On Hasse’s Unit Index

Djordjo Milovic*

Department of Mathematics, University College London

January 22, 2020

Abstract

We study the distribution of Hasse’s unit index $Q(L)$ for the CM-fields $L = \mathbb{Q}(\sqrt{d}, \sqrt{-1})$ as $d$ varies among positive squarefree integers. We prove that the number of $d \leq X$ such that $Q(L) = 2$ is proportional to $X/\sqrt{\log X}$.

2010 Mathematics Subject Classification. 11R27, 11R29, 11R45

1 Introduction

Let $L$ be a CM biquadratic number field and let $K$ be its quadratic subfield. Hasse [6] considered the unit index

$$Q(L) = [U_L : U_K T_L],$$

where $U_K$ and $U_L$ denote the unit groups of the rings of integers of $K$ and $L$, respectively, and $T_L$ denotes the torsion subgroup of $U_L$. In [7, Theorem 1], Lemmermeyer proved that if $|T_L| = 4$, then $Q(L) \in \{1, 2\}$ and

$$Q(L) = 2 \iff 2 \text{ ramifies in } K \text{ and the prime of } K \text{ lying above } 2 \text{ is principal.}$$

The biquadratic CM fields $L$ satisfying $|T_L| = 4$ are in one-to-one correspondence with squarefree integers $d > 1$, with the correspondence given by

$$d \leftrightarrow \mathbb{Q}(\sqrt{d}, \sqrt{-1}).$$

The prime 2 ramifies in $K = \mathbb{Q}(\sqrt{d})$ if and only if $d \not\equiv 1 \mod 4$. In this case, the prime of $K$ lying above 2 is principal only if there exist integers $x$ and $y$ such that

$$x^2 - dy^2 = \pm 2,$$

which can occur only if $\pm 2$ is a square modulo every odd prime $p$ dividing $d$. Hence, with $L = \mathbb{Q}(\sqrt{d}, \sqrt{-1})$, we have

$$Q(L) = 2 \implies d \in \mathcal{D}_2 \text{ or } d \in \mathcal{D}_{-2},$$

*Gower Street, London, WC1E 6BT, United Kingdom, djordjo.milovic@ucl.ac.uk; supported by
where

$$D_2 = \{d > 1 \text{ squarefree and } \not\equiv 1 \mod 4 : p \text{ prime dividing } d \Rightarrow p \not\equiv 3, 5 \mod 8\}$$

and

$$D_{-2} = \{d > 1 \text{ squarefree and } \not\equiv 1 \mod 4 : p \text{ prime dividing } d \Rightarrow p \not\equiv 5, 7 \mod 8\}.$$

These sets are analogous to the set of special discriminants appearing in the work of Fouvry and Klüners in the context of the negative Pell equation [3]. For a subset $\Omega$ of the natural numbers and a real number $X > 0$, we will write $\Omega(X)$ for the set of $n \in \Omega$ such that $n \leq X$. As $X \to \infty$, we have

$$|D_2(X)| \sim \frac{2C_2}{3} \frac{X}{\sqrt{\log X}}$$

and

$$|D_{-2}(X)| \sim \frac{2C_{-2}}{3} \frac{X}{\sqrt{\log X}},$$

where $C_2$ and $C_{-2}$ are positive real numbers defined in (3.1). Setting

$$S = \{d > 1 \text{ squarefree : } Q(L) = 2\},$$

where as before $L = \mathbb{Q}(\sqrt{d}, \sqrt{-1})$, we immediately deduce that

$$|S(X)| \ll \frac{X}{\sqrt{\log X}}.$$

Our main goal is to give a relatively simple proof that $|S(X)| \gg \frac{X}{\sqrt{\log X}}$.

**Theorem 1.** As $X \to \infty$, we have

$$c_1 \frac{X}{\sqrt{\log X}} (1 - o(1)) \leq |S(X)| \leq c_2 \frac{X}{\sqrt{\log X}} (1 + o(1)),$$

where

$$c_1 = \frac{C_2}{6} \prod_{j=1}^{\infty} (1 - 2^{-j}) > 0$$

and

$$c_2 = \frac{2C_2 + 2C_{-2}}{3}.$$

Our proof relies on computing the distribution of the 4-rank of narrow class groups $\text{Cl}^+(8d)$ of the real quadratic fields $\mathbb{Q}(\sqrt{2d})$ for $2d \in D_2$. For $2d \in D_2$, the 4-rank of these groups turns out to be substantially larger on average than the 4-rank of narrow class groups of real quadratic fields; compare [2] (7), p. 458 to (5.1). As a result, unlike in the case of generic real quadratic fields, it is not possible to deduce a positive proportion of $2d \in D_2$ with 4-rank of $\text{Cl}^+(8d)$ equal to 0 by simply studying the first moment of the 4-rank. We thus compute the full distribution of the 4-rank of $\text{Cl}^+(8d)$ via the method of moments developed by Fouvry and Klüners [2]. The implementation of this method to the family of $2d \in D_2$ necessitates a new combinatorial argument.

For stronger results on the Hasse unit index in the context of certain thin families of discriminants, see [8, Corollary 3, p. 2]. Finally, although our work concerns the same biquadratic fields as those appearing in the recent work [5], our results have been developed independently.
2 Algebraic preliminaries

2.1 Criteria for solvability over \( \mathbb{Z} \)

Given a fundamental discriminant \( D \), let \( \text{Cl}^+(D) \) denote the narrow class group of the quadratic number field \( \mathbb{Q}(\sqrt{D}) \). We will denote the group operation in \( \text{Cl}^+(D) \) by multiplication, as it is induced by multiplication of ideals. The Artin map gives a canonical isomorphism

\[
\text{Art} : \text{Cl}^+(D) \rightarrow \text{Gal}(H_D/\mathbb{Q}(\sqrt{D})),
\]

where \( H_D \) is the maximal abelian extension of \( \mathbb{Q}(\sqrt{D}) \) that is unramified at all finite primes. Between \( \mathbb{Q}(\sqrt{D}) \) and \( H_D \) lies the genus field of \( \mathbb{Q}(\sqrt{D}) \), which we denote by \( G_D \). It is the subfield of \( H_D \) fixed by the image of the squares in the narrow class group, i.e.,

\[
G_D = H_D^{\text{Art}([\text{Cl}^+(D)])^2},
\]

and it can also be characterized as the maximal abelian extension of \( \mathbb{Q} \) contained in \( H_D \).

Being able to compute the restriction of the image of the Artin map to \( G_D \) allows us to check if a given ideal class in \( \text{Cl}^+(D) \) is a square. Indeed, if we denote the class of an ideal \( \mathfrak{a} \) by \([\mathfrak{a}]\), then we have

\[
[a] \in \text{Cl}^+(D)^2 \iff \text{Art}(a)|_{G_D} = 1. \tag{2.1}
\]

Let \( p_1, \ldots, p_t \) denote the primes dividing \( D \), with \( p_2, \ldots, p_t \) odd. Then \( G_D \) can be generated as the mutiquadratic field

\[
G_D = \mathbb{Q}(\sqrt{D}, \sqrt{p_2^2, \ldots, \sqrt{p_t^2}}),
\]

where, for an odd prime \( p \), we write

\[
p^* = (-1)^{(p-1)/2}p = \left(\frac{-1}{p}\right)p.
\]

Here and henceforth, \( (\cdot) \) denotes the Jacobi symbol. Note that

\[
\text{Gal}(G_D/\mathbb{Q}(\sqrt{D})) \cong \mathbb{F}_2^{t-1} \quad \text{and} \quad |G_D : \mathbb{Q}(\sqrt{D})| = 2^{t-1}. \tag{2.2}
\]

The 2-torsion subgroup of \( \text{Cl}^+(D) \) is generated by the classes of the prime ideals \( p_1, \ldots, p_t \) lying above \( p_1, \ldots, p_t \), respectively. For each \( \mathfrak{e} = (e_1, \ldots, e_t) \in \mathbb{F}_2^t \), we define the ideal \( \mathfrak{a}_e = p_1^{e_1} \cdots p_t^{e_t} \), and we write \( a_e \) for the absolute norm of \( \mathfrak{a}_e \). By (2.2), there exists a unique non-zero \( \mathfrak{e} \in \mathbb{F}_2^t \) such that the class of \( \mathfrak{a}_e \) is trivial. Supposing for simplicity that \( D \equiv 0 \pmod{4} \) and setting \( d = D/4 \), we see that the equation \( x^2 - dy^2 = a_e \) is solvable over \( \mathbb{Z} \) for exactly one non-zero \( e \in \mathbb{F}_2^t \). Since \( a_e \) varies over the positive squarefree divisors of \( D \) as \( e \) varies over \( \mathbb{F}_2^t \), we see that there exists exactly one squarefree integer \( a > 1 \) such that \( a \) divides \( D \) and such that \( x^2 - dy^2 = a \) is solvable over \( \mathbb{Z} \).

Now suppose that \( D = da \) or \( D = 4da \), where \( d \) and \( a \) are coprime positive squarefree integers, and consider the equation

\[
x^2 - day^2 = a. \tag{2.3}
\]

Let \( \mathfrak{a} \) be the unique ideal of the form \( \mathfrak{a}_e \) as above of absolute norm \( a \). Then (2.3) is solvable over \( \mathbb{Z} \) if and only if the class of \( \mathfrak{a} \) is trivial in \( \text{Cl}^+(D) \). Suppose that the class of \( \mathfrak{a} \) is a square in \( \text{Cl}^+(D) \). Since \([\mathfrak{a}]\) is a 2-torsion element in \( \text{Cl}^+(D) \), this indicates the existence of
an element of order 4 in \( \text{Cl}^+(D) \), unless of course \([a]\) is trivial. Therefore, if \([a] \in \text{Cl}^+(D)^2\) and \( \text{Cl}^+(D) \) has no elements of order 4, then \([a]\) must be trivial and hence the equation (2.3) must be solvable over \( \mathbb{Z} \).

Similarly, consider the equation

\[
x^2 - day^2 = -a,
\]

solvable over \( \mathbb{Z} \) if and only if \( x^2 - day^2 = d \) is solvable over \( \mathbb{Z} \). Let \( \mathfrak{a} \) be the unique ideal of the form \( a_{e} \) as above of absolute norm \( d \). Similarly as above, if \([\mathfrak{a}] \in \text{Cl}^+(D)^2\) and \( \text{Cl}^+(D) \) has no elements of order 4, then \([\mathfrak{a}]\) must be trivial and hence the equation (2.4) must be solvable over \( \mathbb{Z} \).

With \( a = 2 \), these observations lead us to the following propositions for the solvability of (1.1).

**Proposition 2.1.** Let \( d \) be a positive odd squarefree integer. Suppose that

- the narrow class group of \( \mathbb{Q}(\sqrt{2d}) \) has no elements of order 4, and
- \( \left( \frac{d}{p} \right) = 1 \) for all primes \( p \) dividing \( d \).

Then the equation

\[
x^2 - 2dy^2 = 2
\]

has a solution in integers \( x \) and \( y \).

**Proof.** Suppose that \( d = p_1 \cdots p_r \). Let \( p_i \) (resp. \( t \)) denote the ideal of \( \mathbb{Z}[\sqrt{2d}] \) lying above \( p_i \) (resp. 2). Let \( D = 8d \) be the discriminant of \( \mathbb{Q}(\sqrt{2d}) \). By the first assumption and the observation above, it suffices to show that in each case we have \([t] \in \text{Cl}^+(D)^2\). By (2.1), \([t] \in \text{Cl}^+(D)^2\) if and only if \( \text{Art}(t)|_{G_D} = 1 \).

We have

\[
G_D = \mathbb{Q}(\sqrt{2\varepsilon}, \sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_r}),
\]

where

\[
\varepsilon = (-1)^{(d-1)/2} \in \{\pm 1\}.
\]

The prime \( t \) splits in \( \mathbb{Q}(\sqrt{2\varepsilon}, \sqrt{2d}) \) if and only if \( d\varepsilon \equiv \pm 1 \bmod 8 \), i.e., if and only if \( d \equiv \pm 1 \bmod 8 \). Moreover, \( t \) splits in \( \mathbb{Q}(\sqrt{2d}, \sqrt{p_i}) \) if and only if \( p_i \equiv \pm 1 \bmod 8 \), i.e., if and only if \( p_i \equiv \pm 1 \bmod 8 \). Thus \( \text{Art}(t)|_{G_D} \) can be viewed as the element

\[
\left( \left( \frac{2}{d} \right), \left( \frac{2}{p_1} \right), \ldots, \left( \frac{2}{p_r} \right) \right)
\]

of

\[
\Gamma = \text{Gal}(G_D/\mathbb{Q}(\sqrt{D})) \cong \{(a_1, \ldots, a_{r+1}) \in \{\pm 1\}^{r+1} : a_1 \cdots a_{r+1} = 1\}.
\]

Hence \([t] \in \text{Cl}^+(D)^2\) if and only if

\[
\left( \frac{2}{p_i} \right) = 1 \quad \text{for all } i.
\]
Proposition 2.2. Let \( d \) be a positive odd squarefree integer. Suppose that

- the narrow class group of \( \mathbb{Q}(\sqrt{2d}) \) has no elements of order 4, and
- \( \left( \frac{-2}{p} \right) = 1 \) for all odd primes \( p \) dividing \( d \).

Then the equation

\[
x^2 - 2dy^2 = -2
\]

has a solution in integers \( x \) and \( y \).

Proof. Let \( p_i, p_1, t, D, r, \varepsilon, \text{ and } \Gamma \) be as in the proof of Proposition 2.1. Let \( \mathfrak{d} = p_1 \cdots p_r \). By the first assumption and the observation above, it suffices to show that in each case we have \( \mathfrak{b} \in \text{Cl}^+(D)^2 \). By [2,1], \( \mathfrak{b} \in \text{Cl}^+(D)^2 \) if and only if

\[
\text{Art}(\mathfrak{d})|_{G_D} = \text{Art}(p_1)|_{G_D} \cdots \text{Art}(p_r)|_{G_D} = 1.
\]

The Artin symbol \( \text{Art}(p_i)|_{G_D} \) viewed as an element of \( \Gamma \) is equal to

\[
\left( \frac{2\varepsilon}{p_i} \right), \left( \frac{p_i^*}{p_i} \right), \ldots, \left( \frac{2d/p_i^*}{p_i} \right), \left( \frac{p_i^{r+1}}{p_i} \right), \ldots, \left( \frac{p_r^*}{p_i} \right).
\]

Then, by multiplicativity of the Artin symbol, we have

\[
\text{Art}(\mathfrak{d})|_{G_D} = \left( \frac{2\varepsilon}{d} \right), \left( \frac{p_1^*}{d/p_1} \right), \ldots, \left( \frac{2d/p_r^*}{p_r} \right) \in \Gamma.
\]

Hence \( \mathfrak{b} \in \text{Cl}^+(D)^2 \) if and only if

\[
\left( \frac{2\varepsilon}{d} \right) = 1
\]

and

\[
1 = \left( \frac{p_i^*}{d/p_i} \right) \left( \frac{2d/p_i^*}{p_i} \right) = \left( \frac{d/p_i}{p_i} \right) \left( \frac{2d/p_i^*}{p_i} \right) = \left( \frac{2}{p_i} \right) \left( \frac{-1}{p_i} \right) = \left( \frac{-2}{p_i} \right) \quad \text{for all } i,
\]

where the second equality follows from the law of quadratic reciprocity. Of course, as the product of the \( r + 1 \) entries of \( \text{Art}(\mathfrak{d})|_{G_D} \in \Gamma \) is equal to 1, the condition (2.5) implies that \( \left( \frac{2\varepsilon}{d} \right) = 1 \). \( \square \)

2.2 Formula for the 4-rank

Let \( D \) be a fundamental discriminant. In [2], Fouvry and Klüners give the following formula for the 4-rank of \( \text{Cl}^+(D) \), i.e., for the quantity

\[
| \text{Cl}^+(D)^2 / \text{Cl}^+(D)^4 | =: 2^{4k_D} \text{Cl}^+(D).
\]

We are interested in the fields \( \mathbb{Q}(\sqrt{2d}) \). Writing \( D = 8d \) with \( d \) odd and squarefree, Fouvry and Klüners [2, (111), p. 503] prove that

\[
2^{4k_D} \text{Cl}^+(8d) = \frac{1}{2} \cdot 2^{\omega(d)} \sum_{d=D_0D_1D_2D_3} \left( \frac{2}{D_3} \right) \left( \frac{D_2}{D_0} \right) \left( \frac{D_1}{D_3} \right) \left( \frac{D_0}{D_3} \right) \left[ \left( \frac{-1}{D_0} \right) + \left( \frac{-1}{D_3} \right) \right].
\]

Here the sum is over 4-tuples of positive integers \( (D_0, D_1, D_2, D_3) \) such that \( D_0D_1D_2D_3 = d \). Now suppose that \( 2d \in \mathcal{D}_2 \), so that every prime \( p \) dividing \( d \) satisfies \( \left( \frac{2}{p} \right) = 1 \). Then the factor
such that $d^2$ ensues. The ensuing formula allows us to rewrite (2.6) for $2d \in \mathcal{D}_2$ as

$$2^r k_4 \mathcal{C}_1^+(8d) = \frac{1}{2^{\omega(d)}} \sum_{d = D_0 D_1 D_2 D_3} \left( -1 \right) \left( \frac{D_2}{D_0} \right) \left( \frac{D_1}{D_3} \right) \left( \frac{D_0}{D_3} \right),$$

(2.7)

where now the sum is over 4-tuples of positive integers $(D_0, D_1, D_2, D_3)$ such that $D_0 D_1 D_2 D_3 = d \in \mathcal{D}_2$.

Relabelling the indices in (2.7) as in [2] by converting them into their binary expansions, so that $D_0$ becomes $D_{00}$, $D_1$ becomes $D_{01}$, etc., we obtain

$$2^r k_4 \mathcal{C}_1^+(8d) = \frac{1}{2^{\omega(d)}} \sum_{d = D_{00} D_{01} D_{10} D_{11}} \left( \prod_{u \in \mathbb{F}_2^2} \left( -1 \right) \left( \frac{D_u}{D_1} \right) \right) \left( \prod_{(u, v) \in \mathbb{F}_2^2} \left( \frac{D_u}{D_v} \right) \Phi_1(u, v) \right),$$

(2.8)

where $\lambda_1$ is the $\mathbb{F}_2$-valued function defined by

$$\lambda_1(u) = u_1 u_2, \quad u = (u_1, u_2).$$

(2.9)

We will compute the average of $k$th moments of $2^r k_4 \mathcal{C}_1^+(8d)$ as $2d$ varies among elements of $\mathcal{D}_2$ such that $d \equiv 3 \mod 4$. We remark that when $2d \in \mathcal{D}_2$ and $d \equiv 1 \mod 4$, then $r k_4 \mathcal{C}_1^+(8d) \geq 1$, and so Proposition 2.1 cannot be applied for such $d$.

Raising both sides of (2.8) to the $k$th power and decomposing the summation variables into products of their mutual greatest common denominators, as in [2] (22), p. 471], we obtain the following analogue of [2, Lemma 28, p. 493]:

$$S(X, k; 3, 4) := \sum_{2d \in \mathcal{D}_2(X)} 2^r k_4 \mathcal{C}_1^+(8d) = \sum_{(D_u)} \left( 2^{-k \omega(D_u)} \right) \left( \prod_{u \in \mathbb{F}_2^2} \left( -1 \right) \left( \frac{D_u}{D_1} \right) \right) \left( \prod_{u, v \in \mathbb{F}_2^2} \left( \frac{D_u}{D_v} \right) \Phi_k(u, v) \right),$$

(2.10)

where the sum is over $4^k$-tuples $(D_u)$ of integers $D_u \in \mathcal{D}_2$ indexed by elements $u$ of $\mathbb{F}_2^{2k}$ and satisfying

$$\prod_{u \in \mathbb{F}_2^{2k}} D_u \leq X/2, \quad \prod_{u \in \mathbb{F}_2^{2k}} D_u \equiv 3 \mod 4;$$

where the function $\lambda_k : \mathbb{F}_2^{2k} \rightarrow \mathbb{F}_2$ is defined by

$$\lambda_k(u) = \sum_{j=0}^{k-1} u_{2j+1} u_{2j+2};$$

(2.11)

and where the function $\Phi_k : \mathbb{F}_2^{2k} \times \mathbb{F}_2^{2k} \rightarrow \mathbb{F}_2$ is defined by

$$\Phi_k(u_1, \ldots, u_{2k}, v_1, \ldots, v_{2k}) = \Phi_1(u_1, u_2, v_1, v_2) + \cdots + \Phi_1(u_{2k-1}, u_{2k}, v_{2k-1}, v_{2k})$$

(2.12)

$$= (u_1 + v_1)(u_1 + v_2) + \cdots + (u_{2k-1} + v_{2k-1})(u_{2k-1} + v_{2k}).$$

(2.13)
3 Analytic preliminaries

We first state the asymptotic formulas for the size of \( D_{\pm 2}(X) \). Recall that we defined the sets

\[
D_{\pm 2} = \{ d > 1 \text{ squarefree and } \not\equiv 1 \mod 4 : \left( \frac{\pm 2}{p} \right) = 1 \text{ for all odd primes } p|d \}.
\]

Define the sets

\[
P_{\pm 2} = \{ p \text{ prime number} : \text{if } p \text{ is odd, then } \left( \frac{\pm 2}{p} \right) = 1 \}.
\]

and define the positive constants

\[
C_{\pm 2} = \frac{1}{\sqrt{\pi}} \lim_{s \to 1} \left( \sqrt{s-1} \prod_{p \in P_{\pm 2}} \left( 1 + \frac{1}{p^s} \right) \right).
\]

Then, similarly as in [9], one can use results from [10] to deduce that

\[
D_{\pm 2}(X) = 2C_{\pm 2} 3^\frac{1}{2} X \sqrt{\log X} + O \left( \frac{X}{(\log X)^{\frac{1}{2}}} \right),
\]

where the implied constant is absolute. Again as in [9], we can refine these formulas by restricting to congruence classes. The particular asymptotic formula that we need is

\[
A(X; 3, 4) := |\{2d \in D_2 : d \leq X/2, d \equiv 3 \mod 4\}| \sim \frac{C_2}{6} X \sqrt{\log X}.
\]

The treatment of \( S(X; 2; 3, 4) \), which is by now standard due to the work of Fouvry and Klüners [2, 3, 4] and Park [9], proceeds in several steps, culminating in the following formula analogous to [2, Proposition 5, p. 483]:

\[
S(X, k; 3, 4) = A(X; 3, 4) \cdot 2^{1-2k} \sum_{\mathcal{U}} \gamma^+(\mathcal{U}, 1) + O_e \left( X(\log X)^{-\frac{1}{2} - \frac{1}{2k} + \epsilon} \right)
\]

where the sum is over all maximal unlinked subsets \( \mathcal{U} \) of \( \mathbb{F}_2^k \) and where \( \gamma^+(\mathcal{U}) \) is defined as in [2] (81), p. 493], i.e.,

\[
\gamma^+(\mathcal{U}, 1) = \sum_{(h_u)_{u \in \mathcal{U}}} \left( \prod_{u \in \mathcal{U}} (-1)^{h_u} \frac{h_u - 1}{2} \right) \left( \prod_{u, v} (-1)^{\Phi_k(u,v) \cdot \frac{h_u - 1}{2} \cdot \frac{h_v - 1}{2}} \right),
\]

where the sum is over \((h_u)_{u \in \mathcal{U}} \in \{\pm 1 \mod 4\}^{2k} \) satisfying \( \prod_{u \in \mathcal{U}} h_u \equiv 3 \mod 4 \) and where the last product is over unordered pairs \( \{u, v\} \subset \mathcal{U} \). We recall that two indices \( u \) and \( v \) in \( \mathbb{F}_2^k \) are said to be unlinked if \( \Phi(u, v) = \Phi(v, u) \).

We will now say a few words about the derivation of the formula (3.3). First, the sum \( S(X, k; 3, 4) \) is estimated by (i) bounding the contribution of terms where the number of prime factors of \( D_u \) is too large, as in [2] Section 5.3], (ii) partitioning the tuples \( \{D_u\} \) into “diadic” boxes of reasonable size, as in [2] Section 5.4, p. 474-475], (iii) bounding the contribution from boxes featuring “double oscillation” of characters, as in [2] Section 5.4, p. 476], and
(iv) bounding the contribution from boxes featuring linked variables of vastly different sizes, as in [2, Section 5.4, p. 476-478]. Once this is accomplished, we arrive at an analogue of [2, Proposition 3, p. 479], at which point we partition the sum according to the congruence classes of $D_u$ modulo 4. We then use quadratic reciprocity to pull out the factor $\sum U \gamma^+(U, 1)$. Via a variant of the prime number theorem, as in [2, Lemma 19, p. 480] or [9, Lemma 6.3, p. 21], we then remove the congruence conditions on the $D_u$ modulo 4, which recovers $A(X; 3, 4)$ but comes with the cost of a factor of $2^{k-1}$ (as $\prod U D_u \equiv 3 \mod 4$, fixing $2^k - 1$ of the variables $D_u$ modulo 4 determines the remaining variable modulo 4).

4 Combinatorics of the coefficient of the main term

In this section, we analyze the coefficients of the main terms in the asymptotic formulas for the $k$th moments of the 4-rank.

As in [2] (87), for $\nu \in \mathbb{F}_2$, we let

$$\gamma^+(U, \nu) = \sum_{S \subseteq U, s \equiv \nu \mod 2} (-1)^{e^+(S)},$$

where

$$e^+(S) = \sum_{u \in S} \lambda_k(u) + \sum_{u, v} \Phi(u, v),$$

where the last sum is over unordered pairs $\{u, v\} \subseteq U$. This generalizes the quantity $\gamma^+(U, 1)$, which we aim to compute. The argument in [2, Section 6] culminates in the formula [2, (105), p. 499]

$$\sum U \gamma^+(U, 0) = 2^{k-1} (N(k+1, 2) - N(k, 2)).$$

Here, as in [2], $N(m, 2)$ denotes the total number of $\mathbb{F}_2$-vector subspaces of $\mathbb{F}_2^m$. We will now adapt this argument to show that

$$\sum U \gamma^+(U, 1) = 2^{k-1} N(k, 2). \quad (4.1)$$

The same argument as that for [2] (101), p. 498] yields the formula

$$\sum U \gamma^+(U, 1) = 2^{-k} \sum_{U_0 \text{ good}} \sum_{c \in \mathbb{F}_2^{2k}} \sum_{s \text{ odd}} (-1)^{\lambda_k(s)}.$$

Consider the group homomorphism

$$\mu : \mathcal{P}(c + U_0) \to U_0 \oplus (c + U_0) \quad (4.2)$$

given by

$$\mu(S) = \sigma.$$

We check that $\mu$ is surjective. First, note that $\mu(\emptyset) = 0$. If $\sigma \in U_0 \setminus \{0\}$, then $\mu(c, c + \sigma) = \sigma$. Finally, if $c + \sigma \in c + U_0$, then $\mu(c + \sigma) = c + \sigma$. Hence, counting the cardinalities of the
domain and the codomain of $\mu$, we find that each fiber of $\mu$ has cardinality $2^k/2^{k+1} = 2^{k-1}$. Also note that the image of $P_1(\mathbf{c} + U_0)$ under $\mu$ is exactly $\mathbf{c} + U_0$. This implies that
\[
\sum_{\mathcal{U}} \gamma^+(\mathcal{U}, 1) = 2^{2k-k-1} \sum_{\mathcal{U}_0 \text{ good}} \sum_{c \in \mathbb{F}_2^k} \sum_{\sigma \in \mathbb{F}_2} (-1)^{\lambda_k(\sigma)}.
\]
Since $U_0$ is a $k$-dimensional vector subspace of $\mathbb{F}_2^k$, for each coset $\mathcal{U}$ of $U_0$ in $\mathbb{F}_2^k$, there are exactly $2^k$ vectors $c \in \mathbb{F}_2^k$ such that $\mathcal{U} = \mathbf{c} + U_0$. Hence
\[
\sum_{\mathcal{U}} \gamma^+(\mathcal{U}, 1) = 2^{2k-k-1} \sum_{\mathcal{U}_0 \text{ good}} \sum_{\mathcal{U} \text{ coset of } U_0} \sum_{\sigma \in \mathbb{F}_2^k} (-1)^{\lambda_k(\sigma)}
= 2^{2k-k-1} \sum_{\mathcal{U}_0 \text{ good}} \sum_{\sigma \in \mathbb{F}_2^k} (-1)^{\lambda_k(\sigma)}
= 2^{2k-k-1} N(k, 2) \sum_{\sigma \in \mathbb{F}_2^k} (-1)^{\lambda_k(\sigma)}.
\]
It remains to compute $\sum_{\sigma \in \mathbb{F}_2^k} (-1)^{\lambda_k(\sigma)}$. Recall that $\lambda_k(\sigma) = \sum_{j=0}^{k} \sigma_{2j+1} \sigma_{2j+2}$. Let
\[
m(\sigma) = \#\{j \in \{0, \ldots, k-1\} : \sigma_{2j+1} = \sigma_{2j+2} = 1\},
\]
so that $\lambda_k(\sigma) \equiv m(\sigma) \mod 2$. For each $m \in \{0, \ldots, k\}$, the number of $\sigma \in \mathbb{F}_2^k$ such that $m(\sigma) = m$ is equal to
\[
\binom{k}{m} \cdot 3^{k-m},
\]
since for each of the $k-m$ choices of $j$ for which $(\sigma_{2j+1}, \sigma_{2j+2}) \neq (1, 1)$, the pair $(\sigma_{2j+1}, \sigma_{2j+2})$ can take one of three possible values, namely $(0, 0)$, $(0, 1)$, and $(1, 0)$. Thus
\[
\sum_{\sigma \in \mathbb{F}_2^k} (-1)^{\lambda_k(\sigma)} = \sum_{m=0}^{k} \binom{k}{m} \cdot 3^{k-m} \cdot (-1)^m = (3 - 1)^k = 2^k,
\]
by the binomial theorem. In conclusion, we find that
\[
\sum_{\mathcal{U}} \gamma^+(\mathcal{U}, 1) = 2^{2k-k-1} N(k, 2) \cdot 2^k = 2^{2k-1} N(k, 2),
\]
as was claimed in (4.1).

5 Conclusion of the proof of Theorem

Substituting (4.1) into (3.3), we obtain the asymptotic
\[
S(X, k; 3, 4) \sim N(k, 2) \cdot A(X; 3, 4).
\]
Note that the average of the $k$th moment for $2d \in D_2$ with $d \equiv 3 \mod 4$ is the same as the average of the $k$th moment for general negative discriminants; see [2 Equations (4), (6), (8)].
Putting the formula (5.1) for the $k$th moments through the machinery in [1] or [3, Section 2, p. 2046-2049], we deduce that for each integer $r \geq 0$, we have

$$|\{2d \in D_2 : d \leq X/2, d \equiv 3 \mod 4, \text{rk}_4 \text{Cl}^+(8d) = r\}| \sim 2^{-r^2} \eta_\infty(2) \eta_r(2)^{-2} A(X; 3, 4), \ (5.2)$$

where

$$\eta_k(2) = \prod_{j=1}^{k} (1 - 2^{-j}) \text{ for } k = r, \infty.$$ 

This is the same distribution as that for the 4-rank of class groups of imaginary quadratic fields. Using (5.2) with $r = 0$ in conjunction with Proposition 2.1, we conclude that

$$|S(X)| \gg \eta_\infty(2) A(X; 3, 4) \gg \eta_\infty(2) C_2^2 \frac{X}{\sqrt{\log X}},$$

as was to be shown.

**Acknowledgements**

The author is supported by ERC grant agreement No. 670239.

**References**

[1] É. Fouvry and J. Klüners. Cohen-Lenstra heuristics of quadratic number fields. In *Algorithmic number theory*, volume 4076 of *Lecture Notes in Comput. Sci.*, pages 40–55. Springer, Berlin, 2006.

[2] É. Fouvry and J. Klüners. On the 4-rank of class groups of quadratic number fields. *Invent. Math.*, 167(3):455–513, 2007.

[3] É. Fouvry and J. Klüners. On the negative Pell equation. *Ann. of Math. (2)*, 172(3):2035–2104, 2010.

[4] É. Fouvry and J. Klüners. The parity of the period of the continued fraction of $\sqrt{d}$. *Proc. Lond. Math. Soc. (3)*, 101(2):337–391, 2010.

[5] É. Fouvry and P. Koymans. On Dirichlet biquadratic fields. *arXiv e-prints*, page arXiv:2001.05350, Jan 2020.

[6] H. Hasse. *Über die Klassenzahl abelscher Zahlkörper*. Springer-Verlag, Berlin, first edition, 1985. With an introduction to the reprint edition by Jacques Martinet.

[7] F. Lemmermeyer. Ideal class groups of cyclotomic number fields. I. *Acta Arith.*, 72(4):347–359, 1995.

[8] D. Z. Milovic. On the equations $x^2 - 2py^2 = -1, \pm 2$. *arXiv e-prints*, page arXiv:1812.02650, Dec 2018.

[9] J. Park. On the parity of ideal classes over a fixed prime. *Amer. J. Math.*, 142(1):1–27, 2020.
[10] G. Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 163 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, third edition, 2015. Translated from the 2008 French edition by Patrick D. F. Ion.