Research Article

Maciej Grześkowiak*

A variant of the large sieve inequality with explicit constants

<https://doi.org/10.1515/jmc-2019-0022>

Received Jul 05, 2019; accepted May 06, 2020

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.

Keywords: Large sieve, computational complexity of algorithms

2010 Mathematics Subject Classification: 11L40, 11N36, 68Q25

1 Introduction

We begin by recalling the following form of the large sieve inequality [1]. Let

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

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

$$\|x_r - x_s\| \geq \delta \quad (2)$$

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

$$\sum_{r=1}^R |S(x_r)|^2 \leq \Delta \sum_{n=M+1}^{M+N} |c_n|^2, \quad (3)$$

where $\Delta = \delta^{-1} + N - 1$. Huxley [2] generalized the above inequality to algebraic number fields K of degree k over the field $\mathbb{Q}$ of rational numbers. In his paper the integers $M+1 \leq n \leq M+N$ are replaced by algebraic integers of $\alpha \in K$ such that

$$\alpha = n_1 \omega_1 + \dots + n_k \omega_k, \quad M_i + 1 \leq n_i \leq M_i + N_i, \quad i = 1, \dots, k, \quad (4)$$

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 [3]. 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 , that is certain parallelotopes independent of a basis are considered. In 1987 Hinz proved a variant of the large sieve inequality to algebraic numbers [4]. His proof is based on the ideas presented in [2], [3], [5].

***Corresponding Author: Maciej Grześkowiak:** Adam Mickiewicz University, Faculty of Mathematics and Computer Science, Umultowska 87, 61-614 Poznań, Poland; Email: maciejg@amu.edu.pl

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

$$\sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^q |S(a/q)|^2 \leq (N + Q^2) \sum_{n=M+1}^{M+N} |c_n|^2, \quad (5)$$

where the summation is over primes q . The analogous version to algebraic number fields of the above estimation was given in [4], [2], [3], [5]. However, in [4] the inequality stated above depends on a numerical constant not explicitly given. A second application of the large sieve inequality to number theory arises from the following estimation of a character sum.

$$\sum_{q \leq Q} \frac{q}{\varphi(q)} \sum_{\chi \bmod q}^* \left| \sum_{n=M+1}^{M+N} c_n \chi(n) \right|^2 \leq (N + Q^2) \sum_{n=M+1}^{M+N} |c_n|^2, \quad (6)$$

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 authors of [4], [2], [3], [5]. Let us mention that in [4] the inequality (6) depends on a constant, which not given explicitly. The inequality stated above and its generalizations are essential tools in studying L-functions and distribution of prime numbers. It is central to the proof of various version of the Bombieri-Vinogradov theorem [6], [7], [8]. As an example of the application of the large sieve inequality to computational number theory and cryptography we refer the reader to [9], [10], [11]. In [9] 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

$$|t| \leq 2\sqrt{p}, \quad q \mid p + 1 - t, \quad 4p - t^2 = \Delta f^2. \quad (7)$$

Let $E : y^2 = x^3 + ax + b$ be an elliptic curve defined over $\mathbb{F}_p$. 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 [12], [13]. 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 [9] a polynomial time algorithm for constructing primes of the form (7) is given. The main idea of the algorithm is as follows. Let $D < 0$ be a square-free integer. Fix $K = \mathbb{Q}(\sqrt{D})$ with the corresponding ring of integers $\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$, where $\omega = \frac{1+\sqrt{D}}{2}$, if $D \equiv 1 \pmod{4}$, or $\omega = \sqrt{D}$, if $D \equiv 2, 3 \pmod{4}$. Let $\bar{\alpha}$ denote the complex conjugate of α . By $N_{K/\mathbb{Q}}(\alpha) = \alpha\bar{\alpha}$ we denote the norm of an element $\alpha \in \mathcal{O}_K$. 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 (7) satisfying $(\log p)/(\log q) \ll 5/(2 - 5\varepsilon)$ [9]. However, it is interesting to know 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 [9]. In [14] 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 (7). In order to analyze the second procedure explicitly it is necessary to compute the numerical value of the constant occurring in the variant of the Bombieri-Vinogradov theorem presented in [7]. To do this, bounding of a character sum [4] analogous to (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 $\mathfrak{q}$ be an integral ideal of $\mathcal{O}_K$. By $N\mathfrak{q}$ we denote the norm of $\mathfrak{q}$ with respect to $\mathbb{Q}$, and by $\Phi(\mathfrak{q})$ we denote the generalized Euler's function. The modulus of a complex number α will be denoted by $|\alpha|$. Let χ be a multiplicative character modulo $\mathfrak{q}$. Let $x > 1$ be an arbitrary but fixed number. We define

$$\mathfrak{R} = \{\beta \in \mathcal{O}_K : |\beta| < \sqrt{x}\}. \quad (8)$$

We prove the following theorem.

Theorem 1.2. Fix $Q > 1$. We have

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

where $f(x, \mathfrak{a}, Q) = \left(2.14 \left(\frac{x}{N\mathfrak{a}} \right)^{\frac{1}{4}} + c_0 |D|^{\frac{1}{4}} Q^{\frac{1}{2}} \right)^4$,

$$c_0 = \begin{cases} 1.53 & \text{if } D \equiv 1 \pmod{4}, \\ 2.19 & \text{if } D \equiv 2, 3 \pmod{4}. \end{cases}$$

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

Proof. In Section 2. □

2 The Proof of Theorem 1.2

Let σ be an additive character modulo $\mathfrak{q}$, that is, a function defined for all integers $\alpha \in \mathcal{O}_K$ which depends only on $\alpha \bmod \mathfrak{q}$ and satisfies

$$\sigma(\alpha + \beta) = \sigma(\alpha)\sigma(\beta), \quad \alpha, \beta \in \mathcal{O}_K$$

and is not always 0. The number of distinct additive characters is $N\mathfrak{q}$. Hence we have

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

and

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

We denote by σ_0 the principal additive character modulo $\mathfrak{q}$, and we say that a character is primitive if it is not a character mod $\mathfrak{b}$ for any ideal $\mathfrak{b}$ which properly divides $\mathfrak{q}$. There is an isomorphism between the additive characters σ to a given modulus $\mathfrak{q}$, and the residue classes of integers mod $\mathfrak{q}$. In this isomorphism, primitive characters correspond to residue classes relatively prime to $\mathfrak{q}$. For this reason the number of primitive additive characters modulo $\mathfrak{q}$ is $\Phi(\mathfrak{q})$.

The residue classes of integers relatively prime to $\mathfrak{q}$ form an Abelian group under multiplication of order $\Phi(\mathfrak{q})$. Let χ be character modulo $\mathfrak{q}$ on this group, that is, a function defined for all integers $\alpha \bmod \mathfrak{q}$ which depends only on $\alpha \bmod \mathfrak{q}$ and satisfies

$$\chi(\alpha\beta) = \chi(\alpha)\chi(\beta), \quad \alpha, \beta \in \mathcal{O}_K$$

and is 0 if α is not relatively prime to q but is not always 0. We have

$$\sum_{\alpha \pmod{q}} \chi(\xi) = \begin{cases} \Phi(q) & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0, \end{cases} \quad (9)$$

where the summation is over any representative set of modulo q . We denote by χ_0 the principal multiplicative character modulo q , and we define primitive characters modulo q in the usual way. We define the generalized Gaussian sum $\tau(\sigma, \chi)$ by

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

In the proof of Theorem 1.2 we shall need the following auxiliary theorems and lemmas.

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

$$\chi(\beta) \tau(\sigma, \bar{\chi}) = \sum_{\xi \pmod{q}} \bar{\chi}(\xi) \sigma(\beta \xi). \quad (10)$$

Proof. See [4, Lemma 2, p. 190]. □

Lemma 2.2. *Let σ be a primitive additive character modulo q and let χ be a primitive multiplicative character modulo q . We have*

$$|\tau(\sigma, \bar{\chi})|^2 = Nq \quad (11)$$

Proof. See [4, Corollary, p. 190]. □

Theorem 2.3.

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

where $f(x, a, Q) = \left(2.14 \left(\frac{x}{N\alpha} \right)^{\frac{1}{4}} + c_0 |D|^{\frac{1}{4}} Q^{\frac{1}{2}} \right)^4$,

$$c_0 = \begin{cases} 1.53 & \text{if } D \equiv 1 \pmod{4}, \\ 2.19 & \text{if } D \equiv 2, 3 \pmod{4}. \end{cases}$$

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

Proof. In Section 3. □

Now, we prove Theorem 1.2.

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

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

By Lemma 2.2 we have

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

where $\sum^*$ denotes summation over primitive multiplicative characters $(\bmod q)$. By (9),

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

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

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

where $\sum'$ denotes summation over primitive multiplicative characters $(\bmod q)$. By the above,

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

Theorem 2.3 shows that

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

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

3 The Proof of Theorem 2.3

Let

$$F(x, y) = Ax^2 + Bxy + Cy^2, \quad (A, B, C) = 1, \quad A, B, C \in \mathbb{Z}$$

be a primitive binary quadratic form. We denote by $D(F) = B^2 - 4AC$ its discriminant. If $D(F) < 0$ and $A > 0$ the form $F(x, y)$ represents only positive integers and is called positive definite. We say that two forms $F(x, y)$ and $G(x, y)$ are equivalent if there exists a matrix

$$U = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbb{Z})$$

such that

$$F(x, y) = G(ax + by, cx + dy).$$

Every primitive positively definite quadratic form is equivalent to form $G(x, y) = Ax^2 + Bxy + Cy^2$ which satisfies

$$|B| \leq A \leq C.$$

We call such form reduced form. Let $D < 0$ be a square-free integer. Fix $K = \mathbb{Q}(\sqrt{D})$ with the corresponding ring of integers $\mathcal{O}_K = \{a + b\omega : a, b \in \mathbb{Z}\}$, where $\omega = \frac{1+\sqrt{D}}{2}$, if $D \equiv 1 \pmod{4}$, or $\omega = \sqrt{D}$, if $D \equiv 2, 3 \pmod{4}$. 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

$$\Delta(\alpha_1, \alpha_2) = \det \begin{bmatrix} \alpha_1 & \alpha_2 \\ \bar{\alpha}_1 & \bar{\alpha}_2 \end{bmatrix} \quad (12)$$

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

$$\Delta(1, \omega) = \begin{cases} \sqrt{D} & \text{if } D \equiv 1 \pmod{4}, \\ 2\sqrt{D} & \text{if } D \equiv 2, 3 \pmod{4} \end{cases} \quad (13)$$

is different of the field K , and

$$D = \Delta^2(1, \omega)$$

is the discriminant of the field K . We denote by $\mathfrak{d}$ the different ideal of K , that is the ideal generated by different of the field K . We recall [15, see Th. 76, p. 87] that

$$N\mathfrak{a} = \frac{|\Delta(\alpha_1, \alpha_2)|}{|\sqrt{D}|}. \quad (14)$$

Two ideals $\mathfrak{a}, \mathfrak{b}$ of $\mathcal{O}_K$ are said to be equivalent if there are $\alpha, \beta \in \mathcal{O}_K$ such that $\alpha\mathfrak{a} = \beta\mathfrak{b}$. This equivalence splits the set of ideals of $\mathcal{O}_K$ into a finite number of classes. The set of all equivalence classes is called the class group of the field K . We will denote it by $H(K)$. If $D(F)$ is equal to D , then quadratic form is primitive. There is a connection between equivalence classes of primitive positive definite binary quadratic forms of a given discriminant D and the ideal classes in the ring $\mathcal{O}_K$ in the field $K = \mathbb{Q}(\sqrt{D})$. Let $\mathfrak{a} = (\alpha_1, \alpha_2)$ be an ideal of $\mathcal{O}_K$, where pair α_1, α_2 is ordered in such a way that the number $\Delta(\alpha_1, \alpha_2)$ lies in the upper half-plane. For every such pair (α_1, α_2) we define

$$F(x, y) = N_{K/\mathbb{Q}}(\alpha_1 x + \alpha_2 y) / N\mathfrak{a}.$$

Then $F(x, y)$ is a primitive positive definite binary quadratic forms over $\mathbb{Z}$ of discriminant D . On the other hand, every $F(x, y) = Ax^2 + Bxy + Cy^2$ a primitive positive definite binary quadratic form of discriminant D is equals to $N_{K/\mathbb{Q}}(\alpha_1 x + \alpha_2 y) / N\mathfrak{a}$ with $\mathfrak{a} = (\alpha_1, \alpha_2)$, where $\alpha_1 = B + \sqrt{D}$ if $C > 0$ or $\alpha_1 = B - \sqrt{D}$ if $C < 0$ and $\alpha_2 = 2C$. Consequently, if ideals $\mathfrak{a} = (\alpha_1, \alpha_2)$ and $\mathfrak{b} = (\beta_1, \beta_2)$ are equivalent then the corresponding forms are equivalent and conversely [16, see Proposition 5.2]. 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 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*

$$|\alpha_i| \leq 1.14 (DN\mathfrak{a})^{\frac{1}{2}}, \quad i = 1, 2. \quad (15)$$

Proof. Let $\alpha \in \mathfrak{a}$, $\alpha = \alpha_1 x + \alpha_2 y$, where α_1, α_2 is an integral basis of $\mathfrak{a}$ ordered in such a way that the number $\Delta(\alpha_1, \alpha_2)$ lies in the upper half-plane, where $x, y \in \mathbb{Z}$. Then

$$\frac{N_{K/\mathbb{Q}}(\alpha)}{N\mathfrak{a}} = Ax^2 + Bxy + Cy^2 = F(x, y) \quad (16)$$

is a primitive positive quadratic form over $\mathbb{Z}$ with discriminant D [16, see Proposition 5.2]. Let $X \in H(K)$ be the ideal class containing $\mathfrak{a}$. Hence F belong to the corresponding the equivalence class of primitive positive definite binary quadratic forms. In this class there is a reduced form G equivalent to F [16, 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

$$G = \frac{N_{K/\mathbb{Q}}(\beta_1 x + \beta_2 y)}{N\mathfrak{b}} = \frac{N_{K/\mathbb{Q}}(\beta_1)}{N\mathfrak{b}} x^2 + \frac{\Delta(\beta_1, \beta_2)}{N\mathfrak{b}} xy + \frac{N_{K/\mathbb{Q}}(\beta_2)}{N\mathfrak{b}} y^2, \quad (17)$$

where $N\mathfrak{b}$ divides $N_{K/\mathbb{Q}}(\beta_i)$, $i = 1, 2$. By [17, see Theorem 3, p. 69] we obtain

$$\frac{N_{K/\mathbb{Q}}(\beta_i)}{DN\mathfrak{b}} \leq \frac{N_{K/\mathbb{Q}}(\beta_1)N_{K/\mathbb{Q}}(\beta_2)}{DN\mathfrak{b}^2} \leq \left(\frac{4}{\pi}\right)^2 \left(\Gamma\left(\frac{3}{2}\right)\right)^2 \leq \left(\frac{4}{\pi}\right)^2 0.786 \leq 1.28, \quad i = 1, 2, \quad (18)$$

where Γ is the gamma function. (Compare the above estimation to Hermite's constant $\gamma_2 = \frac{4}{3}$ (see [17], p. 71)). Hence,

$$|\beta_i|^2 \leq 1.28DN\mathfrak{b}, \quad i = 1, 2. \quad (19)$$

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 $\mathfrak{a}$, where $\alpha'_1 = \delta\beta_1$, $\alpha'_2 = \delta\beta_2$ such that

$$|\alpha'_i|^2 = |\delta\beta_i|^2 \leq 1.28DN\mathfrak{b}N(\delta) = 1.28DN\mathfrak{a}, \quad i = 1, 2,$$

and consequently

$$|\alpha'_i| \leq (1.28DN\mathfrak{a})^{\frac{1}{2}} \leq 1.14(DN\mathfrak{a})^{\frac{1}{2}} \quad i = 1, 2.$$

This finishes the proof. $\square$

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

$$|\alpha_i| \leq 1.14(DN\mathfrak{a})^{\frac{1}{2}}, \quad i = 1, 2. \quad (20)$$

Let $\alpha \in \mathfrak{A}$ 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 (8)

$$|\alpha| \leq \sqrt{x}, \quad |\bar{\alpha}| \leq \sqrt{x}. \quad (21)$$

We have

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

so by (14), (20) and (21) we obtain

$$\begin{aligned} |m_1| &\leq \frac{|\bar{\alpha}_2\alpha - \alpha_2\bar{\alpha}|}{|\Delta(\alpha_1, \alpha_2)|} \leq 2.28(N\mathfrak{a})^{-\frac{1}{2}}\sqrt{x}, \\ |m_2| &\leq \frac{|\alpha_1\bar{\alpha} - \bar{\alpha}_1\alpha|}{|\Delta(\alpha_1, \alpha_2)|} \leq 2.28(N\mathfrak{a})^{-\frac{1}{2}}\sqrt{x}. \end{aligned} \quad (22)$$

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

$$(\rho) = \frac{\mathfrak{b}}{\mathfrak{q}\mathfrak{d}}, \quad (\mathfrak{b}, \mathfrak{q}) = 1. \quad (23)$$

Suppose that $\gamma_j \in \mathcal{O}_K$, $(\gamma_j, \mathfrak{q}) = 1$ run through a complete residue system $(\bmod \mathfrak{q})$. The number of residue classes relatively prime to $\mathfrak{q}$ is equal to $\Phi(\mathfrak{q})$, so $j = 1, \dots, \Phi(\mathfrak{q})$. By [3, Lemma 1, p. 253] the numbers $\rho\gamma_j$ run through a complete system of numbers which are pairwise incongruent $(\bmod \mathfrak{d}^{-1})$, and

$$(\rho\gamma_j)\mathfrak{d} = \frac{(\gamma_j)\mathfrak{b}}{\mathfrak{q}}, \quad ((\gamma_j)\mathfrak{b}, \mathfrak{q}) = 1. \quad (24)$$

Let $\sigma(\alpha)$ be an additive character modulo $\mathfrak{q}$. By [4, Lemma 1, p. 186] all primitive additive characters $\sigma \pmod{\mathfrak{q}}$ have the form

$$\sigma_j(\alpha) = e(\text{Tr}(\rho\gamma_j\alpha)), \quad e(\theta) = 2\pi i\theta, \quad j = 1, \dots, \Phi(\mathfrak{q}). \quad (25)$$

We define

$$\mathcal{R} = \{\xi = m_1\alpha_1 + m_2\alpha_2 \in \mathfrak{a}, \quad |m_i| \leq 2.28(N\alpha)^{-\frac{1}{2}}\sqrt{x}, \quad m_i \in \mathbb{Z}, \quad i = 1, 2\}.$$

By [15, Th. 102, p. 118] the numbers

$$\beta_1 = \frac{\bar{\alpha}_2}{\Delta(\alpha_1, \alpha_2)}, \quad \beta_2 = \frac{-\bar{\alpha}_1}{\Delta(\alpha_1, \alpha_2)} \quad (26)$$

form a basis for the ideal $(\mathfrak{a}\mathfrak{d})^{-1}$, and by (20)

$$|\beta_i| \leq 1.14(N\alpha)^{-\frac{1}{2}} \quad i = 1, 2. \quad (27)$$

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

$$\rho\gamma_j = s_{1j}\beta_1 + s_{2j}\beta_2, \quad s_{ij} \in \mathbb{Q}, \quad i = 1, 2, \quad j = 1, \dots, \Phi(q). \quad (28)$$

Since $\bar{\beta}_1 = -\frac{\alpha_2}{\Delta(\alpha_1, \alpha_2)}$ and $\bar{\beta}_2 = \frac{\alpha_1}{\Delta(\alpha_1, \alpha_2)}$, by (12) we obtain

$$\text{Tr}(\rho\gamma_j\xi) = s_{1j}m_1 + s_{2j}m_2, \quad (29)$$

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

$$c'(\xi) = \begin{cases} c(\xi) & \text{for } \xi \in \mathfrak{R}, \quad \xi \in \mathfrak{a}, \\ 0 & \text{for } \xi \in \mathcal{R}, \quad \xi \notin \mathfrak{R}, \end{cases} \quad (30)$$

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 $|m_i| \leq 2.28(N\alpha)^{-\frac{1}{2}}\sqrt{x}$, $i = 1, 2$, and $c(m_1, m_2) = c'(\xi)$ for $\xi = m_1\alpha_1 + m_2\alpha_2$, $\xi \in \mathfrak{a}$, $\xi \in \mathfrak{R}$. 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

$$\rho\gamma = s_1\beta_1 + s_2\beta_2, \quad \rho'\gamma' = s'_1\beta_1 + s'_2\beta_2, \quad s_j, s'_j \in \mathbb{Q}, \quad j = 1, 2, \quad (31)$$

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

$$\max_{j=1}^2 \|s_j - s'_j\|, \quad j = 1, 2,$$

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

$$\rho\gamma - \rho'\gamma' = t_1\beta_1 + t_2\beta_2 + \delta, \quad \delta \in \frac{1}{\mathfrak{a}\mathfrak{d}}, \quad (32)$$

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 (24) we have

$$(\rho\gamma)\mathfrak{d} = \frac{(\gamma)\mathfrak{b}}{\mathfrak{q}}, \quad (\rho'\gamma')\mathfrak{d} = \frac{(\gamma')\mathfrak{b}'}{\mathfrak{q}'}, \quad ((\gamma)\mathfrak{b}, \mathfrak{q}) = ((\gamma')\mathfrak{b}', \mathfrak{q}') = 1. \quad (33)$$

From (32) we obtain

$$\mathfrak{a}(\gamma)\mathfrak{b}\mathfrak{q}' = \mathfrak{a}\mathfrak{q}\mathfrak{q}'(\rho\gamma)\mathfrak{d} = \mathfrak{a}\mathfrak{q}\mathfrak{q}'(\rho'\gamma' + \delta)\mathfrak{d} = \mathfrak{q}\mathfrak{c}, \quad (34)$$

$$\mathfrak{a}(\gamma')\mathfrak{b}'\mathfrak{q} = \mathfrak{a}\mathfrak{q}\mathfrak{q}'(\rho'\gamma')\mathfrak{d} = \mathfrak{a}\mathfrak{q}\mathfrak{q}'(\rho\gamma + \delta)\mathfrak{d} = \mathfrak{q}\mathfrak{c}', \quad (35)$$

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

$$\rho\gamma - \rho'\gamma' - \delta = t_1\beta_1 + t_2\beta_2 \neq 0, \quad \rho\gamma - \rho'\gamma' - \delta \in \frac{1}{a\delta qq'}.$$
 (36)

Hence,

$$\begin{aligned} \|s_j - s'_j\| &= |t_j| \geq |\rho\gamma - \rho'\gamma' - \delta| - |t_i\beta_i| \geq (Na\delta qq')^{-\frac{1}{2}} - 0.57(Na)^{-\frac{1}{2}} \\ &\geq (1 - 0.57)(N\delta)^{-\frac{1}{2}}(Nqq')^{-\frac{1}{2}}, \end{aligned}$$

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

$$\max_{j=1}^2 \|s_j - s'_j\| \geq \begin{cases} 0.43|D|^{-\frac{1}{2}}Q^{-1} & \text{if } D \equiv 1 \pmod{4}, \\ 0.21|D|^{-\frac{1}{2}}Q^{-1} & \text{if } D \equiv 2, 3 \pmod{4}. \end{cases}$$

By [2, Theorem 1] we obtain

$$\sum_{\substack{Nq \leq Q \\ (q, a)=1}} \sum'_{\sigma \pmod{q}} \left| \sum_{\substack{\alpha \in \mathfrak{R} \\ \alpha \equiv 0 \pmod{a}}} c(\alpha)\sigma(\alpha) \right|^2 \leq \left(\sqrt{4.56} \left(\frac{x}{Na} \right)^{\frac{1}{4}} + c_0 |D|^{\frac{1}{4}} Q^{\frac{1}{2}} \right)^4 \sum_{\substack{\alpha \in \mathfrak{R} \\ \alpha \equiv 0 \pmod{a}}} |c(\alpha)|^2,$$

where

$$c_0 = \begin{cases} 1.53 & \text{if } D \equiv 1 \pmod{4}, \\ 2.19 & \text{if } D \equiv 2, 3 \pmod{4}. \end{cases}$$

This finishes the proof. $\square$

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

References

- [1] E. Bombieri and H. Davenport, On the Large Sieve Method, "Number Theory and Analysis: A Collection of Papers in Honor of Edmund Landau (1877–1938)", Springer, (1969), 9–22.
- [2] M. Huxley, The large sieve inequality for algebraic number fields, *Mathematika*, 15 (1968), no.2, 178–187.
- [3] W. Schaal, On the large sieve method in algebraic number fields, *Journal of Number Theory*, 2 (1970), no. 3, 249–270.
- [4] J. Hinz, Methoden des grossen Siebes in algebraischen Zahlkörpern, *Manuscripta Math.*, 57 (1987), no. 2, 181–194.
- [5] R. Wilson, The large sieve in algebraic number fields, *Mathematika*, 16 (1969), no. 2, 189–204.
- [6] E. Bombieri, On the large sieve, *Mathematika*, 12 (1965), no. 2, 201–225.
- [7] J. Hinz, A generalization of Bombieri's prime number theorem to algebraic number fields. *Acta Arith.*, 51 (1988), no. 2, 173–193.
- [8] M. Huxley, The large sieve inequality for algebraic number fields. III. Zero-density results, *J. London Math. Soc.*, 2 (1971), no. 3, 233–240.
- [9] M. Grześkowiak, An algorithmic construction of finite elliptic curves of order divisible by a large prime. *Fundam. Inf.*, 136 (2015), no. 4, 331–343.
- [10] K. Durnoga and J. Pomykała, Large sieve, Miller-Rabin compositeness witnesses and integer factoring problem, *Fundamenta Inf.*, 156 (2017), no. 2, 179–185.
- [11] J. Pomykała, On exponents of modular subgroups generated by small consecutive integers. *Acta Arith.*, 176 (2016), no. 4, 321–342.
- [12] A. Atkin and F. Morain, Elliptic curves and primality proving, Technical report, Projet ICSLA RR-1256, INRIA, 1990.
- [13] 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.
- [14] M. Grześkowiak, Explicit bound for the prime ideal theorem in residue classes, *Number-Theoretic Methods in Cryptology 2017, LNCS 10737*, (2018), 48–68.
- [15] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer-Verlag, (1981).
- [16] W. Narkiewicz, *Classical Problems in Number Theory*, Monografie Matematyczne, Pan. Wyd. Naukowe, (1986).
- [17] C. Lekkerkerker and P. Gruber, *Geometry of Numbers*, North-Holland Mathematical Library, Elsevier Science, (1987).