} \in \mathrm{Cl}(K)$ as in (3.2), so $a = b = 1, c = (1-p)/4$. Since $p \equiv 1 \pmod 8$, both $c = (1-p)/4$ and $a+b+c$ are even integers, This implies that $\chi_4(c) = \chi_4(a+b+c) = 0$. So $S_1(\mathcal{O}_K) = 0$. Moreover, $\chi_4(a) = \chi_4(1) = 1$ shows that

$$t_{\mathrm{id}} = S_2(\mathcal{O}_K) = -3\Psi(1+\sqrt{p}) + 2\Psi(2+2\sqrt{p}).$$

Letting $a = 1, b = 0, d = 4p$ and $c = -p$ in Proposition 2.6 gives $\Psi(1+\sqrt{p}) = \Psi(\sqrt{p}) = 0$, so $t_{\mathrm{id}} = 2\Psi(2+2\sqrt{p}) = 2\Psi(2\sqrt{p})$. ■

The analog of formula (2.9) given below follows easily from Lemmas 3.1 and 3.3.

Corollary 3.4 (Lu [15, p. 371, Example 4]). *If* $p \equiv 1 \pmod 8$ *is prime and* $h(p) = 1$, *then*

$$h(-p) = \tfrac{1}{3}\Psi(2\sqrt{p}) = m(4p).$$

Lemma 3.5. *In the notation above, if* $p \equiv 1 \pmod 8$, *then* $t_{\mathfrak{I}} \equiv t_{\mathfrak{I}'} \pmod 8$ *for any* $\mathfrak{I}, \mathfrak{I}' \in \mathrm{Cl}(K)$.

*Proof.* The technique used in the proof below is similar to that of [3, Theorem 1.1]. We frequently use Zagier's results stated in Subsection 2.3 to replace Hirzebruch sums in Lemma 3.1 by Dedekind sums. It suffices to prove the conclusion when $\mathfrak{I}' = \mathrm{id} \in \mathrm{Cl}(K)$, i.e., we only need to show that $t_{\mathfrak{I}} - t_{\mathrm{id}} \equiv 0 \pmod 8$, where $t_{\mathrm{id}} = 2\Psi(\sqrt{4p})$ by Lemma 3.3. Choose $I = [a, (-b+\sqrt{d})/2] \in \mathfrak{I}$ as in (3.2), so $t_{\mathfrak{I}} = t_I$ and it suffices to prove $t_I - t_{\mathrm{id}} \equiv 0 \pmod 8$.

Let $\epsilon$ be the unique fundamental unit of $K = \mathbb{Q}(\sqrt{p})$ larger than 1, and let $\epsilon_+$ be the totally positive fundamental unit. Since $p \equiv 1 \pmod 8$, we have $N_{K/\mathbb{Q}}(\epsilon) = -1$ and $\epsilon_+ = \epsilon^2$. By [5, p. 372, §3, Proposition], we can write $\epsilon = r + s\sqrt{p}$, where $r$ and $s$ are positive integers satisfying $r \equiv 0 \pmod 4$ and $s \equiv 1 \pmod 4$. Thus $\epsilon_+ = \epsilon^2 = r^2 + s^2p + 2rs\sqrt{p}$. From now on, we set

$\epsilon_+ = R + S\sqrt{p}$, where $R = r^2 + s^2 p \equiv 1 \pmod 8$ and $S = 2rs \equiv 0 \pmod 8$. Then $N_{K/\mathbb{Q}}(\epsilon_+) = 1$ implies $R^2 - pS^2 = 1$.

From $p = b^2 - 4ac \equiv 1 \pmod 8$, it follows that $b$ must be odd and thus $b^2 \equiv 1 \pmod 8$, and $a$ and $c$ cannot both be odd. To eliminate the influence of the character $\chi_4$ during our proof, we divide the proof into six cases according to the parity of $a, b$ and $c$:

Case (1): $a \equiv 1 \pmod 4$ and $c \equiv 0 \pmod 2$;
Case (2): $a \equiv 3 \pmod 4$ and $c \equiv 0 \pmod 2$;
Case (3): $a \equiv 0 \pmod 2$ and $c \equiv 1 \pmod 4$;
Case (4): $a \equiv 0 \pmod 2$ and $c \equiv 3 \pmod 4$;
Case (5): $a \equiv c \equiv 0 \pmod 2$ and $a + b + c \equiv 1 \pmod 4$;
Case (6): $a \equiv c \equiv 0 \pmod 2$ and $a + b + c \equiv 3 \pmod 4$.

Case (1). As $a \equiv 1 \pmod 4$, $c \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 2$, we have $\chi_4(a) = 1$ and $\chi_4(c) = \chi_4(a + b + c) = 0$. By Lemmas 3.1 and 3.3, we have $t_I = -3\Psi\big(\frac{b+\sqrt{p}}{a}\big) + 2\Psi\big(\frac{2b+2\sqrt{p}}{a}\big)$, and thus

$$t_I - t_{\mathrm{id}} = -3\Psi\left(\frac{b+\sqrt{p}}{a}\right) + 2\Psi\left(\frac{2b+2\sqrt{p}}{a}\right) - 2\Psi(2\sqrt{p}). \tag{3.3}$$

We now show in detail how to represent the Hirzebruch sum $\Psi(2\sqrt{p})$ by Dedekind sums, as the techniques used here will be applied in all other cases. We have $\mathcal{O}_K = \big[\frac{1+\sqrt{p}}{2}, 1\big]$ with oriented generators (i.e., $\frac{1+\sqrt{p}}{2} > 0$ and $\frac{1+\sqrt{p}}{2} \cdot 1' - \big(\frac{1+\sqrt{p}}{2}\big)' \cdot 1 = \sqrt{p} > 0$). Consider the action of the linear transformation on $\mathcal{O}_K$ via multiplication by $\epsilon_+$ on the basis:

$$\epsilon_+\begin{pmatrix}(1+\sqrt{p})/2\\ 1\end{pmatrix} = \begin{pmatrix}R+S & (p-1)S/2\\ 2S & R-S\end{pmatrix}\begin{pmatrix}(1+\sqrt{p})/2\\ 1\end{pmatrix}.$$

Consider the free $\mathbb{Z}$-module $M_0 = [2\sqrt{p}, 1] = 2\sqrt{p}\mathbb{Z} \oplus \mathbb{Z}$ of rank 2 with oriented generators; it is easy to check that $\epsilon_+ M_0 = M_0$. The basis transformation from $\mathcal{O}_K$ to $M_0$ is given by

$$\begin{pmatrix}2\sqrt{p}\\ 1\end{pmatrix} = \begin{pmatrix}4 & -2\\ 0 & 1\end{pmatrix}\begin{pmatrix}(1+\sqrt{p})/2\\ 1\end{pmatrix}.$$

By linear algebra (see for example [21, p. 375, Corollary 4.73]), multiplication by $\epsilon_+$ on $M_0$ gives rise to the matrix

$$A_0 = \begin{pmatrix}4 & -2\\ 0 & 1\end{pmatrix}\begin{pmatrix}R+S & (p-1)S/2\\ 2S & R-S\end{pmatrix}\begin{pmatrix}4 & -2\\ 0 & 1\end{pmatrix}^{-1} = \begin{pmatrix}R & 2pS\\ S/2 & R\end{pmatrix}.$$

It is clear that $A_0 \in \mathrm{SL}(2,\mathbb{Z})$, $\mathrm{Tr}(A_0) = 2R > 2$, i.e., $A_0$ is hyperbolic. So $A_0$ has two real fixed points in $\mathbb{C}$ as a linear fractional transformation. Actually, one can verify that $2\sqrt{p}$ is the larger fixed point, and $\epsilon_+$ is the larger eigenvalue of $A_0$.

This $A_0$ can be used to represent $\Psi(2\sqrt{p})$ through Dedekind sums as follows. By (2.5)–(2.7), noting that $\kappa = 1$ there by the choice of $V$, we have

$$\Psi(2\sqrt{p}) = 3m(4p) = n_{A_0} = 4R/S - 3 - 12s(R, S/2). \tag{3.4}$$

To write $\Psi\big(\frac{b+\sqrt{p}}{a}\big)$ and $\Psi\big(\frac{2b+2\sqrt{p}}{a}\big)$ as Dedekind sums, we consider the modules $M_1 = [b+\sqrt{p}, a]$ and $M_2 = [2b+2\sqrt{p}, a]$, where the generators have been oriented. After computations as above, we get two matrices

$$A_1 = \begin{pmatrix} R+bS & (p-b^2)S/a \\ aS & R-bS \end{pmatrix}, \qquad A_2 = \begin{pmatrix} R+bS & 2(p-b^2)S/a \\ aS/2 & R-bS \end{pmatrix}.$$

It is easy to verify that $A_1$ and $A_2$ are hyperbolic, their larger fixed points are $(b+\sqrt{p})/a$ and $(2b+2\sqrt{p})/a$ respectively, and they have the same larger eigenvalue $\epsilon_+$. From (2.5)–(2.7) again, we obtain

$$\Psi\bigg(\frac{b+\sqrt{p}}{a}\bigg) = \frac{2R}{aS} - 3 - 12s(R-bS, aS), \tag{3.5}$$

$$\Psi\bigg(\frac{2b+2\sqrt{p}}{a}\bigg) = \frac{4R}{aS} - 3 - 12s(R-bS, aS/2). \tag{3.6}$$

After substituting (3.4)–(3.6) into (3.3), Proposition 2.9 yields

$$\begin{aligned} t_I - t_{\mathrm{id}} &= -\frac{(8a-2)R}{aS} + 9 + 24(s(R, S/2) - s(R-bS, aS/2)) \\ &\quad + 36s(R-bS, aS) \\ &= -\frac{(8a-2)R}{aS} + 9 + 24(s(E, S/2) - s(E, aS/2)) \\ &\quad + 36s(E, aS), \end{aligned} \tag{3.7}$$

where $E = R+(a-b)S$. Note that $E > 0$ since $|b| \le a$ implies $a-b \ge 0$. To prove $t_I - t_{\mathrm{id}} \equiv 0 \pmod 8$, we need to make some transformations by using the reciprocity theorem for Dedekind sums. From Proposition 2.10, we have

$$s(E, S/2) = -s(S/2, E) - \frac{1}{4} + \frac{1}{12}\bigg(\frac{2E}{S} + \frac{2}{ES} + \frac{S}{2E}\bigg), \tag{3.8}$$

$$s(E, aS/2) = -s(aS/2, E) - \frac{1}{4} + \frac{1}{12}\bigg(\frac{2E}{aS} + \frac{2}{aES} + \frac{aS}{2E}\bigg), \tag{3.9}$$

$$s(E, aS) = -s(aS, E) - \frac{1}{4} + \frac{1}{12}\bigg(\frac{E}{aS} + \frac{1}{aES} + \frac{aS}{E}\bigg). \tag{3.10}$$

Substituting (3.8)–(3.10) into (3.7), and noting that $N_{K/\mathbb{Q}}(\epsilon_+) = R^2 - pS^2 = 1$, we get

$$t_I - t_{\mathrm{id}} = W_1 + 24(s(aS/2, E) - s(S/2, E)) - 36s(aS, E), \tag{3.11}$$

where

$$\begin{aligned}W_1 &= -\tfrac{(8a-2)R}{aS} + 9 + 24\big(\tfrac{1}{12}\big(\tfrac{2E}{S} + \tfrac{2}{ES} + \tfrac{S}{2E} - \tfrac{2E}{aS} - \tfrac{2}{aES} - \tfrac{aS}{2E}\big)\big)\\ &\quad + 36\big(-\tfrac{1}{4} + \tfrac{1}{12}\big(\tfrac{E}{aS} + \tfrac{1}{aES} + \tfrac{aS}{E}\big)\big)\\ &= \tfrac{1}{aES}(-2(4a-1)ER + (4a-1)E^2 + (2a^2+a)S^2 + 4a - 1)\\ &= \tfrac{1}{aES}(-(4a-1)R^2 + (2a^2 + a + (4a-1)(a-b)^2)S^2 + 4a - 1)\\ &= \tfrac{1}{aE}(-(4a-1)p + 2a^2 + a + (4a-1)(a-b)^2)S.\end{aligned}$$

Here we have replaced $E$ by $R + (a-b)S$ for the third equality, and $R^2$ by $pS^2 + 1$ for the last equality. Noting that $a \equiv 1 \pmod 4$, $b$ is odd and $p \equiv 1 \pmod 8$, we have $-(4a-1)p + 2a^2 + a + (4a-1)(a-b)^2 \equiv 0 \pmod 4$. And since $R \equiv 1 \pmod 8$ and $S \equiv 0 \pmod 8$, we have $E = R + (a-b)S \equiv 1 \pmod 8$. Therefore $W_1 \equiv 0 \pmod{2^5}$.

Now according to (3.11), we see that to prove $t_I - t_{\mathrm{id}} \equiv 0 \pmod 8$, it suffices to show that $s(aS/2, E) - s(S/2, E) \equiv 0 \pmod 2$ and $s\,(aS, E) \equiv 0 \pmod 2$. By Proposition 2.11, we consider the following Kronecker symbols:

$$\left(\frac{aS/2}{E}\right) = (-1)^{(E-1)/4 - 3Es(aS/2,E)} = (-1)^{s(aS/2,E)}, \tag{3.12}$$

$$\left(\frac{S/2}{E}\right) = (-1)^{(E-1)/4 - 3Es(S/2,E)} = (-1)^{-s(S/2,E)}, \tag{3.13}$$

$$\left(\frac{aS}{E}\right) = (-1)^{(E-1)/4 - 3Es(aS,E)} = (-1)^{s(aS,E)}, \tag{3.14}$$

where we have used the fact that $E \equiv 1 \pmod 8$ and $(-1)^{-1} = -1$.

Now we multiply (3.12) by (3.13). According to [12, Chapter 3] and noting that $E = R + (a-b)S \equiv 1 \pmod 8$, and that the odd integer $a$ satisfies $\gcd(E, a) = 1$ since $A_1 \in \mathrm{SL}(2, \mathbb{Z})$, we have

$$\begin{aligned}(-1)^{s(aS/2,E)-s(S/2,E)} &= \left(\frac{a}{E}\right) = (-1)^{\frac{a-1}{2}\frac{E-1}{2}}\left(\frac{E}{a}\right) = \left(\frac{E}{a}\right) = \left(\frac{R - bS}{a}\right)\\ &= \left(\frac{R \pm S\sqrt{p}}{a}\right) = \left(\frac{\epsilon^2 \text{ (or } \epsilon'^2)}{a}\right) = 1.\end{aligned}$$

Here we have used the fact that $R + S\sqrt{p} = \epsilon_+ = \epsilon^2$ (resp. $R - S\sqrt{p} = \epsilon'_+ = \epsilon'^2$), and $p = b^2 - 4ac \equiv b^2 \pmod a$ which implies that $b$ can be viewed as a square root of $p$ modulo $a$, thus the fifth equality holds. This implies that $s(aS/2, E) - s(S/2, E) \equiv 0 \pmod 2$.

Similarly, we write $S = 2^l S_0$ with $2 \nmid S_0$ and $l \geq 3$ in (3.14). By [12, Chapter 3] and [12, §12.3, Theorem 3.1], noting that $E \equiv 1 \pmod 8$ implies $E^2 \equiv 1 \pmod{16}$, and both $a$ and $S_0$ are odd integers such that $\gcd(E, aS) = 1$ as $A_1 \in \mathrm{SL}(2, \mathbb{Z})$, we have

$$\begin{aligned}(-1)^{s(aS,E)} &= \left(\frac{aS}{E}\right) = \left(\frac{2}{E}\right)^{l}(-1)^{\frac{aS_0-1}{2}\frac{E-1}{2}}\left(\frac{E}{aS_0}\right) = \left(\frac{E}{aS_0}\right)\\ &= \left(\frac{R-bS}{aS_0}\right) = \left(\frac{R-bS}{a}\right)\left(\frac{R-bS}{S_0}\right) = \left(\frac{R\pm\sqrt{p}\,S}{a}\right)\left(\frac{R}{S_0}\right)\\ &= \left(\frac{\epsilon^2\ (\text{or } \epsilon'^2)}{a}\right)\left(\frac{R}{S_0}\right) = \left(\frac{R}{S_0}\right) = \left(\frac{\epsilon^2}{S_0}\right) = 1,\end{aligned}$$

where we have used the fact that $S_0 \mid S$ and $\epsilon^2 = \epsilon_+ = R+S\sqrt{p} \equiv R \pmod{S}$ for the ninth equality. Thus we conclude that $s(aS,E) \equiv 0 \pmod 2$.

Combining these congruences with (3.11), we get $t_I - t_{\mathrm{id}} \equiv 0 \pmod 8$.

Case (2). As $a \equiv 3 \pmod 4$, $c \equiv 0 \pmod 2$ and $b \equiv 1 \pmod 2$, we have $\chi_4(a) = -1$ and $\chi_4(c) = \chi_4(a+b+c) = 0$. By Lemmas 3.1 and 3.3, we have $t_I = 3\Psi\big(\frac{b+\sqrt{p}}{a}\big) - 2\Psi\big(\frac{2b+2\sqrt{p}}{a}\big)$, and thus

$$t_I - t_{\mathrm{id}} = 3\Psi\left(\frac{b+\sqrt{p}}{a}\right) - 2\Psi\left(\frac{2b+2\sqrt{p}}{a}\right) - 2\Psi(2\sqrt{p}).$$

By (3.4)–(3.6) and Proposition 2.9, we get

$$\begin{aligned}t_I - t_{\mathrm{id}} &= -\frac{(8a+2)R}{aS} + 3 + 24\big(s(R,S/2) + s(R-bS,aS/2)\big)\\ &\quad - 36s(R-bS,aS)\\ &= -\frac{(8a+2)R}{aS} + 3 + 24\big(s(E,S/2) + s(E,aS/2)\big) - 36s(E,aS),\end{aligned}$$

where $E = R + (a-b)S > 0$ as in Case (1).

By the reciprocity theorem for Dedekind sums, applying (3.8)–(3.10), and noting that $N_{K/\mathbb{Q}}(\epsilon_+) = R^2 - pS^2 = 1$, we have

$$t_I - t_{\mathrm{id}} = W_2 - 24\big(s(aS/2,E) + s(S/2,E)\big) + 36s(aS,E)), \tag{3.15}$$

where

$$\begin{aligned}W_2 &= -\tfrac{(8a+2)R}{aS} + 3 + 24\big(-\tfrac{1}{2} + \tfrac{1}{12}\big(\tfrac{2E}{S} + \tfrac{2}{ES} + \tfrac{S}{2E} + \tfrac{2E}{aS} + \tfrac{2}{aES} + \tfrac{aS}{2E}\big)\big)\\ &\quad - 36\big(-\tfrac{1}{4} + \tfrac{1}{12}\big(\tfrac{E}{aS} + \tfrac{1}{aES} + \tfrac{aS}{E}\big)\big)\\ &= -\tfrac{(8a+2)R}{aS} + \tfrac{4E}{S} + \tfrac{4}{ES} + \tfrac{S}{E} + \tfrac{E}{aS} + \tfrac{1}{aES} - \tfrac{2aS}{E}\\ &= \tfrac{1}{aES}\big(-(8a+2)RE + (4a+1)E^2 + (a-2a^2)S^2 + 4a + 1\big)\\ &= \tfrac{1}{aES}\big(-(4a+1)R^2 + (a-2a^2+(4a+1)(a-b)^2)S^2 + 4a + 1\big)\\ &= \tfrac{S}{aE}\big(-(4a+1)p + a - 2a^2 + (4a+1)(a-b)^2\big).\end{aligned}$$

Note that $a \equiv 3 \pmod 4$, $b$ is odd, $E \equiv 1 \pmod 8$, and $S \equiv 0 \pmod 8$. It is easy to see that $-(4a+1)p + a - 2a^2 + (4a+1)(a-b)^2 \equiv 0 \pmod 4$. Therefore $W_2 \equiv 0 \pmod{2^5}$.

From the proof of Case (1), we know that $s(aS/2,E) + s(S/2,E) \equiv s(aS/2,E) - s(S/2,E) \equiv 0 \pmod 2$ and $s(aS,E) \equiv 0 \pmod 2$ in (3.15). It is now obvious that $t_I - t_{\mathrm{id}} \equiv 0 \pmod 8$.

Case (3). As $a \equiv 0 \pmod 2$, $c \equiv 1 \pmod 4$ and $b \equiv 1 \pmod 2$, we see that $\chi_4(a) = \chi_4(a+b+c) = 0$ and $\chi_4(c) = 1$. By Lemmas 3.1 and 3.3, we have $t_I = \Psi\big(\frac{b+\sqrt{p}}{8a}\big) - \Psi\big(\frac{4a+b+\sqrt{p}}{8a}\big)$, and

$$t_I - t_{\mathrm{id}} = \Psi\bigg(\frac{b+\sqrt{p}}{8a}\bigg) - \Psi\bigg(\frac{4a+b+\sqrt{p}}{8a}\bigg) - 2\Psi(2\sqrt{p}). \tag{3.16}$$

To represent the Hirzebruch sums on the right hand side of (3.16) as Dedekind sums, we consider the modules $M_3 = [b+\sqrt{p}, 8a]$ and $M_4 = [4a+b+\sqrt{p}, 8a]$ with oriented generators. Multiplication by $\epsilon_+$ on $M_3$ and $M_4$ gives rise to the matrices

$$A_3 = \begin{pmatrix} R+bS & \frac{(p-b^2)S}{8a} \\ 8aS & R-bS \end{pmatrix}, \qquad A_4 = \begin{pmatrix} R+(4a+b)S & \frac{(p-(4a+b)^2)S}{8a} \\ 8aS & R-(4a+b)S \end{pmatrix}.$$

It is easy to check that they are hyperbolic with larger fixed points $\frac{b+\sqrt{p}}{8a}$ and $\frac{4a+b+\sqrt{p}}{8a}$ respectively, and with the same larger eigenvalue $\epsilon_+$. Using (2.5)–(2.7) again, we have

$$\Psi\bigg(\frac{b+\sqrt{p}}{8a}\bigg) = \frac{R}{4aS} - 3 - 12s(R-bS, 8aS), \tag{3.17}$$

$$\Psi\bigg(\frac{4a+b+\sqrt{p}}{8a}\bigg) = \frac{R}{4aS} - 3 - 12s(R-(4a+b)S, 8aS). \tag{3.18}$$

Set $F_1 = R+(4a-b)S$ and $F_2 = R+(8a-b)S$. Noting that $|b| \le a$ by the choice of $I$, it follows that $8a-b \ge 4a-b \ge 0$. So $F_1$ and $F_2$ are positive integers. By Proposition 2.9, we have $s(R,S/2) = s(F_1,S/2) = s(F_2,S/2)$, $s(R-bS,8aS) = s(F_2,8aS)$, and $s(R-(4a+b)S,8aS) = s(F_1,8aS)$. Substituting (3.17), (3.18) and (3.4) into (3.16), we have

$$\begin{aligned} &t_I - t_{\mathrm{id}} \\ &= 12\big(s(R-(4a+b)S,8aS) - s(R-bS,8aS)\big) - 8R/S + 6 + 24s(R,S/2) \\ &= 12\big(s(F_1,8aS) + s(F_1,S/2)\big) - 12\big(s(F_2,8aS) - s(F_2,S/2)\big) - 8R/S + 6. \end{aligned} \tag{3.19}$$

Now Proposition 2.10 gives

$$s(F_1,8aS) = -s(8aS,F_1) - \frac{1}{4} + \frac{1}{12}\bigg(\frac{F_1}{8aS} + \frac{1}{8aSF_1} + \frac{8aS}{F_1}\bigg), \tag{3.20}$$

$$s(F_1,S/2) = -s(S/2,F_1) - \frac{1}{4} + \frac{1}{12}\bigg(\frac{2F_1}{S} + \frac{2}{SF_1} + \frac{S}{2F_1}\bigg), \tag{3.21}$$

$$s(F_2,8aS) = -s(8aS,F_2) - \frac{1}{4} + \frac{1}{12}\bigg(\frac{F_2}{8aS} + \frac{1}{8aSF_2} + \frac{8aS}{F_2}\bigg), \tag{3.22}$$

$$s(F_2,S/2) = -s(S/2,F_2) - \frac{1}{4} + \frac{1}{12}\bigg(\frac{2F_2}{S} + \frac{2}{SF_2} + \frac{S}{2F_2}\bigg). \tag{3.23}$$

We substitute (3.20)–(3.23) into (3.19), and notice that $N_{K/\mathbb{Q}}(\epsilon_+) = R^2 - pS^2 = 1$, to obtain

$$t_I - t_{\mathrm{id}} = W_3 - 12\big(s(S/2, F_1) + s(8aS, F_1)\big) \\ - 12\big(s(S/2, F_2) - s(8aS, F_2)\big), \tag{3.24}$$

where

$$\begin{aligned} W_3 &= -\tfrac{8R}{S} + 6 + 12\big(-\tfrac{1}{2} + \tfrac{1}{12}\big(\tfrac{F_1}{8aS} + \tfrac{1}{8aSF_1} + \tfrac{8aS}{F_1} + \tfrac{2F_1}{S} + \tfrac{2}{SF_1} + \tfrac{S}{2F_1}\big)\big) \\ &\quad -12\big(\tfrac{1}{12}\big(\tfrac{F_2}{8aS} + \tfrac{1}{8aSF_2} + \tfrac{8aS}{F_2} - \tfrac{2F_2}{S} - \tfrac{2}{SF_2} - \tfrac{S}{2F_2}\big)\big) \\ &= -\tfrac{8R}{S} - \tfrac{F_2-F_1}{8aS} + \tfrac{F_2-F_1}{8aSF_1F_2} + \tfrac{8aS(F_2-F_1)}{F_1F_2} + \tfrac{2(F_1+F_2)}{S} + \tfrac{2(F_1+F_2)}{SF_1F_2} \\ &\quad + \tfrac{S(F_1+F_2)}{2F_1F_2} \\ &= \tfrac{1}{2SF_1F_2}\big(-16RF_1F_2 - SF_1F_2 + S + 64a^2S^3 \\ &\quad + 4F_1F_2(F_1+F_2) + 4(F_1+F_2) + S^2(F_1+F_2)\big) \\ &= \tfrac{1}{2SF_1F_2}\big(-8R^3 - (48a - 8b + 1)R^2S \\ &\quad + (320a^2 - 96ab + 8b^2 - 12a + 2b + 2)RS^2\big) + 8R \\ &\quad + (1536a^3 + 32a^2 - 832a^2b + 144ab^2 + 12ab + 12a \\ &\quad - 8b^3 - b^2 - 2b)S^3 + (48a - 8b + 1)S \\ &= \tfrac{1}{F_1F_2}\big((-4p + 160a^2 - 48ab + 4b^2 - 6a + b + 1)RS \\ &\quad + (-24ap + 4bp - (p + b^2)/2 + 768a^3 + 16a^2 - 416a^2b \\ &\quad + 72ab^2 + 6ab + 6a - 4b^3 - b)S^2\big), \end{aligned}$$

where $(p + b^2)/2 \in \mathbb{Z}$. Note that $R \equiv 1 \pmod 8$ and $S \equiv 0 \pmod 8$ implies $F_1 \equiv F_2 \equiv 1 \pmod 8$, and $b \equiv 1 \pmod 2$ implies $-4p + 160a^2 - 48ab + 4b^2 - 6a + b + 1 \equiv 0 \pmod 2$. It follows that $W_3 \equiv 0 \pmod{16}$. So (3.24) gives

$$t_I - t_{\mathrm{id}} \equiv 12\big(s(S/2, F_1) + s(8aS, F_1)\big) \\ - 12\big(s(S/2, F_2) - s(8aS, F_2)\big) \pmod{16}. \tag{3.25}$$

To prove $t_I - t_{\mathrm{id}} \equiv 0 \pmod 8$, we only need to show that $s(S/2, F_1) + s(8aS, F_1) \equiv 0 \pmod 2$ and $s(S/2, F_2) - s(8aS, F_2) \equiv 0 \pmod 2$. By Proposition 2.11 again, we get the following equalites connecting Kronecker symbols with Dedekind sums:

$$\left(\frac{S/2}{F_1}\right) = (-1)^{(F_1-1)/4 - 3F_1 s(S/2, F_1)} = (-1)^{s(S/2, F_1)}, \tag{3.26}$$

$$\left(\frac{8aS}{F_1}\right) = (-1)^{(F_1-1)/4 - 3F_1 s(8aS, F_1)} = (-1)^{s(8aS, F_1)}, \tag{3.27}$$

$$\left(\frac{S/2}{F_2}\right) = (-1)^{(F_2-1)/4 - 3F_2 s(S/2, F_2)} = (-1)^{s(S/2, F_2)}, \tag{3.28}$$

$$\left(\frac{8aS}{F_2}\right) = (-1)^{(F_2-1)/4 - 3F_2 s(8aS, F_2)} = (-1)^{s(8aS, F_2)}, \tag{3.29}$$

where we have used the fact that $F_i \equiv 1 \pmod 8$ for $i = 1, 2$.

As in Case (1), we now write $a = 2^m a_0$, where $2 \nmid a_0$ and $0 < m \in \mathbb{Z}$. Note that $F_i \equiv 1 \pmod 8$ gives $F_i^2 \equiv 1 \pmod{16}$. Multiplying (3.26) by (3.27), according to [12, §12.3, Theorem 3.1] we have

$$\begin{aligned}
&(-1)^{s(S/2,F_1)+s(8aS,F_1)}\\
&= \left(\frac{a(2S)^2}{F_1}\right) = \left(\frac{a}{F_1}\right) = \left(\frac{2}{F_1}\right)^m (-1)^{\frac{a_0-1}{2}\frac{F_1-1}{2}} \left(\frac{F_1}{a_0}\right) = \left(\frac{F_1}{a_0}\right)\\
&= \left(\frac{R+(4a-b)S}{a_0}\right) = \left(\frac{R-bS}{a_0}\right) = \left(\frac{R \pm S\sqrt{p}}{a_0}\right) = \left(\frac{\epsilon^2 \text{ (or } \epsilon'^2)}{a_0}\right) = 1.
\end{aligned}$$

It follows that $s(S/2, F_1) + s(8aS, F_1) \equiv 0 \pmod 2$. Similarly, dividing (3.29) by (3.28), we have

$$\begin{aligned}
&(-1)^{s(8aS,F_2)-s(S/2,F_2)}\\
&= \left(\frac{16a}{F_2}\right) = \left(\frac{a}{F_2}\right) = \left(\frac{2}{F_2}\right)^m (-1)^{\frac{a_0-1}{2}\frac{F_2-1}{2}} \left(\frac{F_2}{a_0}\right) = \left(\frac{F_2}{a_0}\right)\\
&= \left(\frac{R+(8a-b)S}{a_0}\right) = \left(\frac{R-bS}{a_0}\right) = \left(\frac{R \pm S\sqrt{p}}{a_0}\right) = \left(\frac{\epsilon^2 \text{ (or } \epsilon'^2)}{a_0}\right) = 1.
\end{aligned}$$

This implies that $s(8aS, F_2) - s(S/2, F_2) \equiv 0 \pmod 2$.

Combining these congruences with (3.25) yields $t_I - t_{\mathrm{id}} \equiv 0 \pmod 8$.

Case (4). Here we apply (3.17)–(3.18), (3.20)–(3.23) and (3.26)–(3.29). The only difference from Case (3) is in (3.24). We omit the details.

Case (5). As $a \equiv c \equiv 0 \pmod 2$ and $a + b + c \equiv 1 \pmod 4$, it follows that $\chi_4(a) = \chi_4(c) = 0$ and $\chi_4(a + b + c) = 1$. By Lemmas 3.1 and 3.3, we have $t_I = \Psi\big(\frac{2a+b+\sqrt{p}}{8a}\big) - \Psi\big(\frac{-2a+b+\sqrt{p}}{8a}\big)$, and

$$t_I - t_{\mathrm{id}} = \Psi\left(\frac{2a+b+\sqrt{p}}{8a}\right) - \Psi\left(\frac{-2a+b+\sqrt{p}}{8a}\right) - 2\Psi(2\sqrt{p}). \tag{3.30}$$

As before, we first represent the Hirzebruch sums on the right hand side of (3.30) as Dedekind sums by considering the modules $M_5 = [2a+b+\sqrt{p}, 8a]$ and $M_6 = [-2a + b + \sqrt{p}, 8a]$ with oriented generators. Multiplication by $\epsilon_+$ on $M_5$ and $M_6$ gives rise to the matrices

$$A_5 = \begin{pmatrix} R + (2a+b)S & \frac{(p-(2a+b)^2)S}{8a} \\ 8aS & R - (2a+b)S \end{pmatrix},$$

$$A_6 = \begin{pmatrix} R - (2a-b)S & \frac{(p-(2a-b)^2)S}{8a} \\ 8aS & R + (2a-b)S \end{pmatrix}.$$

It is easy to verify that they are hyperbolic, their larger fixed points are $\frac{2a+b+\sqrt{p}}{8a}$ and $\frac{-2a+b+\sqrt{p}}{8a}$ respectively, and they have the same larger eigenvalue $\epsilon_+$. Using (2.5)–(2.7) again, we get

$$\Psi\left(\frac{2a+b+\sqrt{p}}{8a}\right)=\frac{R}{4aS}-3-12s(R-(2a+b)S,8aS), \tag{3.31}$$

$$\Psi\left(\frac{-2a+b+\sqrt{p}}{8a}\right)=\frac{R}{4aS}-3-12s(R+(2a-b)S,8aS). \tag{3.32}$$

Let $F_3=R+(2a-b)S$ and $F_4=R+(6a-b)S$. As $|b|\le a$ by the choice of $I$, it follows that $6a-b\ge 2a-b\ge 0$. Therefore $F_3$ and $F_4$ are positive integers. By Proposition 2.9, $s(R,S/2)=s(F_3,S/2)=s(R+(6a-b)S,S/2)$ and $s(R-(2a+b)S,S/2)=s(F_4,S/2)$. Substituting (3.31), (3.32) and (3.4) into (3.30), we get

$$\begin{aligned} t_I-t_{\mathrm{id}} &= 12\big(s(R+(2a-b)S,8aS)-s(R-(2a+b)S,8aS)\big)\\ &\quad -8R/S+6+24s(R,S/2)\\ &= 12\big(s(F_3,8aS)+s(F_3,S/2)\big)-12\big(s(F_4,8aS)-s(F_4,S/2)\big)-8R/S+6. \end{aligned} \tag{3.33}$$

Now Proposition 2.10 gives

$$s(F_3,8aS)=-s(8aS,F_3)-\frac{1}{4}+\frac{1}{12}\left(\frac{F_3}{8aS}+\frac{1}{8aSF_3}+\frac{8aS}{F_3}\right), \tag{3.34}$$

$$s(F_3,S/2)=-s(S/2,F_3)-\frac{1}{4}+\frac{1}{12}\left(\frac{2F_3}{S}+\frac{2}{SF_3}+\frac{S}{2F_3}\right), \tag{3.35}$$

$$s(F_4,8aS)=-s(8aS,F_4)-\frac{1}{4}+\frac{1}{12}\left(\frac{F_4}{8aS}+\frac{1}{8aSF_4}+\frac{8aS}{F_4}\right), \tag{3.36}$$

$$s(F_4,S/2)=-s(S/2,F_4)-\frac{1}{4}+\frac{1}{12}\left(\frac{2F_4}{S}+\frac{2}{SF_4}+\frac{S}{2F_4}\right). \tag{3.37}$$

Substituting (3.34)–(3.37) into (3.33), and noticing that $N_{K/\mathbb{Q}}(\epsilon_+)=R^2-pS^2=1$, we get

$$\begin{aligned} t_I-t_{\mathrm{id}} &= W_5-12\big(s(8aS,F_3)+s(S/2,F_3)\big)\\ &\quad +12\big(s(8aS,F_4)-s(S/2,F_4)\big), \end{aligned} \tag{3.38}$$

where

$$\begin{aligned} W_5 &= -\tfrac{8R}{S}+6+12\big(-\tfrac{1}{2}+\tfrac{1}{12}\big(\tfrac{F_3}{8aS}+\tfrac{1}{8aSF_3}+\tfrac{8aS}{F_3}+\tfrac{2F_3}{S}+\tfrac{2}{SF_3}+\tfrac{S}{2F_3}\big)\big)\\ &\quad -12\big(\tfrac{1}{12}\big(\tfrac{F_4}{8aS}+\tfrac{1}{8aSF_4}+\tfrac{8aS}{F_4}-\tfrac{2F_4}{S}-\tfrac{2}{SF_4}-\tfrac{S}{2F_4}\big)\big)\\ &= -\tfrac{8R}{S}+\tfrac{F_3-F_4}{8aS}+\tfrac{F_4-F_3}{8aSF_3F_4}+\tfrac{8aS(F_4-F_3)}{F_3F_4}\\ &\quad +\frac{2(F_3+F_4)}{S}+\frac{2(F_3+F_4)}{SF_3F_4}+\frac{S(F_3+F_4)}{2F_3F_4}\\ &= \tfrac{1}{2SF_3F_4}\big(-8R^3+(-32a+8b-1)R^2S\\ &\quad +(160a^2-64ab+8b^2-8a+2b+2)RS^2+8R+(32a-8b+1)S\\ &\quad +(384a^3-352a^2b+96ab^2-8b^3+52a^2+8ab+8a-b^2-2b)S^3\big) \end{aligned}$$

$$= \tfrac{1}{F_3F_4}\big((-4p+160a^2-64ab+8b^2-8a+2b+2)RS \\ + (-16ap+4bp+192a^3-176a^2b+48ab^2-4b^3+26a^2 \\ +4ab+4a-b-(p+b^2)/2)S^2\big),$$

with $(p+b^2)/2 \in \mathbb{Z}$. Note that $R \equiv 1 \pmod 8$ and $S \equiv 0 \pmod 8$ implies $F_3 \equiv F_4 \equiv 1 \pmod 8$. And $-4p+160a^2-64ab+8b^2-8a+2b+2 \equiv 0 \pmod 4$ since $b$ is odd. It follows that $W_5 \equiv 0 \pmod{32}$. Then (3.38) gives

$$t_I - t_{\mathrm{id}} \equiv -12\big(s(8aS,F_3)+s(S/2,F_3)\big) \\ + 12\big(s(8aS,F_4)-s(S/2,F_4)\big) \pmod{32}. \tag{3.39}$$

To prove $t_I - t_{\mathrm{id}} \equiv 0 \pmod 8$, we only need to show that $s(8aS,F_3)+s(S/2,F_3) \equiv 0 \pmod 2$ and $s(8aS,F_4)-s(S/2,F_4) \equiv 0 \pmod 2$. By Proposition 2.11 again, we obtain the following equalities connecting Kronecker symbols with Dedekind sums:

$$\left(\frac{8aS}{F_3}\right) = (-1)^{(F_3-1)/4-3F_3s(8aS,F_3)} = (-1)^{s(8aS,F_3)}, \tag{3.40}$$

$$\left(\frac{S/2}{F_3}\right) = (-1)^{(F_3-1)/4-3F_3s(S/2,F_3)} = (-1)^{s(S/2,F_3)}, \tag{3.41}$$

$$\left(\frac{8aS}{F_4}\right) = (-1)^{(F_4-1)/4-3F_4s(8aS,F_4)} = (-1)^{s(8aS,F_4)}, \tag{3.42}$$

$$\left(\frac{S/2}{F_4}\right) = (-1)^{(F_4-1)/4-3F_4s(S/2,F_4)} = (-1)^{s(S/2,F_4)}, \tag{3.43}$$

where we have used the fact that $F_i \equiv 1 \pmod 8$ for $i = 3,4$.

As in Case (1), we now write $a = 2^n a_0$, where $2 \nmid a_0$ and $0 < n \in \mathbb{Z}$. Note that $F_3 \equiv 1 \pmod 8$ implies $F_3^2 \equiv 1 \pmod{16}$. Multiplying (3.40) by (3.41), and applying [12, §12.3, Theorem 3.1], we see that

$$(-1)^{s(8aS,F_3)+s(S/2,F_3)} = \left(\frac{a(2S)^2}{F_3}\right) = \left(\frac{a}{F_3}\right) = \left(\frac{2}{F_3}\right)^n (-1)^{\frac{a_0-1}{2}\frac{F_3-1}{2}} \left(\frac{F_3}{a_0}\right) \\ = \left(\frac{F_3}{a_0}\right) = \left(\frac{R+(2a-b)S}{a_0}\right) = \left(\frac{R-bS}{a_0}\right) \\ = \left(\frac{R \pm S\sqrt{p}}{a_0}\right) = \left(\frac{\epsilon^2 \ (\text{or } \epsilon'^2)}{a_0}\right) = 1.$$

It follows that $s(8aS,F_3)+s(S/2,F_3) \equiv 0 \pmod 2$. Similarly, dividing (3.42) by (3.43), we have

$$\begin{aligned}(-1)^{s(8aS,F_4)-s(S/2,F_4)} &= \left(\frac{16a}{F_4}\right) = \left(\frac{a}{F_4}\right) = \left(\frac{2}{F_4}\right)^n (-1)^{\frac{a_0-1}{2}\frac{F_4-1}{2}} \left(\frac{F_4}{a_0}\right) \\ &= \left(\frac{F_4}{a_0}\right) = \left(\frac{R+(6a-b)S}{a_0}\right) = \left(\frac{R-bS}{a_0}\right) \\ &= \left(\frac{R \pm S\sqrt{p}}{a_0}\right) = \left(\frac{\epsilon^2 \text{ (or } \epsilon'^2)}{a_0}\right) = 1.\end{aligned}$$

This gives $s(8aS, F_4) - s(S/2, F_4) \equiv 0 \pmod 2$.

Combining these congruences with (3.39) yields $t_I - t_{\mathrm{id}} \equiv 0 \pmod 8$.

Case (6). Here we apply (3.31)–(3.32), (3.34)–(3.37) and (3.40)–(3.43). The only difference from Case (5) is in (3.38). We omit the details. ■

**3.2. Proof of Theorem 1.2.** Now we use Lemmas 3.1–3.5 to prove Theorem 1.2. Since $p \equiv 1 \pmod 4$, the ideal class number $h(p)$ of $K = \mathbb{Q}(\sqrt{p})$ satisfies $h(p) \equiv 1 \pmod 2$ (see for example [8, p. 182, Corollary 2] or [2, p. 100, §3]). We split the ideal class group $\mathrm{Cl}(K)$ into three disjoint parts:

$$\mathrm{Cl}(K) = \{\mathrm{id}\} \cup C \cup C^{-1}, \tag{3.44}$$

where $C$ is taken to be the subset of $\mathrm{Cl}(K) \setminus \{\mathrm{id}\}$ consisting of all $\mathfrak{I} \in C$ such that $\mathfrak{I}^{-1} \notin C$, and $C^{-1} = \{\mathfrak{I}^{-1} \mid \mathfrak{I} \in C\}$. Then $\mathrm{id} \notin C \cup C^{-1}$, $C \cap C^{-1} = \emptyset$ and $|C^{-1}| = |C| = \frac{1}{2}(h(p)-1)$.

From Proposition 2.4 we know $m(4p) = \frac{1}{3}\Psi(2\sqrt{p})$. On account of Lemma 3.1 and the partition in (3.44), we have

$$\begin{aligned}&h(-p) - h(p)m(4p) \\ &\quad= \frac{1}{6}\sum_{\mathfrak{I}\in \mathrm{Cl}(K)} t_{\mathfrak{I}} - \sum_{\mathfrak{I}\in \mathrm{Cl}(K)} m(4p) = \frac{1}{6}\sum_{\mathfrak{I}\in \mathrm{Cl}(K)} (t_{\mathfrak{I}} - 2\Psi(2\sqrt{p})) \\ &\quad= \frac{1}{6}\Big(t_{\mathrm{id}} - 2\Psi(2\sqrt{p}) + \sum_{\mathfrak{I}\in C}(t_{\mathfrak{I}} - 2\Psi(2\sqrt{p})) + \sum_{\mathfrak{I}\in C^{-1}}(t_{\mathfrak{I}} - 2\Psi(2\sqrt{p}))\Big) \\ &\quad= \frac{1}{6}\sum_{\mathfrak{I}\in C}(t_{\mathfrak{I}} - t_{\mathrm{id}}) + \frac{1}{6}\sum_{\mathfrak{I}\in C}(t_{\mathfrak{I}^{-1}} - t_{\mathrm{id}}) = \frac{1}{3}\sum_{\mathfrak{I}\in C}(t_{\mathfrak{I}} - t_{\mathrm{id}}),\end{aligned}$$

where we have applied Lemmas 3.3 and 3.2 for the last two equalities respectively. Finally, we deduce from Lemma 3.5 that $h(-p) - h(p)m(4p) \equiv 0 \pmod 8$. This completes the proof.

**3.3. More lemmas.** In this subsection, we give some more lemmas which will be used in the proof of Theorem 1.3. For the remainder of this section, we always let $p \equiv 5 \pmod 8$ be a prime number and $K = \mathbb{Q}(\sqrt{p})$. Suppose that $\epsilon = (t + u\sqrt{p})/2 > 1$ is the minimal fundamental unit of $K$ such that $t \equiv u \equiv 0 \pmod 2$, and let $\epsilon_+ = (T + U\sqrt{p})/2$ be the totally positive fundamental unit of $K$. Then $\epsilon_+ = \epsilon^2$ still holds.

LEMMA 3.6. *In the notation above, we have* $4 \,\|\, t, 2 \,\|\, u$, $8 \,\|\, U$ *and* $T \equiv 2 \pmod 8$, *where* $2^l \,\|\, u$ *means that* $2^l \mid u$ *and* $2^{l+1} \nmid u$.

*Proof.* According to [23, p. 241], we see that $4 \,\|\, t$ and $2 \,\|\, u$. Furthermore, as $\epsilon_+ = \epsilon^2 = \frac{1}{4}(t^2 + pu^2 + 2tu\sqrt{p})$, we have $T = \frac{1}{2}(t^2 + pu^2)$ and $U = tu$. Since $p \equiv 5 \pmod 8$, the lemma follows. Although the proof is trivial, the consequences of this lemma are of major importance for our later proof. ■

Similarly to the proof of Lemma 3.3, one can show

COROLLARY 3.7 (Lu [15, p. 371, Example 5]). *In the notation above,* $t_{\mathrm{id}} = 2\Psi(2\sqrt{p}) + 2\chi(c)\big(\Psi\big(\frac{1+\sqrt{p}}{8}\big) - \Psi\big(\frac{3+\sqrt{p}}{8}\big)\big)$.

LEMMA 3.8. *In the notation above,* $t_{\mathrm{id}} \equiv 2\Psi(2\sqrt{p}) \pmod 8$.

*Proof.* By Corollary 3.7, it suffices to prove that $\Psi\big(\frac{1+\sqrt{p}}{8}\big) - \Psi\big(\frac{3+\sqrt{p}}{8}\big) \equiv 0 \pmod 4$. For $i = 1, 2$, set $\beta_i = (b_i + \sqrt{p})/8$, where $b_1 = 1$ and $b_2 = 3$. For each $i$, consider the rank 2 free $\mathbb{Z}$-module $M_i = [b_i + \sqrt{p}, 8]$ contained in $\mathcal{O}_K$. Then there exists a hyperbolic matrix $A_i$ given by $\epsilon_+\binom{b_i+\sqrt{p}}{8} = A_i\binom{b_i+\sqrt{p}}{8}$.

Note that $\mathcal{O}_K = [(1+\sqrt{p})/2, 1]$, $\epsilon_+\binom{(1+\sqrt{p})/2}{1} = \left(\begin{smallmatrix}(T+U)/2 & ((p-1)U)/4\\ U & (T-U)/2\end{smallmatrix}\right)\binom{(1+\sqrt{p})/2}{1}$, and $\binom{b_i+\sqrt{p}}{8} = \left(\begin{smallmatrix}2 & b_i-1\\ 0 & 8\end{smallmatrix}\right)\binom{(1+\sqrt{p})/2}{1}$. By linear algebra (see for example [21, p. 375, Corollary 4.73]), multiplication by $\epsilon_+$ on the generators of $M_i$ gives rise to the matrix

$$\begin{aligned} A_i &= \begin{pmatrix}2 & b_i-1\\ 0 & 8\end{pmatrix}\begin{pmatrix}(T+U)/2 & (p-1)U/4\\ U & (T-U)/2\end{pmatrix}\begin{pmatrix}2 & b_i-1\\ 0 & 8\end{pmatrix}^{-1} \\ &= \begin{pmatrix}(T+b_iU)/2 & (p-b_i^2)U/16\\ 4U & (T-b_iU)/2\end{pmatrix}. \end{aligned}$$

Obviously, $\mathrm{tr}(A_i) = T = (t^2 + pu^2)/2 > 2$; $\det(A_i) = (T^2 - pU^2)/4 = 1$; and $2 \mid p - b_i^2$, $2 \mid T \pm b_iU$, thus $A_i \in \mathrm{SL}(2, \mathbb{Z})$ is hyperbolic. And it is easy to verify that the larger fixed point of $A_i$ is $\left(\begin{smallmatrix}2 & b_i-1\\ 0 & 8\end{smallmatrix}\right)\frac{1+\sqrt{p}}{2} = \frac{b_i+\sqrt{p}}{8} = \beta_i$, and the larger eigenvalue of $A_i$ is $\frac{T+U\sqrt{p}}{2} = \epsilon_+$.

Hence we may write the Hirzebruch sums as Dedekind sums according to (2.5)–(2.7). It follows that

$$\Psi(\beta_i) = \frac{T}{4U} - 3 - 12s\bigg(\frac{T-b_iU}{2}, 4U\bigg). \tag{3.45}$$

Note that $A_i \in \mathrm{SL}(2, \mathbb{Z})$ implies $\gcd\big(\frac{T-b_iU}{2}, 4U\big) = \gcd\big(\frac{T+(8-b_i)U}{2}, 4U\big) = 1$. By Propositions 2.9 and 2.10, we have $s\big(\frac{T-b_iU}{2}, 4U\big) = s\big(\frac{T+(8-b_i)U}{2}, 4U\big) = -s\big(4U, \frac{T+(8-b_i)U}{2}\big) - \frac{1}{4} + \frac{1}{12}\big(\frac{T+(8-b_i)U}{8U} + \frac{1}{2U(T+(8-b_i)U)} + \frac{8U}{T+(8-b_i)U}\big)$. It is easy to compute that

$$\begin{aligned}(3.46)\qquad \Psi(w_1)-\Psi(w_2)&=12\left(s\left(\frac{T+5U}{2},4U\right)-s\left(\frac{T+7U}{2},4U\right)\right)\\ &=\frac{-T^2-12TU+29U^2+4}{4(T+7U)(T+5U)}+12\left(s\left(4U,\frac{T+7U}{2}\right)-s\left(4U,\frac{T+5U}{2}\right)\right).\end{aligned}$$

Now we determine the right hand side of (3.46) modulo 4. Applying Lemma 3.6 and recalling that $N(\epsilon_+)=\frac{1}{4}(T^2-pU^2)=1$, i.e. $T^2=pU^2+4$, it is easy to see that the numerator $-T^2-12TU+29U^2+4$ is $(-p+29)U^2-12TU\equiv 0 \pmod{64}$. And the denominator satisfies $16\parallel 4(T+7U)(T+5U)$ for the same reason. Thus $\frac{-T^2-12TU+29U^2+4}{4(T+7U)(T+5U)}\equiv 0 \pmod 4$ in (3.46).

Furthermore, by Lemma 3.6, it is easy to verify that $\frac{T+5U}{2}\geq 1$, $\frac{T+7U}{2}\geq 1$, $\frac{T+5U}{2}\equiv 1 \pmod 8$ and $\frac{T+7U}{2}\equiv 1 \pmod 8$. Set $L=\frac{1}{4}(T+5U)(T+7U)$; then $L\equiv 1 \pmod 8$. By Proposition 2.11, we get

$$\left(\frac{4U}{(T+5U)/2}\right)=(-1)^{\frac{\frac{T+5U}{2}-1}{4}-3\frac{T+5U}{2}s(4U,\frac{T+5U}{2})}=(-1)^{-s(4U,\frac{T+5U}{2})+\frac{\frac{T+5U}{2}-1}{4}},$$

$$\left(\frac{4U}{(T+7U)/2}\right)=(-1)^{\frac{\frac{T+7U}{2}-1}{4}-3\frac{T+7U}{2}s(4U,\frac{T+7U}{2})}=(-1)^{s(4U,\frac{T+7U}{2})-\frac{\frac{T+7U}{2}-1}{4}}.$$

Multiplying the two symbols, we conclude that

$$(3.47)\qquad \left(\frac{4U}{L}\right)=\left(\frac{U}{L}\right)=(-1)^{s(4U,\frac{T+7U}{2})-s(4U,\frac{T+5U}{2})},$$

where we have used the fact that $(-1)^{\frac{\frac{T+7U}{2}-1}{4}-\frac{\frac{T+5U}{2}-1}{4}}=(-1)^{-U/4}=1$. Now applying [12, §12.3, Theorem 3.1] and writing $U=2^3U_0$ with $U_0\equiv 1 \pmod 2$, we get $\left(\frac{U}{L}\right)=\left(\frac{2}{L}\right)^3(-1)^{\frac{U_0-1}{2}\frac{L-1}{2}}\left(\frac{L}{U_0}\right)=\left(\frac{2}{L}\right)\left(\frac{(T/2)^2}{U_0}\right)=(-1)^{\frac{L^2-1}{8}}$ $=1$, where we have used the fact that $L\equiv 1 \pmod 8$. So (3.47) becomes

$$(-1)^{s(4U,\frac{T+7U}{2})-s(4U,\frac{T+5U}{2})}=1,$$

which implies that

$$(3.48)\qquad s\left(4U,\frac{T+7U}{2}\right)-s\left(4U,\frac{T+5U}{2}\right)\equiv 0 \pmod 2.$$

Now substituting (3.48) into (3.46), we easily obtain $\Psi\left(\frac{1+\sqrt{p}}{8}\right)-\Psi\left(\frac{3+\sqrt{p}}{8}\right)\equiv 0 \pmod 4$. ∎

Lemma 3.9. *In the notation above, $t_{\mathfrak{I}}\equiv t_{\mathfrak{I}'} \pmod 4$ for any $\mathfrak{I},\mathfrak{I}'$ in* $\mathrm{Cl}(K)$.

*Proof.* As in the proof of Lemma 3.5, it suffices to prove that $t_{\mathfrak{I}}-t_{\mathrm{id}}\equiv 0 \pmod 4$, where $t_{\mathrm{id}}$ is given by Corollary 3.7 and Lemma 3.8. Take $I=\left[a,\frac{-b+\sqrt{d}}{2}\right]\in\mathfrak{I}$ as before. Then $t_{\mathfrak{I}}=t_I$ and it is sufficient to prove that $t_I-t_{\mathrm{id}}\equiv 0 \pmod 4$. Note that we have actually proved that $S_1(\mathrm{id})\equiv$

$0 \pmod 4$ in Lemma 3.8, so it remains to show that $S_1(I)+S_2(I)-S_2(\mathrm{id}) \equiv 0 \pmod 4$.

Set $\beta_i = \frac{b_i+\sqrt{p}}{8a}$ for $3 \le i \le 6$ and $b_3 = b$, $b_4 = 4a+b$, $b_5 = 2a+b$, $b_6 = 6a+b$. Consider the free $\mathbb{Z}$-module $M_i = [b_i+\sqrt{p}, 8a]$, and let $A_i$ be the matrix given by multiplication by $\epsilon_+$ on $M_i$. Since $\left(\begin{smallmatrix} b_i+\sqrt{p} \\ 8a \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & b_i-1 \\ 0 & 8a \end{smallmatrix}\right)\left(\begin{smallmatrix} (1+\sqrt{p})/2 \\ 1 \end{smallmatrix}\right)$, we have

$$A_i = \begin{pmatrix} 2 & b_i-1 \\ 0 & 8a \end{pmatrix}\begin{pmatrix} \frac{T+U}{2} & \frac{(p-1)U}{4} \\ U & \frac{T-U}{2} \end{pmatrix}\begin{pmatrix} 2 & b_i-1 \\ 0 & 8a \end{pmatrix}^{-1} = \begin{pmatrix} \frac{T+b_iU}{2} & \frac{(p-b_i^2)U}{16a} \\ 4aU & \frac{T-b_iU}{2} \end{pmatrix},$$

where the intermediate matrix $\left(\begin{smallmatrix} (T+U)/2 & ((p-1)U)/4 \\ U & (T-U)/2 \end{smallmatrix}\right)$ comes from the second paragraph of the proof of Lemma 3.8. Obviously, $\mathrm{tr}(A_i) = T = (t^2+pu^2)/2 > 2$; $\det(A_i) = (T^2-pU^2)/4 = 1$; and $p = b^2-4ac$ implies $2a \mid p-b_i^2$, and note that $8 \,\|\, U$, thus $A_i \in \mathrm{SL}(2,\mathbb{Z})$ is hyperbolic. Furthermore, it is easy to verify that the larger fixed point of $A_i$ is $\left(\begin{smallmatrix} 2 & b_i-1 \\ 0 & 8a \end{smallmatrix}\right)\frac{1+\sqrt{p}}{2} = \frac{b_i+\sqrt{p}}{8a} = \beta_i$, and the larger eigenvalue of $A_i$ is $\frac{T+U\sqrt{p}}{2} = \epsilon_+$.

Similarly, define $\beta_7 = \frac{b+\sqrt{p}}{a}$, $\beta_8 = \frac{2b+2\sqrt{p}}{a}$, $\beta_9 = \sqrt{p}, \beta_0 = 2\sqrt{p}$; and consider the $\mathbb{Z}$-modules $M_7 = [b+\sqrt{p}, a], M_8 = [2b+2\sqrt{p}, a], M_9 = [\sqrt{p}, 1], M_0 = [2\sqrt{p}, 1]$. Let $A_i$ be the matrix given by multiplication by $\epsilon_+$ on $M_i$ for $i \in \{7,8,9,0\}$. Since $\left(\begin{smallmatrix} b+\sqrt{p} \\ a \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & b-1 \\ 0 & a \end{smallmatrix}\right)\left(\begin{smallmatrix} (1+\sqrt{p})/2 \\ 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 2b+2\sqrt{p} \\ a \end{smallmatrix}\right) = \left(\begin{smallmatrix} 4 & 2b-2 \\ 0 & a \end{smallmatrix}\right)\left(\begin{smallmatrix} (1+\sqrt{p})/2 \\ 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} \sqrt{p} \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 2 & -1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} (1+\sqrt{p})/2 \\ 1 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 2\sqrt{p} \\ 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 4 & -2 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} (1+\sqrt{p})/2 \\ 1 \end{smallmatrix}\right)$, we have

$$A_7 = \begin{pmatrix} 2 & b-1 \\ 0 & a \end{pmatrix}\begin{pmatrix} \frac{T+U}{2} & \frac{(p-1)U}{4} \\ U & \frac{T-U}{2} \end{pmatrix}\begin{pmatrix} 2 & b-1 \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} \frac{T+bU}{2} & \frac{(p-b^2)U}{2a} \\ \frac{aU}{2} & \frac{T-bU}{2} \end{pmatrix},$$

$$A_8 = \begin{pmatrix} 4 & 2b-2 \\ 0 & a \end{pmatrix}\begin{pmatrix} \frac{T+U}{2} & \frac{(p-1)U}{4} \\ U & \frac{T-U}{2} \end{pmatrix}\begin{pmatrix} 4 & 2b-2 \\ 0 & a \end{pmatrix}^{-1} = \begin{pmatrix} \frac{T+bU}{2} & \frac{(p-b^2)U}{a} \\ \frac{aU}{4} & \frac{T-bU}{2} \end{pmatrix},$$

$$A_9 = \begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{T+U}{2} & \frac{(p-1)U}{4} \\ U & \frac{T-U}{2} \end{pmatrix}\begin{pmatrix} 2 & -1 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} T/2 & pU/2 \\ U/2 & T/2 \end{pmatrix},$$

$$A_0 = \begin{pmatrix} 4 & -2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \frac{T+U}{2} & \frac{(p-1)U}{4} \\ U & \frac{T-U}{2} \end{pmatrix}\begin{pmatrix} 4 & -2 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} T/2 & pU \\ U/4 & T/2 \end{pmatrix}.$$

It is easy to verify that $A_7, A_8, A_9, A_0$ are hyperbolic matrices in $\mathrm{SL}(2,\mathbb{Z})$, their larger fixed points are $\beta_7, \beta_8, \beta_9, \beta_0$ respectively, and they have the same larger eigenvalue $\epsilon_+$.

We now use the above hyperbolic matrices to represent Hirzebruch sums as Dedekind sums. In what follows, let $X_i = T+(8a-b_i)U$ for $3 \le i \le 6$ and $Y = T+(a-b)U$. Then Lemma 3.6 implies that $X_i \equiv Y \equiv 2 \pmod 8$.

According to (2.5)–(2.7) and Proposition 2.9, we see that

$$\begin{aligned}\Psi(\beta_i) &= \frac{T}{4aU} - 3 - 12s\left(\frac{T-b_iU}{2}, 4aU\right)\\ &= \frac{T}{4aU} - 3 - 12s(X_i/2, 4aU) \quad \text{for } 3 \le i \le 6,\end{aligned} \tag{3.49}$$

where $X_i/2 = \frac{1}{2}(T+(8a-b_i)U) > 0$ and $4aU > 0$ since $|b| \le a \le -c$, with $\gcd(X_i/2, 4aU) = 1$ since $A_i \in \mathrm{SL}(2,\mathbb{Z})$. Similarly,

$$\Psi(\beta_7) = \frac{2T}{aU} - 3 - 12s(Y/2, aU/2), \tag{3.50}$$

$$\Psi(\beta_8) = \frac{4T}{aU} - 3 - 12s(Y/2, aU/4), \tag{3.51}$$

$$\Psi(\beta_9) = \frac{2T}{U} - 3 - 12s(Y/2, U/2), \tag{3.52}$$

$$\Psi(\beta_0) = \frac{4T}{U} - 3 - 12s(Y/2, U/4). \tag{3.53}$$

By Proposition 2.10, we get

$$s(X_i/2, 4aU) = -\frac{1}{4} + \frac{1}{12}\left(\frac{X_i}{8aU} + \frac{1}{2aUX_i} + \frac{8aU}{X_i}\right) - s(4aU, X_i/2), \tag{3.54}$$

$$s(Y/2, aU/2) = -\frac{1}{4} + \frac{1}{12}\left(\frac{Y}{aU} + \frac{4}{aUY} + \frac{aU}{Y}\right) - s(aU/2, Y/2), \tag{3.55}$$

$$s(Y/2, aU/4) = -\frac{1}{4} + \frac{1}{12}\left(\frac{2Y}{aU} + \frac{8}{aUY} + \frac{aU}{2Y}\right) - s(aU/4, Y/2), \tag{3.56}$$

$$s(Y/2, U/2) = -\frac{1}{4} + \frac{1}{12}\left(\frac{Y}{U} + \frac{4}{UY} + \frac{U}{Y}\right) - s(U/2, Y/2), \tag{3.57}$$

$$s(Y/2, U/4) = -\frac{1}{4} + \frac{1}{12}\left(\frac{2Y}{U} + \frac{8}{UY} + \frac{U}{2Y}\right) - s(U/4, Y/2). \tag{3.58}$$

Having disposed of these preliminary computations, we can now return to the proof of the lemma. To show the congruence $S_1(I)+S_2(I)-S_2(\mathrm{id}) \equiv 0 \pmod 4$, it will be necessary to divide the proof into the following two steps.

Step I. $S_1(I) \equiv 0 \pmod 4$.

From (3.49) and (3.54) we have

$$\begin{aligned}\Psi(\beta_3) - \Psi(\beta_4) &= 12\big(s(X_4/2, 4aU) - s(X_3/2, 4aU)\big)\\ &= 12\big(s(4aU, X_3/2) - s(4aU, X_4/2)\big) + V_{34},\end{aligned} \tag{3.59}$$

where

$$\begin{aligned}V_{34} &= \tfrac{X_4}{8aU} + \tfrac{1}{2aUX_4} + \tfrac{8aU}{X_4} - \tfrac{X_3}{8aU} - \tfrac{1}{2aUX_3} - \tfrac{8aU}{X_3} = \tfrac{1}{2} + \tfrac{2}{X_3X_4} + \tfrac{32a^2U^2}{X_3X_4}\\ &= \tfrac{1}{2X_3X_4}\big(4 - T^2 - 2(6a-b)TU + (64a^2 - (4a-b)(8a-b))U^2\big)\\ &= \tfrac{1}{2X_3X_4}\big(-pU^2 - 2(6a-b)TU + (64a^2 - (4a-b)(8a-b))U^2\big).\end{aligned}$$

Here we have used $X_3 = T+(8a-b)U$, $X_4 = T+(4a-b)U$ and $T^2-pU^2 = 4$. Lemma 3.6 makes it obvious that $2^2 \parallel X_3X_4$ and $-pU^2-2(6a-b)TU+(64a^2-(4a-b)(8a-b))U^2 \equiv 0 \pmod{2^5}$. It follows that $V_{34} \equiv 0 \pmod 4$.

In the same manner we can see that

$$\Psi(\beta_5) - \Psi(\beta_6) = 12\big(s(4aU, X_5/2) - s(4aU, X_6/2)\big) + V_{56}, \tag{3.60}$$

where $X_5 = T + (6a - b)U$, $X_6 = T + (2a - b)U$, and $V_{56} = \frac{1}{2X_5X_6}(-pU^2 - 2(4a-b)TU + (64a^2 - (2a-b)(6a-b))U^2) \equiv 0 \pmod 4$.

Note that $\chi_4(c), \chi_4(a+b+c) \in \{0, \pm 1\}$. Lemma 3.1 says that to show $S_1(I) \equiv 0 \pmod 4$, we only need to prove that

$$\Psi(\beta_3) - \Psi(\beta_4) \equiv \Psi(\beta_5) - \Psi(\beta_6) \equiv 0 \pmod 4. \tag{3.61}$$

From (3.59) and (3.60) it is sufficient to prove that $s\big(4aU, X_3/2\big) - s(4aU, X_4/2) \equiv s(4aU, X_5/2) - s(4aU, X_6/2) \equiv 0 \pmod 2$.

First of all, by Proposition 2.11,

$$\begin{aligned}\left(\frac{4aU}{X_3/2}\right) &= (-1)^{\frac{1}{4}(X_3/2-1)-\frac{3}{2}X_3 s(4aU, X_3/2)} \\ &= (-1)^{\frac{1}{4}(X_3/2-1)-s(4aU,X_3/2)} = (-1)^{\frac{1}{4}(1-X_3/2)+s(4aU,X_3/2)},\end{aligned} \tag{3.62}$$

where we have used the fact that $X_3 \equiv 2 \pmod 8$ for the second equality and $(-1)^{-1} = -1$ for the third equality. For the same reason,

$$\left(\frac{4aU}{X_4/2}\right) = (-1)^{\frac{1}{4}(X_4/2-1)-s(4aU,X_4/2)}. \tag{3.63}$$

Now we multiply the Kronecker symbols in (3.62) and (3.63). By Lemma 3.6, we write $T = 2^3T' + 2, U = 2^3U'$, where $U'$ is an odd integer. Set $D' = \frac{1}{4}X_3X_4 = \frac{1}{4}(T^2 + 2(6a-b)TU + (4a-b)(8a-b)U^2)$; it is easy to check that $D' \equiv 1 \pmod 8$. And note that $a$ is odd for otherwise $p$ will be congruent to 1 modulo 8. On the one hand, from [12, §12.3, Theorem 3.1] we have $\big(\frac{4aU}{D'}\big) = (-1)^{\frac{aU'-1}{2}\frac{D'-1}{2}}\big(\frac{D'}{aU'}\big)\big(\frac{2}{D'}\big)^5 = \big(\frac{(T-bU)/2}{aU'}\big)^2\big(\frac{2}{D'}\big)^5 = \big(\frac{2}{D'}\big) = (-1)^{\frac{D'^2-1}{8}} = 1$, where we have used the fact that $aU' \mid aU$ for the second equality. On the other hand, we get $(-1)^{(X_4-X_3)/8+s(4aU,X_3/2)-s(4aU,X_4/2)} = (-1)^{s(4aU,X_3/2)-s(4aU,X_4/2)}$. Combining these, we obtain

$$(-1)^{s(4aU,X_3/2)-s(4aU,X_4/2)} = 1.$$

It is immediate that

$$s(4aU, X_3/2) - s(4aU, X_4/2) \equiv 0 \pmod 2. \tag{3.64}$$

Secondly, by similar considerations,

$$\begin{aligned}\left(\frac{4aU}{X_5/2}\right) &= (-1)^{\frac{1}{4}(1-X_5/2)+s(4aU,X_5/2)}, \\ \left(\frac{4aU}{X_6/2}\right) &= (-1)^{\frac{1}{4}(X_6/2-1)-s(4aU,X_6/2)}.\end{aligned}$$

Let $D'' = \frac{1}{4}X_5X_6 = \frac{1}{4}(T^2 + 2(4a-b)TU + (2a-b)(6a-b)U^2)$; it is easy to check that $D'' \equiv 1 \pmod 8$. Multiplying the above two symbols and applying [12, §12.3, Theorem 3.1], we get

$$(-1)^{s(4aU,X_5/2)-s(4aU,X_6/2)} = \left(\frac{4aU}{D''}\right) = (-1)^{\frac{aU'-1}{2}\frac{D''-1}{2}}\left(\frac{D''}{aU'}\right)\left(\frac{2}{D''}\right)^5$$
$$= \left(\frac{(T-bU)/2}{aU'}\right)^2\left(\frac{2}{D''}\right)^5 = \left(\frac{2}{D''}\right) = 1,$$

where we have used the fact that $aU' \mid aU$ for the third equality. Hence

$$s(4aU, X_5/2) - s(4aU, X_6/2) \equiv 0 \pmod 2. \tag{3.65}$$

Combining (3.64) and (3.65) we conclude that $S_1(I) \equiv 0 \pmod 4$.

Step II. $S_2(I) - S_2(\mathrm{id}) \equiv 0 \pmod 4$.

Since $S_2(I) - S_2(\mathrm{id}) = \chi_4(a)(-3\Psi(\beta_7) + 2\Psi(\beta_8)) + 3\Psi(\beta_9) - 2\Psi(\beta_0) = 2(\chi_4(a)\Psi(\beta_8) - \Psi(\beta_0)) - 3(\chi_4(a)\Psi(\beta_7) - \Psi(\beta_9))$, it is sufficient to prove that $\chi_4(a)\Psi(\beta_8) - \Psi(\beta_0) \equiv \Psi(\beta_8) - \Psi(\beta_0) \equiv 0 \pmod 2$ and $\chi_4(a)\Psi(\beta_7) - \Psi(\beta_9) \equiv 0 \pmod 4$.

From (3.51) and (3.53), and applying (3.56) and (3.58), we have

$$\begin{aligned}\Psi(\beta_8) - \Psi(\beta_0) &= \frac{4(1-a)T}{aU} - 12\big(s(Y/2, aU/4) - s(Y/2, U/4)\big)\\ &= V_{80} + 12\big(s(aU/4, Y/2) - s(U/4, Y/2)\big),\end{aligned} \tag{3.66}$$

where

$$\begin{aligned}V_{80} &= \tfrac{4(1-a)T}{aU} - \left(\tfrac{2Y}{aU} + \tfrac{8}{aUY} + \tfrac{aU}{2Y} - \tfrac{2Y}{U} - \tfrac{8}{UY} - \tfrac{U}{2Y}\right)\\ &= \tfrac{1-a}{2aUY}(8TY - 4Y^2 - 16 + aU^2) = \tfrac{1-a}{2aUY}\big(4T^2 - 16 + (a - 4(a-b)^2)U^2\big)\\ &= \tfrac{(1-a)U}{2aY}(4p + a - 4(a-b)^2).\end{aligned}$$

Here we have used the fact that $T^2 - pU^2 = 4$ for the last equality. Note that $(1-a)/2 \in \mathbb{Z}$, $2 \parallel Y, 2^3 \parallel U$. It follows that $V_{80} \equiv 0 \pmod 4$.

By Proposition 2.11, and noting that $Y \equiv 2 \pmod 8$ implies that $Y/2 \equiv 1 \pmod 4$, we have

$$\left(\frac{aU/4}{Y/2}\right) = (-1)^{\frac{1}{4}(Y/2-1)+s(aU/4,Y/2)}, \qquad \left(\frac{U/4}{Y/2}\right) = (-1)^{\frac{1}{4}(Y/2-1)-s(U/4,Y/2)}.$$

Multiplying the above two symbols yields

$$(-1)^{s(aU/4,Y/2)-s(U/4,Y/2)} = \left(\frac{a(U/4)^2}{Y/2}\right) = \left(\frac{a}{Y/2}\right) = (-1)^{\frac{Y/2-1}{2}\cdot\frac{a-1}{2}}\left(\frac{Y/2}{a}\right)$$
$$= \left(\frac{(T+(a-b)U)/2}{a}\right) = \left(\frac{(T+bU)/2}{a}\right) = \left(\frac{\epsilon^2(\text{or } \epsilon'^2)}{a}\right) = 1.$$

Here we have used the quadratic reciprocity law for the third equality, and for the sixth equality the fact that $p = b^2 - 4ac \equiv 5 \pmod 8$ implies $a, b$ are odd and one can assert that $b \equiv \pm\sqrt{p} \pmod a$. Hence

$$s(aU/4, Y/2) - s(U/4, Y/2) \equiv 0 \pmod 2. \tag{3.67}$$

Combining this with (3.66) we get $\Psi(\beta_8) - \Psi(\beta_0) \equiv 0 \pmod 2$.

To prove that $\chi_4(a)\Psi(\beta_7) - \Psi(\beta_9) \equiv 0 \pmod 4$, we only handle the case of $\chi_4(a) = 1$ because almost the same considerations apply to $\chi_4(a) = -1$.

So assume $\chi_4(a) = 1$. From (3.50) and (3.52), and applying (3.55) and (3.57), we have

$$\begin{aligned} \Psi(\beta_7) - \Psi(\beta_9) &= \frac{2(1-a)T}{aU} + 12\big(s(Y/2, U/2) - s(Y/2, aU/2)\big) \\ &= V_{79} + 12\big(s(aU/2, Y/2) - s(U/2, Y/2)\big), \end{aligned} \tag{3.68}$$

where

$$\begin{aligned} V_{79} &= \tfrac{2(1-a)T}{aU} + \big(\tfrac{Y}{U} + \tfrac{4}{UY} + \tfrac{U}{Y} - \tfrac{Y}{aU} - \tfrac{4}{aUY} - \tfrac{aU}{Y}\big) \\ &= \tfrac{1-a}{aUY}(2TY - Y^2 - 4 + aU^2) \\ &= \tfrac{1-a}{aUY}(T^2 - 4 + (a - (a-b)^2)U^2) = \tfrac{(1-a)U}{aY}(p + a - (a-b)^2). \end{aligned}$$

Here we have used the fact that $T^2 - pU^2 = 4$ for the last equality. Note that $a, b$ are odd, $2 \,\|\, Y$ and $2^3 \,\|\, U$. It follows that $V_{79} \equiv 0 \pmod 4$.

By Proposition 2.11 again, we have

$$\left(\frac{aU/2}{Y/2}\right) = (-1)^{\frac{1}{4}(Y/2-1)+s(aU/2,Y/2)}, \qquad \left(\frac{U/2}{Y/2}\right) = (-1)^{\frac{1}{4}(Y/2-1)-s(U/2,Y/2)}.$$

Multiplying the above two symbols yields $(-1)^{s(aU/2,Y/2)-s(U/2,Y/2)} = \big(\frac{a(U/4)^2}{Y/2}\big)$ $= \big(\frac{a}{Y/2}\big) = 1$. Here we have directly used the computational result in the previous case for the last equality. Hence

$$s(aU/2, Y/2) - s(U/2, Y/2) \equiv 0 \pmod 2. \tag{3.69}$$

Combining this with (3.68) we get $\Psi(\beta_7) - \Psi(\beta_9) \equiv 0 \pmod 4$.

In summary, we have proved that $t_I - t_{\mathrm{id}} \equiv 0 \pmod 4$. This completes the proof. ■

**3.4. Proof of Theorem 1.3.** The proof of Theorem 1.3 is quite similar to that of Theorem 1.2: we only need to replace Lemmas 3.3 and 3.5 by Lemmas 3.8 and 3.9 respectively. The details are omitted.

**4. Remarks.** Finally, for prime $p \equiv 1 \pmod 8$, one may conjecture a slightly stronger congruence than Theorem 1.2, say

$$h(-p) \equiv h(p)m(4p) \pmod{2^4}.$$

We have checked this congruence in Appendix for $p \leq 7001$ by numerical methods. However, from Table 1 it is clear that $h(-p) \equiv h(p)m(4p) \pmod{2^5}$

is not valid anymore. For example, if $p = 401$ then $h(-401) = 20, h(401) = 5$ and $m(4 \cdot 401) = 20$. We see that $h(401)m(4 \cdot 401) - h(-401) = 2^4 \cdot 5$, This shows that $2^4$ is the largest possible modulus in Theorem 1.2 .

Similarly, it would be very interesting to find out whether the congruence (1.5) in Theorem 1.3 is true for all primes $p \equiv 5 \pmod 8$.

**5. Appendix.** In the following two tables, we list the factorizations of $h(-p) - h(p)m(4p)$ for $p \equiv 1 \pmod 8$ ($p \leq 7001$) and $p \equiv 5 \pmod 8$ ($p \leq 500$) respectively. The data from left to right are the prime number $p$, the class numbers $h(-p)$ and $h(p)$, $m(4p)$, and the prime factorization of $h(-p) - h(p)m(4p)$.

**Table 1.** Factorizations of $h(-p) - h(p)m(4p)$ for $p \equiv 1 \pmod 8$ and $p \leq 7001$. We omit the cases when $h(p) = 1$ since Corollary 3.4 implies that $h(-p) = m(4p)$.

| $p$ | $h(-p)$ | $h(p)$ | $m(4p)$ | $h(p)m(4p) - h(-p)$ |
|---|---|---|---|---|
| 257 | 16 | 3 | 16 | $2^5$ |
| 401 | 20 | 5 | 20 | $2^4 \cdot 5$ |
| 761 | 40 | 3 | 24 | $2^5$ |
| 1009 | 20 | 7 | 28 | $2^4 \cdot 11$ |
| 1129 | 16 | 9 | 32 | $2^4 \cdot 17$ |
| 1297 | 12 | 11 | 36 | $2^7 \cdot 3$ |
| 1489 | 20 | 3 | 28 | $2^6$ |
| 1601 | 56 | 7 | 40 | $2^5 \cdot 7$ |
| 2081 | 60 | 5 | 44 | $2^5 \cdot 5$ |
| 2089 | 44 | 3 | 36 | $2^6$ |
| 2153 | 32 | 5 | 48 | $2^4 \cdot 13$ |
| 2713 | 24 | 3 | 24 | $2^4 \cdot 3$ |
| 2777 | 40 | 3 | 56 | $2^7$ |
| 2857 | 20 | 3 | 44 | $2^4 \cdot 7$ |
| 3121 | 40 | 5 | 40 | $2^5 \cdot 5$ |
| 3137 | 56 | 9 | 56 | $2^6 \cdot 7$ |
| 3889 | 36 | 3 | 44 | $2^5 \cdot 3$ |
| 4001 | 72 | 3 | 56 | $2^5 \cdot 3$ |
| 4409 | 68 | 9 | 68 | $2^5 \cdot 17$ |
| 4441 | 56 | 5 | 72 | $2^4 \cdot 19$ |
| 4481 | 64 | 3 | 64 | $2^7$ |
| 4649 | 88 | 3 | 104 | $2^5 \cdot 7$ |
| 4729 | 40 | 3 | 56 | $2^7$ |
| 5081 | 116 | 3 | 76 | $2^4 \cdot 7$ |
| 5273 | 40 | 7 | 72 | $2^4 \cdot 29$ |
| 5281 | 52 | 3 | 108 | $2^4 \cdot 17$ |
| 5297 | 72 | 3 | 72 | $2^4 \cdot 3^2$ |
| 5417 | 72 | 7 | 72 | $2^4 \cdot 3^3$ |
| 5521 | 60 | 9 | 76 | $2^4 \cdot 3 \cdot 13$ |
| 6113 | 68 | 5 | 84 | $2^5 \cdot 11$ |
| 6481 | 56 | 5 | 40 | $2^4 \cdot 3^2$ |
| 7001 | 56 | 1 | 56 | 0 |

**Table 2.** Factorizations of $h(-p) - h(p)m(4p)$ for $p \equiv 5 \pmod 8$ and $p \leq 500$

| $p$ | $h(-p)$ | $h(p)$ | $m(4p)$ | $h(p)m(4p) - h(-p)$ |
|---|---|---|---|---|
| 5 | 2 | 1 | 2 | 0 |
| 13 | 2 | 1 | 2 | 0 |
| 29 | 6 | 1 | 6 | 0 |
| 37 | 2 | 1 | 6 | $2^2$ |
| 53 | 6 | 1 | 6 | 0 |
| 61 | 6 | 1 | 6 | 0 |
| 101 | 14 | 1 | 10 | $-2^2$ |
| 109 | 6 | 1 | 6 | 0 |
| 149 | 14 | 1 | 14 | 0 |
| 157 | 6 | 1 | 6 | 0 |
| 173 | 14 | 1 | 14 | 0 |
| 181 | 10 | 1 | 6 | $-2^2$ |
| 197 | 10 | 1 | 14 | $2^2$ |
| 229 | 10 | 3 | 14 | $2^5$ |
| 269 | 22 | 1 | 18 | $-2^2$ |
| 277 | 6 | 1 | 6 | 0 |
| 293 | 18 | 1 | 18 | 0 |
| 317 | 10 | 1 | 10 | 0 |
| 349 | 14 | 1 | 26 | $2^2 \cdot 3$ |
| 373 | 10 | 1 | 14 | $2^2$ |
| 389 | 22 | 1 | 18 | 0 |
| 397 | 6 | 1 | 6 | 0 |
| 421 | 10 | 1 | 10 | 0 |
| 461 | 30 | 1 | 30 | 0 |

**Acknowledgements.** The authors thank the referees for their careful reading of the manuscript and many valuable suggestions that helped improving the presentation.

This work was supported by National Natural Science Foundation of China (Grant Nos. 11571163 and 11631009). The first author was also supported by Scientific and Technological Research Program of Chongqing Municipal Education Commission (Grant No. KJQN201900613) and Scientific Research Foundation from CQUPT (Grant No. A2019-104).

## References

[1] E. Brown, *The power of 2 dividing the class-number of a binary quadratic discriminant*, J. Number Theory 5 (1973), 413–419.

[2] E. Brown, *Class numbers of real quadratic number fields*, Trans. Amer. Math. Soc. 190 (1974), 99–107.

[3] L. Chua, B. Gunby, S. Park, and A. Yuan, *Proof of a conjecture of Guy on class numbers*, Int. J. Number Theory 11 (2015), 1345–1355.

[4] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, Berlin, 1993.

[5] H. Cohn and G. Cooke, *Parametric form of an eight class field*, Acta Arith. 30 (1976), 367–377.

[6] A. Eustis, *The negs and regs of continued fractions*, senior thesis, Harvey Mudd College, 2006; https://www.math.hmc.edu/seniorthesis/archives/2006/aeustis/aeustis-2006-thesis.pdf.

[7] K. Feng, *Algebraic Number Theory*, Science Press, Beijing, 2000 (in Chinese).

[8] A. Fröhlich and M. J. Taylor, *Algebraic Number Theory*, Cambridge Stud. Adv. Math. 27, Cambridge Univ. Press, Cambridge, 1993.

[9] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 6th ed., edited and revised by D. R. Heath-Brown and J. H. Silverman, Oxford Univ. Press, Oxford, 2008.

[10] F. Herzog, *On the continued fractions of conjugate quadratic irrationalities*, Canad. Math. Bull. 23 (1980), 199–206.

[11] F. E. P. Hirzebruch, *Hilbert modular surfaces*, Enseign. Math. (2) 19 (1973), 183–281.

[12] L.-K. Hua, *Introduction to Number Theory*, Springer, Berlin, 1982.

[13] H. Lu, *Kronecker limit formula of real quadratic fields. I*, Sci. Sinica Ser. A 27 (1984), 1233–1250.

[14] H. Lu, *Hirzebruch sum and class number of the quadratic fields*, Chinese Sci. Bull. 36 (1991), 1145–1147.

[15] H. Lu, *Gauss's Conjectures on Quadratic Number Fields*, Shanghai Scientific and Technical Publ., Shanghai, 1994 (in Chinese).

[16] H. Lu, C. Ji, and R. Jiao, *Kronecker limit formula for real quadratic number fields. III*, Sci. China Ser. A 44 (2001), 1132–1138.

[17] H. Lu and M. Zhang, *On Kronecker limit formula for real quadratic fields. II*, Sci. China Ser. A 32 (1989), 1409–1422.

[18] C. Meyer, *Die Berechnung der Klassenzahl Abelscher Körper über quadratischen Zahlkörpern*, Akademie-Verlag, Berlin, 1957.

[19] O. Perron, *Die Lehre von den Kettenbrüchen. Bd. I. Elementare Kettenbrüche*, 3th ed., B. G. Teubner, Stuttgart, 1954.

[20] H. Rademacher and E. Grosswald, *Dedekind Sums*, Carus Math. Monogr. 16, Math. Assoc. America, Washington, DC, 1972.

[21] J. J. Rotman, *A First Course in Abstract Algebra*, Prentice-Hall, Upper Saddle River, NJ, 1996.

[22] C. L. Siegel, *Advanced Analytic Number Theory*, 2nd ed., Tata Inst. Fund. Res. Stud. Math. 9, Tata Institute of Fundamental Research, Bombay, 1980.

[23] K. S. Williams, *The class number of* $\mathbb{Q}(\sqrt{p})$ *modulo* 4, *for* $p \equiv 5 \pmod 8$ *a prime*, Pacific J. Math. 92 (1981), 241–248.

[24] D. Zagier, *A Kronecker limit formula for real quadratic fields*, Math. Ann. 213 (1975), 153–184.

[25] D. Zagier, *Nombres de classes et fractions continues*, Astérisque 24–25 (1975), 81–97.

Weidong Cheng
Department of Mathematics
Nanjing University
Nanjing, 210093 Jiangsu, China
E-mail: chengwd@smail.nju.edu.cn
*Current address:*
School of Science
Chongqing University of Posts and Telecommunications
Chongqing, 400065 Chongqing, China
E-mail: chengwd@cqupt.edu.cn

Xuejun Guo
Department of Mathematics
Nanjing University
Nanjing, 210093 Jiangsu, China
E-mail: guoxj@nju.edu.cn