A variant of the large sieve inequality with explicit constants

Maciej Grześkowiak

Abstract. We give an effective version with explicit constants of the large sieve inequality for imaginary quadratic fields. Explicit results of this kind are useful for estimating the computational complexity of algorithms which generate elements, whose norm is a rational prime, in an arithmetic progression of the corresponding ring of integers.

1. Introduction

We begin by recalling the following form of the large sieve inequality [**3**]. Let

$$S(x) = \sum_{n=M+1}^{M+N} c_n e(nx), \qquad e(\theta) = e^{2\pi i\theta}, \tag{1.1}$$

where the c_n are arbitrary complex number. Let $x_1, \dots x_R$ be points which are well spaced modulo 1 in the sense that

$$\|x_r - x_s\| \geq \delta \tag{1.2}$$

for $s \neq r$, where $0 < \delta \leq \frac{1}{2}$ and $\|\theta\| = \min_n |\theta - n|$ denotes the distance to the nearest integer. The large sieve is an inequality of the form

$$\sum_{r=1}^{R} |S(x_r)|^2 \leq \Delta \sum_{n=M+1}^{M+N} |c_n|^2, \tag{1.3}$$

where $\Delta = \Delta(N, \delta)$. Huxley [**11**] generalized the above inequality to algebraic number fields K of degree k over the field $\mathbb{Q}$ of rational numbers. In his papers the integers $M+1 \leq n \leq M+N$ are replaced by algebraic integers of $\alpha \in K$ such that

$$\alpha = n_1\omega_1 + \ldots + n_k\omega_k, \qquad M_i + 1 \leq n_i \leq M_i + N_i, \quad i = 1, \dots k, \tag{1.4}$$

where $\omega_1, \dots, \omega_k$ is an integral basis of K, M_i, n_i are integers and N_i is a positive integer for $i = 1, \dots k$. Another generalization of the large sieve inequality was given by Schaal in [**16**]. He replaced the integers $M + 1 \leq n \leq M + N$ by algebraic integers $\alpha \in K$ lying in the domains which not necessarily depend on special integer basis of K. In 1987 Hinz proved a variant of the large sieve inequality to algebraic number [**9**]. His proof is based on the ideas presented in [**11**], [**16**], [**17**].

The author was partially supported by the grant no. DEC-2017/25/B/ST1/00208 from National Science Centre.

Many applications of the large sieve inequality to number theory, including the computational complexity of algorithms, follows from the formula below.

$$\sum_{q\leq Q}\sum_{\substack{a=1\\(a,q)=1}}^{q}|S(a/q)|^2\leq (N+Q^2)\sum_{n=M+1}^{M+N}|c_n|^2, \tag{1.5}$$

where the summation is over primes q. The analogous version to algebraic number fields of the above estimation was given in [**9**], [**11**], [**16**], [**17**]. However, in [**9**] the inequality stated above depends on a numerical constant not explicitly given. A second application of the large sieve inequality to number theory arise from the following estimation of a character sum.

$$\sum_{q\leq Q}\frac{q}{\varphi(q)}\sum_{\chi \bmod q}^{*}\left|\sum_{n=M+1}^{M+N}c_n\chi(n)\right|^2\leq (N+Q^2)\sum_{n=M+1}^{M+N}|c_n|^2, \tag{1.6}$$

where the summation is over primes q and $\sum^*$ denotes summation over primitive multiplicative characters $\chi \pmod q$. The above inequality was generalized to algebraic number fields by the authors of [**9**], [**11**], [**16**], [**17**]. Let us mention that in [**9**] the inequality (1.6) depends on a constant, which not given explicitly in this paper. The inequality stated above and its generalizations are essential tools in studying L-functions and distribution of prime numbers. It is a central to the proof of various version of the Bombieri-Vinogradov theorem [**2**], [**10**], [**12**]. As an example of the application of the large sieve inequality to computational number theory and cryptography we refer the reader to [**6**], [**5**], [**15**]. In [**6**] author proposes the polynomial time algorithm that generates primes satisfying the following definition.

Definition 1.1. Let p, q be a pair of primes and let $\Delta<0$ be an integer. The primes p,q are defined to be CM-primes with respect to Δ if there exist integers f and t such that

$$|t|\leq 2\sqrt{p},\quad q\mid p+1-t,\quad 4p-t^2=\Delta f^2. \tag{1.7}$$

Let us denote by $E(\mathbb{F}_p)$ the group of points on E over $\mathbb{F}_p$, and let $|E(\mathbb{F}_p)|$ be the order of $E(\mathbb{F}_p)$. If CM-primes p and q with respect to Δ and integers f,t are given, then an ordinary elliptic curve $E(\mathbb{F}_p)$ of cardinality $|E(\mathbb{F}_p)|=p+1-t$ can be constructed using complex multiplication method [**1**], [**4**]. The group $E(\mathbb{F}_p)$ can be used to implement public key cryptographic systems, based on intractability of the discrete logarithm problem (DLP). To make the DLP in $E(\mathbb{F}_p)$ intractable, it is essential to generate a large prime p, and a curve E defined over $\mathbb{F}_p$, such that $|E(\mathbb{F}_p)|$ has a large prime factor q.

In [**6**] a polynomial time algorithm for constructing primes of the form (1.7) is given. The main idea of the algorithm is as follows. Let $\Delta<0$ be a square-free. Fix $K=\mathbb{Q}(\sqrt{\Delta})$ with the corresponding ring of integers $\mathcal{O}_K=\{a+b\omega : a,b\in\mathbb{Z}\}$, where $\omega=\frac{1+\sqrt{\Delta}}{2}$, if $\Delta\equiv 1 \pmod 4$, or $\omega=\sqrt{\Delta}$, if $\Delta\equiv 2,3 \pmod 4$. In the first procedure, the algorithm finds $\alpha\in\mathcal{O}_K$ such that $N_{K/\mathbb{Q}}(\alpha)=q$ is a prime. Given α, the second procedure generates $\beta\in\mathcal{O}_K$ such that $\beta\equiv 1 \pmod{(\alpha)}$ and $N_{K/\mathbb{Q}}(\beta)=p$ is a prime. For sufficiently large p, q and $0<\varepsilon<\frac{2}{5}$ the algorithm finds primes (1.7) satisfying $(\log p)/(\log q)\ll 5/(2-5\varepsilon)$ [**6**]. However, it is interesting to known whether the order of magnitude of the generated primes coincide with practical expectations. In order to do this, it is necessary to compute the numerical

value of the constants occurring in the theorem that author utilized to analysis the complexity of the algorithm [**6**]. In [**7**] explicit numerical estimates for the generalized Chebyshev functions is given. The result presented there can be used for estimating explicitly the computational complexity of the first procedure above and obtaining the exact order of magnitude of the prime p of the form (1.7). In order to analyze the second procedure explicitly it is necessary to compute the numerical value of the constants occurring in the variant of the Bombieri-Vinogradov theorem presented in [**10**]. To do this, bounding of a character sum [**9**] analogous to (1.6) is required. The aim of this paper is to prove the corresponding estimation with exact numerical value of the constants in the case of imaginary quadratic number fields.

Let $D < 0$ be a square-free rational integer, and let $K = \mathbb{Q}(\sqrt{D})$ be the quadratic field with the corresponding ring of integers $\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$, where $\omega = \frac{1+\sqrt{D}}{2}$ when $D \equiv 1 \pmod 4$ and $\omega = \sqrt{D}$ for $D \equiv 2, 3 \pmod 4$. Let $\overline{\alpha}$ denote the complex conjugate of α. Let $\mathfrak{q}$ be an integral ideal of K. By $N\mathfrak{q}$ we denote the norm of $\mathfrak{q}$ with respect to $\mathbb{Q}$, and by $\Phi(\mathfrak{q})$ the generalized Euler's function. Let χ be a multiplicative character modulo $\mathfrak{q}$. Let $x > 1$ be an arbitrary but fixed number. We define

$$\mathfrak{R} = \{\beta \in \mathcal{O}_K : \quad |\beta| < \sqrt{x}\}. \tag{1.8}$$

We prove the following theorem.

THEOREM 1.2. *Fix $Q > 1$. We have*

$$\sum_{N\mathfrak{q} \le Q} \frac{N\mathfrak{q}}{\Phi(\mathfrak{q})} \sideset{}{^*}\sum_{\chi \bmod \mathfrak{q}} \left| \sum_{\substack{\alpha \in \mathfrak{R} \\ \alpha \equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\chi(\alpha) \right|^2 \le f(x, \mathfrak{a}, Q) \sum_{\substack{\alpha \in \mathfrak{R} \\ \alpha \equiv 0 \pmod{\mathfrak{a}}}} |c(\alpha)|^2,$$

where $f(x, \mathfrak{a}, Q) = \left(\frac{\sqrt{8}}{\sqrt[4]{3}} \left(\frac{x}{N\mathfrak{a}} \right)^{\frac{1}{4}} + c_0 |D|^{\frac{1}{4}} Q^{\frac{1}{2}} \right)^4$,

$$c_0 = \begin{cases} \left(1 - \frac{1}{\sqrt{3}}\right)^{-\frac{1}{2}} & \text{if} \quad D \equiv 1 \pmod 4, \\ \left(\frac{1}{2} - \frac{1}{2\sqrt{3}}\right)^{-\frac{1}{2}} & \text{if} \quad D \equiv 2, 3 \pmod 4, \end{cases}$$

and $\sum^*$ *denotes summation over primitive multiplicative characters* $\pmod{\mathfrak{q}}$*, and the* $c(\alpha)$ *are any complex numbers.*

PROOF. See Section 2. □

2. The Proof of Theorem 1.2

In the proof of Theorem 1.2 we shall need the following auxiliary theorems and lemmas. Let σ be an additive character modulo $\mathfrak{q}$. The number of distinct additive characters is $N\mathfrak{q}$. We denote by σ_0 the principal additive character modulo $\mathfrak{q}$. We have

$$\sum_{\xi \pmod{\mathfrak{q}}} \sigma(\xi) = \begin{cases} N\mathfrak{q} & \text{if} \quad \sigma = \sigma_0 \\ 0 & \text{if} \quad \sigma \neq \sigma_0, \end{cases}$$

$$\sum_{\sigma \pmod{\mathfrak{q}}} \sigma(\xi) = \begin{cases} N\mathfrak{q} & \text{if} \quad \xi \equiv 0 \pmod{\mathfrak{q}} \\ 0 & \text{if} \quad \xi \not\equiv 0 \pmod{\mathfrak{q}}. \end{cases}$$

The number of primitive additive characters modulo $\mathfrak{q}$ is $\Phi(\mathfrak{q})$. Let χ a multiplicative character modulo $\mathfrak{q}$. We denote by χ_0 the principal multiplicative character modulo $\mathfrak{q}$. We have

$$\sum_{\xi \pmod{\mathfrak{q}}} \chi(\xi) = \begin{cases} \Phi(\mathfrak{q}) & \text{if} \quad \chi = \chi_0 \\ 0 & \text{if} \quad \chi \neq \chi_0, \end{cases}, \tag{2.1}$$

where the summation is over any representative set of modulo $\mathfrak{q}$. We define the generalized Gaussian sum $\tau(\sigma, \chi)$ by

$$\tau(\sigma, \chi) = \sum_{\xi \pmod{\mathfrak{q}}} \sigma(\xi)\chi(\xi).$$

LEMMA 2.1. *Let σ be a primitive additive character modulo $\mathfrak{q}$ and let be χ a primitive multiplicative character modulo $\mathfrak{q}$. For any integer $\beta \in \mathcal{O}_K$ we have*

$$\chi(\beta)\tau(\sigma, \overline{\chi}) = \sum_{\xi \pmod{\mathfrak{q}}} \overline{\chi}(\xi)\sigma(\beta\xi). \tag{2.2}$$

PROOF. See [**9**, Lemma 2, p. 190]. □

LEMMA 2.2. *Let σ be a primitive additive character modulo $\mathfrak{q}$ and let χ be a primitive multiplicative character modulo $\mathfrak{q}$. We have*

$$|\tau(\sigma, \overline{\chi})|^2 = N\mathfrak{q} \tag{2.3}$$

PROOF. See [**9**, Corollary, p. 190]. □

THEOREM 2.3.

$$\sum_{\substack{N\mathfrak{q} \leq Q \\ (\mathfrak{q}, \mathfrak{a}) = 1}} \sum_{\sigma \bmod \mathfrak{q}}{}' \left| \sum_{\alpha \equiv 0 \pmod{\mathfrak{a}}} c(\alpha)\sigma(\alpha) \right|^2 \leq f(x, \mathfrak{a}, Q) \sum_{\substack{\alpha \in \mathfrak{R} \\ \alpha \equiv 0 \pmod{\mathfrak{a}}}} |c(\alpha)|^2,$$

where $f(x, \mathfrak{a}, Q) = \left(\frac{\sqrt{8}}{\sqrt[4]{3}} \left(\frac{x}{N\mathfrak{a}} \right)^{\frac{1}{4}} + c_0 |D|^{\frac{1}{4}} Q^{\frac{1}{2}} \right)^4$,

$$c_0 = \begin{cases} \left(1 - \frac{1}{\sqrt{3}}\right)^{-\frac{1}{2}} & \text{if} \quad D \equiv 1 \pmod 4, \\ \left(\frac{1}{2} - \frac{1}{2\sqrt{3}}\right)^{-\frac{1}{2}} & \text{if} \quad D \equiv 2, 3 \pmod 4, \end{cases}$$

and $\sum'$ *denotes summation over primitive additive characters* $\pmod{\mathfrak{q}}$*, and the* $c(\alpha)$ *are any complex number.*

PROOF. See Section 3. □

Now, we prove Theorem 1.2.

PROOF. If $(\mathfrak{a},\mathfrak{q}) \neq 1$ the proof is immediate. We can assume that $(\mathfrak{a},\mathfrak{q}) = 1$. Multiplying (2.1) by $c(\alpha)$ and summing over $\alpha \in \mathfrak{R}$, $\alpha \equiv 0 \pmod{\mathfrak{a}}$, we obtain

$$\begin{aligned}\tau(\sigma,\overline{\chi}) \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\chi(\alpha) &= \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha) \sum_{\xi \pmod{\mathfrak{q}}} \overline{\chi}(\xi)\sigma(\alpha\xi)\\ &= \sum_{\xi \pmod{\mathfrak{q}}} \overline{\chi}(\xi) \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\sigma(\alpha\xi).\end{aligned}$$

By Lemma 2.2 we have

$$N\mathfrak{q} \sum_{\chi \bmod \mathfrak{q}}^{*} \left| \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\chi(\alpha)\right|^2 \leq \sum_{\chi \bmod \mathfrak{q}} \left| \sum_{\xi \pmod{\mathfrak{q}}} \overline{\chi}(\xi) \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\sigma(\alpha\xi)\right|^2,$$

where $\sum^{*}$ denotes summation over primitive multiplicative characters $\pmod{\mathfrak{q}}$. By (2.1),

$$\sum_{\chi \bmod \mathfrak{q}} \left| \sum_{\xi \pmod{\mathfrak{q}}} \overline{\chi}(\xi) \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\sigma(\alpha\xi)\right|^2 = \Phi(\mathfrak{q}) \sum_{\substack{\xi \pmod{\mathfrak{q}}\\ (\xi,\mathfrak{q})=1}} \left| \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\sigma(\alpha\xi)\right|^2.$$

Since σ is a primitive character, $\sigma(\alpha\xi)$ runs through all the primitive characters modulo $\mathfrak{q}$ as ξ runs through the relative prime residues modulo $\mathfrak{q}$. Indeed, if $\sigma(\alpha\xi_1) = \sigma(\alpha\xi_2)$, then $\sigma(\alpha(\xi_1 - \xi_2)) = 1$ for $\alpha \in \mathfrak{R}$. So $\sigma(\eta) = 1$ for all η divisible by the ideal $(\xi_1 - \xi_2, \mathfrak{q})$. But this is possible by $\xi_1 \equiv \xi_2 \pmod{\mathfrak{q}}$. Hence,

$$\Phi(\mathfrak{q}) \sum_{\substack{\xi \pmod{\mathfrak{q}}\\ (\xi,\mathfrak{q})=1}} \left| \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\sigma(\alpha\xi)\right|^2 = \Phi(\mathfrak{q}) \sum_{\sigma \bmod \mathfrak{q}}{}' \left| \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\sigma(\alpha)\right|^2,$$

where $\sum'$ denotes summation over primitive multiplicative characters $\pmod{\mathfrak{q}}$. By the above,

$$N\mathfrak{q} \sum_{\chi \bmod \mathfrak{q}}^{*} \left| \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\chi(\alpha)\right|^2 \leq \Phi(\mathfrak{q}) \sum_{\sigma \bmod \mathfrak{q}}{}' \left| \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\sigma(\alpha)\right|^2.$$

Theorem 2.3 shows that

$$\sum_{\substack{N\mathfrak{q}\leq Q\\ (\mathfrak{q},\mathfrak{a})=1}} \frac{N\mathfrak{q}}{\Phi(\mathfrak{q})} \sum_{\chi \bmod \mathfrak{q}}^{*} \left| \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\chi(\alpha)\right|^2 \leq f(x,\mathfrak{a},Q) \sum_{\substack{\alpha\in\mathfrak{R}\\ \alpha\equiv 0 \pmod{\mathfrak{a}}}} |c(\alpha)|^2,$$

where $f(x,\mathfrak{a},Q)$ is defined in Theorem 2.3. This finishes the proof. □

3. The Proof of Theorem 2.3

Let $\mathfrak{a} = (\alpha_1, \alpha_2)$ be an ideal of K, where α_1, α_2 is an integral basis of $\mathfrak{a}$. We denote by

$$\Delta(\alpha_1, \alpha_2) = \begin{vmatrix} \alpha_1 & \alpha_2 \\ \overline{\alpha}_1 & \overline{\alpha}_2 \end{vmatrix} \tag{3.1}$$

the different of the ideal $\mathfrak{a}$. In particular,

$$\Delta(1, \omega) = \begin{cases} \sqrt{D} & \text{if} \quad D \equiv 1 \pmod 4, \\ 2\sqrt{D} & \text{if} \quad D \equiv 2, 3 \pmod 4. \end{cases} \tag{3.2}$$

Let

$$d(K) = \Delta^2(1, \omega) \tag{3.3}$$

denote the discriminant of the field K. We recall [**8**, see Th. 76, p. 87] that

$$N\mathfrak{a} = \frac{|\Delta(\alpha_1, \alpha_1)|}{|\sqrt{d(K)}|}. \tag{3.4}$$

We denote by $\mathfrak{d}$ the different ideal of K. The following lemma will be useful.

LEMMA 3.1. *Let $K = \mathbb{Q}(\sqrt{D})$ be an imaginary quadratic field with the corresponding ring of integers $\mathcal{O}_K$, and let $d(K)$ be the fundamental discriminant of the field K. Let $\mathfrak{a}$ be an integral ideal of K. There exist the basis α_1, α_2 of $\mathfrak{a}$ such that*

$$|\alpha_i| \leq \left(\frac{4}{3} d(K) N(\mathfrak{a})\right)^{\frac{1}{2}}, \qquad |\overline{\alpha}_i| \leq \left(\frac{4}{3} d(K) N(\mathfrak{a})\right)^{\frac{1}{2}}, \qquad i = 1, 2. \tag{3.5}$$

PROOF. Let $\alpha \in \mathfrak{a}$, $\alpha = \alpha_1 x + \alpha_2 y$, where α_1, α_2 is an integral basis of $\mathfrak{a}$, $x, y \in \mathbb{Z}$. Then

$$\frac{N(\alpha)}{N(\mathfrak{a})} = ax^2 + bxy + cy^2 = f(x, y) \tag{3.6}$$

is a primitive positive quadratic form over $\mathbb{Z}$ with discriminant $d(K)$ [**14**, see Proposition 5.2]. It is well known that there is one-to-one correspondence between the set of all classes of primitive positive definite binary quadratic forms of discriminant $d(K)$ and the group of ideal classes $H(K)$ of field K [**14**, see Proposition 5.2]. Let $X \in H(K)$ be the ideal class containing $\mathfrak{a}$, and let X_f be the corresponding the equivalence class of primitive positive definite binary quadratic forms. Hence $f \in X_f$, and there is a reduced form g equivalent to f [**14**, see Proposition 5.1]. Let $\mathfrak{b} \in X$ be an ideal equivalent to $\mathfrak{a}$ corresponding to g. Let β_1, β_2 be an basis of $\mathfrak{b}$, and let $\beta = \beta_1 x + \beta_2 y$, where $\beta \in \mathfrak{b}$, $x, y \in \mathbb{Z}$. Then

$$g = \frac{N(\beta_1 x + \beta_2 y)}{N(\mathfrak{b})} = \frac{N(\beta_1)}{N(\mathfrak{b})} x^2 + \frac{\Delta(\beta_1, \beta_2)}{N(\mathfrak{b})} xy + \frac{N(\beta_2)}{N(\mathfrak{b})} y^2, \tag{3.7}$$

where $N(\mathfrak{b})$ divides $N(\beta_i)$, $i = 1, 2$. By [**13**, see Theorem 3, p. 69] we obtain

$$\frac{N(\beta_i)}{d(K) N(\mathfrak{b})} \leq \frac{N(\beta_1) N(\beta_2)}{d(K) N(\mathfrak{b})^2} \leq \left(\frac{4}{\pi}\right)^2 \left(\Gamma\left(\frac{3}{2}\right)\right)^2 \leq 1.28 \leq \frac{4}{3}, \quad i = 1, 2, \tag{3.8}$$

where Γ is the gamma function. (Compare the above estimation to Hermite's constant $\gamma_2 = \frac{4}{3}$ (see [**13**], p. 71)). Hence,

$$|\beta_i|^2 \leq \frac{4}{3} d(K) N(\mathfrak{b}), \qquad |\overline{\beta}_i|^2 \leq \frac{4}{3} d(K) N(\mathfrak{b}), \qquad i = 1, 2. \tag{3.9}$$

Since $\mathfrak{a}, \mathfrak{b} \in X$, there is $\delta \in K$ such that $\mathfrak{a} = \delta\mathfrak{b} = (\delta\beta_1, \delta\beta_2)$. Thus, there is a basis α_1', α_2' of $\mathfrak{a}$ such that

$$|\alpha_i'|^2 \leq |\delta\beta_i|^2 \leq \frac{4}{3}d(K)N(\mathfrak{b})N(\delta) = \frac{4}{3}d(K)N(\mathfrak{a}), \qquad i = 1, 2,$$

and consequently

$$|\alpha_i'| \ \leq \left(\frac{4}{3}d(K)N(\mathfrak{a})\right)^{\frac{1}{2}}, \qquad |\overline{\alpha'}_i| \leq \left(\frac{4}{3}d(K)N(\mathfrak{a})\right)^{\frac{1}{2}}, \qquad i = 1, 2.$$

This finishes the proof. □

Now, we prove Theorem 2.3.

Proof. Let $\mathfrak{a}$ be an integral ideal of K. Lemma 3.1 shows that there exist the basis α_1, α_2 of $\mathfrak{a}$ such that

$$|\alpha_i| \leq \left(\frac{4}{3}d(K)N(\mathfrak{a})\right)^{\frac{1}{2}}, \qquad |\overline{\alpha}_i| \leq \left(\frac{4}{3}d(K)N(\mathfrak{a})\right)^{\frac{1}{2}}, \qquad i = 1, 2. \tag{3.10}$$

Let $\alpha \in \mathfrak{R}$ and $\alpha \in \mathfrak{a}$. Then α is uniquely expressible in the form $\alpha = m_1\alpha_1 + m_2\alpha_2$, where $m_1, m_2 \in \mathbb{Z}$. From (1.8)

$$|\alpha| \leq \sqrt{x}, \qquad |\overline{\alpha}| \leq \sqrt{x}. \tag{3.11}$$

We have

$$\begin{bmatrix} m_1 \\ m_2 \end{bmatrix} = \begin{bmatrix} \alpha_1 & \alpha_2 \\ \overline{\alpha}_1 & \overline{\alpha}_2 \end{bmatrix}^{-1} \begin{bmatrix} \alpha \\ \overline{\alpha} \end{bmatrix} = \frac{1}{\Delta(\alpha_1, \alpha_2)} \begin{bmatrix} \overline{\alpha}_2 & -\alpha_2 \\ -\overline{\alpha}_1 & \alpha_1 \end{bmatrix} \begin{bmatrix} \alpha \\ \overline{\alpha} \end{bmatrix},$$

so

$$\begin{aligned} |m_1| &\leq \frac{|\overline{\alpha}_2\alpha - \alpha_2\overline{\alpha}|}{|\Delta(\alpha_1, \alpha_2)|} \leq \frac{4}{\sqrt{3}}(N\mathfrak{a})^{-\frac{1}{2}}\sqrt{x}, \\ |m_2| &\leq \frac{|\alpha_1\overline{\alpha} - \overline{\alpha}_1\alpha|}{|\Delta(\alpha_1, \alpha_2)|} \leq \frac{4}{\sqrt{3}}(N\mathfrak{a})^{-\frac{1}{2}}\sqrt{x}. \end{aligned} \tag{3.12}$$

Let $\mathfrak{q}$ be an integral ideal of K, and let $\mathfrak{b}$ be any ideal prime to $\mathfrak{q}$ lying in the same ideal class as $\mathfrak{q}\mathfrak{d}$. There exist $\rho \in K$ such that

$$(\rho) = \frac{\mathfrak{b}}{\mathfrak{q}\mathfrak{d}}, \qquad (\mathfrak{b}, \mathfrak{q}) = 1. \tag{3.13}$$

Suppose that $\gamma_j \in \mathcal{O}_K$, $(\gamma_j, \mathfrak{q}) = 1$ run through a complete residue system (mod $\mathfrak{q}$). The number of residue classes relatively prime to $\mathfrak{q}$ is equal to $\Phi(q)$, so $j = 1, \ldots, \Phi(q)$. By [**16**, Lemma 1, p. 253] the numbers $\rho\gamma_j$ run through a complete system of numbers which are pairwise incongruent (mod $\mathfrak{d}^{-1}$), and

$$(\rho\gamma_j)\mathfrak{d} = \frac{(\gamma_j)\mathfrak{b}}{\mathfrak{q}}, \qquad ((\gamma_j)\mathfrak{b}, \mathfrak{q}) = 1. \tag{3.14}$$

Let $\sigma(\alpha)$ be an additive character modulo $\mathfrak{q}$. By [**9**, Lemma 1, p. 186] all primitive additive characters σ (mod $\mathfrak{q}$) have the form

$$\sigma_j(\alpha) = e(Tr(\rho\gamma_j\alpha)), \qquad e(\theta) = 2\pi i\theta, \qquad j = 1, \ldots, \Phi(\mathfrak{q}). \tag{3.15}$$

We define

$$\mathcal{R} = \{\xi = m_1\alpha_1 + m_2\alpha_2 \in \mathfrak{a}, \quad |m_i| \leq \frac{4}{\sqrt{3}}(N\mathfrak{a})^{-\frac{1}{2}}\sqrt{x}, \quad m_i \in \mathbb{Z}, \quad i = 1, 2\}.$$

By [**8**, Th. 102, p. 118] the numbers

$$\beta_1 = \frac{\overline{\alpha}_2}{\Delta(\alpha_1,\alpha_2)}, \qquad \beta_2 = \frac{-\overline{\alpha}_1}{\Delta(\alpha_1,\alpha_2)} \tag{3.16}$$

form a basis for the ideal $(\mathfrak{a}\mathfrak{d})^{-1}$, and by (3.10)

$$|\beta_i| \leq \frac{2}{\sqrt{3}}(N\mathfrak{a})^{-\frac{1}{2}}, \qquad |\overline{\beta}_i| \leq \frac{2}{\sqrt{3}}(N\mathfrak{a})^{-\frac{1}{2}}, \qquad i=1,2. \tag{3.17}$$

The numbers β_1, β_2 forms the basis of K, so we can write

$$\rho\gamma_j = s_{1j}\beta_1 + s_{2j}\beta_2, \qquad s_{ij} \in \mathbb{Q}, \quad i=1,2, \quad j=1,\ldots,\Phi(\mathfrak{q}). \tag{3.18}$$

Since $\overline{\beta}_1 = -\frac{\alpha_2}{\Delta(\alpha_1,\alpha_2)}$ and $\overline{\beta}_2 = \frac{\alpha_1}{\Delta(\alpha_1,\alpha_2)}$, by (3.1) we obtain

$$Tr(\rho\gamma_j\xi) = s_{1j}m_1 + s_{2j}m_2, \tag{3.19}$$

for $\xi \in \mathcal{R}$. Hence, with the notation

$$c'(\xi) = \begin{cases} c(\xi) & \text{for} \quad \xi \in \mathfrak{R}, \quad \xi \in \mathfrak{a}, \\ 0 & \text{for} \quad \xi \in \mathcal{R}, \quad \xi \notin \mathfrak{R}, \end{cases} \tag{3.20}$$

we have

$$\sum_{\substack{\alpha \in \mathfrak{R} \\ \alpha \equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\sigma(\alpha) = \sum_{\xi \in \mathcal{R}} c'(\xi)\sigma(\xi) = \sum_{\substack{m_1,m_2 \\ m_1\alpha_1+m_2\alpha_2 \in \mathfrak{a}}} c(m_1,m_2)e(m_1s_1+m_2s_2),$$

where $|m_i| \leq \frac{4}{\sqrt{3}}(N\mathfrak{a})^{-\frac{1}{2}}\sqrt{x}$, $i=1,2$. Now, we estimate the above sum. To do this fix two integral ideals $\mathfrak{q}, \mathfrak{q}'$of K such that $(\mathfrak{q},\mathfrak{a}) = (\mathfrak{q}',\mathfrak{a}) = 1$. Let

$$\rho\gamma = s_1\beta_1 + s_2\beta_2, \qquad \rho'\gamma' = s_1'\beta_1 + s_2'\beta_2, \qquad s_j, s_j' \in \mathbb{Q}, \qquad j=1,2, \tag{3.21}$$

where $(\gamma,\mathfrak{q}) = (\gamma',\mathfrak{q}') = 1$, and $\gamma \not\equiv \gamma' \pmod{\mathfrak{q}}$ if $\mathfrak{q} = \mathfrak{q}'$. We estimate

$$\max_{j=1}^{2} \|s_j - s_j'\|, \qquad j=1,2,$$

where $\|x\|$ denotes the distance from a real number x to the nearest integer. To do this, we write $s_j - s_j' = t_j + l_j$, where $l_j \in \mathbb{Z}$ and $-\frac{1}{2} < t_j \leq \frac{1}{2}$, $j=1,2$. Then

$$\rho\gamma - \rho'\gamma' = t_1\beta_1 + t_2\beta_2 + \delta, \qquad \delta \in \frac{1}{\mathfrak{a}\mathfrak{d}}, \tag{3.22}$$

where $\delta = l_1\beta_1 + l_2\beta_2$. We show that at least one $t_j \neq 0$, $j=1,2$. Suppose, contrary to our claim, that $t_1 = t_2 = 0$. Then $\rho\gamma \equiv \rho'\gamma' \pmod{(\mathfrak{a}\mathfrak{d})^{-1}}$. If $\mathfrak{q} = \mathfrak{q}'$, then $\rho = \rho'$ and $(\rho)\mathfrak{a}\mathfrak{d}(\gamma - \gamma') \in \mathcal{O}_K$. This gives $\gamma \equiv \gamma' \pmod{\mathfrak{q}}$, contrary to our assumption. If $\mathfrak{q} \neq \mathfrak{q}'$, by (3.14) we have

$$(\rho\gamma)\mathfrak{d} = \frac{(\gamma)\mathfrak{b}}{\mathfrak{q}}, \qquad (\rho'\gamma')\mathfrak{d} = \frac{(\gamma')\mathfrak{b}'}{\mathfrak{q}'}, \qquad ((\gamma)\mathfrak{b},\mathfrak{q}) = ((\gamma')\mathfrak{b}',\mathfrak{q}') = 1. \tag{3.23}$$

From (3.22) we obtain

$$\mathfrak{a}(\gamma)\mathfrak{b}\mathfrak{q}' = \mathfrak{a}\mathfrak{q}\mathfrak{q}'(\rho\gamma)\mathfrak{d} = \mathfrak{a}\mathfrak{q}\mathfrak{q}'(\rho'\gamma' + \delta)\mathfrak{d} = \mathfrak{q}\mathfrak{c}, \tag{3.24}$$

$$\mathfrak{a}(\gamma')\mathfrak{b}'\mathfrak{q} = \mathfrak{a}\mathfrak{q}\mathfrak{q}'(\rho'\gamma')\mathfrak{d} = \mathfrak{a}\mathfrak{q}\mathfrak{q}'(\rho\gamma + \delta)\mathfrak{d} = \mathfrak{q}\mathfrak{c}', \tag{3.25}$$

where $\mathfrak{c}, \mathfrak{c}'$ are integral ideals of K. This gives $\mathfrak{q} \mid \mathfrak{q}'$ and $\mathfrak{q}' \mid \mathfrak{q}$. This contradicts our assumption. Consequently,

$$\rho\gamma - \rho'\gamma' - \delta = t_1\beta_1 + t_2\beta_2 \neq 0, \qquad \rho\gamma - \rho'\gamma' - \delta \in \frac{1}{\mathfrak{a}\mathfrak{d}\mathfrak{q}\mathfrak{q}'}. \tag{3.26}$$

Hence,

$$\|s_j - s'_j\| = |t_j| \geq |\rho\gamma - \rho'\gamma' - \delta| - |t_i\beta_i| \geq N(\mathfrak{a}\mathfrak{d}\mathfrak{q}\mathfrak{q}')^{-\frac{1}{2}} - \frac{1}{\sqrt{3}}N(\mathfrak{a})^{-\frac{1}{2}}$$
$$\geq \left(1 - \frac{1}{\sqrt{3}}\right) N(\mathfrak{d})^{-\frac{1}{2}} N(\mathfrak{q}\mathfrak{q})^{-\frac{1}{2}},$$

where $i = 2$ if $j = 1$, and $i = 1$ if $j = 2$. Consequently,

$$\max_{j=1}^{2} \|s_j - s'_j\| \geq \begin{cases} \left(1 - \frac{1}{\sqrt{3}}\right) |D|^{-\frac{1}{2}} Q^{-1} & \text{if} \quad D \equiv 1 \pmod 4, \\ \left(\frac{1}{2} - \frac{1}{2\sqrt{3}}\right) |D|^{-\frac{1}{2}} Q^{-1} & \text{if} \quad D \equiv 2, 3 \pmod 4. \end{cases}$$

By [**11**, Theorem 1] we obtain

$$\sum_{\substack{N\mathfrak{q} \leq Q \\ (\mathfrak{q},\mathfrak{a})=1}} \sum_{\sigma \bmod \mathfrak{q}}{}' \left| \sum_{\substack{\alpha \in \mathfrak{R} \\ \alpha \equiv 0 \pmod{\mathfrak{a}}}} c(\alpha)\sigma(\alpha) \right|^2 \leq \left(\frac{\sqrt{8}}{\sqrt[4]{3}} \left(\frac{x}{N\mathfrak{a}}\right)^{\frac{1}{4}} + c_0 |D|^{\frac{1}{4}} Q^{\frac{1}{2}} \right)^4 \sum_{\substack{\alpha \in \mathfrak{R} \\ \alpha \equiv 0 \pmod{\mathfrak{a}}}} |c(\alpha)|^2,$$

where

$$c_0 = \begin{cases} \left(1 - \frac{1}{\sqrt{3}}\right)^{-\frac{1}{2}} & \text{if} \quad D \equiv 1 \pmod 4, \\ \left(\frac{1}{2} - \frac{1}{2\sqrt{3}}\right)^{-\frac{1}{2}} & \text{if} \quad D \equiv 2, 3 \pmod 4. \end{cases}$$

This finishes the proof. □

References

1. A. Atkin and F. Morain, *Elliptic curves and primality proving*, Tech. report, Projet ICSLA RR-1256, INRIA, 1990.
2. E. Bombieri, *On the large sieve*, Mathematica (1965), no. 12, 201–225.
3. E. Bombieri and H. Davenport, *On the large sieve method*, pp. 9–22, Springer US, Boston, MA, 1969.
4. R. Dupont, A. Enge, and F. Morain, *Building curves with arbitrary small mov degree over finite prime fields*, J. Cryptology **18** (2005), no. 2, 79–89.
5. K. Durnoga and J. Pomykała, *Large sieve, miller-rabin compositeness witnesses and integer factoring problem*, Fundamenta Informaticae **156** (2017), no. 2, 179–185.
6. Maciej Grześkowiak, *An algorithmic construction of finite elliptic curves of order divisible by a large prime*, Fundam. Inf. **136** (2015), no. 4, 331–343.
7. ———, *Explicit bound for the prime ideal theorem in residue classes*, Number-Theoretic Methods in Cryptology 2017, LNCS **10737** (2018), 48–68.
8. E. Hecke, *Lectures on the theory of algebraic numbers*, Springer-Verlag, 1981.
9. J. Hinz, *Methoden des grossen Siebes in algebraischen Zahlkörpern.*, Manuscripta Math. **57** (1987), no. 2, 181–194.
10. ———, *A generalization of bombieri's prime number theorem to algebraic number fields*, Acta Arith. **51** (1988), no. 2, 173–193.
11. M. N. Huxley, *The large sieve inequality for algebraic number fields*, Mathematika **15** (1968), no. 2, 178–187.
12. M. N. Huxley, *The large sieve inequality for algebraic number fields. iii. zero-density results*, J. London Math. Soc. **2** (1971), no. 3, 233–240.
13. C.G. Lekkerkerker and P. Gruber, *Geometry of numbers*, North-Holland Mathematical Library, Elsevier Science, 1987.
14. W. Narkiewicz, *Classical problems in number theory*, Monografie Matematyczne, Pan. Wyd. Naukowe, 1986.
15. J. Pomykała, *On exponents of modular subgroups generated by small consecutive integers*, Acta Arith. (2016), no. 176, 321–342.

16. W. Schaal, *On the large sieve method in algebraic number fields*, Journal of Number Theory **2**, no. 3.
17. R. J. Wilson, *The large sieve in algebraic number fields*, Mathematika **16** (1969), no. 2, 189–204.

Adam Mickiewicz University,, Faculty of Mathematics and Computer Science,, Umultowska 87, 61-614 Poznań, Poland

E-mail address: maciejg@amu.edu.pl