ON THE DENSITY FOR SEVERI-BRAUER CONICS AND PERIOD-INDEX DISTRIBUTIONS FOR ELLIPTIC CURVES

CHUANGXUN CHENG, CHENG NIU, AND XIAOGUANG SHANG

Abstract. Let K be a number field with class number 1. In this paper, we study the family of Severi-Brauer conics over K defined by equations $z^2 - ax^2 - by^2 = 0$, where $(a,b) \in K^*/(K^*)^2 \times K^*/(K^*)^2$. We prove that, within this family, the density of the conics admitting at least one nontrivial K-rational point is zero. As an application, for an elliptic curve E/K satisfying $E(K) \supset E[4]$, we show that the subset of $H^1(K,E)[2]$ consisting of classes with equal period and index has density zero. This is closely related to the question proposed in [3, Problem 2].

1. Introduction

Let K be a number field with class number 1. In this paper, we prove that within the family of Severi-Brauer conics parameterized by $K^*/(K^*)^2 \times K^*/(K^*)^2$, the density (cf. Definition 1.1) of the conics admitting at least one nontrivial K-rational point is zero. Our motivation originates from a period-index distribution problem for elliptic curves (cf. [3, Problem 2]). Through O'Neil's obstruction map (cf. Equation (3.3)), which coincides with the Hilbert symbol in our setting, we establish a connection between the period-index distribution problem and the density problem for Severi-Brauer conics. Furthermore, we clarify part of [3, Problem 2] and give an answer for the case that $P = 2$ for number fields with class number 1.

We fix some notation and explain our main results in the following. Let K be a number field. For each pair $(a,b) \in K^* \times K^*$, the associated *Severi-Brauer conic* is defined by the homogeneous equation $z^2 - ax^2 - by^2 = 0$. We study the density of such conics that have at least one nontrivial K-rational point. In the case that K has class number 1, for each prime ideal $\mathfrak{p} \subseteq \mathscr{O}_K$, we fix a generator π of $\mathfrak{p}$ and call π a *prime* of $\mathscr{O}_K$. We say that π is an *odd* prime if $2 \notin (\pi)$. Every $x \in K^*$ admits a unique factorization of the form

$$x = u\pi_1^{\alpha_1}\pi_2^{\alpha_2}\cdots\pi_n^{\alpha_n}, \tag{1.1}$$

where $\alpha_i \in \mathbb{Z}$, $u \in \mathscr{O}_K^*$ and π_i are distinct primes of K. Let $U = \{1,\ u_2, \cdots,\ u_r\} \subseteq \mathscr{O}_K^*$ be a system of representatives of the quotient group $\mathscr{O}_K^*/(\mathscr{O}_K^*)^2$, where 1 is the representative of the identity element. For any $[a] \in K^*/(K^*)^2$, we choose a representative $a \in K^*$ of the form $a = u_a\pi_1\pi_2\cdots\pi_n$, where $u_a \in U$ and π_i are distinct primes of K. This construction gives a one-to-one correspondence ϕ between $K^*/(K^*)^2$ and the set of "square-free numbers":

$$\Sigma_K := \{a \in K^* \mid a = u\prod_{i=1}^{n}\pi_i,\ u \in U,\ \pi_i \text{ are distinct primes}\}.$$

2020 *Mathematics Subject Classification.* 11D09, 11N37, 11G05.

Key words and phrases. Severi-Brauer conics, Hilbert symbol, period-index problem, elliptic curves.

The authors are supported by NSFC 11701272.

In the following, for any $[a] \in K^*/(K^*)^2$, the image of $[a]$ under ϕ is denoted by a.

Definition 1.1. Let K be a number field with class number 1. For $X \in \mathbb{R}_{>0}$, define

$$\Sigma_K^X := \{a \in \Sigma_K \mid -X \leq N(a) \leq X\},$$

and

$$\Sigma_K^{H,X} := \left\{(a,b) \in \Sigma_K^X \times \Sigma_K^X \mid (a,b)_{H,K} = 1\right\},$$

where $(a,b)_{H,K}$ is the Hilbert symbol (cf. Definition 2.1) and N is the field norm $N_{K/\mathbb{Q}}$. The *rational density* of Severi-Brauer conics over K is defined by

$$\delta_{H,K} := \limsup_{X\to+\infty} \frac{|\Sigma_K^{H,X}|}{|\Sigma_K^X|^2}.$$

Our main result is the following theorem.

Theorem 1.2. *Let K be a number field with class number 1. The rational density of Severi–Brauer conics over K is zero.*

As an immediate application to the period-index problem discussed in Section 3, we obtain the following result. See Theorem 3.4 for the precise meaning of density.

Theorem 1.3. *Let K be a number field with class number 1, and let E/K be an elliptic curve with $E(K) \supset E[4]$. Then in $H^1(K,E)[2]$, the density of the subset of classes with coinciding period and index is zero.*

In Section 2, we review basic notions of the Hilbert symbol and prove Theorem 1.2 through analytic number theory techniques.

In Section 3, we review basic notions of period and index of homogeneous spaces for elliptic curves and prove Theorem 3.4, by relating the rational density (cf. Definition 1.1) and the period-index density (cf. Definition 3.3) via O'Neil's obstruction map (cf. Equation (3.3)).

Notation Let $f(x)$ and $g(x)$ be functions defined on $\mathbb{Z}_{>0}$. We employ the following asymptotic notation:

- $f(x) = O(g(x))$ if $\exists\, C > 0$ such that $|f(x)| \leq C|g(x)|$;
- $f(x) = o(g(x))$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$;
- $f(x) \sim g(x)$ if $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

Let K be a number field:

- $\mathcal{O}_K$ denotes the ring of integers of K;
- For an ideal $\mathfrak{a} \subseteq \mathcal{O}_K$, $\omega(\mathfrak{a})$ denotes the number of distinct prime ideal divisors of $\mathfrak{a}$;
- For $a \in \mathcal{O}_K$, $\omega(a) := \omega((a))$;

- $N(\alpha)$ denotes the field norm $N_{K/\mathbb{Q}}(\alpha)$ for $\alpha \in K^*$, and $N(\mathfrak{a})$ denotes the ideal norm $N_{K/\mathbb{Q}}(\mathfrak{a})$ for ideals $\mathfrak{a} \subseteq \mathcal{O}_K$;
- Let K be of degree $n = r_1 + 2r_2$, where r_1 denotes the number of real embeddings and r_2 the number of conjugate pairs of complex embeddings. For $\alpha \in K$, let $\alpha^{(i)}$ $(1 \le i \le r_1)$ denote its real embeddings, and $\alpha^{(j)}$ $(r_1 + 1 \le j \le r_1 + r_2)$ denote a fixed choice of non-conjugate complex embeddings.

For every $v = (v_1, \cdots, v_n) \in \mathbb{R}^n$, $\|v\| := \sqrt{(v_1)^2 + \cdots + (v_n)^2}$.

2. The Hilbert symbol and the rational density

In this section, we provide necessary background on the Hilbert symbol (cf. [16, Chapter 14]) connecting the period-index problem in Section 3 with Theorem 1.2. We then proceed to prove Theorem 1.2, utilizing the computability of Hilbert symbols alongside tools from analytic number theory.

Fix a positive integer n, and let K be a field of characteristic 0 that contains an n-th primitive root of unity. It is well known that $K^*/(K^*)^n \cong H^1(K, \mathbb{Z}/n\mathbb{Z}) \cong \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K), \mathbb{Z}/n\mathbb{Z})$. Thus for any $a \in K^*$, we can associate a character $\chi_a \in H^1(K, \mathbb{Z}/n\mathbb{Z})$.

Definition 2.1. Let $\mathrm{Br}(K)$ be the Brauer group of K and let $\mathrm{Br}(K)[n]$ be its n-torsion subgroup. For $a,\ b \in K^*$, define the symbol $(a, b)_{H_n,K} \in \mathrm{Br}(K)[n]$ to be the cup product

$$b \cup \delta(\chi_a),$$

where $b \in H^0(K, \overline{K}^*) = K^*$, $\chi_a \in H^1(K, \mathbb{Z}/n\mathbb{Z}) \subset H^1(K, \mathbb{Q}/\mathbb{Z})$ and $\delta : H^1(K, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\cong} H^2(K, \mathbb{Z})$ is the connecting homomorphism.

The symbol is a bilinear map from $K^* \times K^*$ to $\mathrm{Br}(K)[n]$. In fact, it induces a bilinear map $(\ ,\ )_{H_n,K}$ from $K^*/(K^*)^n \times K^*/(K^*)^n$ to $\mathrm{Br}(K)[n]$. We call it the *Hilbert symbol* over K. When $n = 2$, we denote $(\ ,\ )_{H_2,K}$ by $(\ ,\ )_{H,K}$. The following proposition gives a necessary and sufficient condition for this Hilbert symbol to be trivial. (cf. [16, Ch. 14, Sec. 2, Prop. 4] or [17, Chapter 3]).

Proposition 2.2. *Let K be a field of characteristic 0. Let $a, b \in K^*$. Then $(a, b)_{H,K} = 1$ if and only if b is a norm of the extension $K(a^{1/2})/K$. In other words, $(a, b)_{H,K} = 1$ if and only if the conic $z^2 - ax^2 - by^2 = 0$ has a nontrivial K-rational point.*

Let $\pi \in \mathcal{O}_K$ be a prime of $\mathcal{O}_K$. For any $a \in \mathcal{O}_K$, define $\left(\frac{a}{\pi}\right)_2$ to be the quadratic residue symbol of a mod (π), i.e.,

$$\left(\frac{a}{\pi}\right)_2 = \begin{cases} 1 & \text{if } a \mod (\pi) \text{ is a square in } \kappa_\pi^*, \\ -1 & \text{if } a \mod (\pi) \text{ is not a square in } \kappa_\pi^*, \\ 0 & \text{if } a \in (\pi). \end{cases}$$

where κ_π is the residue field $\mathcal{O}_K/(\pi)$. For any ideal $I = (\pi_1 \cdots \pi_n) \subseteq \mathcal{O}_K$, denote by $\left(\frac{a}{\pi_1 \cdots \pi_n}\right)_2$ the product $\left(\frac{a}{\pi_1}\right)_2 \cdots \left(\frac{a}{\pi_n}\right)_2$ for any $a \in \mathcal{O}_K$. It is a character of $(\mathcal{O}_K/I)^*$.

Remark 2.3. When $b = -a$, the conic $z^2 - ax^2 + ay^2 = 0$ admits the solution $(x, y, z) = (1, 1, 0)$. Hence there exist infinitely many pairs $(a, b) \in K^*/(K^*)^2 \times K^*/(K^*)^2$ such that $(a, b)_{H,K} = 1$. Thus Theorem 1.2 is not trivial.

Theorem 2.4. *Let $a, b \in \Sigma_K$ such that $a = u_1\pi_1 \ldots \pi_n \cdot \varpi_1 \ldots \varpi_l$ and $b = u_2\pi'_1 \ldots \pi'_m \cdot \varpi_1 \ldots \varpi_l$, with π_i, π'_j, ϖ_k distinct primes. Assume that π is an odd prime among π_i for $1 \leq i \leq n$. Then $(a, b)_{H,K_\mathfrak{p}}$ is trivial if and only if $(\frac{b}{\pi})_2$ is trivial, where $K_\mathfrak{p}$ denotes the completion of K at $\mathfrak{p} := (\pi)$. The symbol $(a, b)_{H,K_\mathfrak{p}}$ is abbreviated as $(a, b)_\mathfrak{p}$ in the following.*

Proof. Let $a' = a\pi^{-1}$. We claim that $(a', b)_\mathfrak{p} = 1$. Assuming this, it follows that $(a, b)_\mathfrak{p} = (a', b)_\mathfrak{p}(\pi, b)_\mathfrak{p} = (\pi, b)_\mathfrak{p} = \left(\frac{b}{\pi}\right)_2$, which completes the proof. To prove the claim, it suffices to show that $a'x^2 + by^2 = z^2$ has a nontrivial solution in $K_\mathfrak{p}$ by Proposition 2.2. Fix a unit $c \in \mathcal{O}^*_{K_\mathfrak{p}}$. As y^2 ranges over squares in $\kappa_\mathfrak{p} = \mathbb{F}_q$ ($q = |\kappa_\mathfrak{p}|$), the values $c^2 - by^2 \mod \mathfrak{p}$ take $\frac{q+1}{2}$ distinct residues. Similarly, the values $a'x^2 \mod \mathfrak{p}$ take $\frac{q+1}{2}$ distinct residues as x ranges over $\mathbb{F}_q$. Thus there exist $x_0, y_0 \in \mathcal{O}_{K_\mathfrak{p}}$ such that

$$a'x_0^2 + by_0^2 \equiv c^2 \pmod{\mathfrak{p}}.$$

The multi-variable version of Hensel's lemma (cf. [19, Ch. 4, Ex. 4.27]) lifts this to a solution $(x_1, y_1, z_1) \neq (0, 0, 0)$ of $a'x^2 + by^2 = z^2$ in $K_\mathfrak{p}$. Thus $(a', b)_\mathfrak{p} = 1$, as claimed. $\square$

By Theorem 2.4, we provide a necessary condition for the vanishing of the Hilbert symbol.

Lemma 2.5. *Let $([a], [b]) \in K^*/(K^*)^2 \times K^*/(K^*)^2$. If $([a], [b])_{H,K} = 1$, then the product $\prod_{\substack{\pi \mid a, \pi \nmid b \\ \pi \text{ odd prime}}} \frac{(1 + \left(\frac{b}{\pi}\right)_2)}{2}$ is equal to 1.*

We now turn to the proof of our main theorem on the rational density of Severi-Brauer conics over K. The proof relies on the following preparatory lemmas, which provide the necessary analytic tools for Theorem 2.13. Let K be a number field. We say that a function f defined on all ideals of K is a multiplicative arithmetic function if for any two coprime ideals $\mathfrak{a}, \mathfrak{b}$, we have $f(\mathfrak{a}\mathfrak{b}) = f(\mathfrak{a})f(\mathfrak{b})$. For any two ideals $\mathfrak{a}, \mathfrak{b}$, $\gcd(\mathfrak{a}, \mathfrak{b})$ denotes the greatest common divisor of $\mathfrak{a}$ and $\mathfrak{b}$, i.e. $\gcd(\mathfrak{a}, \mathfrak{b}) = \mathfrak{a} + \mathfrak{b}$. For any elements $a, b \in \mathcal{O}_K$, $\gcd(a, b) := \gcd((a), (b))$.

Lemma 2.6. *Let λ_1, λ_2 be constants such that $\lambda_1 > 0$ and $0 \leq \lambda_2 < 2$. Let f be a multiplicative arithmetic function satisfying*

$$0 \leq f(\mathfrak{p}^v) \leq \lambda_1 \lambda_2^{v-1} \tag{2.1}$$

for any prime ideal $\mathfrak{p}$ with $N\mathfrak{p} \geq 2$ and any $v \in \mathbb{Z}_{>0}$. Then for any $X \geq 2$, we have

$$\sum_{\substack{N(\mathfrak{a}) \leq X \\ \mathfrak{a} \subseteq \mathcal{O}_K}} f(\mathfrak{a}) = O\Big(X \cdot \prod_{\substack{N(\mathfrak{p}) \leq X \\ \mathfrak{p} \text{ prime ideal}}} (1 - N(\mathfrak{p})^{-1}) \sum_{v=0}^{\infty} f(\mathfrak{p}^v)(N(\mathfrak{p}))^{-v}\Big), \tag{2.2}$$

where O is independent of X.

Proof. By adapting the method of [20, Part III, Ch. 3, Sec. 3, Cor. 3.6] to number fields (with primes replaced by prime ideals and p^{-v} systematically substituted by $N(\mathfrak{p})^{-v}$), we establish the corresponding number field analogue. This completes the proof. $\square$

Lemma 2.7. *Let K be a number field and $X \in \mathbb{R}_{>0}$.*

1. *(Mertens' formula) For every $y \in \mathbb{R}_{>0}$, there exists a positive constant $C_{K,y}$, depending only on K and y, such that* $\prod_{\substack{N\mathfrak{p}\leq X \\ \mathfrak{p} \text{ prime ideal}}} \left(1+\frac{y}{N\mathfrak{p}}\right) \sim C_{K,y}(\log X)^y$ *as $X \to \infty$.*
2. *For any $y \in \mathbb{R}_{>0}$,* $\sum_{\substack{1\leq N(\mathfrak{a})\leq X \\ \mathfrak{a}\subseteq \mathcal{O}_K}} y^{\omega(\mathfrak{a})} = O(X(\log X)^{y-1})$, *where O depending only on K and y.*
3. $\sum_{\substack{1\leq N(\mathfrak{a})\leq X \\ \mathfrak{a}\subseteq \mathcal{O}_K}} \sum_{\substack{1\leq N(\mathfrak{b})\leq X \\ \mathfrak{b}\subseteq \mathcal{O}_K}} \left(\frac{1}{2}\right)^{\omega(\frac{\mathfrak{a}}{\gcd(\mathfrak{a},\mathfrak{b})})} = O\left(\frac{X^2}{(\log X)^{\frac{1}{6}}}\right).$

Proof. **(1).** The proof follows the same argument as that of [20, Part I, Ch. 1, Thm. 1.12] or [5, Theorem 1].

(2). We adapt the strategy of [20, Part III, Ch. 3, Sec. 3, Thm. 6]. Note that the function $\mathfrak{a} \to y^{\omega(\mathfrak{a})}$ is a multiplicative arithmetic function, and satisfies the condition in Lemma 2.6 for $\lambda_1 = 1+y,\ \lambda_2 = 1$. Thus by Lemma 2.6,

$$\sum_{1\leq N(\mathfrak{a})\leq X} y^{\omega(\mathfrak{a})} = O\Big(X \prod_{N(\mathfrak{p})\leq X} (1-N(\mathfrak{p})^{-1})\{1+yN(\mathfrak{p})^{-1}+O(N(\mathfrak{p})^{-2})\}\Big).$$

By Statement (1), the proof is complete.

(3). Note that for any fixed ideal $\mathfrak{b}$, the function $f_{\mathfrak{b}}(\mathfrak{a}) := \left(\frac{1}{2}\right)^{\omega(\frac{\mathfrak{a}}{\gcd(\mathfrak{a},\mathfrak{b})})}$ is a multiplicative arithmetic function such that $0 \leq f_{\mathfrak{b}}(\mathfrak{p}^v) \leq 1\cdot 1^{v-1}$. Therefore

(2.3)

$$\begin{aligned}
&\sum_{1\leq N(\mathfrak{a})\leq X} \sum_{1\leq N(\mathfrak{b})\leq X} \left(\frac{1}{2}\right)^{\omega(\frac{\mathfrak{a}}{\gcd(\mathfrak{a},\mathfrak{b})})} \\
&\leq X \sum_{1\leq N(\mathfrak{b})\leq X} \left(\prod_{\substack{N(\mathfrak{p})\leq X \\ \mathfrak{p}\mid\mathfrak{b}}} (1-N(\mathfrak{p})^{-1}) \sum_{v=0}^{\infty} f_{\mathfrak{b}}(\mathfrak{p}^v)N(\mathfrak{p})^{-v} \right) \cdot \left(\prod_{\substack{N(\mathfrak{p})\leq X \\ \mathfrak{p}\nmid\mathfrak{b}}} (1-N(\mathfrak{p})^{-1}) \sum_{v=0}^{\infty} f_{\mathfrak{b}}(\mathfrak{p}^v)N(\mathfrak{p})^{-v} \right) \\
&\leq X \sum_{N(\mathfrak{b})\leq X} \prod_{N(\mathfrak{p})\leq X} (1-N(\mathfrak{p})^{-1})(1+\sum_{v=1}^{\infty}\frac{1}{2}N(\mathfrak{p})^{-v}) \prod_{\mathfrak{p}\mid\mathfrak{b}} \frac{\sum_{v=0}^{\infty} N(\mathfrak{p})^{-v}}{1+\sum_{v=1}^{\infty}\frac{1}{2}N(\mathfrak{p})^{-v}} \\
&\leq X \prod_{N(\mathfrak{p})\leq X} (1-N(\mathfrak{p})^{-1})(1+\sum_{v=1}^{\infty}\frac{1}{2}N(\mathfrak{p})^{-v}) \sum_{N(\mathfrak{b})\leq X} \prod_{\mathfrak{p}\mid\mathfrak{b}} \frac{\sum_{v=0}^{\infty} N(\mathfrak{p})^{-v}}{1+\sum_{v=1}^{\infty}\frac{1}{2}N(\mathfrak{p})^{-v}}.
\end{aligned}$$

Moreover,

$$\sum_{N(\mathfrak{b})\le X}\prod_{\mathfrak{p}|\mathfrak{b}}\frac{\sum\limits_{v=0}^{\infty}N(\mathfrak{p})^{-v}}{1+\sum\limits_{v=1}^{\infty}\frac{1}{2}N(\mathfrak{p})^{-v}}\le\sum_{N(\mathfrak{b})\le X}\prod_{\mathfrak{p}|\mathfrak{b}}\frac{N(\mathfrak{p})}{N(\mathfrak{p})-\frac{1}{2}}$$
$$\le\sum_{N(\mathfrak{b})\le X}\prod_{\mathfrak{p}|\mathfrak{b}}\left(1+\frac{\frac{1}{2}}{N(\mathfrak{p})-\frac{1}{2}}\right)\le 2\cdot\sum_{N(\mathfrak{b})\le X}\left(1+\frac{1}{3}\right)^{\omega(\mathfrak{b})}.$$

By Statement (2), $\sum\limits_{N(\mathfrak{b})\le X}\left(1+\frac{1}{3}\right)^{\omega(\mathfrak{b})}=O(X(\log X)^{\frac{1}{3}})$. By Statement (1),

$$X\cdot\prod_{N(\mathfrak{p})\le X}(1-N(\mathfrak{p})^{-1})(1+\sum_{v=1}^{\infty}\frac{1}{2}N(\mathfrak{p})^{-v})=O\left(\frac{X}{(\log X)^{\frac{1}{2}}}\right).$$

Thus

$$\sum_{N(\mathfrak{a})\le X}\sum_{N(\mathfrak{b})\le X}\left(\frac{1}{2}\right)^{\omega(\frac{\mathfrak{a}}{\gcd(\mathfrak{a},\mathfrak{b})})}=O\left(\frac{X}{(\log X)^{\frac{1}{2}}}\right)\cdot O(X(\log X)^{\frac{1}{3}})=O\left(\frac{X^2}{(\log X)^{\frac{1}{6}}}\right),$$

which completes the proof. ☐

Let K be a number field with degree $n=r_1+2r_2$. From now on, we fix a basis $\{\epsilon_i\}_{i=1}^{r_1+r_2-1}$ of $\mathscr{O}_K^*/\mu_K$, where μ_K is the group of roots of unity in K. For a constant $C>0$, let $\mathscr{R}_{K,C}$ be the set

$$\{\alpha\in\mathscr{O}_K\mid 0<|\alpha^{(i)}|<C|N(\alpha)|^{\frac{1}{n}},\ 0<|\alpha^{(j)}|^2<C|N(\alpha)|^{\frac{2}{n}}\text{ for } i=1,...,r_1,\ j=r_1+1,...,r_1+r_2\}.$$

In the following we shall demonstrate that there exists a suitable constant $C>0$ such that every element of $\mathscr{O}_K$ can be placed in $\mathscr{R}_{K,C}$ after multiplication by a suitable unit. This construction is designed to facilitate the application of Lemma 2.10 for the analytic estimation of the density.

Lemma 2.8. *Let Λ be a lattice of $\mathbb{R}^n$ with basis $\{v_i\}_{i=1}^n$. For any $a=(a_1,\dots,a_n)\in\mathbb{R}^n$, define*

$$S_a=\left\{x=(x_1,\dots,x_n)\in\mathbb{R}^n\ \middle|\ |x_i-a_i|\le\sum_{i=1}^n\|v_i\|\text{ for all }1\le i\le n\right\}.$$

Then $\Lambda\cap S_a\neq\emptyset$.

Proof. Since $\{v_i\}$ is an $\mathbb{R}$-basis, write $a=\sum_{i=1}^n b_iv_i$ with $b_i\in\mathbb{R}$. Choose integers m_i satisfying $|b_i-m_i|\le\frac{1}{2}$. Then

$$\|a-\sum_{i=1}^n m_iv_i\|\le\sum_{j=1}^n\frac{1}{2}\|v_j\|,$$

which implies $\sum_{i=1}^n m_iv_i\in S_a$ and this completes the proof. ☐

Let l be the map

$$\begin{aligned} l : \mathscr{O}_K^* &\longrightarrow \mathbb{R}^{r_1+r_2}, \\ \eta &\longmapsto \left(\log|\eta^{(1)}|, \dots, \log|\eta^{(r_1)}|, 2\log|\eta^{(r_1+1)}|, \dots, 2\log|\eta^{(r_1+r_2)}|\right). \end{aligned}$$

Lemma 2.9. *Let $\{\epsilon_i\}_{i=1}^{r_1+r_2-1}$ be the fixed basis of $\mathscr{O}_K^*/\mu_K$. For any $\alpha \in \mathscr{O}_K \setminus \{0\}$, there exists a unit $u \in \mathscr{O}_K^*$ such that $\alpha u \in \mathscr{R}_K$, where $\mathscr{R}_K := \mathscr{R}_{K, e^{(n-1)\sum_{k=1}^{r_1+r_2-1}\|v_k\|}}$ and $\{v_i\}_{i=1}^{r_1+r_2-1}$ is the image of $\{\epsilon_i\}_{i=1}^{r_1+r_2-1}$ under l.*

Proof. Let $\alpha \in \mathscr{O}_K \setminus \{0\}$. By Dirichlet's unit theorem, the image $l(\mathscr{O}_K^*)$ forms a full lattice in the hyperplane

$$H := \left\{ (a_1, \dots, a_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \;\middle|\; \sum_{i=1}^{r_1+r_2} a_i = 0 \right\}.$$

Since $\{v_i\}_{i=1}^{r_1+r_2-1}$ is the image of $\{\epsilon_i\}_{i=1}^{r_1+r_2-1}$ under l, $\{v_i\}_{i=1}^{r_1+r_2-1}$ is a basis of $l(\mathscr{O}_K^*)$. For each $m \in \mathbb{Z}_{>0}$, let S_m be the set

$$S_m := \left\{ (b_1, \dots, b_{r_1+r_2}) \in \mathbb{R}^{r_1+r_2} \;\middle|\; \begin{array}{l} \left| b_i - \dfrac{\log|N(\alpha)|}{n} + \log|\alpha^{(i)}| \right| \\ \qquad < m \displaystyle\sum_{k=1}^{r_1+r_2-1} \|v_k\|, \quad 1 \le i \le r_1 \\ \left| b_j - \dfrac{2\log|N(\alpha)|}{n} + 2\log|\alpha^{(j)}| \right| \\ \qquad < m \displaystyle\sum_{k=1}^{r_1+r_2-1} \|v_k\|, \quad r_1+1 \le j \le r_1+r_2 \end{array} \right\}.$$

The lemma is equivalent to showing that $l(\mathscr{O}_K^*) \cap (S_{n-1}) \neq \emptyset$. Let $p \colon \mathbb{R}^{r_1+r_2} \to \mathbb{R}^{r_1+r_2-1}$ be the linear projection

$$p(a_1, \dots, a_{r_1+r_2}) = (a_1, \dots, a_{r_1+r_2-1}). \tag{2.4}$$

Then $p(l(\mathscr{O}_K^*))$ is a full lattice in $\mathbb{R}^{r_1+r_2-1}$. By Lemma 2.8, there exists a unite $u \in \mathscr{O}_K^*$ such that

$$p(l(u)) \in p(l(\mathscr{O}_K^*)) \cap p(S_1),$$

which implies $l(u) \in S_{n-1}$. This completes the proof. □

By Lemma 2.9, for each nonzero $\alpha \in \mathscr{O}_K$, we fix a unit $u_\alpha \in \mathscr{O}_K^*$ such that $u_\alpha \alpha \in \mathscr{R}_K$. Let U be the fixed representatives of $\mathscr{O}_K^*/(\mathscr{O}_K^*)^2$ in Section 1. Since U is finite, by increasing the constant if necessary, we can choose a constant C' such that $u_i^{-1} u_j u_\alpha \alpha \in \{\beta \in \mathscr{O}_K \mid 0 < |\beta^{(i)}| < C'|N(\beta)|^{\frac{1}{n}},\ 0 < |\beta^{(j)}|^2 < C'|N(\beta)|^{\frac{2}{n}}$ for $i = 1, ..., r_1,\ j = r_1+1, ..., r_1+r_2\}$ for any $u_i,\ u_j \in U$. Here the constant C' depends only on K, the choice of basis $\{\epsilon_i\}_{i=1}^{r_1+r_2-1}$ of $\mathscr{O}_K^*/\mu_K$ and the choice of U. For $X \in \mathbb{R}_{>0}$, define

$$\mathscr{R}_K^X := \{\alpha \in \mathscr{O}_K \mid 0 < |\alpha^{(i)}| < C' X^{\frac{1}{n}},\ 0 < |\alpha^{(j)}|^2 < C' X^{\frac{2}{n}} \text{ for } i = 1, ..., r_1,\ j = r_1+1, ..., r_1+r_2\}.$$

The following lemma is an immediate consequence of [14, Theorem 2].

Lemma 2.10. *Let K be a number field of degree $n = r_1 + 2r_2$, and let $\mathfrak{q}$ be an ideal of $\mathcal{O}_K$. Let χ be a nonprincipal character of $(\mathcal{O}_K/\mathfrak{q})^*$. Then*

$$\sum_{\alpha \in \mathcal{R}_K^X} \chi(\alpha) = O((N\mathfrak{q})^{\frac{1}{(r_2+2)}} X^{\frac{r_2}{r_2+2}} \log^{\frac{2r_1}{r_2+2}} X),$$

where O depends only on K.

By Lemma 2.9, for each b of the form $\pi_1 \cdots \pi_t \in \Sigma_K^X$, there exists $u_{\pi_1 \cdots \pi_t} \in \mathcal{O}_K^*$ (fixed for each $\pi_1 \cdots \pi_t$) such that $u_{\pi_1 \cdots \pi_t} \pi_1 \cdots \pi_t \in \mathcal{R}_K$. Choose $u'_{\pi_1 \cdots \pi_t} \in U$ such that $u'_{\pi_1 \cdots \pi_t} \equiv u_{\pi_1 \cdots \pi_t}$ (mod ${\mathcal{O}_K^*}^2$). Then $u'^{-1}_{\pi_1 \cdots \pi_t} u u_{\pi_1 \cdots \pi_t} \pi_1 \cdots \pi_t \in \mathcal{R}_K^X$ for any $u \in U$, which induces a map:

$$i : \Sigma_K^X \longrightarrow \mathcal{R}_K^X,$$
$$u\pi_1 \cdots \pi_t \longmapsto u'^{-1}_{\pi_1 \cdots \pi_t} u u_{\pi_1 \cdots \pi_t} \pi_1 \cdots \pi_t.$$

It is easy to see that i is injective, and b and $i(b)$ represent the same class in $K^*/(K^*)^2$ for every $b \in \Sigma_K^X$. We use this injective map to apply Lemma 2.10 in subsequent computations.

Fix $\alpha \in \mathcal{O}_K$ and $X > 0$. We estimate the cardinality $\left|\alpha \mathcal{O}_K^* \cap \mathcal{R}_K^X\right|$, which is important for the proof of Theorem 2.13.

Lemma 2.11. *Let Λ be a full lattice in $\mathbb{R}^n$. Then there exists a constant C depending only on Λ, such that the number $\#(\Lambda \cap \{x \in \mathbb{R}^n \mid \|x\| < X\})$ is at most $C(X^n + 1)$ for any $X \in \mathbb{R}_{>0}$.*

Proof. See [15, Chapter 3, Lemma 1]. $\square$

Recall that, by Lemma 2.9, for each $\alpha \in \mathcal{O}_K$, we fix a unit $u_\alpha \in \mathcal{O}_K^*$ such that $\alpha u_\alpha \in \mathcal{R}_K$. We denote αu_α by α_u. We have the following lemma.

Lemma 2.12. *Let K be a number field of degree n. Then there exist constants $\tilde{C}', \tilde{C}'' > 0$ such that for all $X \in \mathbb{R}_{>0}$ and for all $\alpha \in \mathcal{O}_K$ with $|N(\alpha)| < X$,*

$$|\alpha_u \mathcal{O}_K^* \cap \mathcal{R}_K^X| < \tilde{C}''((\log X^{1/n} - \log \tilde{\alpha_u}) + \tilde{C}')^n,$$

where $\tilde{\alpha_u} = \min\limits_i \{|\alpha_u^{(i)}|\}$.

Proof. Note that $|\alpha_u \mathcal{O}_K^* \cap \mathcal{R}_K^X| = |\mathcal{O}_K^* \cap \alpha_u^{-1} \mathcal{R}_K^X|$. Define the logarithmic map

$$\ell : \mathcal{O}_K \setminus \{0\} \to \mathbb{R}^{r_1+r_2}, \quad \eta \mapsto \left((\log|\eta^{(i)}|)_{i=1}^{r_1},\ (2\log|\eta^{(i)}|)_{i=r_1+1}^{r_1+r_2} \right).$$

Let $H = \{(s_i) \in \mathbb{R}^{r_1+r_2} \mid \sum\limits_{i=1}^{r_1+r_2} s_i = 0\}$ and $S = \ell(\alpha_u^{-1} \mathcal{R}_K^X \cap \mathcal{O}_K) \cap H$. For any $s \in S$ with $s = \ell(\alpha_u^{-1} b)$, since $s \in H$, the coordinate bounds

$$-\left(\sum_{\substack{j=1 \\ j \neq i}}^{r_1} \log \frac{X^{1/n}}{|\alpha_u^{(j)}|} + \sum_{\substack{j=r_1+1 \\ j \neq i}}^{r_1+r_2} \log \frac{X^{2/n}}{|\alpha_u^{(j)}|^2} + C \right) \leq \log|b^{(i)}| - \log|\alpha_u^{(i)}| \leq \log X^{1/n} - \log \tilde{\alpha_u} + \log C'$$

hold for some $C > 0$. We can therefore choose constants $C'', C''' > 0$ such that

$$S \subset S' := \left\{ (c_i) \in \mathbb{R}^{r_1+r_2} \;\middle|\; |c_i| < C''(\log X^{1/n} - \log \tilde{\alpha_u}) + C''', 1 \leq i \leq r_1 + r_2 \right\}.$$

Let $p : \mathbb{R}^{r_1+r_2} \to \mathbb{R}^{r_1+r_2-1}$ be the projection defined in Equation (2.4). Let $S'' = \{x \in \mathbb{R}^{r_1+r_2-1} \mid \|x\| < \sqrt{n}C''(\log X^{1/n} - \log \tilde{\alpha_u}) + C'''\}$ be a ball that contaning $p(S')$. By Lemma 2.11,

$$|S'' \cap p\ell(\mathscr{O}_K^*)| < \tilde{C}((\log X^{1/n} - \log \tilde{\alpha_u}) + \tilde{C}')^n,$$

for some suitable constants $\tilde{C}, \tilde{C}' > 0$. Since $p|_{\ell(\mathscr{O}_K^*)\cap S}$ is injective and $p(S') \subseteq S''$, we conclude that

$$|\ell(\mathscr{O}_K^* \cap \alpha_u^{-1}\mathscr{R}_K^X)| < \tilde{C}((\log X^{1/n} - \log \tilde{\alpha_u}) + \tilde{C}')^n.$$

Since $\ell|_{\mathscr{O}_K^*}$ has finite kernel, $|\mathscr{O}_K^* \cap \alpha_u^{-1}\mathscr{R}_K^X| < \tilde{C}''((\log X^{1/n} - \log \tilde{\alpha_u}) + \tilde{C}')^n$ for a suitable constant $\tilde{C}'' > 0$ and this completes the proof. □

To compute the rational density $\delta_{H,K}$, we first estimate the size of Σ_K^X. Recall that

$$\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} = \prod_p (1 + p^{-s}) = \frac{\zeta(s)}{\zeta(2s)},$$

where μ is the Möbius function and $\zeta(s)$ is the Riemann zeta function. The right-hand side has a simple pole at $s = 1$ with residue $1/\zeta(2)$. Hence, by the Tauberian theorem (cf. [7, Sec. 5, Cor. 2]), we obtain that

$$\sum_{n \leq X} \mu^2(n) \sim \frac{X}{\zeta(2)} \qquad (\text{as } X \to \infty),$$

which gives the asymptotic formula for the number of square-free positive integers. By the same argument, one obtains

$$\#\{\mathfrak{a} \subseteq \mathscr{O}_K : \mathfrak{a} \text{ square-free ideal}, N\mathfrak{a} < X\} \sim C_K X \qquad (\text{as } X \to \infty)$$

for some positive constant C_K depending only on K. Thus

$$|\Sigma_K^X| \sim rC_K X \qquad (\text{as } X \to \infty),$$

where $r = |U|$ and U is the fixed representatives of $\mathscr{O}_K^*/(\mathscr{O}_K^*)^2$ in Section 1. With the above preparations, we establish our main theorem.

Theorem 2.13. *Let K be a number field of degree $n = r_1 + 2r_2$ with class number 1. Then the rational density $\delta_{H,K} = 0$.*

Proof. Let $\Sigma_K^{H',X} := \{(a, b) \mid (a, b) \in \Sigma_K^X \times \Sigma_K^X,\ (\frac{b}{\pi})_2 = 1 \text{ for every odd prime } \pi \mid a, \pi \nmid b\}$. Since $\Sigma_K^{H,X} \subseteq \Sigma_K^{H',X}$, it suffices to show that

$$\delta_{H',K} := \limsup_{X \to +\infty} \frac{|\Sigma_K^{H',X}|}{|\Sigma_K^X|^2}$$

is zero.

Since $|\Sigma_K^{H',X}| = \sum_{(a,b)\in\Sigma_K^X\times\Sigma_K^X} \prod_{\substack{\pi|a,\pi\nmid b\\ \pi \text{ odd prime}}} \frac{1+(\frac{b}{\pi})_2}{2}$ and $|\Sigma_K^X| \sim rC_K X$, it suffices to show that

$$\sum_{(a,b)\in\Sigma_K^X\times\Sigma_K^X} \prod_{\substack{\pi|a,\pi\nmid b\\ \pi \text{ odd prime}}} \frac{1+(\frac{b}{\pi})_2}{2} = o(X^2). \tag{2.5}$$

By direct computation,

$$\begin{aligned}
&\sum_{(a,b)\in\Sigma_K^X\times\Sigma_K^X} \prod_{\substack{\pi|a,\pi\nmid b\\ \pi \text{ odd prime}}} \frac{1+\left(\frac{b}{\pi}\right)_2}{2}\\
\leq &r\cdot \sum_{\substack{1\leq N((a))\leq X\\ (a)\subseteq\mathscr{O}_K}} \sum_{b\in\mathscr{R}_K^X} \prod_{\substack{\pi|a,\pi\nmid b\\ \pi \text{ odd prime}}} \frac{1+\left(\frac{b}{\pi}\right)_2}{2}\\
\leq &r\cdot \sum_{\substack{1\leq N((a))\leq X\\ (a)\subseteq\mathscr{O}_K}} \sum_{b\in\mathscr{R}_K^X} \sum_{\substack{1\neq(d)|(a)\\ 2\notin(d)\\ d \text{ square free}}} \left(\frac{1}{2}\right)^{\omega(d)} \left(\frac{b}{d}\right)_2 + 2r\cdot \sum_{\substack{1\leq N((a))\leq X\\ (a)\subseteq\mathscr{O}_K}} \sum_{b\in\mathscr{R}_K^X} \left(\frac{1}{2}\right)^{\omega\left(\frac{a}{\gcd(a,b)}\right)}.
\end{aligned}$$

We begin by estimating the summation

$$r\cdot \sum_{\substack{1\leq N((a))\leq X\\ (a)\subseteq\mathscr{O}_K}} \sum_{b\in\mathscr{R}_K^X} \left(\frac{1}{2}\right)^{\omega\left(\frac{a}{\gcd(a,b)}\right)}.$$

Notice that

$$\mathscr{R}_K^X = \coprod_{\mathfrak{b}\subseteq\mathscr{O}_K} \left(b_u\mathscr{O}_K^*\cap\mathscr{R}_K^X\right),$$

where b_u is the fixed generator of the ideal $\mathfrak{b}$ such that $b_u\in\mathscr{R}_K$. By Lemma 2.12, we have

$$\left|b_u\mathscr{O}_K^*\cap\mathscr{R}_K^X\right| < \tilde{C}''\left(\log X^{1/n} - \log\tilde{b}_u + \tilde{C}'\right)^n,$$

where $\tilde{b}_u = \min_i\{|b_u^{(i)}|\}$. We divide the ideals (b_u) into two classes:

- **Class I**: Ideals satisfying

$$\tilde{C}''\left(\log X^{1/n} - \log\tilde{b}_u + \tilde{C}'\right)^n > \log^{1/7} X.$$

- **Class II**: Ideals violating the above inequality.

Equivalently, Class I consists of ideals with

$$\log\tilde{b}_u < \log X^{1/n} - \frac{\log^{1/(7n)} X}{(\tilde{C}'')^{1/n}} + \tilde{C}',$$

while Class II contains the remaining ideals. Since $b_u \in \mathscr{R}_K$, there exists a constant $C_1 > 0$ depending only on K such that $|\frac{b_u^{(i)}}{b_u^{(j)}}| < C_1$ for all $0 < i, j \leq r_1 + r_2$. Thus elements in Class I satisfy

$$|N(b_u)| < \tilde{C}_1 \mathrm{e}^{n\left(\log X^{1/n} - \frac{\log^{1/(7n)} X}{(\tilde{C}'')^{1/n}}\right)}$$

for some constant $\tilde{C}_1 > 0$. Let $A_X := \log X^{1/n} - \frac{\log^{1/(7n)} X}{\tilde{C}''^{1/n}}$. Notice that $\tilde{C}_1 \mathrm{e}^{nA_X} = O(\frac{X}{(\log X)^{n+1}})$. Then

$$\begin{aligned}
&\sum_{\substack{1 \leq N(\mathfrak{a}) \leq X \\ \mathfrak{a} \subseteq \mathscr{O}_K}} \sum_{b \in \mathscr{R}_K^X} \left(\frac{1}{2}\right)^{\omega(\frac{\mathfrak{a}}{\gcd(\mathfrak{a},(b))})} \\
=& \sum_{\substack{1 \leq N(\mathfrak{a}) \leq X \\ \mathfrak{a} \subseteq \mathscr{O}_K}} \sum_{b \in \coprod_{\mathfrak{b} \subseteq \mathscr{O}_K} (b_u \mathscr{O}_K^* \cap \mathscr{R}_K^X)} \left(\frac{1}{2}\right)^{\omega(\frac{\mathfrak{a}}{\gcd(\mathfrak{a},\mathfrak{b})})} \\
\leq& \sum_{\substack{1 \leq N(\mathfrak{a}) \leq X \\ \mathfrak{a} \subseteq \mathscr{O}_K}} \sum_{1 \leq N(\mathfrak{b}) \leq \tilde{C}_1 e^{nA_X}} \tilde{C}'' \left(\log X^{1/n} - \log \tilde{b}_u + \tilde{C}'\right)^n \cdot 1 \\
&+ \sum_{\substack{1 \leq N(\mathfrak{a}) \leq X \\ \mathfrak{a} \subseteq \mathscr{O}_K}} \sum_{\tilde{C}_1 e^{nA_X} \leq N(\mathfrak{b}) \leq C'^n X} \log^{1/7} X \cdot \left(\frac{1}{2}\right)^{\omega(\frac{\mathfrak{a}}{\gcd(\mathfrak{a},\mathfrak{b})})} \\
=& O(\frac{X^2}{\log X}) + O(\frac{X^2}{\log^{\frac{1}{42}} X}) \quad \text{(By Lemma 2.7 (3))}.
\end{aligned}$$

Thus

$$\begin{aligned}
&\sum_{(a,b) \in (\Sigma_K^X)^2} \prod_{\substack{\pi | a, \pi \nmid b \\ \pi \text{ odd prime}}} \frac{(1 + \left(\frac{b}{\pi}\right)_2)}{2} \\
\leq& r \cdot \sum_{\substack{1 \leq N((a)) \leq X \\ (a) \subseteq \mathscr{O}_K}} \sum_{\substack{-X \leq N(b) \leq X \\ b \in \mathscr{R}_K^X}} \sum_{\substack{1 \neq (d) | (a) \\ 2 \notin (d) \\ d \text{ square free}}} \left(\frac{1}{2}\right)^{\omega(d)} \left(\frac{b}{d}\right)_2 + o(X^2) \\
=& r \cdot \sum_{\substack{1 \leq N((a)) \leq X \\ (a) \subseteq \mathscr{O}_K}} \sum_{\substack{1 \neq (d) | (a) \\ 2 \notin (d) \\ d \text{ square free}}} \sum_{\substack{-X \leq N(b) \leq X \\ b \in \mathscr{R}_K^X}} \left(\frac{1}{2}\right)^{\omega(d)} \left(\frac{b}{d}\right)_2 + o(X^2) \\
\leq& r \cdot \sum_{\substack{1 \leq N((a)) \leq X \\ (a) \subseteq \mathscr{O}_K}} \sum_{(d) | (a)} \left(\frac{1}{2}\right)^{\omega(d)} (N((d)))^{\frac{1}{r_2+2}} X^{\frac{r_2}{r_2+2}} \log^{\frac{2r_1}{r_2+2}} X + o(X^2) \quad \text{(By Lemma 2.10)} \\
\leq& r \cdot X^{\frac{r_2+1}{r_2+2}} \log^{\frac{2r_1}{r_2+2}} X \cdot \sum_{\substack{1 \leq N((a)) \leq X \\ (a) \subseteq \mathscr{O}_K}} \sum_{(d) | (a)} \left(\frac{1}{2}\right)^{\omega(d)} + o(X^2).
\end{aligned}$$

Here

$$\sum_{\substack{1\le N((a))\le X\\ (a)\subseteq\mathcal{O}_K}}\sum_{(d)|(a)}\left(\frac{1}{2}\right)^{\omega(d)}$$

$$=\left(\sum_{\substack{1\le N((d_1))\le\sqrt{X}\\ (d_1)\subseteq\mathcal{O}_K}}\left(\frac{1}{2}\right)^{\omega(d_1)}\cdot(\sum_{\substack{\sqrt{X}<N((d_2))\le\frac{X}{N((d_1))}\\ (d_2)\subseteq\mathcal{O}_K}}1)\right)+\left(\sum_{\substack{1\le N((d_2))\le\sqrt{X}\\ (d_2)\subseteq\mathcal{O}_K}}1\cdot(\sum_{\substack{\sqrt{X}\le N((d_1))\le\frac{X}{N((d_2))}\\ (d_1)\subseteq\mathcal{O}_K}}\left(\frac{1}{2}\right)^{\omega(d_1)})\right).$$

We estimate the first term

$$\sum_{\substack{1\le N((d_1))\le\sqrt{X}\\ (d_1)\subseteq\mathcal{O}_K}}\left(\frac{1}{2}\right)^{\omega(d_1)}\cdot(\sum_{\substack{\sqrt{X}<N((d_2))\le\frac{X}{N((d_1))}\\ (d_2)\subseteq\mathcal{O}_K}}1),$$

and the estimation for the second term is the same. Note that

$$\sum_{\substack{\sqrt{X}<N((d_2))\le\frac{X}{N((d_1))}\\ (d_2)\subseteq\mathcal{O}_K}}1\le C_5\left(\frac{X}{N((d_1))}\right)$$

for some constant C_5. Thus

$$\begin{aligned}
&\sum_{\substack{1\le N((d_1))\le\sqrt{X}\\ (d_1)\subseteq\mathcal{O}_K}}\left(\frac{1}{2}\right)^{\omega(d_1)}\cdot(\sum_{\substack{\sqrt{X}<N((d_2))\le\frac{X}{N((d_1))}\\ (d_2)\subseteq\mathcal{O}_K}}1)\\
\le& C_5\cdot\sum_{\substack{1\le N((d_1))\le\sqrt{X}\\ (d_1)\subseteq\mathcal{O}_K}}\left(\frac{1}{2}\right)^{\omega(d_1)}\frac{X}{N((d_1))}\\
\le& C_5X\cdot\sum_{1\le N((d_1))\le\sqrt{X}}\left(\frac{1}{2}\right)^{\omega(d_1)}\cdot\frac{1}{N((d_1))}.
\end{aligned}$$

But

$$\begin{aligned}
\sum_{1\le N((d_1))\le\sqrt{X}}\left(\frac{1}{2}\right)^{\omega(d_1)}\cdot\frac{1}{N((d_1))}&=(\sum_{1\le N((d_1))\le\sqrt{X}}\left(\frac{1}{2}\right)^{\omega(d_1)})\cdot\frac{1}{\sqrt{X}}+\int_1^{\sqrt{X}}\sum_{1\le N((d_1))\le t}\left(\frac{1}{2}\right)^{\omega(d_1)}\frac{1}{t^2}dt\\
&\le\frac{C_6}{\log^{\frac{1}{2}}\sqrt{X}}+C_7\int_2^{\sqrt{X}}\frac{t}{\log^{\frac{1}{2}}t}\frac{1}{t^2}dt\\
&\le\frac{C_6}{\log^{\frac{1}{2}}\sqrt{X}}+C_7\cdot\log^{\frac{1}{2}}\sqrt{X}+C_8,
\end{aligned}$$

where $C_6,\ C_7,\ C_8$ are constants. Therefore

$$\sum_{1\le N((d_1))\le\sqrt{X}}\left(\frac{1}{2}\right)^{\omega(d_1)}\cdot(\sum_{\sqrt{X}<N((d_2))\le\frac{X}{N((d_1))}}1)=O(X\log^{\frac{1}{2}}X).$$

This completes the proof. □

3. The period-index density of elliptic curves

The Hilbert symbol is closely related to the period-index problem of elliptic curves. As an application, we use Theorem 2.13 to compute the period-index density of elliptic curves in a particular situation. In the following, we review the notions of period and index of homogeneous spaces for elliptic curves, and explain the relationship between the Hilbert symbol and the period-index obstruction map.

Let K be a field with absolute Galois group $G_K = \mathrm{Gal}(\overline{K}/K)$, and let E/K be an elliptic curve over K. The Weil-Châtelet group $\mathrm{WC}(E/K)$, which classifies the equivalence classes of homogeneous spaces of E, is canonically isomorphic to the Galois cohomology group $H^1(K, E(\overline{K}))$ (cf. [8, Proposition 4]). Under this isomorphism, each equivalence class of a homogeneous space C of E corresponds to a cohomology class in $H^1(K, E(\overline{K}))$, which we denote by $[C]$. The *period* of a homogeneous space C, denoted by $P(C)$, is defined as the order of $[C]$ in the group $H^1(K, E(\overline{K}))$. The *index* of C, denoted by $I(C)$, is the smallest positive integer d for which there exists a K-rational divisor of degree d on C. When K is a local field, Lichtenbaum [10] (see also [13, Section 5]) proved that $P(C) = I(C)$ holds for all homogeneous spaces C of E/K. In contrast, when K is a number field, the period and index do not necessarily coincide (cf. [1]), but they satisfy the divisibility relation

$$P(C) \mid I(C) \mid P(C)^2 \tag{3.1}$$

as shown in [11, Theorem 8] (see also [13, Proposition 2.4]). Building on this constraint, the necessary conditions for a positive integer pair (P, I) to arise as the period and index of a homogeneous space C are that $I = Pl$ for some positive integer l, and that l divides P. Furthermore, Sharif [18, Theorem 2] proved that for any such pair (P, Pl) with $l \mid P$, there exist infinitely many homogeneous spaces C of E satisfying $P(C) = P$ and $I(C) = Pl$.

A natural question arises: If the period is fixed, how are the possible indices distributed (cf. [3, Problem 2])? In the following, suppose that C is a homogeneous space whose class $[C] \in H^1(K, E)$ has period 2. From the divisibility relation (3.1), $I(C)$ must equal 2 or 4. This reduces to determining the density of the subset

$$\{[C] \mid [C] \in H^1(K, E)[2], I(C) = 2\}$$

within the entire set $H^1(K, E)[2]$.

In the rest of this section, let K be a number field, n be a positive integer and E/K be an elliptic curve defined over K. Recall the following Kummer sequence for the elliptic curve E:

$$0 \to E(K)/nE(K) \xrightarrow{\delta} H^1(K, E[n]) \xrightarrow{\rho} H^1(K, E)[n] \to 0. \tag{3.2}$$

One of the main tools in the study of the period-index problem is the following map constructed by O'Neil:

$$\mathrm{Ob} : H^1(K, E[n]) \to \mathrm{Br}(K). \tag{3.3}$$

The details of the obstruction map can be found in [13]. The map Ob can be used to determine whether or not $I(C) = P(C)$ for a given homogeneous space C. Concretely, we have the following proposition.

Proposition 3.1. *Let $[C] \in H^1(K, E)$ be of period n. Then C has index n if and only if there exists a lift $\zeta \in H^1(K, E[n])$ of $[C]$ such that* $\mathrm{Ob}(\zeta) = 1$.

Proof. This is [2, Theorem 5]. □

We explain the relationship between the Hilbert symbol and the obstruction map. Assume that the entire n-torsion subgroup $E[n] \subset E(K)$. Via the theory of the Weil pairing, the n-th roots of unity μ_n are contained in K. Fix a basis (S, T) of $E[n]$ once and for all. Again by the Weil pairing, $\zeta = e_n(S, T)$ is a generator of μ_n. After making this choice, we have an isomorphism

$$\psi_n : H^1(K, \mu_n) \times H^1(K, \mu_n) \xrightarrow{\sim} H^1(K, E[n]). \tag{3.4}$$

Via the canonical Kummer isomorphism $H^1(K, \mu_n) = K^*/(K^*)^n$, we may equally well view ψ_n as a map defined on $(K^*/(K^*)^n)^2$.

Theorem 3.2. *For $n \in \mathbb{Z}_{>0}$, let n^* be n if n is odd and $2n$ if n is even. If $E[n^*] \subset E(K)$, then* $\mathrm{Ob} \circ \psi_n = (\ ,\ )_{H_n,K}$*, where $(\ ,\ )_{H_n,K}$ is the Hilbert symbol defined in Section 2.*

Proof. This is [4, Theorem 10]. □

Suppose that $[C] \in H^1(K, E)$ with $P(C) = 2$. Then $I(C) = 2$ or 4. Moreover suppose that $E[4] \subset E(K)$. As discussed above, we have an isomorphism $H^1(K, E[2]) \xrightarrow{\sim} K^*/(K^*)^2 \times K^*/(K^*)^2$. Under this isomorphism, we view the map Ob as a map from $K^*/(K^*)^2 \times K^*/(K^*)^2$ to $\mathrm{Br}(K)$. Then by Theorem 3.2, the map Ob coincides with the Hilbert symbol. In summary, replacing $H^1(K, E[2])$ with $K^*/(K^*)^2 \times K^*/(K^*)^2$, we have the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E(K)/2E(K) & \xrightarrow{\delta} & K^*/(K^*)^2 \times K^*/(K^*)^2 & \xrightarrow{\rho} & H^1(K,E)[2] & \longrightarrow & 0. \\ & & & & \Big\downarrow{\scriptstyle \mathrm{Ob}=(\ ,\ )_{H,K}} & & & & \\ & & & & \mathrm{Br}(K) & & & & \end{array} \tag{3.5}$$

Definition 3.3. Let K be a number field with class number 1, and let E/K be an elliptic curve satisfying $E[4] \subset E(K)$. With the notation as above, for homogeneous spaces of period 2, the period-index density Θ is defined as the following limit:

$$\Theta := \limsup_{X \to +\infty} \frac{\left|\{[C] \mid [C] \in \rho(\Sigma_K^X \times \Sigma_K^X), I(C) = 2\}\right|}{\left|\rho(\Sigma_K^X \times \Sigma_K^X)\right|}.$$

Theorem 3.4. *Let K be a number field with class number 1, and let E/K be an elliptic curve satisfying $E[4] \subset E(K)$. Then $\Theta = 0$.*

Proof. By Proposition 3.1, the set $\{[C] \mid [C] \in \rho(\Sigma_K^X \times \Sigma_K^X), I(C) = 2\}$ is equal to the set

$$\{[C] \in \rho(\Sigma_K^X \times \Sigma_K^X) \mid \exists\, (a,b) \in K^*/(K^*)^2 \times K^*/(K^*)^2, \text{ such that } \rho(a,b) = [C] \text{ and } (a,b)_{H,K} = 1\}.$$

Let $\{(a_i, b_i)\}_{i=1}^t$ denote the image of $E(K)/2E(K)$ in $K^*/(K^*)^2 \times K^*/(K^*)^2$. Let A be defined as

$$A = \max\left\{\max_{1\le i\le t} |N(a_i)|, \max_{1\le j\le t} |N(b_j)|\right\}.$$

Then $\{[C] \mid [C] \in \rho(\Sigma_K^X \times \Sigma_K^X),\ I(C) = 2\} \subseteq \{[C] \mid [C] \in \rho(\Sigma_K^{H,A\cdot X})\}$. Thus by Equation (2.5), we have $|\{[C] \mid [C] \in \rho(\Sigma_K^X \times \Sigma_K^X),\ I(C) = 2\}| = o(X^2)$. Hence

$$\begin{aligned}
\Theta &= \limsup_{X\to+\infty} \frac{\left|\{[C] \mid [C] \in \rho(\Sigma_K^X \times \Sigma_K^X),\ I(C) = 2\}\right|}{\left|\rho(\Sigma_K^X \times \Sigma_K^X)\right|} \\
&= \limsup_{X\to+\infty} \frac{o(X^2)}{X^2} \\
&= 0.
\end{aligned}$$

□

Remark 3.5. By the divisibility relation (3.1), every nontrivial element $[C] \in H^1(K,E)[2]$ satisfies $P(C) = 2$ and $I(C) \in \{2,4\}$. This theorem establishes that within the 2-torsion subgroup $H^1(K,E)[2]$, the subset of elements with $I(C) = 2$ is sparse (exhibiting period-index density 0), whereas those with $I(C) = 4$ dominate (attaining period-index density 1) under the conditions specified in Theorem 3.4. Notably, there exist elliptic curves satisfying the hypotheses of Theorem 3.4. A concrete example is the curve **256.b1** in the LMFDB database, whose Weierstrass equation is explicitly given by

$$y^2 = x^3 - 2x.$$

Further instances from the LMFDB database, such as $\mathbf{200.2-a3}$, $\mathbf{225.2-a6}$ and $\mathbf{5525.5-b9}$, also satisfy the conditions in Theorem 3.4.

References

[1] J. W. S. Cassels, *Arithmetic on curves of genus 1, V. Two counterexamples*, J. London Math. Soc. 38 (1963), 244–248.

[2] P. Clark, *The period–index problem in WC-groups I: elliptic curves*, J. Number Theory 114:1 (2005), 193–208.

[3] P. Clark and S. Sharif, *Period, index and potential Sha*, arXiv:0811.3019 [math.NT] (2008).

[4] P. Clark and S. Sharif, *Period, index and potential. III*, Algebra Number Theory 4:2 (2010), 151–174.

[5] S. R. Garcia and E. S. Lee, *Unconditional explicit Mertens' theorems for number fields and Dedekind zeta residue bounds*, The Ramanujan Journal, vol. 57, no. 3, 1169–1191, 2022.

[6] J. G. Hinz, *Character sums in algebraic number fields*, J. Number Theory 17:1 (1983), 52–70.

[7] E. Hlawka, R. Taschner and J. Schoißengeier, *Geometric and Analytic Number Theory*, Universitext, Springer-Verlag, Berlin, Heidelberg, 1991.

[8] S. Lang and J. Tate, *Principal homogeneous spaces over abelian varieties*, Amer. J. Math. 80 (1958), 659–684.

[9] E. S. Lee, *Explicit Mertens' Theorems for Number Fields*, Bull. Austral. Math. Soc. 108(1) (2023), 169–172.

[10] S. Lichtenbaum, *The period-index problem for elliptic curves*, Amer. J. Math. 90 (1968), 1209–1223.

[11] S. Lichtenbaum, *Duality theorems for curves over p-adic fields*, Invent. Math. 7 (1969), 120–136.

[12] J. Neukirch, *Algebraic Number Theory*, Grundlehren der mathematischen Wissenschaften, vol. 322, Springer, 1999.

[13] C. O'Neil, *The period-index obstruction for elliptic curves*, J. Number Theory 95:2 (2002), 329–339.

[14] U. Rausch, *Character Sums in Algebraic Number Fields*, J. Number Theory 46:2 (1994), 179-195.

[15] C. A. Rogers and J. W. S. Cassels, *An Introduction to the Geometry of Numbers*, Springer, 1959.

[16] J.-P. Serre, *Local Fields*, translated by M. J. Atkinson, Graduate Texts in Mathematics, vol. 67, Springer, 2013.

[17] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, vol. 7, Springer, 1973.

[18] S. Sharif, *Period and index of genus one curves over global fields*, Math. Ann 354 (2012), 1029–1047.

[19] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 151, Springer, 1994.

[20] G. Tenenbaum, *Introduction to Analytic and Probabilistic Number Theory*, vol. 163, American Mathematical Society, 2015.

Department of Mathematics, Nanjing University, Nanjing 210093, China

Email address: `cxcheng@nju.edu.cn`

Department of Mathematics, Nanjing University, Nanjing 210093, China

Email address: `chengniu@smail.nju.edu.cn`

Department of Mathematics, Nanjing University, Nanjing 210093, China

Email address: `xgshang@smail.nju.edu.cn`