On the Diophantine equation $ab + bc + ca = N$ and Euler's idoneal numbers

Xue-Bin Liang

Abstract

In this paper, it is proved that every natural number since 1849 can be represented as $ab + bc + ca$ with three distinct positive integers a, b and c. A positive integer N is an Euler's idoneal number if and only if it cannot be written as $ab + bc + ca$ for distinct positive integers a, b and c. Consequently, the number 1848 is the largest Euler's idoneal number, which was conjectured by Euler in 1778 and Gauss in the *Disquisitiones Arithmeticae*.

hexagon:2611.00500v1

1 Introduction

The Diophantine equation $ab + bc + ca = N$ in three variables a, b and c is a classic ternary quadratic form studied extensively. For instance, the number of solutions in positive integers a, b and c of the equation, where N is a given positive integer, was investigated by Mordell [28] in 1923. In this paper, we will prove the following solvability result.

Theorem 1 *Every natural number $N \geq 1849$ can be represented as*

$$N = ab + bc + ca \tag{1}$$

where a, b and c are three distinct positive integers.

In other words, Theorem 1 tells that every even number $2N \geq 3698$ is the surface area, i.e., the sum of areas of the six faces, of a right rectangular prism with three *distinct* edge lengths a, b and c, which has the value of $2ab + 2bc + 2ca$.

The Diophantine equation $ab + bc + ca = N$ in *distinct* positive integers a, b and c for a given positive integer N has the significance that its *nonexistence* of a solution is a characterization of a natural number N to be an Euler's idoneal number (see the survey paper by Kani [22, p. 125]). Idoneal numbers were discovered by Euler [11] around 1778 who used them to find large prime numbers. However, not every natural number is suitable for his method and hence Euler gave the name *numeri idonei* (i.e., suitable or

convenient numbers) to those numbers that are suitable for testing the primality of large integers.

Euler listed the following 65 idoneal numbers:

1	16	48	120	312
2	18	57	130	330
3	21	58	133	345
4	22	60	165	357
5	24	70	168	385
6	25	72	177	408
7	28	78	190	462
8	30	85	210	520
9	33	88	232	760
10	37	93	240	840
12	40	102	253	1320
13	42	105	273	1365
15	45	112	280	1848

Euler discovered that there are 65 idoneal numbers among all positive integers $N \leq 10000$. Using the largest one 1848 in the list, Euler proved that $18518809 = 18480000 + 197^2$ is prime by showing that it has a single representation in the form $1848x^2 + y^2$ (see Weil [47, p. 225]).

Idoneal numbers were later investigated by Gauss [14] in the *Disquisitiones Arithmeticae*. In the language of Gauss's theory of quadratic forms, idoneal numbers correspond to discriminants where there is only one class of binary quadratic forms per genus. Gauss also identified the 65 idoneal numbers (see [14, Article 303]). Euler and Gauss conjectured that this list of 65 idoneal numbers is complete, i.e., that there would not be any more idoneal number for all $N > 10000$.

In 1973, Weinberger [48] showed that there are at most *two* other larger idoneal numbers if they exist, with help of a result due to D. H. Lehmer (see [48, p. 119]). It is obvious that if $ab + bc + ca = N$, then $(2a)(2b) + (2b)(2c) + (2c)(2a) = 4N$. So, in case that $4N$ is one other larger idoneal number for some natural number N, then N is another. Therefore, there exist 65, 66, or 67 idoneal numbers.

By Theorem 1 and Euler's list of 65 idoneal numbers, we obtain

Theorem 2 *The number* 1848 *is the largest Euler's idoneal number.*

This theorem says that the list of 65 idoneal numbers is complete and hence the conjecture of Euler and Gauss is confirmed.

2 Outline of the proof of Theorem 1

In this paper, we will prove the following two propositions.

Proposition 1 *Every squarefree positive integer $N > 1365$ with $N \equiv 1 \pmod 4$ can be represented as*

$$N = ab + bc + ca \tag{2}$$

where a, b and c are three distinct positive integers.

Proposition 2 *Every squarefree positive integer $N > 462$ with $N \equiv 2 \pmod 4$ can be represented as*

$$N = ab + bc + ca \tag{3}$$

where a, b and c are three distinct positive integers.

In the work of Grube [16] published in 1874, Euler's results on idoneal numbers were analyzed and extended by employing Gauss's theory of binary quadratic forms. There are other definition and criterion of an idoneal number that are not the same as but equivalent to Euler's original definition (see Weil [47, Chapter III, Section §X]). Grube proved the following elementary criterion for Euler's idoneal number (see also Frei [12, p. 57, Theorem 14] and Kani [22, p. 204, Proposition 17]).

Lemma 1 (Grube's criterion) *A natural number $N \geq 3$ is an idoneal number if and only if for every $b = 1, \cdots, \lfloor \sqrt{N/3} \rfloor$ and every factorization*

$$N + b^2 = ac \text{ with } c \geq a \geq 2b \tag{4}$$

we have that either $a = c$ or $a = 2b$.

By putting $b = x$, $a = x + y$ and $c = x + z$ in Grube's criterion, we see that a natural number $N \geq 3$ is an idoneal number if and only if the Diophantine equation

$$xy + yz + zx = N$$

has no solution in *distinct* positive integers $0 < x < y < z$.

Based on Grube's and Euler's results as surveyed by Kani [22, Section 2.3], the classification of large idoneal numbers is readily available as follows (see [22, p. 203, Corollary 14]).

Proposition 3 *If a natural number $N > 1848$ is an idoneal number, then $N \not\equiv 3 \pmod 4$. Moreover, if $N \equiv 1, 2 \pmod 4$, then N is squarefree, whereas if $N \equiv 0 \pmod 4$, then $M = N/4$ is a squarefree idoneal number with $M \equiv 2 \pmod 4$.*

For example, if $N > 1848$ and $N = 4L + 3$ for some positive integer L, then N can be expressed as $N = xy + yz + zx$ with $x = 1$, $y = 3$, and $z = L > 3$ and thus N is *not* an idoneal number.

It follows easily from the above Propositions 1, 2 and 3 that every natural number $N > 1848$ cannot be an idoneal number and hence Theorem 1.

In the remainder of this paper, we are going to prove Propositions 1 and 2, which, together with the established classification result in Proposition 3, can imply Theorem 1.

3 An equivalent assertion of Propositions 1 and 2

In this section, we provide one assertion which is equivalent to Propositions 1 and 2 for every squarefree positive integer $N > 10000$, thanks to Euler's result in the range $N \leq 10000$ in which Propositions 1 and 2 are accordingly true.

Define $r_3(n)$ to be the number of representations of a nonnegative integer n as a sum of three squares and let q be a nonzero complex number with $|q| < 1$. Define the generating function

$$R_3(q) = \sum_{n=0}^{\infty} r_3(n)(-q)^n = \left(\sum_{m\in\mathbb{Z}} (-1)^m q^{m^2}\right)^3.$$

In his work regarding mock theta functions of Ramanujan, Andrews found the following representation for $R_3(q)$ by using theory of q-series (see [1, p. 124, Eqn. (5.16)])

$$\sum_{n=0}^{\infty} (-1)^n r_3(n) q^n = 1 + 4\sum_{n=1}^{\infty} \frac{(-1)^n q^n}{1+q^n} - 2\sum_{n=1}^{\infty}\sum_{|j|<n} \frac{(-1)^j q^{n^2-j^2}(1-q^n)}{1+q^n}. \tag{5}$$

It can be readily deduced from Andrews's identity (5) to obtain the following identity due to Crandall ([8, p. 376, Eqn. (6.2)]) that, for every positive integer $N \geq 3$,

$$r_3(N) = 6(-1)^{N+1} \sum_{xy=N} (-1)^{x+y} + 4(-1)^{N+1} \sum_{xy+yz+zx=N} (-1)^{x+y+z} \tag{6}$$

where every summation index integer x, y or z is positive.

Based on the Andrews–Crandall identity in the form of (6), Mortenson proved the following two results (see [29, p. 777]).

Lemma 2 *For every positive integer $N \geq 5$ with $N \equiv 1 \pmod 4$, we have*

$$r_3(N) = 6\sum_{d|N} 1 + 12 \sum_{\substack{x\neq y \\ x^2+2xy=N}} 1 + 24 \sum_{\substack{x<y<z \\ xy+yz+zx=N}} 1 \tag{7}$$

where every summation index integer d, x, y or z is positive.

Lemma 3 *For every positive integer $N \geq 6$ with $N \equiv 2 \pmod 4$, we have*

$$r_3(N) = 12 \sum_{d|(N/2)} 1 + 24 \sum_{\substack{x<y<z \\ xy+yz+zx=N}} 1 \tag{8}$$

where every summation index integer d, x, y or z is positive.

From Lemmas 2 and 3, we have the following two special results.

Corollary 1 *For every squarefree positive integer $N \geq 5$ with $N \equiv 1 \pmod 4$, we have*

$$r_3(N) = 12 \cdot 2^{\omega(N)} + 24 \sum_{\substack{x<y<z \\ xy+yz+zx=N}} 1 \tag{9}$$

where every summation index integer x, y or z is positive and $\omega(N)$ is the number of distinct prime factors of N.

Proof: Let $N = p'_1 \cdots p'_L$, where $p'_1, \cdots, p'_L$ are L distinct *odd* primes. It is obvious that $\sum_{d|N} = 2^L$. We now consider the second sum on the right-hand side of (7).

If $x^2 + 2xy = N$, then $N = x(x + 2y)$ and hence $x \mid N$ and $(x + 2y) \mid N$. Therefore, x and $x + 2y$ are both squarefree positive integers. We pick up a positive integer $d \mid N$, which must be squarefree, then $d \neq N/d$. If $d < N/d$, we choose $x = d$ and $x + 2y = N/d$, i.e., $y = (N/d - d)/2$. If $d > N/d$, we choose $x = N/d$ and $x + 2y = d$, i.e., $y = (d - N/d)/2$. It is clear that $x \equiv 1, 3 \pmod 4$ implying $x^2 \equiv 1 \pmod 4$. Thus, $2xy = N - x^2$ implies $2xy \equiv 0 \pmod 4$ and hence $2 \mid y$ and $x \neq y$. Noting the symmetry in $(d, N/d)$ and $(N/d, d)$, we see that

$$\sum_{\substack{x \neq y \\ x^2+2xy=N}} 1 = 2^{L-1}.$$

Since $\omega(N) = L$, the identity (7) implies (9). Therefore, the proof is complete. □

Corollary 2 *For every squarefree positive integer $N \geq 6$ with $N \equiv 2 \pmod 4$, we have*

$$r_3(N) = 12 \cdot 2^{\omega(N)-1} + 24 \sum_{\substack{x<y<z \\ xy+yz+zx=N}} 1 \tag{10}$$

where every summation index integer x, y or z is positive.

Proof: Let $N = 2p'_1 \cdots p'_L$, where $p'_1, \cdots, p'_L$ are L distinct *odd* primes. Then, $N/2 = p'_1 \cdots p'_L$ and it is obvious that

$$\sum_{d|(N/2)} 1 = 2^L.$$

Noting that $\omega(N) = L + 1$, the identity (8) implies (10). The proof is complete. □

Corollaries 1 and 2 together imply the following

Proposition 4 *For every squarefree positive integer $N > 10000$ with $N \equiv 1, 2 \pmod 4$, we have*

$$r_3(N) = 12 \cdot 2^{\omega(4N)-1} + 24 \sum_{\substack{x<y<z \\ xy+yz+zx=N}} 1 \tag{11}$$

where every summation index integer x, y or z is positive and $\omega(4N)$ is the number of distinct prime factors of $4N$.

The determination of $r_3(N)$ is a major topic in representations of integers as sums of squares (see Bateman [3] and Grosswald's book [15, Chapter 4]). According to Gauss's theorem ([15, p. 51]) and an equality regarding $r_3(N)$ (see [15, Eqn. (4.8), p. 53]), let $h(-4N)$ stand for the number of classes of primitive binary quadratic form corresponding to the discriminant $D = -4N$, then, for every *squarefree* positive integer $N > 10000$ with $N \equiv 1, 2 \pmod 4$,

$$r_3(N) = 12 \cdot h(-4N). \tag{12}$$

Set the Kronecker symbol $\chi(n) = \left(\frac{D}{n}\right)$ with $D = -4N$ for every *squarefree* positive integer $N > 10000$ with $N \equiv 1, 2 \pmod 4$. Define the corresponding L-series

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

for $s > 0$. According to Dirichlet's theorem ([15, p. 56]), if $h(-4N)$ is the number of classes of primitive binary quadratic form $ax^2 + 2bxy + cy^2$ with $N = ac - b^2$, then

$$h(-4N) = \frac{2\sqrt{N}}{\pi} L(1, \chi). \tag{13}$$

There are connection and correspondence between the theory of classes of equivalent quadratic forms and the theory of ideals in quadratic fields (see Davenport's book [9, pp. 51–53]). According to the analytic class number formula for an arbitrary algebraic number field (see, e.g., Neukirch [31, p. 467]), let h_K be the class number of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ with $D = -4N < 0$ for every *squarefree* positive integer $N > 10000$ with $N \equiv 1, 2 \pmod 4$, we have as a special case the following result (see, e.g., [27, p. 391]),

$$h_K = \frac{w\sqrt{|D|}}{2\pi} L(1, \chi) \tag{14}$$

where w denotes the number of roots of unity in the imaginary quadratic field K. Since $w = 2$ for $D < -4$, we see from (13) and (14) that

$$h_K = h(-4N) = \frac{\sqrt{|D|}}{\pi} L(1, \chi). \tag{15}$$

Therefore, by using (12), from Proposition 4 we can deduce the following

Proposition 5 *For every squarefree positive integer $N > 10000$ with $N \equiv 1, 2 \pmod 4$, let h_K be the class number of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ with $D = -4N < 0$, we have*

$$h_K = 2^{\omega(4N)-1} + 2 \sum_{\substack{x<y<z \\ xy+yz+zx=N}} 1 \tag{16}$$

where every summation index integer x, y or z is positive. Consequently, we have $h_K \geq 2^{\omega(4N)-1}$ with equality if and only if the Diophantine equation $xy + yz + zx = N$ has no solution in distinct *positive integers $0 < x < y < z$ for the given number N.*

It is now ready to demonstrate that Propositions 1 and 2 in the range $N > 10000$ is equivalent to the following assertion.

Proposition 6 *For every squarefree positive integer $N > 10000$ with $N \equiv 1, 2 \pmod 4$, let h_K be the class number of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ with $D = -4N < 0$, we have*

$$h_K \neq 2^{\omega(4N)-1}. \tag{17}$$

In fact, if $h_K \neq 2^{\omega(4N)-1}$, then, from Proposition 5, we have $h_K > 2^{\omega(4N)-1}$ and hence N can be expressed as $N = xy + yz + zx$ for some three distinct positive integers x, y and z. Conversely, if N can be written as $N = xy + yz + zx$ with $0 < x < y < z$, it follows from (16) that $h_K > 2^{\omega(4N)-1}$ and hence $h_K \neq 2^{\omega(4N)-1}$. Thus, the assertion of Proposition 6 is equivalent to Proposition 1 together with Proposition 2.

In the remainder of this paper, we are going to prove Proposition 6, which implies Propositions 1 and 2 and, in turn, Theorem 1 as shown in Section 2.

4 Reduction of range in Proposition 6 by existing numerical results for imaginary quadratic fields

Let $N > 10000$ be a squarefree positive integer with $N \equiv 1, 2 \pmod 4$. In this scenario, the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-N})$ has the fundamental discriminant $D = -4N < 0$ and $K = \mathbb{Q}(\sqrt{D})$.

Let I_K denote the multiplicative group of nonzero fractional ideals of K, and P_K its subgroup of nonzero principal fractional ideals of K. The quotient group I_K/P_K, denoted by Cl_K, is called the ideal class group of K, which is a *finite* abelian group. The order of the ideal class group Cl_K is called the class number of K, denoted by $h_K = \#Cl_K$.

On the contrary we assume that

$$\#Cl_K = 2^{\omega(4N)-1}. \tag{18}$$

By Lagrange's theorem in group theory, any subgroup H of the finite group Cl_K must divide the order of the group, namely, $\#H \mid \#Cl_K$, and hence $\#H = 2^m$ for some nonnegative integer m. By the structure theorem for finite abelian groups (see, e.g., [20]), the ideal class group Cl_K is isomorphic to a unique direct product of a collection of cyclic groups. Then, we have

$$Cl_K \cong \mathbb{Z}_{2^{m_1}} \times \cdots \times \mathbb{Z}_{2^{m_r}}$$

where $r \geq 1$ and $m_1, \cdots, m_r$ are nonnegative integers with $0 \leq m_1 \leq \cdots \leq m_r$ and $m_r \geq 1$. The direct product can be rewritten as

$$Cl_K \cong {\mathbb{Z}_2}^{a_1} \times {\mathbb{Z}_{2^2}}^{a_2} \cdots \times {\mathbb{Z}_{2^t}}^{a_t} \tag{19}$$

where $t \geq 1$ and $a_1, \cdots, a_t$ are nonnegative integers with $a_t \geq 1$. Here, a_ℓ denotes the number of occurrences of $\mathbb{Z}_{2^\ell}$ in the direct product for $1 \leq \ell \leq t$. By genus theory, $a_1 + \cdots + a_t = \omega(|D|) - 1$, where $D = -4N$ is the discriminant of the field K (see [10, p. 222]).

It follows from (18) and (19) that

$$2^{\omega(4N)-1} = \#Cl_K = 2^{a_1} \cdot 2^{2a_2} \cdots 2^{ta_t} \geq 2^{a_1+\cdots+a_t} \cdot 2^{(t-1)a_t} = 2^{\omega(|D|)-1} \cdot 2^{(t-1)a_t}.$$

So, there must be $t = 1$ and $a_t = \omega(|D|) - 1$. Hence, from (19),

$$Cl_K \cong {\mathbb{Z}_2}^{\omega(|D|)-1}. \tag{20}$$

Due to the computational work by Mosunov and Jacobson [30] in 2016, we know that up to 2^{40} the largest in its absolute value of the fundamental discriminant D with Cl_K isomorphic to ${\mathbb{Z}_2}^\ell$ for some positive integer ℓ is $D = -5460$. Since (18) implying (20) and $N = |D|/4$, we see that Proposition 6 is true in the range up to $N \leq 2^{38}$.

The range has been further expanded owing to the computational work by Elsenhans, Klüners and Nicolae [10] in 2020. They showed that for imaginary quadratic fields $K = \mathbb{Q}(\sqrt{D})$ with discriminant $D < 0$ up to $|D| \leq 3.1 \cdot 10^{20}$, the largest one in its absolute value with Cl_K isomorphic to ${\mathbb{Z}_2}^\ell$ for some positive integer ℓ is still $D = -5460$. As a result, Proposition 6 is true in the range up to $N \leq 7.5 \cdot 10^{19}$.

Thanks to the existing numerical works in [30] and [10], it suffices to prove Proposition 6 for every squarefree positive integer $N > 7.5 \cdot 10^{19}$ with $N \equiv 1, 2 \pmod 4$. In the following two sections, we will prepare to develop an explicit lower bound for the class number h_K of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-N})$ for such N. Then, we will provide a proof of Proposition 6 and, in turn, Theorem 1.

5 An explicit Hecke's theorem

Let N be any given squarefree positive integer with $N > 7.5 \cdot 10^{19}$ and $N \equiv 1, 2 \pmod 4$. Based on the class number formula (15) for the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ with $D = -4N < 0$, an available lower bound for $L(1, \chi)$ will induce a lower bound for the class number h_K of the quadratic field K, and vice versa.

In 1918 Hecke [18] demonstrated a fundamental link between the real zeros of Dirichlet L-functions for the quadratic Dirichlet characters and the class numbers of imaginary quadratic fields. An effective Hecke's theorem was proved by Mahler [26, p. 302, Theorem 2] in 1934 as stated below (see also Friedlander and Iwaniec [13, p. 344]).

Theorem 3 (Hecke's theorem) *Suppose that g is a positive constant and that the integer $d > 1$ is greater than a certain number d_1 which depends only on g. Then, if the L-series denoted by $L_d(s)$ has no zero in the interval*

$$1 - \frac{g}{\log d} \le s \le 1,$$

there exists a number $G > 0$, depending only on g, such that the class number h of $\mathbb{Q}(\sqrt{-d})$ satisfies

$$h \ge G \frac{\sqrt{d}}{\log d}.$$

For the application in this paper, an *explicit* Hecke's theorem is needed. There have been some results in the respect and, in particular, those proved by Tatuzawa [43] in 1951 and by Hoffstein [19] in 1980. In the following, we are going to establish an explicit Hecke's theorem with a different and rigorous proof which employs algebraic number theory to obtain *explicit* constants best suited for the forthcoming application.

Let K be an algebraic number field with degree $m = [K : \mathbb{Q}]$ over the field $\mathbb{Q}$ of rational numbers. We denote by O_K the ring of integers of K and by Δ_K the discriminant of O_K over the ring $\mathbb{Z}$ of rational integers. If K has r real embeddings and t pairs of complex conjugate embeddings, then we have $r + 2t = m$. We let $\sigma_1, \cdots, \sigma_r : K \hookrightarrow \mathbb{R}$ be the r real embeddings and $\sigma_{r+1}, \overline{\sigma_{r+1}}, \cdots, \sigma_{r+t}, \overline{\sigma_{r+t}} : K \hookrightarrow \mathbb{C}$ the t pairs of complex conjugate embeddings of K. For each $a \in K$, the field norm $\mathrm{N}_{K/\mathbb{Q}}(a) \in \mathbb{Q}$ is defined to be (see, e.g., [42, p. 49])

$$\mathrm{N}_{K/\mathbb{Q}}(a) = \sigma_1(a) \cdots \sigma_r(a) \sigma_{r+1}(a) \overline{\sigma_{r+1}}(a) \cdots \sigma_{r+t}(a) \overline{\sigma_{r+t}}(a).$$

It is clear that, for $a \in K$ and $b \in K$, we have $\mathrm{N}_{K/\mathbb{Q}}(ab) = \mathrm{N}_{K/\mathbb{Q}}(a)\mathrm{N}_{K/\mathbb{Q}}(b)$. If $a \neq 0$, then $\mathrm{N}_{K/\mathbb{Q}}(a) \neq 0$. If $a \in O_K$, then $\mathrm{N}_{K/\mathbb{Q}}(a) \in \mathbb{Z}$. If $a \in \mathbb{Q}$, then $\mathrm{N}_{K/\mathbb{Q}}(a) = a^{[K:\mathbb{Q}]} = a^m$.

Let $\mathfrak{a}$ be a nonzero integral ideal of O_K. Then, the quotient ring $O_K/\mathfrak{a}$ is finite. The norm of $\mathfrak{a}$ is defined by $\mathfrak{N}(\mathfrak{a}) = |O_K/\mathfrak{a}|$. If $\mathfrak{p}$ is a nonzero prime ideal of O_K, then the residue ring $O_K/\mathfrak{p}$ is a finite field, which is called the residue class field of O_K modulo $\mathfrak{p}$. The norm of $\mathfrak{p}$ is $\mathfrak{N}(\mathfrak{p}) = |O_K/\mathfrak{p}|$ being a prime power. If $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero integral ideals of O_K, then $\mathfrak{N}(\mathfrak{ab}) = \mathfrak{N}(\mathfrak{a})\mathfrak{N}(\mathfrak{b})$. Note that the norm of the nonzero principal ideal $\mathfrak{a} = aO_K$ is equal to the absolute value of the field norm $\mathrm{N}_{K/\mathbb{Q}}(a)$ [42, Corollary 5.10], i.e., if $a \in O_K$ with $a \neq 0$, then $\mathfrak{N}(aO_K) = |\mathrm{N}_{K/\mathbb{Q}}(a)|$. Therefore, if $a \in O_K$ with $a \neq 0$ and $\mathfrak{b}$ is a nonzero integral ideal of O_K, then $\mathfrak{N}(a\mathfrak{b}) = \mathfrak{N}(aO_K\mathfrak{b}) = \mathfrak{N}(aO_K)\mathfrak{N}(\mathfrak{b}) = |\mathrm{N}_{K/\mathbb{Q}}(a)|\mathfrak{N}(\mathfrak{b})$.

The Dedekind zeta function $\zeta_K(s)$ of $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$ for the number field K is defined by

$$\zeta_K(s) = \sum_{\mathfrak{a}} \frac{1}{\mathfrak{N}(\mathfrak{a})^s} = \prod_{\mathfrak{p}} \frac{1}{1 - \mathfrak{N}(\mathfrak{p})^{-s}} \tag{21}$$

where $\mathfrak{a}$ varies over the nonzero integral ideals of K and $\mathfrak{p}$ runs through the nonzero prime ideals of K. The infinite product over all nonzero prime ideals $\mathfrak{p}$ of O_K is the Euler product of the field K. It is known that the Dedekind zeta function $\zeta_K(s)$ can be analytically continued to $\mathbb{C} \setminus \{1\}$ and that it has a simple pole at $s = 1$ (see [31, p. 467]).

In the following, we specify $K = \mathbb{Q}(\sqrt{D})$ with $D = -4N < 0$ for the given squarefree positive integer $N > 7.5 \cdot 10^{19}$ with $N \equiv 1, 2 \pmod 4$. The field K is an imaginary quadratic field with discriminant $\Delta_K = D$, thus Δ_K is a *fundamental discriminant*. According to [5, Theorem 2.2.15], the Kronecker symbol $\left(\frac{\Delta_K}{n}\right)$, $n \in \mathbb{Z}$, defines a real primitive Dirichlet character modulo $|\Delta_K| = |D| = 4N$. We note that if $n = p$, p an odd prime, then the Kronecker symbol $\left(\frac{\Delta_K}{n}\right)$ has the same value as that of the Legendre symbol $\left(\frac{\Delta_K}{p}\right)$. Note that for an odd prime p and an integer $a \in \mathbb{Z}$, the Legendre symbol $\left(\frac{a}{p}\right) \in \{-1, 0, 1\}$ is function of a and p defined as 0 when $p \mid a$ and ± 1 depending on whether a is a quadratic residue modulo p when $p \nmid a$.

It is well known that, for a prime $p \in \mathbb{Z}$, the principal ideal pO_K decomposes in O_K as follows. If $p \mid |\Delta_K|$, then p ramifies in O_K and $pO_K = \mathfrak{p}^2$ where $\mathfrak{p}$ is a prime ideal. In this case, $\left(\frac{\Delta_K}{p}\right) = 0$. In particular, since $2 \mid |\Delta_K|$, we have $\left(\frac{\Delta_K}{2}\right) = 0$ and $2O_K = \hat{\mathfrak{p}}^2$, where $\hat{\mathfrak{p}} \mid 2$ is the prime ideal of O_K lying over the prime number $2 \in \mathbb{Z}$.

If p is an odd prime and $\left(\frac{\Delta_K}{p}\right) = 1$, then p splits completely in O_K and $pO_K = \mathfrak{p}_1\mathfrak{p}_2$ where $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are two different prime ideals. If p is an odd prime and $\left(\frac{\Delta_K}{p}\right) = -1$, then p is inert in O_K and $\mathfrak{p} = pO_K$ itself is a prime ideal of O_K.

Let $\chi(n) = \left(\frac{\Delta_K}{n}\right)$ be the real primitive Dirichlet character of K and $L(s, \chi)$ be the corresponding Dirichlet L-function. According to the above decomposition rule and the Euler product in (21), we can obtain

$$\zeta_K(s) = \zeta(s)L(s, \chi) \tag{22}$$

for $s \in \mathbb{C}$ with $\mathrm{Re}(s) > 1$, where $\zeta(s)$ is the Riemann zeta function.

The Riemann zeta function $\zeta(s)$ is a meromorphic function on the whole complex plane, which is holomorphic everywhere except for a simple pole at $s = 1$ with residue 1. Since χ is nonprincipal and primitive, Dirichlet L-function $L(s, \chi)$ is entire on the whole complex plane $s \in \mathbb{C}$. Thus, the above relation (22) can be employed as an alternative approach to providing the same analytic continuation of $\zeta_K(s)$ defined in (21) to $\mathbb{C} \setminus \{1\}$ which has a simple pole at $s = 1$ with residue $L(1, \chi)$. It is known that $L(1, \chi) \neq 0$ (see [2, Theorem 6.20]).

Remind that $K = \mathbb{Q}(\sqrt{\Delta_K})$ is an imaginary quadratic field with discriminant $\Delta_K = -4N < 0$. Let

$$\xi_K(s) = \left(\frac{|\Delta_K|}{4\pi^2}\right)^{s/2} \Gamma(s)\zeta_K(s)$$

where $\Gamma(s)$ is the gamma function. It is known that $\xi_K(s)$ satisfies the following functional equation (see Stark [41, p. 965])

$$\xi_K(1 - s) = \xi_K(s).$$

Therefore, the functional equation for $\zeta_K(s)$ is given by

$$\Gamma(1 - s)\zeta_K(1 - s) = \left(\frac{|\Delta_K|}{4\pi^2}\right)^{s-1/2} \Gamma(s)\zeta_K(s). \tag{23}$$

We need to use the following lemma (see Ingham [21, p. 31]).

Lemma 4 *If k is a positive integer, $c > 0$, $y > 0$, then*

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{y^s}{s(s+1)\cdots(s+k)} ds = \begin{cases} 0, & \text{if } y < 1, \\ \frac{1}{k!}\left(1 - \frac{1}{y}\right)^k, & \text{if } y \geq 1. \end{cases} \tag{24}$$

Lemma 4 implies the following result.

Lemma 5 *If k is a positive integer with $k \geq 2$, $c > 0$, $y > 0$, then*

$$\frac{1}{2\pi i}\int_{c-i\infty}^{c+i\infty} \frac{y^s}{s(s+2)\cdots(s+k)} ds = \begin{cases} 0, & \text{if } y < 1, \\ \frac{1}{k!}\left(1 - \frac{1}{y}\right)^{k-1}\left(1 + \frac{k-1}{y}\right), & \text{if } y \geq 1. \end{cases} \tag{25}$$

In fact, noticing that $\frac{1}{s} = \frac{1}{s(s+1)} + \frac{1}{s+1}$ and using the change of variable, for $y \geq 1$ the integral in (25) equals

$$\frac{1}{k!}\left(1-\frac{1}{y}\right)^k + \frac{1}{y}\frac{1}{(k-1)!}\left(1-\frac{1}{y}\right)^{k-1} = \frac{1}{k!}\left(1-\frac{1}{y}\right)^{k-1}\left(1-\frac{1}{y}+\frac{k}{y}\right).$$

Since $L(1,\chi) \neq 0$, there exists a number $\beta \in (0,1)$ such that $L(s,\chi) \neq 0$ for s in the interval $[\beta, 1)$. Note that the series $\zeta_K(s)$ in (21) converges absolutely and uniformly in the domain $\mathrm{Re}(s) \geq 1+\delta$ for every $\delta > 0$ and that $\zeta_K(s) = \zeta(s)L(s,\chi)$. For a given number $y > 1$, we consider the following complex integral

$$\mathcal{I} = \frac{1}{2\pi i}\int_{2-\beta-i\infty}^{2-\beta+i\infty} \frac{\zeta_K(s+\beta)y^s}{s\prod_{\ell=2}^{9}(s+\ell)}ds = \sum_{\mathfrak{N}(\mathfrak{a})\leq y} \frac{1}{\mathfrak{N}(\mathfrak{a})^\beta}\frac{1}{9!}\left(1-\frac{\mathfrak{N}(\mathfrak{a})}{y}\right)^8\left(1+8\frac{\mathfrak{N}(\mathfrak{a})}{y}\right) \quad (26)$$

where we choose $c = 2-\beta > 1$ and $k = 9$ in Lemma 5. It is clear that $\mathcal{I}$ is a real number.

Let $T \geq 2$ be any given truncation parameter and the complex variable $s = \sigma + it$. Define the function

$$f(s) = \frac{\zeta_K(s+\beta)y^s}{s\prod_{\ell=2}^{9}(s+\ell)} = \frac{\zeta(s+\beta)L(s+\beta,\chi)y^s}{s\prod_{\ell=2}^{9}(s+\ell)} \quad (27)$$

in the rectangle $\mathcal{R}$ with $-1-\beta \leq \sigma \leq 2-\beta$ and $-T \leq t \leq T$. It is seen that $f(s)$ has two poles in $\mathcal{R}$ at $s = 0$ and $s = 1-\beta \in (0,1)$.

Using Cauchy's residue theorem, we obtain

$$\frac{1}{2\pi i}\left\{\int_{2-\beta-iT}^{2-\beta+iT} - \int_{-1-\beta+iT}^{2-\beta+iT} - \int_{-1-\beta-iT}^{-1-\beta+iT} + \int_{-1-\beta-iT}^{2-\beta-iT}\right\} f(s)ds = \operatorname*{Res}_{s=0} f(s) + \operatorname*{Res}_{s=1-\beta} f(s). \quad (28)$$

We can prove that the second and fourth integrals in (28) will approach 0 as $T \to \infty$.

Lemma 6 *For a given number $\beta \in (0,1)$ and the function $f(s)$ given in (27), we have*

$$\lim_{T\to\infty}\int_{-1-\beta+iT}^{2-\beta+iT} f(s)ds = \lim_{T\to\infty}\int_{-1-\beta-iT}^{2-\beta-iT} f(s)ds = 0. \quad (29)$$

Proof: See Appendix A. □

For the given number $y > 1$, we consider the following complex integral

$$\mathcal{J} = \frac{1}{2\pi i}\int_{-1-\beta-i\infty}^{-1-\beta+i\infty} \frac{\zeta_K(s+\beta)y^s}{s\prod_{\ell=2}^{9}(s+\ell)}ds. \quad (30)$$

Noting (26), (29) and (30) and taking the limit $T \to \infty$ in (28), we can obtain

$$\mathcal{I} = \mathcal{J} + \operatorname*{Res}_{s=0} f(s) + \operatorname*{Res}_{s=1-\beta} f(s). \tag{31}$$

Since the class number $h_K \geq 1$, we see from the class number formula (15) that

$$L(1,\chi) = h_K \frac{\pi}{\sqrt{|D|}} > 0.$$

Hence, $L(s,\chi) > 0$ for s in the interval $[\beta, 1)$. Therefore, we have

$$\operatorname*{Res}_{s=0} f(s) = \frac{1}{9!}\zeta_K(\beta) = \frac{1}{9!}\zeta(\beta)L(\beta,\chi) < 0.$$

Note that $\zeta(s)$ has a simple pole at $s = 1$ with residue 1. We get

$$\operatorname*{Res}_{s=1-\beta} f(s) = \frac{L(1,\chi)}{1-\beta}\frac{y^{1-\beta}}{\prod_{\ell=2}^{9}(1-\beta+\ell)} < \frac{y^{1-\beta}}{9!}\frac{L(1,\chi)}{1-\beta}.$$

We can deduce from (31) that the complex integral $\mathcal{J}$ defined in (30) is a real number and that

$$\mathcal{I} < \mathcal{J} + \frac{y^{1-\beta}}{9!}\frac{L(1,\chi)}{1-\beta}. \tag{32}$$

It is now ready to prove an explicit Hecke's theorem as follows.

Proposition 7 *Let N be any given squarefree positive integer with $N > 7.5 \cdot 10^{19}$ and $N \equiv 1, 2 \pmod 4$ and put $D = -4N$ and $q = 4N$. Let $\chi(n) = \left(\frac{D}{n}\right)$ be the Kronecker symbol with the corresponding Dirichlet L-function $L(s,\chi)$. If $L(s,\chi) \neq 0$ for s in the interval $[\beta, 1)$ with $0 < \beta < 1$ satisfying*

$$1 - \beta < 0.015\frac{1}{\log q}, \tag{33}$$

then

$$L(1,\chi) > 2.43(1-\beta). \tag{34}$$

Proof: We choose the number $y = q = 4N > 3 \cdot 10^{20}$. By using $s = -1 - \beta + it$ with $-\infty < t < \infty$, the complex integral $\mathcal{J} \in \mathbb{R}$ given by (30) can be rewritten as

$$\mathcal{J} = \frac{1}{2\pi}\int_{-\infty}^{\infty} \frac{\zeta_K(-1+it)y^{-1-\beta+it}}{(-1-\beta+it)\prod_{\ell=2}^{9}(-1-\beta+it+\ell)}dt = \frac{1}{2\pi}\int_{-\infty}^{\infty} f(-1-\beta+it)dt. \tag{35}$$

By using the functional equation (23) for $\zeta_K(s)$, we get

$$\Gamma(-1+it)\zeta_K(-1+it) = \left(\frac{|\Delta_K|}{4\pi^2}\right)^{3/2-it} \Gamma(2-it)\zeta_K(2-it) \tag{36}$$

where $|\Delta_K| = 4N = q$. Hence,

$$|\zeta_K(-1+it)| = \left(\frac{|\Delta_K|}{4\pi^2}\right)^{3/2} \frac{|\Gamma(2-it)|}{|\Gamma(-1+it)|}|\zeta_K(2-it)| = \left(\frac{|\Delta_K|}{4\pi^2}\right)^{3/2} |t|(1+t^2)|\zeta_K(2-it)|. \tag{37}$$

Note that $|\zeta_K(2-it)| \le |\zeta_K(2)| = |\zeta(2)| \cdot |L(2,\chi)| \le |\zeta(2)|^2 = \pi^4/36$. We have

$$|f(-1-\beta+it)| \le \frac{1}{y^{1+\beta}}\frac{\pi^4}{36}\left(\frac{|\Delta_K|}{4\pi^2}\right)^{3/2} \frac{|t|(1+t^2)}{|-1-\beta+it|\prod_{\ell=2}^{9}|-1-\beta+it+\ell|}$$

and hence

$$|f(-1-\beta+it)| \le \frac{1}{y^{1+\beta}}\frac{\pi^4}{36}\left(\frac{|\Delta_K|}{4\pi^2}\right)^{3/2} \frac{1}{1+t^2}. \tag{38}$$

Thus, we obtain

$$|\mathcal{J}| \le \frac{1}{2\pi}\int_{-\infty}^{\infty}|f(-1-\beta+it)|dt \le \frac{1}{2}\frac{1}{y^{1+\beta}}\frac{\pi^4}{36}\left(\frac{|\Delta_K|}{4\pi^2}\right)^{3/2}. \tag{39}$$

It follows from (26) that

$$\mathcal{I} \ge \sum_{\mathfrak{N}(\mathfrak{a})\le y}\frac{1}{\mathfrak{N}(\mathfrak{a})^{\beta}}\frac{1}{9!}\left(1-8\frac{\mathfrak{N}(\mathfrak{a})}{y}\right)\left(1+8\frac{\mathfrak{N}(\mathfrak{a})}{y}\right) \ge \sum_{\mathfrak{N}(\mathfrak{a})\le 2\cdot 10^{10}}\frac{1}{\mathfrak{N}(\mathfrak{a})}\frac{1}{9!}\left(1-64\frac{\mathfrak{N}(\mathfrak{a})^2}{y^2}\right) \tag{40}$$

Combining (32) with (39) and (40), we obtain

$$\frac{L(1,\chi)}{1-\beta} > \frac{9!}{y^{1-\beta}}\mathcal{I} - \frac{9!}{y^{1-\beta}}|\mathcal{J}| \ge \frac{0.9999}{y^{1-\beta}}\sum_{\mathfrak{N}(\mathfrak{a})\le 2\cdot 10^{10}}\frac{1}{\mathfrak{N}(\mathfrak{a})} - \frac{9!}{72}\frac{\pi^4}{y^2}\left(\frac{y}{4\pi^2}\right)^{3/2}$$

Noticing that $y^{1-\beta} \le q^{0.015\frac{1}{\log q}} = e^{0.015}$ by (33), we get

$$\frac{L(1,\chi)}{1-\beta} > 0.985\sum_{\mathfrak{N}(\mathfrak{a})\le 2\cdot 10^{10}}\frac{1}{\mathfrak{N}(\mathfrak{a})} - 0.000001. \tag{41}$$

For every positive integer $a \le 10^5$, we choose $\mathfrak{a} = aO_K$ and have $\mathfrak{N}(\mathfrak{a}) = \mathfrak{N}(aO_K) = |\mathrm{N}_{K/\mathbb{Q}}(a)| = a^{[K:\mathbb{Q}]} = a^2 \le 10^{10}$. Moreover, we have seen that $2O_K = \hat{\mathfrak{p}}^2$, where $\hat{\mathfrak{p}} \mid 2$ is the prime ideal of O_K lying over $2 \in \mathbb{Z}$, and hence $\mathfrak{N}(\hat{\mathfrak{p}}) = 2$. We choose $\mathfrak{a} = a\hat{\mathfrak{p}}$ with $\mathfrak{N}(\mathfrak{a}) = |\mathrm{N}_{K/\mathbb{Q}}(a)|\mathfrak{N}(\hat{\mathfrak{p}}) = 2a^2 \le 2\cdot 10^{10}$. It is obvious that, for any two positive integers a_1 and a_2, there is $a_1^2 \ne 2a_2^2$, since $\sqrt{2}$ is irrational. Therefore, it follows from (41) that

$$\frac{L(1,\chi)}{1-\beta} > 0.985\sum_{n=1}^{100000}\left(\frac{1}{n^2}+\frac{1}{2n^2}\right) - 0.000001 > 2.43$$

which implies (34). The proof of Proposition 7 is complete. □

6 An explicit zero-free interval for $L(s, \chi)$

Let N be any given squarefree positive integer with $N > 7.5 \cdot 10^{19}$ and $N \equiv 1, 2 \pmod 4$. The Kronecker symbol $\chi(n) = \left(\frac{\Delta_K}{n}\right)$ is the real primitive Dirichlet character of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{\Delta_K})$ with discriminant $\Delta_K = -4N < 0$. The corresponding Dirichlet L-function $L(s, \chi)$ of $s \in \mathbb{C}$ is entire on the complex plane. We need to search for a number $\beta \in (0, 1)$ such that $L(s, \chi) \neq 0$ for s in the interval $(\beta, 1)$.

Hecke's conjecture on Dirichlet L-functions asserts that, for every *real* Dirichlet character χ, we have $L(s, \chi) \neq 0$ for $0 < s < 1$ (See Pan and Pan [34, p. 267]). It is a long-standing conjecture in analytic number theory. As stated in Theorem 3, in 1918 Hecke [18] recognized the profound impact that *nonexistence* of real zeros of Dirichlet L-functions associated with real quadratic characters have on the arithmetic of quadratic fields.

A partial result in the respect was given by Conrey and Soundararajan [7, p. 2, Theorem 1]. Their result demonstrated that Hecke's conjecture holds true for imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-8d})$ for at least 20% of the odd square free integers d. A computational work was performed by Watkins [46], who showed that $L(s, \chi)$ has no positive real zero for each real *odd* Dirichlet character of modulus up to $3 \cdot 10^8$.

In the other respect, if a real zero $\beta \in (0, 1)$ very close to 1 exists, i.e., $L(\beta, \chi) = 0$, it is called a Landau–Siegel zero or an exceptional zero. In 1935, Siegel [39] proved that for any given number $\varepsilon > 0$ and any real primitive character χ of modulus q, if $\beta \in (0, 1)$ is a real zero of $L(s, \chi)$, then $1 - \beta \geq C(\varepsilon) q^{-\varepsilon}$ for some constant $C(\varepsilon) > 0$. Thus, if $1 - \beta < C(\varepsilon) q^{-\varepsilon}$, then $L(s, \chi) \neq 0$ for $\beta < s < 1$. Note that the constant $C(\varepsilon)$ in Siegel's result is *ineffective*, in that whose existence is proven but it cannot be explicitly calculated by the proof method. The Siegel–Walfisz theorem was obtained in 1937 (see Walfisz [45]) as an application of Siegel's result to distribution of primes in arithmetic progressions. With the Siegel–Walfisz theorem, in 1937 Vinogradov [44] found an *unconditional* proof of the three primes Goldbach conjecture for all sufficiently large odd integers. Vinogradov's theorem states that every sufficiently large odd integer can be expressed as a sum of three primes. Hardy and Littlewood [17] had shown earlier in 1924 that the same result follows from the generalized Riemann hypothesis (GRH), which, however, remains unproven.

The most recent progress in Landau–Siegel zeros was presented in manuscript [32] titled "Uniform exclusion of Landau–Siegel zeros". It claims that there is an absolute constant $c > 0$ such that every real zero $\beta \in (0, 1)$ of every primitive nonprincipal real Dirichlet L-function $L(s, \chi)$ of conductor $q \geq 3$, *if it exists*, satisfies $(1 - \beta) \log q \geq c$. In other words, if $1 - \beta < \frac{c}{\log q}$, then $L(s, \chi) \neq 0$ for $\beta < s < 1$. This assertion has remarkably improved Siegel's result.

In the current scenario, we need to obtain an effective zero-free interval for $L(s,\chi)$ with *explicit* constants, which will be utilized by the application for establishing Theorem 1. The arguments presented in [32] are the basis and will be employed appropriately. We will develop a rigorous and complete proof, which involves detailed derivations that do not appear in [32]. Moreover, effective constants will be *explicitly calculated*, which are best suited to the demands of the application.

In the following, we will focus on Dirichlet L-functions $L(s,\chi)$ associated with the real primitive Dirichlet characters χ of the imaginary quadratic fields $K=\mathbb{Q}(\sqrt{-N})$ with discriminant $\Delta_K=-4N<0$ for all squarefree positive integers $N>7.5\cdot 10^{19}$ with $N\equiv 1,2 \pmod 4$. Let

$$q=|\Delta_K|=4N>3\cdot 10^{20},$$

then $\chi(n)=\left(\frac{\Delta_K}{n}\right)\in\{-1,0,1\}$ is a real primitive Dirichlet character of modulus q.

It appears to be out of reach of the current approach to prove Hecke's conjecture for the *nonexistence* of real zeros of Dirichlet L-function $L(s,\chi)$ for every real Dirichlet character χ in the whole interval $0<s<1$. Instead, we will investigate, under the assumption that a real zero $\beta\in(0,1)$ of $L(s,\chi)$ exists, how far that β has to be away from 1. We assume that the number $\beta\in(0,1)$ is the Landau–Siegel zero of $L(s,\chi)$ satisfying

$$L(\beta,\chi)=0.$$

It is known that the Landau–Siegel zero β is *real* and *simple* (see [27, p. 360, Theorem 11.3]).

According to Stark's lemma [40, p. 139, Lemma 3] (see also Stark [41, p. 965]), which can be derived from the Hadamard product of the Dedekind zeta-function of $\zeta_K(s)$, we have, for $s\in\mathbb{C}$,

$$\sum_{\rho}\frac{1}{s-\rho}=\frac{1}{s-1}+\frac{1}{2}\log|\Delta_K|+\frac{1}{s}-\log\pi+\frac{\Gamma'(s)}{\Gamma(s)}-\log 2+\frac{\zeta_K'(s)}{\zeta_K(s)} \tag{42}$$

where ρ runs through the zeros of $\zeta_K(s)$ in the strip $0<\mathrm{Re}(s)<1$ and the ρ and $\bar\rho$ terms must be grouped together. For $s=\sigma>1$, we have

$$\frac{1}{\sigma-\rho}+\frac{1}{\sigma-\bar\rho}=2\frac{\sigma-\mathrm{Re}(\rho)}{|\sigma-\rho|^2}>0.$$

Remind that $\zeta_K(s)=\zeta(s)L(s,\chi)$ for $s\in\mathbb{C}$ and hence $\zeta_K(\beta)=0$. We have, for $\sigma>1$,

$$-\frac{\zeta_K'(\sigma)}{\zeta_K(\sigma)}<-\frac{1}{\sigma-\beta}+\frac{1}{\sigma-1}+\frac{1}{2}\log|\Delta_K|+\frac{1}{\sigma}-\log\pi+\frac{\Gamma'(\sigma)}{\Gamma(\sigma)}-\log 2. \tag{43}$$

Note that $\frac{\Gamma'(s)}{\Gamma(s)} < \frac{\Gamma'(2)}{\Gamma(2)} = 1 - \gamma$ for $0 < s < 2$, where γ is Euler's constant. Thus, we have, for $1 < \sigma < 2$,

$$-\frac{\zeta_K'(\sigma)}{\zeta_K(\sigma)} < -\frac{1}{\sigma - \beta} + \frac{1}{\sigma - 1} + \frac{1}{2}\log|\Delta_K| + 1 - \log\pi + (1 - \gamma) - \log 2$$

and, consequently,

$$-\frac{\zeta_K'(\sigma)}{\zeta_K(\sigma)} < -\frac{1}{\sigma - \beta} + \frac{1}{\sigma - 1} + \frac{1}{2}\log|\Delta_K| < \frac{1}{2}\log|\Delta_K| + \frac{1 - \beta}{(\sigma - 1)^2}. \tag{44}$$

It follows from (21) that, for $\sigma > 1$,

$$-\frac{\zeta_K'(\sigma)}{\zeta_K(\sigma)} = \sum_{\mathfrak{p}} \frac{\log \mathfrak{N}(\mathfrak{p})}{\mathfrak{N}(\mathfrak{p})^\sigma - 1} \tag{45}$$

where $\mathfrak{p}$ runs through the nonzero prime ideals of K. By using $\zeta_K(\sigma) = \zeta(\sigma)L(\sigma, \chi)$, we also have

$$-\frac{\zeta_K'(\sigma)}{\zeta_K(\sigma)} = -\frac{\zeta'(\sigma)}{\zeta(\sigma)} - \frac{L'(\sigma, \chi)}{L(\sigma, \chi)} = \sum_{n=1}^{\infty}(1 + \chi(n))\frac{\Lambda(n)}{n^\sigma} \tag{46}$$

for $\sigma > 1$, where $\Lambda(n)$ is the von Mangoldt function defined as $\log p$ if $n = p^k$ for some prime p and integer $k \geq 1$ and 0 otherwise.

We know that Galois extension $K/\mathbb{Q}$ is uniquely determined by the set of prime numbers which split completely in K, as a consequence of Chebotarev's density theorem (see Neukirch [31, Chapter VII, Section §13]). For instance, the dominating terms in the summation (45) are in the prime ideals $\mathfrak{p} \mid p$ where the prime p splits completely in K and hence $\mathfrak{N}(\mathfrak{p}) = p$. If the prime p is inert in the imaginary quadratic field K and $\mathfrak{p} \mid p$, then $\chi(p) = \left(\frac{\Delta_K}{p}\right) = -1$, $\mathfrak{p} = pO_K$ and $\mathfrak{N}(\mathfrak{p}) = p^2$. Furthermore, it is seen from (46) that the dominating terms in the summation are in the primes p with $\chi(p) = \left(\frac{\Delta_K}{p}\right) = 1$, which splits completely in K.

If we take $\sigma = 1 + 2/\log X < 2$, where $X \geq q$ is a real variable, then, from (44) and (46), we get

$$\frac{1}{2}\log|\Delta_K| + \frac{1}{4}(1 - \beta)(\log X)^2 > \sum_{p}(1 + \chi(p))\frac{\log p}{p}\frac{1}{p^{2/\log X}} > \frac{1}{e^2}\sum_{p \leq X}(1 + \chi(p))\frac{\log p}{p}$$

where the infinite series $\sum_p$ runs over the primes $p \in \mathbb{Z}$. Therefore, noticing that $\chi(p) \in \{-1, 0, 1\}$ and that $\chi(p) = 0$ if and only if $p \mid q$, we obtain

$$\sum_{\substack{p \leq X \\ \chi(p) = 1}} \frac{\log p}{p} + \frac{1}{2}\sum_{\substack{p \leq X \\ p \mid q}} \frac{\log p}{p} < \frac{e^2}{4}\log|\Delta_K| + \frac{e^2}{8}(1 - \beta)(\log X)^2 \tag{47}$$

for all $X \geq q$. Moreover, by noticing that $q = |\Delta_K| = 4N$ and N is a squarefree positive integer, we have

$$\sum_{\substack{p \leq X \\ p|q}} \frac{\log p}{p} = \sum_{p|q} \frac{\log p}{p} = \frac{\log 2}{2} + \sum_{\substack{p|q \\ p>2}} \frac{\log p}{p} \leq \frac{\log 2}{2} + \frac{1}{3} \log N < \frac{1}{3} \log q.$$

It follows from (47) that, for all $X \geq q$,

$$\sum_{\substack{p \leq X \\ \chi(p) \neq -1}} \frac{\log p}{p} = \sum_{\substack{p \leq X \\ \chi(p)=1}} \frac{\log p}{p} + \sum_{\substack{p \leq X \\ p|q}} \frac{\log p}{p} < \left(\frac{1}{6} + \frac{e^2}{4} \right) \log q + \frac{e^2}{8} (1-\beta)(\log X)^2. \quad (48)$$

It is well known that $\sum_{p \leq X} \frac{\log p}{p} \sim \log X$ as $X \to \infty$. By (48) in the case that q is fixed or that $\log q$ is *relatively small* to $\log X$ for large X, if the real zero $\beta \in (0,1)$ were so close to 1 that $(1-\beta) \log X$ is *extremely small*, then the primes $p \leq X$, which are *not inert* in K, would be *very rare*. The nature of Landau–Siegel zeros extremely close to 1 in this respect had also been discussed by Friedlander and Iwaniec [13].

The effect of Landau–Siegel zeros β extremely close to 1 causing the primes *not inert in* K to be very rare has been employed significantly in [32] to achieve a discovery that the real zero β has to be at least $c/\log q$ away from 1 for an absolute constant $c > 0$, which is much greater than Siegel's distance $C(\varepsilon)/q^{\varepsilon}$ for an arbitrary positive number $\varepsilon > 0$ with some constant $C(\varepsilon) > 0$ depending on ε.

A basic strategy in [32] is to construct a *nonzero* algebraic integer, denoted by Δ, in a biquadratic field L/K, which has all small enough primes *inert* in K as its prime factors. Then, one can obtain a *larger* lower bound for the absolute value of the field norm $|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$ when the primes *not inert* in K becomes *more rare* due to the real zero β being *closer* to 1. On the other hand, the quantity $|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$ must have an upper bound, depending only on q, which arises from its definition in terms of real and complex embeddings, since Δ is actually defined as the determinant of a full-rank square matrix with entries in O_L, the ring of integers of L, with predefined bounded $\mathbb{Z}$-coordinates in terms of q. Using the lower and upper bounds of $|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$, we see that the rarity (or abundance) of primes $p \leq X$ which are *not inert* in K must have a bound from above (or below). By the nature of the Landau–Siegel zero β extremely close to 1 as shown in (48), combing the available lower and upper bounds of $|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$ will yield a lower bound for $(1-\beta) \log X$. Hence, the distance $1-\beta$ between the real zero β and 1 will have a nontrivial lower bound, implying a remarkably enlarged zero-free interval $(\beta, 1)$ for $L(s, \chi)$.

The *method of the field norm* using the lower and upper bounds of its absolute value has been previously employed in 1986 by Lenstra [23] in theory of codes from geometry of

numbers. Lenstra used this simple method to construct the code from algebraic number fields and provided some heuristic to show that the code would be of high quality in the sense that the minimum distance of the code can potentially be relatively large for a fixed rate of the code. The author of this paper has used the same *method of the field norm* in [24] to simplify the construction of codes and further analyzed the Lenstra codes, which have been demonstrated to be of high quality as expected.

However, it is *crucial* for the achievement in [32] to construct a specific *nonzero* algebraic integer $\Delta \in O_L$ with a biquadratic field L/K, which has the property that all small enough primes *inert* in K are its prime factors.

In the following, we are going to present the construction of Δ given in [32] and verify the properties of Δ by providing accurate and accessible arguments in details for the purpose of rigor and completeness.

We introduce a biquadratic field as follows. For the given two quadratic fields

$$K = \mathbb{Q}(\sqrt{-N}) \text{ and } F = \mathbb{Q}(\sqrt{2})$$

we define a number field L as the composite field

$$L = KF = \mathbb{Q}(\sqrt{-N}, \sqrt{2}).$$

We need to find the Galois group of L for the calculation of the field norm $\mathrm{N}_{L/\mathbb{Q}}(\cdot)$. The Galois group of K is $\mathrm{Gal}(K/\mathbb{Q}) = \{e_1, \sigma_1\}$, where e_1 is the identity element and σ_1 is defined by $\sigma_1(\sqrt{-N}) = -\sqrt{-N}$. The Galois group of F is $\mathrm{Gal}(F/\mathbb{Q}) = \{e_2, \tau_2\}$, where e_2 is the identity element and τ_2 is defined by $\tau_2(\sqrt{2}) = -\sqrt{2}$. Since $K \cap F = \mathbb{Q}$, the Galois group of L is isomorphic to the direct product

$$\mathrm{Gal}(L/\mathbb{Q}) = \{e, \sigma, \tau, \sigma\tau\} \cong \mathrm{Gal}(K/\mathbb{Q}) \times \mathrm{Gal}(F/\mathbb{Q})$$

where $e = (e_1, e_2)$, $\sigma = (\sigma_1, e_2)$ and $\tau = (e_1, \tau_2)$. Hence, $\sigma\tau = \tau\sigma = (\sigma_1, \tau_2)$ with

$$\sigma(\sqrt{-N}) = (\sigma_1, e_2)|_K(\sqrt{-N}) = \sigma_1(\sqrt{-N}) = -\sqrt{-N}$$

and

$$\tau(\sqrt{2}) = (e_1, \tau_2)|_F(\sqrt{2}) = \tau_2(\sqrt{2}) = -\sqrt{2}.$$

It is clear that

$$\sigma(\sqrt{2}) = (\sigma_1, e_2)|_F(\sqrt{2}) = e_2(\sqrt{2}) = \sqrt{2}$$

and

$$\tau(\sqrt{-N}) = (e_1, \tau_2)|_K(\sqrt{-N}) = e_1(\sqrt{-N}) = \sqrt{-N}.$$

An integral basis of K is $\{1, \sqrt{-N}\}$ and hence $O_K = \mathbb{Z}[\sqrt{-N}]$. The field F has an integral basis of $\{1, \sqrt{2}\}$ and therefore the ring of algebraic integers $O_F = \mathbb{Z}[\sqrt{2}]$. The

determination of the ring of algebraic integers O_L for the biquadratic field L had been explicitly provided by Williams [49]. It is seen that

$$\mathcal{R} = \mathbb{Z}[\sqrt{-N}, \sqrt{2}] \subset O_L$$

which is a proper *subring* of O_L. Let $W \geq q$ be a positive integer. We consider the following subset

$$B_W = \{n_1 + n_2 a + n_3 b + n_4 ab \mid 0 \leq n_i \leq W - 1 \text{ for } i = 1, 2, 3, 4\} \subset \mathcal{R}$$

where $n_i \in \mathbb{Z}$ for $1 \leq i \leq 4$ with

$$a = \sqrt{-N} \text{ and } b = \sqrt{2}.$$

It is noted that $\{1, a, b, ab\}$ is the $\mathbb{Q}$-basis of the extension $L/\mathbb{Q}$ of degree $[L : \mathbb{Q}] = 4$. Thus, the four numbers 1, a, b and $ab = \sqrt{-2N}$ are linearly independent over the rational field $\mathbb{Q}$.

Let $\vec{n} = (n_1, n_2, n_3, n_4)^\top$ be a column vector, where $n_i \in \mathbb{Z}$ for $1 \leq i \leq 4$ and $\top$ denotes the transpose. We set

$$\theta_{\vec{n}} = n_1 + n_2 a + n_3 b + n_4 ab \in \mathcal{R}.$$

It is clear that $e(\theta_{\vec{n}}) = \theta_{\vec{n}}$,

$$\sigma(\theta_{\vec{n}}) = n_1 + n_2\sigma(a) + n_3\sigma(b) + n_4\sigma(a)\sigma(b) = n_1 - n_2 a + n_3 b - n_4 ab \in \mathcal{R}$$

and

$$\tau(\theta_{\vec{n}}) = n_1 + n_2\tau(a) + n_3\tau(b) + n_4\tau(a)\tau(b) = n_1 + n_2 a - n_3 b - n_4 ab \in \mathcal{R}.$$

Moreover, we have

$$\sigma\tau(\theta_{\vec{n}}) = n_1 + n_2\sigma\tau(a) + n_3\sigma\tau(b) + n_4\sigma\tau(a)\sigma\tau(b) = n_1 - n_2 a - n_3 b + n_4 ab \in \mathcal{R}.$$

Let $\mathbb{Z}_{\geq 0}$ denote the set of all nonnegative integers. Note that the subset B_W of $\mathcal{R}$ has the cardinality of $\#B_W = W^4$. For each $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{Z}^3_{\geq 0}$, we define a row vector of dimension W^4 as follows

$$R_\alpha = (\theta_{\vec{n}}^{\alpha_1} \sigma(\theta_{\vec{n}})^{\alpha_2} \sigma\tau(\theta_{\vec{n}})^{\alpha_3})$$

where $\theta_{\vec{n}} \in B_W \subset \mathcal{R}$. The W^4 algebraic integers $\theta_{\vec{n}}$ in B_W and correspondingly the W^4 entries in R_α can be placed in a lexicographical order, namely, the alphabetical order. When $\vec{n} = (0, 0, 0, 0)^\top$, it is agreed that the *first* entry in the row vector R_α is defined

as 1 for $\alpha = (0,0,0)$ and 0 for $\alpha \neq (0,0,0)$. We can see that every entry of the vector R_α is an algebraic integer in $\mathcal{R} \subset O_L$.

We choose the parameter H with the value

$$H = 10^6$$

and define the following four numbers in terms of W

$$U = W^{4/3}, \;\; T_1 = \lceil 8H^{2/3}U \rceil, \;\; T_2 = T_2 = \lceil 8H^{-1/3}U \rceil. \tag{49}$$

Let $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{Z}^3_{\geq 0}$ with $\alpha_j \leq T_j$ for $j = 1,2,3$. We define the matrix $\mathcal{M}$ with

$$T = (T_1 + 1)(T_2 + 1)(T_3 + 1)$$

row vectors of dimension W^4 as follows. The row vectors of $\mathcal{M}$ are indexed by $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ with the alphabetical order and the row vector with index α of $\mathcal{M}$ equals R_α. It is clear that $T > 512U^3 = 512W^4 > W^4$, i.e., the number of row vectors of the $T \times W^4$ matrix $\mathcal{M}$ is greater than the number of its column vectors.

The following lemma is a fundamental result which has essentially been given in [32]. Based on the arguments provided by [32], we will present a detailed proof with extra arguments and derivations which are entailed but do not appear in [32].

Lemma 7 *The matrix $\mathcal{M}$ has full column rank, i.e., the rank of $\mathcal{M}$ equals W^4, the number of its columns.*

Proof: See Appendix B. □

Note that every entry of the matrix $\mathcal{M}$ is an algebraic integer in $\mathcal{R} \subset O_L$. The row rank and the column rank of any matrix are always equal. Lemma 7 guarantees that there exist W^4 row vectors of $\mathcal{M}$ which are linearly independent in the number field L.

6.1 A specific nonzero algebraic integer Δ in O_L

The row vectors R_α of the matrix $\mathcal{M}$ are indexed by $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{Z}^3_{\geq 0}$ with $\alpha_j \leq T_j$ for $j = 1,2,3$. We define the H-weight of the index α as

$$\mathrm{wt}(\alpha) = \alpha_1 + H\alpha_2 + H\alpha_3$$

where $H = 10^6$ is the chosen parameter.

We arrange the order of indices α of the row vectors R_α in the matrix $\mathcal{M}$ by increasing $\mathrm{wt}(\alpha)$. In the case that $\mathrm{wt}(\alpha) = \mathrm{wt}(\hat{\alpha})$ for two different indices $\alpha \neq \hat{\alpha}$, the arrangement to break tie resorts to using their alphabetical order.

It is clear that the first index is $\alpha = (0, 0, 0)$ and the corresponding row vector R_α is an all-one vector. Starting from the first retained index $\alpha = (0, 0, 0)$, we consider the next index α in the order of the H-weight. It will be retained if the row vector R_α can increase the span of the earlier retained rows, namely, if the augmented submatrix consisting of the earlier retained rows appended with the row vector R_α continues to have full row rank. According to Lemma 7, this procedure of selection will proceed in a unique way and end with W^4 retained rows of the matrix $\mathcal{M}$. Let $\mathcal{P}_{ri}$ be the set of the retained indices α, which is uniquely determined by the procedure with the H-weight.

It is clear that the ordered set $\mathcal{P}_{ri}$ of retained indices has the cardinality of

$$\#\mathcal{P}_{ri} = W^4.$$

We denote by $\mathcal{M}_{ri}$ the submatrix of the matrix $\mathcal{M}$ consisting of the row vectors R_α with $\alpha \in \mathcal{P}_{ri}$ in the order of the H-weight. Remind that R_α is of dimension W^4. We see that $\mathcal{M}_{ri}$ is a *full-rank* square matrix of size $W^4 \times W^4$, every entry of which is an algebraic integer in $\mathcal{R} \subset O_L$. The determinant of $\mathcal{M}_{ri}$ is thus *nonzero*.

We define the *nonzero* algebraic integer

$$\Delta = \det(\mathcal{M}_{ri}) \in O_L \setminus \{0\} \tag{50}$$

which will play a vital role in the following process. The algebraic integer Δ induces, via the field norm, a *nonzero* rational integer given by

$$\mathrm{N}_{L/\mathbb{Q}}(\Delta) \in \mathbb{Z} \setminus \{0\}. \tag{51}$$

The following result on the set $\mathcal{P}_{ri}$ of retained indices will be needed.

Lemma 8 *We put*

$$S_1 = \sum_{\alpha \in \mathcal{P}_{ri}} \alpha_1 \text{ and } S_2 = \sum_{\alpha \in \mathcal{P}_{ri}} (\alpha_2 + \alpha_3).$$

Then, we have

$$S_1 \geq \frac{1}{135} W^4 H^{2/3} U \text{ and } S_2 \leq 18 W^4 H^{-1/3} U.$$

Proof: Since $U = W^{4/3}$ with $W \geq q > 3 \cdot 10^{20}$, $0 \leq \alpha_2 \leq T_2 = \lceil 8H^{-1/3}U \rceil$ and $0 \leq \alpha_3 \leq T_3 = \lceil 8H^{-1/3}U \rceil$, we have

$$S_2 \leq 2\lceil 8H^{-1/3}U \rceil \sum_{\alpha \in \mathcal{P}_{ri}} 1 = 2W^4 \lceil 8H^{-1/3}U \rceil \leq 18 W^4 H^{-1/3} U.$$

For any fixed α_1 with $0 \le \alpha_1 \le T_1 = \lceil 8H^{2/3}U \rceil$, there are at most

$$Q_0 = (T_2+1)(T_3+1) \le (8H^{-1/3}U+2)^2 \le 66H^{-2/3}U^2 = 66H^{-2/3}W^{8/3}$$

retained indices $\alpha = (\alpha_1, \alpha_2, \alpha_3)$.

We rearrange elements in the set

$$\{\alpha_1 \mid \alpha = (\alpha_1, \alpha_2, \alpha_3) \in \mathcal{P}_{ri}\}$$

by sorting in a nondecreasing order and get the following set

$$\{b_1, b_2, \cdots, b_{W^4}\}$$

where $W^4 = \#\mathcal{P}_{ri}$. Therefore,

$$S_1 = \sum_{\alpha \in \mathcal{P}_{ri}} \alpha_1 = \sum_{\ell=1}^{W^4} b_\ell.$$

It is seen that $0 = b_1 \le b_2 \le \cdots \le b_{W^4} \le T_1$ and each value of b_ℓ can repeat itself at most Q_0 times. There exists a positive integer k such that

$$(k+1)Q_0 \le W^4 < (k+2)Q_0.$$

Then, we have

$$S_1 \ge \sum_{m=0}^{k} mQ_0 = \frac{k(k+1)}{2}Q_0 \ge \frac{Q_0}{2}\left(\frac{W^4}{Q_0} - 2\right)\left(\frac{W^4}{Q_0} - 1\right) \ge \frac{0.99}{2}Q_0\frac{W^4}{Q_0}\frac{W^4}{Q_0}$$

and hence

$$S_1 \ge \frac{0.99}{2}W^4\frac{W^4}{66H^{-2/3}W^{8/3}} = \frac{0.99}{132}W^4H^{2/3}U \ge \frac{1}{135}W^4H^{2/3}U.$$

The proof of Lemma 8 is complete. □

By Lemma 8, the ratio of S_2 to S_1 has an upper bound given by

$$\frac{S_2}{S_1} \le \frac{18 \cdot 135}{H} = \frac{2430}{10^6} = 0.00243. \tag{52}$$

6.2 An upper bound for $|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$

Ostrowski's theorem for a number field says that every nontrivial absolute value on L is equivalent to either a $\mathfrak{p}$-adic nonarchimedean absolute value for a nonzero prime ideal $\mathfrak{p}$ of O_L or an archimedean absolute value associated to a real or complex-conjugate pair of embeddings of L (see [33] and [6]).

For a given nonzero integer $\Delta \in O_L \setminus \{0\}$, the archimedean absolute value $v|\infty$ that corresponds to a real embedding $\sigma : K \hookrightarrow \mathbb{R}$ is defined as $|\Delta|_v = |\sigma(\Delta)|$. For archimedean $v|\infty$ that corresponds to a complex embedding $\sigma : K \hookrightarrow \mathbb{C}$, $|\Delta|_v = |\sigma(\Delta)|^2$. For the $\mathfrak{p}$-adic nonarchimedean absolute value, we define

$$|\Delta|_{\mathfrak{p}} = \mathfrak{N}(\mathfrak{p})^{-v_{\mathfrak{p}}(\Delta)}$$

where $v_{\mathfrak{p}}(\Delta) \in \mathbb{Z}_{\geq 0}$ is the $\mathfrak{p}$-adic valuation of Δ.

The archimedean and nonarchimedean absolute values on L can be tied together by a product formula as follows (see [6]).

Lemma 9 *For $\Delta \in O_L \setminus \{0\}$, we have*

$$\prod_v |\Delta|_v = 1$$

where the product runs over the absolute values v on L.

Suppose that the principal integral ideal ΔO_L is factored into prime ideals

$$\Delta O_L = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$$

where a_j is a positive integer and $\mathfrak{p}_j$'s are distinct prime ideals for $j = 1, \cdots, r$. While the archimedean contribution to $\prod_v |\Delta|_v$ is $|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$, the nonarchimedean contribution to $\prod_v |\Delta|_v$ is given by

$$\prod_{j=1}^{r} \mathfrak{N}(\mathfrak{p}_j)^{-v_{\mathfrak{p}_j}(\Delta)} = \prod_{j=1}^{r} \mathfrak{N}(\mathfrak{p}_j)^{-a_j}.$$

From the product formula, it follows that

$$\prod_{v|\infty} |\Delta|_v = |\mathrm{N}_{L/\mathbb{Q}}(\Delta)| = \prod_{j=1}^{r} \mathfrak{N}(\mathfrak{p}_j)^{a_j}. \tag{53}$$

We note that the product formula reduces to the fundamental theorem of arithmetic in the case that $L = \mathbb{Q}$.

In the method of the field norm, we use the left-hand (or right-hand) side of its absolute value in (53) to find an upper (or a lower) bound for $|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$.

In the current scenario, the field L is $\mathbb{Q}(\sqrt{-N}, \sqrt{2})$ with $\mathrm{Gal}(L/\mathbb{Q}) = \{e, \sigma, \tau, \sigma\tau\}$. It is seen that $\{e, \sigma\}$ and $\{\tau, \sigma\tau\}$ are two pairs of complex embeddings. Therefore,

$$|\mathrm{N}_{L/\mathbb{Q}}(\Delta)| = |\Delta|^2 |\tau(\Delta)|^2.$$

By using (50), it is clear that

$$\tau(\Delta) = \tau(\det(\mathcal{M}_{ri})) = \det(\tau(\mathcal{M}_{ri}))$$

and hence

$$|\mathrm{N}_{L/\mathbb{Q}}(\Delta)| = |\det(\mathcal{M}_{ri})|^2 |\det(\tau(\mathcal{M}_{ri}))|^2.$$

We introduce the following subset

$$C_W = \{n_1 + n_2 a + n_3 b + n_4 ab \mid -W + 1 \leq n_i \leq W - 1 \text{ for } i = 1, 2, 3, 4\} \subset \mathcal{R}$$

where $n_i \in \mathbb{Z}$ for $1 \leq i \leq 4$. We have $B_W \subset C_W$. If $\theta_{\vec{n}} \in C_W$, then $\sigma(\theta_{\vec{n}}) \in C_W$ and $\tau(\theta_{\vec{n}}) \in C_W$ and thus $\sigma\tau(\theta_{\vec{n}}) \in C_W$.

Every entry in the matrix $\mathcal{M}_{ri}$ has the form of $\theta_{\vec{n}}^{\alpha_1} \sigma(\theta_{\vec{n}})^{\alpha_2} \sigma\tau(\theta_{\vec{n}})^{\alpha_3}$ where

$$\theta_{\vec{n}} \in B_W \subset C_W$$

and $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in \mathcal{P}_{ri}$. Thus, every entry in the matrix $\tau(\mathcal{M}_{ri})$ has the form of

$$\tau(\theta_{\vec{n}}^{\alpha_1} \sigma(\theta_{\vec{n}})^{\alpha_2} \sigma\tau(\theta_{\vec{n}})^{\alpha_3}) = \tau(\theta_{\vec{n}})^{\alpha_1} \sigma\tau(\theta_{\vec{n}})^{\alpha_2} \sigma(\theta_{\vec{n}})^{\alpha_3}$$

where $\sigma\tau = \tau\sigma$ and $\sigma\sigma = \tau\tau = e$ in the Galois group $\mathrm{Gal}(L/\mathbb{Q})$.

It is clear that, for any $\theta_{\vec{n}} = n_1 + n_2 a + n_3 b + n_4 ab \in C_W$,

$$|\theta_{\vec{n}}| \leq (W-1)(1 + |a| + |b| + |ab|) = (W-1)(1 + \sqrt{N} + \sqrt{2} + \sqrt{2N})$$

and hence from $q = 4N > 3 \cdot 10^{20}$ that

$$|\theta_{\vec{n}}| \leq W(1+\sqrt{2})(1+\sqrt{N}) = W(1+\sqrt{2})(1+\sqrt{q}/2) \leq 1.3W\sqrt{q} = \theta_{max}. \tag{54}$$

Therefore, every row vector indexed by $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in \mathcal{P}_{ri}$ of the two matrices $\mathcal{M}_{ri}$ and $\tau(\mathcal{M}_{ri})$, which both have the same size of $W^4 \times W^4$, has the length at most

$$\sqrt{W^4}\theta_{max}^{\alpha_1+\alpha_2+\alpha_3} = W^2 \theta_{max}^{\alpha_1+\alpha_2+\alpha_3}.$$

Hadamard's inequality provides an upper bound on the determinant of a square matrix, whose entries are complex numbers, in terms of the lengths of its row vectors. According to Hadamard's inequality, we have

$$\max\{|\det(\mathcal{M}_{ri})|, |\det(\tau(\mathcal{M}_{ri}))|\} \leq \prod_{\alpha \in \mathcal{P}_{ri}} W^2 \theta_{max}^{\alpha_1+\alpha_2+\alpha_3} = W^{2W^4} \theta_{max}^{S_1+S_2}.$$

Therefore, we obtain

$$|\mathrm{N}_{L/\mathbb{Q}}(\Delta)| = |\det(\mathcal{M}_{ri})|^2 |\det(\tau(\mathcal{M}_{ri}))|^2 \leq \left(W^{2W^4} \theta_{max}^{S_1+S_2}\right)^4$$

and hence

$$\log |\mathrm{N}_{L/\mathbb{Q}}(\Delta)| \leq 4 \log \left(W^{2W^4} \theta_{max}^{S_1+S_2}\right).$$

By noting (54), we can attain the following upper bound

$$\frac{1}{4} \log |\mathrm{N}_{L/\mathbb{Q}}(\Delta)| \leq 2W^4 \log W + (S_1 + S_2)(\log W + \log \sqrt{q} + \log 1.3). \tag{55}$$

6.3 A lower bound for $|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$

In the following, we use the right-hand side in (53) to find a lower bound of $|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$.

We consider all primes $p > H$ which are *inert* in K. It is to be seen that if $p \leq \alpha_1$ for some $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in \mathcal{P}_{ri}$, then p must be a prime factor of Δ in the sense that $\Delta = pt$ for some algebraic integer $t \in O_L$.

Let $p \in \mathbb{Z}$ with $p > H$ and $\chi(p) = -1$. Thus, p is an odd prime and $p \nmid |\Delta_K|$. Remind that $a = \sqrt{-N}$, $b = \sqrt{2}$ and $\mathcal{R} = \mathbb{Z}[a, b]$. By Euler's criterion, we have

$$\chi(p) = \left(\frac{\Delta_K}{p}\right) = \left(\frac{-4N}{p}\right) = \left(\frac{-N}{p}\right) \equiv (-N)^{\frac{p-1}{2}} \pmod{p\mathbb{Z}}$$

and hence

$$a^p = (-N)^{\frac{p-1}{2}} a \equiv -a \pmod{p\mathcal{R}} \tag{56}$$

In a similar fashion, we get

$$b^p = 2^{\frac{p-1}{2}} b \equiv \left(\frac{2}{p}\right) b \pmod{p\mathcal{R}} \tag{57}$$

Since p is odd, there is $\left(\frac{2}{p}\right) \in \{-1, 1\}$.

In the first case that $\left(\frac{2}{p}\right) = 1$, by using (57) we have

$$b^p \equiv b \pmod{p\mathcal{R}} \tag{58}$$

Let $\theta_{\vec{n}} = n_1 + n_2 a + n_3 b + n_4 ab \in \mathcal{R}$. Then, by using the multinomial theorem and Fermat's little theorem, we obtain

$$\theta_{\vec{n}}^p \equiv n_1^p + n_2^p a^p + n_3^p b^p + n_4^p a^p b^p \equiv n_1 + n_2 a^p + n_3 b^p + n_4 a^p b^p \pmod{p\mathcal{R}}$$

and hence, from (56) and (58),

$$\theta_{\vec{n}}^p \equiv n_1 - n_2 a + n_3 b - n_4 ab \pmod{p\mathcal{R}}$$

i.e.,

$$\theta_{\vec{n}}^p \equiv \sigma(\theta_{\vec{n}}) \pmod{p\mathcal{R}}. \tag{59}$$

For each $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in \mathcal{P}_{ri}$ with $\alpha_1 \geq p$, we have $\alpha_1 = pk + r$ with $0 \leq r < p$ and

$$k = \left\lfloor \frac{\alpha_1}{p} \right\rfloor \geq 1.$$

Comparing with the row vector $R_\alpha = (\theta_{\vec{n}}^{\alpha_1} \sigma(\theta_{\vec{n}})^{\alpha_2} \sigma\tau(\theta_{\vec{n}})^{\alpha_3})$ in the matrix $\mathcal{M}_{ri}$, we define the following row vector

$$\widetilde{R}_\alpha = ((\theta_{\vec{n}}^p - \sigma(\theta_{\vec{n}}))^k \theta_{\vec{n}}^r \sigma(\theta_{\vec{n}})^{\alpha_2} \sigma\tau(\theta_{\vec{n}})^{\alpha_3}) \tag{60}$$

if $p \leq \alpha_1$ and define $\widetilde{R}_\alpha = R_\alpha$ if $p > \alpha_1$ to get a new matrix $\widetilde{\mathcal{M}}_{ri}$ with row vectors $\widetilde{R}_\alpha$.

Since

$$(\theta_{\vec{n}}^p - \sigma(\theta_{\vec{n}}))^k \theta_{\vec{n}}^r = \sum_{m=0}^{k} \binom{k}{m} (-1)^m (\sigma(\theta_{\vec{n}}))^m \theta_{\vec{n}}^{pk+r-pm},$$

we have

$$(\theta_{\vec{n}}^p - \sigma(\theta_{\vec{n}}))^k \theta_{\vec{n}}^r = \theta_{\vec{n}}^{\alpha_1} + \sum_{m=1}^{k} \binom{k}{m} (-1)^m \theta_{\vec{n}}^{\alpha_1 - pm} (\sigma(\theta_{\vec{n}}))^m.$$

Hence, for each $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in \mathcal{P}_{ri}$ with $\alpha_1 \geq p$,

$$\widetilde{R}_\alpha = R_\alpha + \sum_{m=1}^{k} \binom{k}{m} (-1)^m R_{\alpha - (pm, -m, 0)} \tag{61}$$

which is the α-indexed row vector in the matrix $\widetilde{\mathcal{M}}_{ri}$.

It is claimed that $\det(\widetilde{\mathcal{M}}_{ri}) = \det(\mathcal{M}_{ri})$.

In fact, for the *first* index $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in \mathcal{P}_{ri}$ for which $\widetilde{R}_\alpha \neq R_\alpha$, it is clear that $\alpha \neq (0, 0, 0)$ and the H-weight $\mathrm{wt}(\alpha) > 0$. Note that the index $\alpha - (pm, -m, 0)$ of $R_{\alpha - (pm, -m, 0)}$ in (61) *may or may not* be in the ordered set $\mathcal{P}_{ri}$ of retained indices.

For $p > H$, the index $\alpha - (pm, -m, 0) = (\alpha_1 - pm, \alpha_2 + m, \alpha_3)$ has the H-weight

$$\mathrm{wt}(\alpha - (pm, -m, 0)) = \mathrm{wt}((\alpha_1 - pm, \alpha_2 + m, \alpha_3)) = \mathrm{wt}(\alpha) - (p - H)m < \mathrm{wt}(\alpha) \tag{62}$$

for $1 \leq m \leq k$. According to the procedure of selection for the index set $\mathcal{P}_{ri}$, it follows from (62) that the row vector $R_{\alpha - (pm, -m, 0)}$ must be in the span of the retained row vectors before R_α. Therefore, by using (61) and (62), we attain

$$\widetilde{R}_\alpha = R_\alpha + \sum_{\hat{\alpha}} c_{\hat{\alpha}} R_{\hat{\alpha}} \tag{63}$$

where the summation $\sum_{\hat{\alpha}}$ runs over $\hat{\alpha} \in \mathcal{P}_{ri}$ with $\mathrm{wt}(\hat{\alpha}) < \mathrm{wt}(\alpha)$ and the coefficients $c_{\hat{\alpha}} \in L$ are obtained in the operation for the form of linear combination. Since $\alpha \in \mathcal{P}_{ri}$ is the *first* index for which $\widetilde{R}_\alpha \neq R_\alpha$, all $R_{\hat{\alpha}}$ in the summation (63) are row vectors in the matrix $\widetilde{\mathcal{M}}_{ri}$, i.e., $R_{\hat{\alpha}} = \widetilde{R}_{\hat{\alpha}}$. Applying the theory of determinants, while the row vector $\widetilde{R}_\alpha$ in the matrix $\widetilde{\mathcal{M}}_{ri}$ is replaced by R_α, the determinant of the matrix remains *unchanged*. For this updated matrix after row replacement, we will repeat the process, but the determinant of the matrix keeping the same. At the end of the procedure, the matrix $\widetilde{\mathcal{M}}_{ri}$ reduces to the matrix $\mathcal{M}_{ri}$. So, we have proved that

$$\det(\widetilde{\mathcal{M}}_{ri}) = \det(\mathcal{M}_{ri}) = \Delta.$$

It can be seen from (59) and (60) that every entry in the row vector $\widetilde{R}_\alpha$ belongs to $p^k\mathcal{R}$. Applying the theory of determinants, we have

$$\Delta = \det(\widetilde{\mathcal{M}}_{ri}) \in p^k\mathcal{R}.$$

In the second case that $\left(\frac{2}{p}\right) = -1$, by using (57) we have

$$b^p \equiv -b \pmod{p\mathcal{R}} \tag{64}$$

It follows from (56) and (64) that

$$\theta_{\vec{n}}^p \equiv n_1 + n_2 a^p + n_3 b^p + n_4 a^p b^p \equiv n_1 - n_2 a - n_3 b + n_4 ab \pmod{p\mathcal{R}}$$

i.e.,

$$\theta_{\vec{n}}^p \equiv \sigma\tau(\theta_{\vec{n}}) \pmod{p\mathcal{R}}$$

We can use the same proof as that in the first case with corresponding replacements such as the row vector in (60) replaced by

$$\widetilde{R}_\alpha = ((\theta_{\vec{n}}^p - \sigma\tau(\theta_{\vec{n}}))^k \theta_{\vec{n}}^r \sigma(\theta_{\vec{n}})^{\alpha_2} \sigma\tau(\theta_{\vec{n}})^{\alpha_3}) \tag{65}$$

and the row vectors $R_{\alpha-(pm,-m,0)}$ with indices $\alpha - (pm, -m, 0)$ in (61) replaced by the row vectors $R_{\alpha-(pm,0,-m)}$ with indices $\alpha - (pm, 0, -m)$.

In both cases of $\left(\frac{2}{p}\right) = 1$ and -1, respectively, we can achieve the following result. For each $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in \mathcal{P}_{ri}$ with $\alpha_1 \geq p$,

$$\Delta \in p^k\mathcal{R} \text{ with } k = \left\lfloor \frac{\alpha_1}{p} \right\rfloor.$$

Therefore, we have

$$\Delta \in p^{E_p}\mathcal{R} \text{ with } E_p = \sum_{\alpha\in\mathcal{P}_{ri}} \left\lfloor \frac{\alpha_1}{p} \right\rfloor.$$

According to (50), we have $\Delta \in O_L$ and $\Delta \neq 0$. Note that $\mathcal{R} \subset O_L$. We can write $\Delta = p^{E_p}t$ with $t \in \mathcal{R}$ and $t \neq 0$. Thus, $\mathrm{N}_{L/\mathbb{Q}}(t) \in \mathbb{Z}$ is a *nonzero* integer and

$$|\mathrm{N}_{L/\mathbb{Q}}(\Delta)| = |\mathrm{N}_{L/\mathbb{Q}}(p^{E_p})||\mathrm{N}_{L/\mathbb{Q}}(t)| = (p^{E_p})^{[L:\mathbb{Q}]}|\mathrm{N}_{L/\mathbb{Q}}(t)| = p^{4E_p}|\mathrm{N}_{L/\mathbb{Q}}(t)| \geq p^{4E_p}.$$

Consequently, $p^{4E_p} \mid |\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$ for all primes $p > H$ with $\chi(p) = -1$, and hence the following lower bound

$$\frac{1}{4}\log|\mathrm{N}_{L/\mathbb{Q}}(\Delta)| \geq \sum_{\substack{p>H \\ \chi(p)=-1}} E_p \log p \text{ with } E_p = \sum_{\alpha\in\mathcal{P}_{ri}} \left\lfloor \frac{\alpha_1}{p} \right\rfloor. \tag{66}$$

6.4 Estimation of the distance between the real zero β and 1

We have analyzed the effect of the Landau–Siegel zero β extremely close to 1 causing the primes *not inert* in the imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-N})$ to be very rare,

whose estimation has been given in (48). In the following, the method of the field norm using the upper bound of its absolute value $|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$ given in (55) and the lower bound given in (66) will be employed to attain an estimation for the distance between the real zero β and 1.

Suppose that the Landau–Siegel zero $\beta \in (0,1)$ of $L(s,\chi)$ exists, which is real and simple and satisfies $L(\beta,\chi)=0$.

Let $W=\lfloor q^{\eta}\rfloor$ with parameter $\eta \geq 16$ to be determined later. Remind that $U = W^{4/3} > q$. We choose the real variable $X = U$ in (48) and obtain

$$\sum_{\substack{p\leq U\\ \chi(p)\neq -1}} \frac{\log p}{p} < \left(\frac{1}{6}+\frac{e^2}{4}\right)\log q + \frac{e^2}{8}(1-\beta)(\log U)^2.$$

The lower bound for $|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$ given in (66) yields the following

$$\frac{1}{4}\log|\mathrm{N}_{L/\mathbb{Q}}(\Delta)| \geq \sum_{\substack{H<p\leq U\\ \chi(p)=-1}}\sum_{\alpha\in\mathcal{P}_{ri}}\left\lfloor\frac{\alpha_1}{p}\right\rfloor\log p \geq S_1\sum_{\substack{H<p\leq U\\ \chi(p)=-1}}\frac{\log p}{p} - W^4\sum_{p\leq U}\log p$$

where $\lfloor r\rfloor \geq r-1$ for $r\in\mathbb{R}$ is used.

According to [37, p. 70, (3.24)], we have $\sum_{p\leq H}\frac{\log p}{p}\leq \log H$. By [37, p. 70, (3.21)] and [37, p. 65, (2.11)], we get $\sum_{p\leq U}\frac{\log p}{p}\geq \log U - 1.333 - 1/(2\log U)$. Therefore,

$$\sum_{\substack{H<p\leq U\\ \chi(p)=-1}}\frac{\log p}{p} \geq \sum_{p\leq U}\frac{\log p}{p} - \sum_{\substack{p\leq U\\ \chi(p)\neq -1}}\frac{\log p}{p} - \sum_{p\leq H}\frac{\log p}{p} \geq \log U - 1.5 - \sum_{\substack{p\leq U\\ \chi(p)\neq -1}}\frac{\log p}{p} - \log H.$$

According to [37, p. 71, (3.32)] and [36, p. 212], we have $\sum_{p\leq U}\log p \leq 1.0163U$. Combining the above inequalities, we obtain the following lower bound with explicit constants

$$\begin{aligned}&\frac{1}{4}\log|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|\\ &\geq\ S_1[\log U - \log H - 1.5 - (1/6+e^2/4)\log q - (e^2/8)(1-\beta)(\log U)^2] - 1.0163W^4U\end{aligned}$$

where $H = 10^6$. On the other hand, from (55) we have the following upper bound

$$\frac{1}{4}\log|\mathrm{N}_{L/\mathbb{Q}}(\Delta)| \leq 2W^4\log W + (S_1+S_2)(\log W + \log\sqrt{q} + 0.2624).$$

Remind that $S_1 \geq \frac{1}{135}H^{2/3}W^4U$ and $S_2 \leq 18H^{-1/3}W^4U$ in Lemma 8, which satisfy $S_2/S_1 \leq 0.00243$ given by (52). Therefore, we obtain

$$\frac{\log|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|}{4S_1\log U} \leq 270\frac{\log W}{H^{2/3}U\log U} + 1.00243\left(\frac{\log W}{\log U} + \frac{\log q}{2\log U} + \frac{0.2624}{\log U}\right).$$

Note that $q > 3 \cdot 10^{20}$. It is clear that $W = \lfloor q^{\eta} \rfloor$ with $\eta \geq 16$ satisfies $q^{15} \leq W \leq q^{\eta}$. We have put $U = W^{4/3}$ and $H = 10^6$. Therefore,

$$\frac{\log |\mathrm{N}_{L/\mathbb{Q}}(\Delta)|}{4S_1 \log U} \leq 1.00243\frac{3}{4} + \frac{1.00243 \log q}{2 \log U} + 0.001 < 0.7529 + 0.5013\frac{\log q}{\log U}.$$

Since $S_1 \geq \frac{1}{135} H^{2/3} W^4 U$, we have

$$1.0163\frac{W^4 U}{S_1 \log U} \leq 1.0163\frac{135}{10000 \log U} < 0.0001.$$

Combining the lower and upper bounds of $|\mathrm{N}_{L/\mathbb{Q}}(\Delta)|$, we can attain

$$1 - \frac{\log H}{\log U} - \frac{1.5}{\log U} - 0.7530 \leq \left(\frac{1}{6} + \frac{e^2}{4} + 0.5013\right)\frac{\log q}{\log U} + \frac{e^2}{8}(1-\beta)\log U.$$

It is estimated that $\log H / \log U \leq 6/400 = 0.015$. Thus, we have

$$0.229 < \left(\frac{1}{6} + \frac{e^2}{4} + 0.5013\right)\frac{\log q}{\log U} + \frac{e^2}{8}(1-\beta)\log U < 2.5153\frac{\log q}{\log U} + 0.9237(1-\beta)\log U.$$

In $W = \lfloor q^{\eta} \rfloor$, we choose

$$\eta = 16.4751.$$

Then, $W = \lfloor q^{16.4751} \rfloor \geq q^{16.4751} - 1 = q^{16.4750}(q^{0.0001} - q^{-16.4750}) > q^{16.4750}$. Noting that $\log U = (4/3)\log W \leq (4/3)\eta \log q$, we get

$$0.229 < 2.5153\frac{3}{4 \cdot 16.4750} + 0.9237\frac{4}{3}\eta(1-\beta)\log q$$

and hence

$$(1-\beta)\log q > \frac{3(0.229 - 0.1146)}{3.6948\eta} > 0.005638,$$

i.e.,

$$1 - \beta > 0.005638\frac{1}{\log q}. \tag{67}$$

We can summarize the above result with explicit constants in the form of a zero-free interval located in $(0,1)$ for $L(s,\chi)$, which will be utilized in the next section.

Proposition 8 *Let N be any given squarefree positive integer with $N > 7.5 \cdot 10^{19}$ and $N \equiv 1, 2 \pmod 4$ and put $D = -4N$ and $q = 4N$. Let $\chi(n) = \left(\frac{D}{n}\right)$ be the real primitive Dirichlet character of $K = \mathbb{Q}(\sqrt{D})$ and $L(s,\chi)$ be the corresponding Dirichlet L-function. If the number $\beta \in (0,1)$ satisfies*

$$1 - \beta \leq 0.0056\frac{1}{\log q} \tag{68}$$

then $L(s,\chi) \neq 0$ for s in the interval $[\beta, 1)$.

7 Proof of Proposition 6

It is now ready to prove Proposition 6 for every squarefree positive integer $N > 7.5 \cdot 10^{19}$ with $N \equiv 1, 2 \pmod 4$, which, in turn, proves Theorem 1 as stated in Section 4.

By using the class number formula given in (15), it is clear that Proposition 7 together with Proposition 8 can imply the following result.

Theorem 4 *Let N be any given squarefree positive integer with $N > 7.5 \cdot 10^{19}$ and $N \equiv 1, 2 \pmod 4$ and put $D = -4N$ and $q = 4N$. Let h_K be the class number of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{D})$ and $\chi(n) = \left(\frac{D}{n}\right)$ be the Kronecker symbol with the corresponding Dirichlet L-function $L(s, \chi)$. Then, we have*

$$L(1, \chi) > 0.013608 \frac{1}{\log q} \tag{69}$$

and

$$h_K > 0.00433 \frac{\sqrt{q}}{\log q}. \tag{70}$$

In fact, from Proposition 8 we can choose $\beta = 1 - 0.0056/\log q \in (0, 1)$, which satisfies (33) in applying Proposition 7.

We are going to prove that (17) in Proposition 6 holds, namely,

$$h_K \neq 2^{\omega(4N)-1}$$

where $\omega(4N)$ is the number of distinct prime factors of $4N$.

If the squarefree positive integer N satisfies $N \equiv 1 \pmod 4$, we can write

$$N = p_1' \cdots p_\ell'$$

where $p_1', \cdots, p_\ell'$ are ℓ distinct *odd* primes with an even number of primes $\equiv 3 \pmod 4$. For any squarefree positive integer N with $N \equiv 2 \pmod 4$, we can write

$$N = 2p_1' \cdots p_\ell'$$

where $p_1', \cdots, p_\ell'$ are ℓ distinct *odd* primes. In both cases, we have $\omega(4N) = \ell + 1$. Therefore, we need to prove that

$$h_K \neq 2^\ell. \tag{71}$$

Since $N > 7.5 \cdot 10^{19}$, we have $q = 4N > 3 \cdot 10^{20}$. By using (70), we get

$$h_K > 0.00433 \frac{\sqrt{q}}{\log q} > 1590610.$$

In the case that $1 \le \ell \le 20$, we have

$$2^\ell \le 2^{20} = 1048576 < h_K.$$

For any given $\ell \ge 21$, we have

$$q = 4N > 2p_1' \cdots p_\ell'$$

where $p_1', \cdots, p_\ell'$ are ℓ distinct *odd* primes.

The primorial $p_n\#$ is defined as the product of the first n primes

$$p_n\# = \prod_{k=1}^{n} p_k$$

where p_k is the kth prime number. Therefore, $q > p_{\ell+1}\#$.

It is clear that the function $\frac{x}{\log x}$ of real variable $x > e$ is an increasing function. For $\ell \ge 21$, we have $p_{\ell+1}\# > p_{21}^{\ell-19} p_{20}\#$ and hence

$$\frac{\sqrt{q}}{\log q} \ge \frac{\sqrt{p_{\ell+1}\#}}{\log(p_{\ell+1}\#)} \ge \frac{(\sqrt{p_{21}})^{\ell-19}\sqrt{p_{20}\#}}{(\ell-19)\log p_{21} + \log(p_{20}\#)}.$$

Therefore, by using (70), we obtain for $\ell \ge 21$

$$\frac{h_K}{2^\ell} > \frac{0.00433}{2^\ell}\frac{\sqrt{q}}{\log q} \ge \frac{0.00433}{2^{19}}\frac{(\sqrt{p_{21}}/2)^{\ell-19}\sqrt{p_{20}\#}}{(\ell-19)\log p_{21} + \log(p_{20}\#)}$$

where $p_{20} = 71$ and $p_{21} = 73$. Since $(\ell-19)\log p_{21} + \log(p_{20}\#) \le (\ell-19)\log p_{21}\log(p_{20}\#)$ for $\ell \ge 21$, we have

$$\frac{h_K}{2^\ell} \ge \frac{0.00433}{2^{19}\log p_{21}}\frac{\sqrt{p_{20}\#}}{\log(p_{20}\#)}\frac{(\sqrt{p_{21}}/2)^{\ell-19}}{\ell-19}.$$

Noting that the right-hand side is an increasing function for $\ell \ge 21$, we can attain

$$\frac{h_K}{2^\ell} \ge \frac{0.00433}{2^{19}\log p_{21}}\frac{\sqrt{p_{20}\#}}{\log(p_{20}\#)}\frac{(\sqrt{p_{21}}/2)^{2}}{2}.$$

It is easily checked that

$$\frac{0.00433}{\log p_{21}}\frac{(\sqrt{p_{21}}/2)^2}{2} = \frac{0.00433}{\log 73}\frac{(\sqrt{73}/2)^2}{2} > 0.0092$$

and

$$\frac{\sqrt{p_{20}\#}}{\log(p_{20}\#)} > 3.8353 \cdot 10^{11}.$$

Thus,

$$\frac{h_K}{2^\ell} > \frac{0.0092}{2^{19}} \cdot 3.8353 \cdot 10^{11} > 1.$$

Therefore, we obtain $h_K > 2^\ell$ and hence $h_K \ne 2^\ell$ in (71) for all $\ell \ge 1$.

The proof of Proposition 6 is complete. □

Appendix A: Proof of Lemma 6

For $T \geq T_0$, where $T_0 \geq 2$ is a sufficiently large but fixed positive number, we consider the following integral

$$\rho(T) = \int_{-1-\beta+iT}^{2-\beta+iT} f(s)ds$$

where the number $\beta \in (0,1)$ is fixed and the function $f(s)$ is defined by

$$f(s) = \frac{\zeta_K(s+\beta)y^s}{s\prod_{\ell=2}^{9}(s+\ell)} = \frac{\zeta(s+\beta)L(s+\beta,\chi)y^s}{s\prod_{\ell=2}^{9}(s+\ell)}$$

for a given number $y > 1$.

By using $s = \sigma + iT$ with $-1-\beta \leq \sigma \leq 2-\beta$, the complex integral $\rho(T)$ can be rewritten as

$$\rho(T) = \int_{-1-\beta}^{2-\beta} f(\sigma+iT)d\sigma.$$

With a change of variable, we obtain

$$\rho(T) = \int_{-1}^{2} f(\sigma-\beta+iT)d\sigma = \int_{-1}^{2} \frac{\zeta(\sigma+iT)L(\sigma+iT,\chi)y^{\sigma-\beta+iT}}{(\sigma-\beta+iT)\prod_{\ell=2}^{9}(\sigma-\beta+iT+\ell)}d\sigma.$$

We are going to prove that $\lim_{T\to\infty}|\rho(T)| = 0$ and hence $\lim_{T\to\infty}\rho(T) = 0$. It is clear that

$$|\rho(T)| \leq \int_{-1}^{0} |f(\sigma-\beta+iT)|d\sigma + \int_{0}^{1} |f(\sigma-\beta+iT)|d\sigma + \int_{1}^{2} |f(\sigma-\beta+iT)|d\sigma. \quad (72)$$

In the case that $0 \leq \sigma \leq 1$, we can use the properties of $\zeta(s)$ and $L(s,\chi)$, where $s = \sigma + iT$. Since $T \geq T_0$, we have (see [34, p. 142, Theorem 4])

$$|\zeta(\sigma+iT)| \leq C_1 T^{(1-\sigma)/2}\log T$$

for $0 \leq \sigma \leq 1$, where $C_1 > 0$ is an absolute constant. Moreover, since χ is a real primitive character of modulus $q \geq 3$, it is known that (see [34, p. 269, Theorem 4])

$$|L(\sigma+iT,\chi)| \leq C_2(qT)^{(1-\sigma)/2}\log(qT)$$

for $0 \leq \sigma \leq 1$, where $C_2 > 0$ is an absolute constant. Therefore,

$$\int_0^1 |f(\sigma-\beta+iT)|d\sigma = \int_0^1 \frac{|\zeta(\sigma+iT)||L(\sigma+iT,\chi)|y^{\sigma-\beta}}{|\sigma-\beta+iT|\prod_{\ell=2}^{9}|\sigma-\beta+iT+\ell|}d\sigma \leq C_3\frac{y^{1-\beta}}{T} \quad (73)$$

where $C_3 = C_3(q) > 0$ is a constant.

In the case that $1 \leq \sigma \leq 2$, we split it into two situations of $1 \leq \sigma \leq 3/2$ and $3/2 < \sigma \leq 2$. Applying the Phragmén–Lindelöf principle, Rademacher proved the following upper bound [35, p. 200]

$$|\zeta_K(\sigma + iT)| \leq 3\frac{|1+\sigma+iT|}{|1-\sigma-iT|}\left(\frac{|\Delta_K|}{4\pi^2}|1+\sigma+iT|^2\right)^{\frac{3/2-\sigma}{2}}\zeta(3/2)^2$$

for $1 \leq \sigma \leq 3/2$. On the other hand, we have

$$|\zeta_K(\sigma + iT)| \leq \zeta(\sigma)^2 \leq \zeta(3/2)^2$$

for $3/2 \leq \sigma \leq 2$. Therefore,

$$\int_1^2 |f(\sigma-\beta+iT)|d\sigma = \int_1^2 \frac{|\zeta_K(\sigma+iT)|y^{\sigma-\beta}}{|\sigma-\beta+iT|\prod_{\ell=2}^9|\sigma-\beta+iT+\ell|}d\sigma \leq C_4\frac{y^{2-\beta}}{T} \tag{74}$$

where $C_4 = C_4(q) > 0$ is a constant.

In the case that $-1 \leq \sigma \leq 0$, we apply the function equation (23) for $\zeta_K(s)$ to obtain

$$|\Gamma(1-\sigma-iT)||\zeta_K(1-\sigma-iT)| = \left(\frac{|\Delta_K|}{4\pi^2}\right)^{\sigma-1/2}|\Gamma(\sigma+iT)||\zeta_K(\sigma+iT)|.$$

Thus, we have

$$\begin{aligned}
&\int_{-1}^0 |f(\sigma-\beta+iT)|d\sigma \\
&= \int_{-1}^0 \frac{|\zeta_K(\sigma+iT)|y^{\sigma-\beta}}{|\sigma-\beta+iT|\prod_{\ell=2}^9|\sigma-\beta+iT+\ell|}d\sigma \\
&= \int_{-1}^0 \left(\frac{|\Delta_K|}{4\pi^2}\right)^{1/2-\sigma}\frac{|\Gamma(1-\sigma-iT)||\zeta_K(1-\sigma-iT)|y^{\sigma-\beta}}{|\Gamma(\sigma+iT)||\sigma-\beta+iT|\prod_{\ell=2}^9|\sigma-\beta+iT+\ell|}d\sigma \\
&= \int_1^2 \left(\frac{|\Delta_K|}{4\pi^2}\right)^{\sigma-1/2}\frac{|\Gamma(\sigma-iT)||\zeta_K(\sigma-iT)|y^{1-\sigma-\beta}}{|\Gamma(1-\sigma+iT)||1-\sigma-\beta+iT|\prod_{\ell=2}^9|1-\sigma-\beta+iT+\ell|}d\sigma \\
&\leq \left(\frac{|\Delta_K|}{4\pi^2}\right)^{3/2}\int_1^2 \frac{|\Gamma(\sigma-iT)||\zeta_K(\sigma-iT)|}{|\Gamma(1-\sigma+iT)||1-\sigma-\beta+iT|\prod_{\ell=2}^9|1-\sigma-\beta+iT+\ell|}d\sigma
\end{aligned}$$

Remind that we have Rademacher's upper bound

$$|\zeta_K(\sigma - iT)| \leq 3\frac{|1+\sigma-iT|}{|1-\sigma+iT|}\left(\frac{|\Delta_K|}{4\pi^2}|1+\sigma-iT|^2\right)^{\frac{3/2-\sigma}{2}}\zeta(3/2)^2$$

for $1 \leq \sigma \leq 3/2$ and the following bound

$$|\zeta_K(\sigma - iT)| \leq \zeta(\sigma)^2 \leq \zeta(3/2)^2$$

for $3/2 \leq \sigma \leq 2$.

By using Stirling's formula for the gamma function $\Gamma(s)$, we can obtain (see [34, p. 55])

$$|\Gamma(\sigma+it)| = \sqrt{2\pi}e^{-\frac{\pi}{2}|t|}|t|^{\sigma-1/2}(1+O(1/|t|))$$

for $|t| \geq 1$ and $-5 < \sigma < 5$ with an absolute implied constant. Thus, when $T \geq T_0$ with T_0 sufficiently large but fixed, there is

$$\frac{|\Gamma(\sigma-iT)|}{|\Gamma(1-\sigma+iT)|} = |T|^{2\sigma-1}(1+O(1/|T|)) \leq C_5|T|^3$$

for $1 \leq \sigma \leq 2$, where $C_5 > 0$ is an absolute constant.

Therefore, combing the given upper bounds, we get

$$\int_{-1}^{0} |f(\sigma-\beta+iT)|d\sigma \leq C_6\frac{1}{T} \tag{75}$$

for $T \geq T_0$, where $C_6 = C_6(q) > 0$ is a constant.

Noting (73), (74) and (75), it follows from (72) that

$$|\rho(T)| \leq C_3\frac{y^{1-\beta}}{T} + C_4\frac{y^{2-\beta}}{T} + C_6\frac{1}{T}$$

for $T \geq T_0$, which implies $|\rho(T)| \to 0$ as $T \to \infty$. In a similar fashion, it can be shown that the following integral

$$\int_{-1-\beta-iT}^{2-\beta-iT} f(s)ds \to 0$$

when $T \to \infty$. The proof of Lemma 6 is complete. □

Appendix B: Proof of Lemma 7

In this section, we are going to demonstrate that the matrix $\mathcal{M}$ given in Section 6 has full column rank.

Remind that the matrix $\mathcal{M}$ is of size $T \times W^4$, where W is a positive integer with $W \geq q > 3 \cdot 10^{20}$ and $T = (T_1+1)(T_2+1)(T_3+1)$ with

$$H = 10^6, \;\; U = W^{4/3}, \;\; T_1 = \lceil 8H^{2/3}U \rceil, \;\; T_2 = T_2 = \lceil 8H^{-1/3}U \rceil.$$

It is clear that the matrix $\mathcal{M}$ has more rows than columns due to the following

$$T \geq 8H^{2/3}U(8H^{-1/3}U)^2 = 512U^3 = 512W^4 > W^4.$$

We have $T_j \geq 8H^{-1/3}U = 8(W/H)^{1/3}W > 10^5 W > 3(W-1)$ for $j = 1, 2, 3$ and

$$\prod_{j=1}^{3}[T_j - 3(W-1) + 1] > \prod_{j=1}^{3}(T_j + 1 - 3W) > T - 6W(T_1T_2 + T_2T_3 + T_3T_1)$$

and hence, from $T_1 > T_2 = T_3$,

$$\prod_{j=1}^{3}[T_j - 3(W-1) + 1] > T - 6W(3T_1T_2) > T - (18/10^5)T_1T_2T_3 > 0.99T > 500W^4.$$

We put $b_j = T_j - 3(W-1) \geq 1$ for $j = 1, 2, 3$, which satisfies

$$\prod_{j=1}^{3}(b_j + 1) > 500W^4 > (4W-3)^4.$$

We define the following subset of column indices

$$E_W = \{\vec{n} = (n_1, n_2, n_3, n_4)^\top \mid 0 \leq n_i \leq W-1 \text{ for } i = 1, 2, 3, 4\} \subset \mathbb{Z}^4.$$

We denote $\vec{0} = (0, 0, 0, 0)^\top \in E_W$ as the index of the first column in the matrix $\mathcal{M}$.

The row indices are $\alpha = (\alpha_1, \alpha_2, \alpha_3) \in \mathbb{Z}^3$ with $0 \leq \alpha_j \leq T_j$ for $j = 1, 2, 3$. Both row and column indices are, respectively, arranged in a lexicographical order, namely, the alphabetical order.

The entry of the matrix $\mathcal{M}$ at row $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ and column $\vec{n} \in E_W$ is given by

$$\mathcal{M}_{\alpha,\vec{n}} = \theta_{\vec{n}}^{\alpha_1}\sigma(\theta_{\vec{n}})^{\alpha_2}\sigma\tau(\theta_{\vec{n}})^{\alpha_3} \tag{76}$$

with

$$\theta_{\vec{n}} = n_1 + n_2 a + n_3 b + n_4 ab \in \mathcal{R} = \mathbb{Z}[a, b].$$

Remind that $a = \sqrt{-N}$ and $b = \sqrt{2}$. It is agreed that for $\vec{n} = \vec{0}$ with $\theta_{\vec{0}} = 0$, $\mathcal{M}_{\alpha,\vec{n}}$ is defined as 1 for $\alpha = (0, 0, 0)$ and 0 for $\alpha \neq (0, 0, 0)$. We can see that every entry $\mathcal{M}_{\alpha,\vec{n}}$ of the matrix $\mathcal{M}$ is an algebraic integer in $\mathcal{R} \subset O_L$.

Let R_α denote the W^4-dimensional row vector of $\mathcal{M}$ with row index α and $C_{\vec{n}}$ the T-dimensional column vector of $\mathcal{M}$ with column index $\vec{n} \in E_W$. It is clear that the first row $R_{(0,0,0)}$ in $\mathcal{M}$ is an all-one vector and the first column $C_{\vec{0}}$ in $\mathcal{M}$ is a standard unit vector with 1 in the first position.

On the contrary, we assume that the matrix $\mathcal{M}$ does not have full column rank.

As a consequence, all the column vectors $C_{\vec{n}}$, $\vec{n} \in E_W$, of the matrix $\mathcal{M}$ must be linearly dependent in the number field L. Thus, there exist numbers $v_{\vec{n}} \in L$, not all zeros, such that

$$\sum_{\vec{n} \in E_W} v_{\vec{n}} C_{\vec{n}} = \mathbf{0} \in L^T \tag{77}$$

where $\mathbf{0} \in L^T$ is the zero vector. We define the support subset

$$\mathcal{S} = \{\vec{n} \in E_W \mid v_{\vec{n}} \neq 0\} \subseteq E_W \subset \mathbb{Z}^4 \tag{78}$$

which has the cardinality $\#\mathcal{S} \geq 2$, since every column vector of $\mathcal{M}$ is a nonzero vector with 1 in the first position.

By noticing (76), we see from (77) that, for every row index $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ of the matrix $\mathcal{M}$,

$$\sum_{\vec{n} \in \mathcal{S}} v_{\vec{n}} \theta_{\vec{n}}^{\alpha_1} \sigma(\theta_{\vec{n}})^{\alpha_2} \sigma\tau(\theta_{\vec{n}})^{\alpha_3} = 0.$$

Therefore, we have

$$0 = \sum_{\alpha} c_\alpha \sum_{\vec{n} \in E_W} v_{\vec{n}} \theta_{\vec{n}}^{\alpha_1} \sigma(\theta_{\vec{n}})^{\alpha_2} \sigma\tau(\theta_{\vec{n}})^{\alpha_3} = \sum_{\vec{n} \in E_W} v_{\vec{n}} \sum_{\alpha} c_\alpha \theta_{\vec{n}}^{\alpha_1} \sigma(\theta_{\vec{n}})^{\alpha_2} \sigma\tau(\theta_{\vec{n}})^{\alpha_3} \tag{79}$$

where the summation $\sum_\alpha$ runs over the row indices α of $\mathcal{M}$ and $c_\alpha \in \mathbb{C}$ are arbitrarily given complex numbers. Put the 3×4 matrix

$$A = \begin{pmatrix} 1 & a & b & ab \\ 1 & -a & b & -ab \\ 1 & -a & -b & ab \end{pmatrix} \tag{80}$$

we get the following equality, for $\vec{n} \in E_W \subset \mathbb{Z}^4$,

$$A\vec{n} = (\theta_{\vec{n}}, \sigma(\theta_{\vec{n}}), \sigma\tau(\theta_{\vec{n}}))^\top \in \mathcal{R}^3.$$

We introduce the following arbitrary 3-variate polynomial arising from (79)

$$B(z_1, z_2, z_3) = \sum_{\alpha} c_\alpha z_1^{\alpha_1} z_2^{\alpha_2} z_3^{\alpha_3} = \sum_{\alpha_1=0}^{T_1} \sum_{\alpha_2=0}^{T_2} \sum_{\alpha_3=0}^{T_3} c_{(\alpha_1,\alpha_2,\alpha_3)} z_1^{\alpha_1} z_2^{\alpha_2} z_3^{\alpha_3} \tag{81}$$

with complex variables z_1, z_2 and z_3. It is defined that $z_j^0 = 1$ for $j = 1, 2, 3$ in the ring of polynomials $\mathbb{C}[z_1, z_2, z_3]$. We call $B(z_1, z_2, z_3)$ as a zero polynomial if all coefficients c_α's are equal to zero. We have, from (79), that

$$\sum_{\vec{n} \in E_W} v_{\vec{n}} B(A\vec{n}) = \sum_{\vec{n} \in \mathcal{S}} v_{\vec{n}} B(A\vec{n}) = 0$$

for every *nonzero* polynomial $B(z_1, z_2, z_3)$ with complex variables z_1, z_2 and z_3, given in (81), where $\sum_\alpha$ is a summation over the row indices $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ of the matrix $\mathcal{M}$.

In the following, we will construct a *nonzero* polynomial

$$\hat{B}(z_1, z_2, z_3) = \sum_{\alpha_1=0}^{T_1} \sum_{\alpha_2=0}^{T_2} \sum_{\alpha_3=0}^{T_3} \hat{c}_{(\alpha_1,\alpha_2,\alpha_3)} z_1^{\alpha_1} z_2^{\alpha_2} z_3^{\alpha_3}$$

with complex variables z_1, z_2 and z_3, whose coefficients $\hat{c}_{(\alpha_1,\alpha_2,\alpha_3)}$'s are not all zeros, such that

$$\sum_{\vec{n}\in\mathcal{S}} v_{\vec{n}} \hat{B}(A\vec{n}) \neq 0, \tag{82}$$

which gives a *contradiction*. As a result, the matrix $\mathcal{M}$ must have full column rank.

We define

$$\mathcal{P} = \mathrm{conv}(\mathcal{S}) \subset [0, W-1]^4 \subset \mathbb{R}^4 \text{ and } \mathcal{K} = 4\mathcal{P}.$$

Remind that $b_j = T_j - 3(W-1) \geq 1$ for $j = 1, 2, 3$. It is seen that

$$\mathcal{K} \subset [0, 4(W-1)]^4 \subset \mathbb{R}^4 \text{ and } \#(\mathcal{K} \cap \mathbb{Z}^4) \leq (4W-3)^4 < \prod_{j=1}^{3}(b_j+1).$$

Therefore, there exists a *nonzero* 3-variate polynomial

$$R(z_1, z_2, z_3) = \sum_{\alpha_1=0}^{b_1} \sum_{\alpha_2=0}^{b_2} \sum_{\alpha_3=0}^{b_3} \hat{r}_{(\alpha_1,\alpha_2,\alpha_3)} z_1^{\alpha_1} z_2^{\alpha_2} z_3^{\alpha_3} \tag{83}$$

with complex variables z_1, z_2 and z_3 and $\hat{r}_{(\alpha_1,\alpha_2,\alpha_3)} \in \mathbb{C}$ such that

$$R(A\vec{k}) = 0 \text{ for all } \vec{k} \in \mathcal{K} \cap \mathbb{Z}^4 \tag{84}$$

since $A\vec{k} \in \mathbb{C}^3$ and $\#\{A\vec{k} \mid \vec{k} \in \mathcal{K} \cap \mathbb{Z}^4\} \leq \#(\mathcal{K} \cap \mathbb{Z}^4)$.

The 3×4 matrix A given by (80) has full row rank. Thus, for any vector $z \in \mathbb{C}^3$, there is a vector $x \in \mathbb{C}^4$ such that $Ax = z$. As a consequence, the 4-variate polynomial $R(Ax)$ with complex variables $x = (x_1, x_2, x_3, x_4)^\top$ is *nonzero*.

By using the fundamental theorem of algebra and the method of mathematical induction, we can readily prove that the nonzero 4-variate polynomial $R(Ax)$ cannot vanish on the entire integer lattice $\mathbb{Z}^4$. Noting (84), we see that there exists an $\vec{m} \in \mathbb{Z}^4$ but $\vec{m} \notin \mathcal{K}$ such that $R(A\vec{m}) \neq 0$.

It is clear that $\mathcal{K}$ is a nonempty, closed and convex subset of $\mathbb{R}^4$. The projection of a point $\vec{m} \in \mathbb{R}^4$ onto the set $\mathcal{K}$, denoted by $\mathrm{Proj}_{\mathcal{K}}(\vec{m})$, is defined as the solution (which must exist and be unique) to the mathematical program of $\min_{x\in\mathcal{K}} \|\vec{m} - x\|$, where $\|x\| = \sqrt{x^\top x}$ denotes the Euclidean norm or 2-norm of the column vector $x \in \mathbb{R}^4$. Moreover, we denote the distance between the point $\vec{m}$ and the closed convex subset $\mathcal{K}$ by $\mathrm{dist}(\vec{m}, \mathcal{K}) = \min_{x\in\mathcal{K}} \|\vec{m} - x\| = \|\vec{m} - \mathrm{Proj}_{\mathcal{K}}(\vec{m})\|$. For $x \in \mathbb{R}^4$ and $y \in \mathbb{R}^4$, the inner product of x and y is given by

$$\langle x, y \rangle = x^\top y$$

which implies that $\langle x, y \rangle = \langle y, x \rangle$ and $\langle x, x \rangle = \|x\|^2$. The projection operator $\mathrm{Proj}_{\mathcal{K}}(\cdot)$ has the following property (see, e.g., [25, Lemma 1]). If $x \in \mathcal{K}$, then, for any $\vec{m} \in \mathbb{R}^4$,

$$\langle \vec{m} - \mathrm{Proj}_{\mathcal{K}}(\vec{m}), x - \mathrm{Proj}_{\mathcal{K}}(\vec{m}) \rangle \leq 0.$$

We can choose a specific element from the set of all $\vec{m} \in \mathbb{Z}^4 \setminus \mathcal{K}$ satisfying

$$R(A\vec{m}) \neq 0$$

which has the *shortest* distance $\text{dist}(\vec{m}, \mathcal{K})$ from $\mathcal{K}$, which is still denoted by $\vec{m} \in \mathbb{Z}^4$. We define two points $\vec{p} \in \mathbb{R}^4$ and $\vec{h} \in \mathbb{R}^4$ as follows

$$\vec{p} = \text{Proj}_{\mathcal{K}}(\vec{m}) \text{ and } \vec{h} = \vec{m} - \vec{p} \tag{85}$$

which has the property that, for all $x \in \mathcal{K} = 4\mathcal{P} \subset \mathbb{R}^4$,

$$\langle \vec{h}, x - \vec{p} \rangle = \langle \vec{m} - \vec{p}, x - \vec{p} \rangle \leq 0.$$

For all $\vec{v} \in \mathcal{P} \subset \mathbb{R}^4$, we have $4\vec{v} \in \mathcal{K} = 4\mathcal{P}$ and therefore $\langle \vec{h}, 4\vec{v} - \vec{p} \rangle \leq 0$. Hence,

$$\langle \vec{h}, \vec{v} \rangle \leq \langle \vec{h}, \vec{p}/4 \rangle \tag{86}$$

where $\vec{p}/4 \in \mathcal{P}$ due to $\vec{p} \in \mathcal{K}$. We introduce the following supporting face

$$\mathcal{G} = \{\vec{v} \in \mathcal{P} \mid \langle \vec{h}, \vec{v} \rangle = \max_{\vec{w} \in \mathcal{P}} \langle \vec{h}, \vec{w} \rangle\} \subset \mathbb{R}^4 \tag{87}$$

which has dimensions *at most three*. It is clear from (86) that $\vec{p}/4 \in \mathcal{G}$.

According to Carathéodory's convexity theorem [4], if the convex hull of a set of points has ℓ dimensions, then any point in the convex hull can be written as a convex combination of at most $\ell + 1$ vertices.

Since $\vec{p}/4 \in \mathcal{P} \subset \mathbb{R}^4$, there exist k vertices $\vec{v}_1, \cdots, \vec{v}_k \in \mathcal{S} \subset \mathcal{P} = \text{conv}(\mathcal{S})$ with $1 \leq k \leq 5$ such that

$$\vec{p}/4 = \sum_{\ell=1}^{k} \lambda_\ell \vec{v}_\ell$$

where $\lambda_\ell > 0$ for $1 \leq \ell \leq k$ and $\sum_{\ell=1}^{k} \lambda_\ell = 1$. We can prove that it is enough for k to be at most four. In fact, if $k = 5$, then, by using (86),

$$\langle \vec{h}, \vec{p}/4 \rangle = \left\langle \vec{h}, \sum_{\ell=1}^{5} \lambda_\ell \vec{v}_\ell \right\rangle = \sum_{\ell=1}^{5} \lambda_\ell \langle \vec{h}, \vec{v}_\ell \rangle \leq \sum_{\ell=1}^{5} \lambda_\ell \langle \vec{h}, \vec{p}/4 \rangle = \langle \vec{h}, \vec{p}/4 \rangle$$

which implies that, for $1 \leq \ell \leq 5$,

$$\langle \vec{h}, \vec{v}_\ell \rangle = \langle \vec{h}, \vec{p}/4 \rangle.$$

Therefore, by (87), we have $\vec{v}_\ell \in \mathcal{G}$ for $1 \leq \ell \leq 5$. It follows that

$$\vec{p}/4 \in \text{conv}(\{\vec{v}_1, \vec{v}_2, \vec{v}_3, \vec{v}_4, \vec{v}_5\}) \subset \mathcal{G}$$

which has dimensions at most three. By using Carathéodory's theorem again, $\vec{p}/4$ can be written as a convex combination of at most four vertices in $\{\vec{v}_1, \vec{v}_2, \vec{v}_3, \vec{v}_4, \vec{v}_5\}$. Therefore, combining the above results, there exist k vertices $\vec{u}_1, \cdots, \vec{u}_k \in \mathcal{S} \cap \mathcal{G}$ with $1 \leq k \leq 4$ such that

$$\vec{p}/4 = \sum_{\ell=1}^{k} \lambda_\ell \vec{u}_\ell$$

where $\lambda_1 \geq \cdots \geq \lambda_k > 0$ and $\sum_{\ell=1}^{k} \lambda_\ell = 1$. Thus, there must be $\lambda_1 \geq 1/4$. We define the point

$$\vec{u} = \vec{u}_1 \in \mathcal{S} \cap \mathcal{G} \tag{88}$$

which has the property of

$$\vec{p} - \vec{u} = 4 \sum_{\ell=1}^{k} \lambda_\ell \vec{u}_\ell - \vec{u} = (4\lambda_1 - 1)\vec{u}_1 + \sum_{\ell=2}^{k} 4\lambda_\ell \vec{u}_\ell \in 3\mathcal{P}.$$

In the case that $\mathcal{S} \setminus \mathcal{G} \neq \emptyset$, for every $\vec{n} \in \mathcal{S} \setminus \mathcal{G} \subset \mathcal{P}$, by noting (87) we have

$$\langle \vec{h}, \vec{u} - \vec{n} \rangle = \langle \vec{h}, \vec{u} \rangle - \langle \vec{h}, \vec{n} \rangle > 0.$$

We define two points $\vec{p}_1$ and $\vec{m}_1$ by

$$\vec{p}_1 = \vec{p} - \vec{u} + \vec{n} \in \mathcal{K} = 4\mathcal{P} \text{ and } \vec{m}_1 = \vec{m} - \vec{u} + \vec{n} \in \mathbb{Z}^4.$$

It is clear that $\vec{m}_1 = \vec{p}_1 + \vec{h}$, where $\vec{h} = \vec{m} - \vec{p} = \vec{m} - \mathrm{Proj}_{\mathcal{K}}(\vec{m})$. For any $0 < \tau < 1$, we have $\tau\vec{p} + (1-\tau)\vec{p}_1 \in \mathcal{K}$ and

$$\|\vec{m}_1 - [\tau\vec{p} + (1-\tau)\vec{p}_1]\|^2 = \|\vec{h} - \tau(\vec{u} - \vec{n})]\|^2 = \|\vec{h}\|^2 - 2\tau\langle \vec{h}, \vec{u} - \vec{n} \rangle + \tau^2 \|\vec{u} - \vec{n}\|^2.$$

Let $\eta = 2\langle \vec{h}, \vec{u} - \vec{n} \rangle / \|\vec{u} - \vec{n}\|^2 > 0$. Then, for any $0 < \tau < \min\{1, \eta\}$, we get

$$(\mathrm{dist}(\vec{m}_1, \mathcal{K}))^2 \leq \|\vec{m}_1 - [\tau\vec{p} + (1-\tau)\vec{p}_1]\|^2 < \|\vec{h}\|^2.$$

Hence, $\mathrm{dist}(\vec{m}_1, \mathcal{K}) < \|\vec{h}\| = \|\vec{m} - \mathrm{Proj}_{\mathcal{K}}(\vec{m})\| = \mathrm{dist}(\vec{m}, \mathcal{K})$. According to the property of the chosen point $\vec{m}$, we obtain

$$R(A\vec{n} + A(\vec{m} - \vec{u})) = R(A\vec{m}_1) = 0 \text{ for } \vec{n} \in \mathcal{S} \setminus \mathcal{G}. \tag{89}$$

Remind that $\#\mathcal{S} \geq 2$ and the point $\vec{u} \in \mathcal{S} \cap \mathcal{G}$. It is clear that

$$\mathcal{S} = (\mathcal{S} \cap \mathcal{G}) \cup (\mathcal{S} \setminus \mathcal{G}).$$

In the case that $\#(\mathcal{S} \cap \mathcal{G}) \geq 2$, there exists at least one $\vec{n} \in \mathcal{S} \cap \mathcal{G}$ with $\vec{n} \neq \vec{0}$. Every $\vec{n} \in \mathcal{S} \cap \mathcal{G} \subset \mathbb{Z}^4$ locates in the affine space $\mathcal{G} \subset \mathbb{R}^4$ of dimensions at most three.

By using Gaussian elimination, the data-fitting linear equations arising from the integer coordinates of all $\vec{n} \in \mathcal{S} \cap \mathcal{G}$ can be solved in the rational field $\mathbb{Q}$ via *exact* arithmetic. Therefore, we can find four rational numbers $\widetilde{r}_1$, $\widetilde{r}_2$, $\widetilde{r}_3$ and $\widetilde{r}_4$, which are not all zeros, and the fifth number $\widetilde{k} \in \mathbb{Q}$ such that every $\vec{n} = (n_1, n_2, n_3, n_4)^\top \in \mathcal{S} \cap \mathcal{G}$ satisfies the following affine equation

$$\widetilde{r}_1 n_1 + \widetilde{r}_2 n_2 + \widetilde{r}_3 n_3 + \widetilde{r}_4 n_4 = \widetilde{k}.$$

Multiplying both sides of the equation by the largest denominator of the nonzero numbers in $\{\widetilde{r}_1, \widetilde{r}_2, \widetilde{r}_3, \widetilde{r}_4, \widetilde{k}\} \subset \mathbb{Q}$, the above equation is equivalent to

$$r_1 n_1 + r_2 n_2 + r_3 n_3 + r_4 n_4 = k$$

where $r_1, r_2, r_3, r_4, k \in \mathbb{Z}$ with $r_1^2 + r_2^2 + r_3^2 + r_4^2 > 0$. We can define the following affine hyperplane

$$\mathcal{H}_x = \{x \in \mathbb{C}^4 \mid r_1 x_1 + r_2 x_2 + r_3 x_3 + r_4 x_4 = k\} \tag{90}$$

where $x = (x_1, x_2, x_3, x_4)^\top$ is a column vector. Therefore,

$$\mathcal{S} \cap \mathcal{G} \subset \mathcal{H}_x.$$

The 3×4 matrix A given by (80) has the following four 3×3 submatrices by deleting one of the four columns of the matrix

$$\begin{pmatrix} a & b & ab \\ -a & b & -ab \\ -a & -b & ab \end{pmatrix}, \begin{pmatrix} 1 & b & ab \\ 1 & b & -ab \\ 1 & -b & ab \end{pmatrix}, \begin{pmatrix} 1 & a & ab \\ 1 & -a & -ab \\ 1 & -a & ab \end{pmatrix} \text{ and } \begin{pmatrix} 1 & a & b \\ 1 & -a & b \\ 1 & -a & -b \end{pmatrix}$$

which have *nonzero* determinants of $4a^2b^2$, $-4ab^2$, $-4a^2b$ and $4ab$, respectively. Without loss of generality, we can assume that

$$r_4 \neq 0$$

and will work with the fourth 3×3 submatrix. Note that if $r_4 = 0$ but $r_j \neq 0$ for some $j \in \{1, 2, 3\}$, we can work with the jth 3×3 submatrix in a similar fashion.

We introduce the following matrix and its inverse

$$\Gamma = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline r_1 & r_2 & r_3 & r_4 \end{array}\right) \text{ and } \Gamma^{-1} = \left(\begin{array}{ccc|c} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \hline -r_1/r_4 & -r_2/r_4 & -r_3/r_4 & 1/r_4 \end{array}\right). \tag{91}$$

Then, under the invertible linear transformation of $y = \Gamma x$, the image of the affine hyperplane $\mathcal{H}_x$ given by (90) becomes the following affine hyperplane

$$\mathcal{H}_y = \{y \in \mathbb{C}^4 \mid y_4 = k\} \tag{92}$$

where $y = (y_1, y_2, y_3, y_4)^\top$ is a column vector. We can define the following linear transformation

$$z = A\Gamma^{-1}y$$

where $z = (z_1, z_2, z_3)^\top$ is a column vector and $A\Gamma^{-1}$ is a 3×4 matrix with full row rank.

It can be computed that

$$z = C(y_1, y_2, y_3)^\top + \frac{k}{r_4}(ab, -ab, ab)^\top$$

where C is a 3×3 matrix given by

$$C = \begin{pmatrix} 1 & a & b \\ 1 & -a & b \\ 1 & -a & -b \end{pmatrix} + \begin{pmatrix} ab \\ -ab \\ ab \end{pmatrix} (-r_1/r_4, -r_2/r_4, -r_3/r_4).$$

It is easily calculated that

$$1 + (-r_1/r_4, -r_2/r_4, -r_3/r_4) \begin{pmatrix} 1 & a & b \\ 1 & -a & b \\ 1 & -a & -b \end{pmatrix}^{-1} \begin{pmatrix} ab \\ -ab \\ ab \end{pmatrix} = 1 + \frac{r_3}{r_4}a - \frac{r_2}{r_4}b - \frac{r_1}{r_4}ab$$

which must be *nonzero* since $\{1, a, b, ab\}$ is the $\mathbb{Q}$-basis of the extension $L/\mathbb{Q}$ of degree $[L : \mathbb{Q}] = 4$. By using the Sherman–Morrison formula [38], we see that the 3×3 matrix C is invertible and its inverse C^{-1} can be given explicitly. Therefore, we obtain

$$(y_1, y_2, y_3)^\top = C^{-1}(z_1, z_2, z_3)^\top - \frac{k}{r_4}C^{-1}(ab, -ab, ab)^\top.$$

Hence, we can define the following three linear polynomials

$$L_j(z) = y_j = c_{j1}z_1 + c_{j2}z_2 + c_{j3}z_3 + d_j \text{ for } j = 1, 2, 3 \tag{93}$$

where the numbers $c_{j1}, c_{j2}, c_{j3}, d_j \in L$ for $j = 1, 2, 3$.

It is clear that the invertible linear transformation $y = \Gamma x$ implies that $y_j = x_j$ for $j = 1, 2, 3$ and that $z = A\Gamma^{-1}y = Ax$. By (93), the linear polynomials $L_j(z)$'s have the property that for all $x = (x_1, x_2, x_3, x_4)^\top \in \mathcal{H}_x$,

$$L_j(Ax) = L_j(z) = y_j = x_j \text{ for } j = 1, 2, 3.$$

In particular, every $\vec{n} = (n_1, n_2, n_3, n_4)^\top \in \mathcal{S} \cap \mathcal{G} \subset \mathcal{H}_x$ satisfies

$$L_j(A\vec{n}) = n_j \text{ for } j = 1, 2, 3.$$

Remind that $\vec{u} = (u_1, u_2, u_3, u_4)^\top \in \mathcal{S} \cap \mathcal{G} \subset \mathcal{H}_x$ is given by (88). If $\vec{n} \in \mathcal{S} \cap \mathcal{G}$ but $\vec{n} \neq \vec{u}$, then

$$(n_1, n_2, n_3) \neq (u_1, u_2, u_3).$$

Otherwise, by using (90) and $r_4 \neq 0$, we have $n_4 = u_4$ and hence $\vec{n} = \vec{u}$.

We set the Lagrange-type interpolating polynomial of z_1, z_2 and z_3 as follows

$$Q(z) = \prod_{\substack{1 \leq j \leq 4 \\ j \neq 4}} \prod_{\substack{0 \leq a \leq W-1 \\ a \neq u_j}} \frac{L_j(z) - a}{u_j - a}$$

where $\vec{u} = (u_1, u_2, u_3, u_4)^\top \in \mathcal{S} \cap \mathcal{G} \subset E_W$. It is clear that $Q(z)$ is a *nonzero* 3-variate polynomial of total degree at most $3(W-1)$ and it has the following property

$$Q(A\vec{n}) = \begin{cases} 1, & \text{if } \vec{n} = \vec{u}, \\ 0, & \text{if } \vec{n} \in \mathcal{S} \cap \mathcal{G} \text{ but } \vec{n} \neq \vec{u}. \end{cases} \tag{94}$$

It is now ready to construct a *nonzero* polynomial $\hat{B}(z) = \hat{B}(z_1, z_2, z_3)$ as follows. We note that $\#(\mathcal{S} \cap \mathcal{G}) + \#(\mathcal{S} \setminus \mathcal{G}) = \#\mathcal{S} \geq 2$ and the specific point $\vec{u} \in \mathcal{S} \cap \mathcal{G}$.

If $\mathcal{S} \setminus \mathcal{G} = \emptyset$, then $\#(\mathcal{S} \cap \mathcal{G}) = \#\mathcal{S} \geq 2$. We can set $\hat{B}(z) = Q(z)$, which satisfies

$$\sum_{\vec{n} \in \mathcal{S}} v_{\vec{n}} \hat{B}(A\vec{n}) = \sum_{\vec{n} \in \mathcal{S} \cap \mathcal{G}} v_{\vec{n}} Q(A\vec{n}) = v_{\vec{u}} Q(A\vec{u}) = v_{\vec{u}} \neq 0.$$

If $\mathcal{S} \setminus \mathcal{G} \neq \emptyset$ and $\mathcal{S} \cap \mathcal{G} = \{\vec{u}\}$, we can set $\hat{B}(z) = R(z + A(\vec{m} - \vec{u}))$. It is clear that

$$\sum_{\vec{n} \in \mathcal{S}} v_{\vec{n}} \hat{B}(A\vec{n}) = \sum_{\vec{n} \in \mathcal{S} \setminus \mathcal{G}} v_{\vec{n}} \hat{B}(A\vec{n}) + v_{\vec{u}} \hat{B}(A\vec{u}) = \sum_{\vec{n} \in \mathcal{S} \setminus \mathcal{G}} v_{\vec{n}} R(A\vec{m}_1) + v_{\vec{u}} R(A\vec{m})$$

where $\vec{m}_1 = \vec{n} + \vec{m} - \vec{u} \in \mathbb{Z}^4$. Hence, from (89),

$$\sum_{\vec{n} \in \mathcal{S}} v_{\vec{n}} \hat{B}(A\vec{n}) = v_{\vec{u}} R(A\vec{m}) \neq 0.$$

If $\mathcal{S} \setminus \mathcal{G} \neq \emptyset$ and $\#(\mathcal{S} \cap \mathcal{G}) \geq 2$, we set $\hat{B}(z) = R(z + A(\vec{m} - \vec{u}))Q(z)$. Then, we have

$$\sum_{\vec{n} \in \mathcal{S}} v_{\vec{n}} \hat{B}(A\vec{n}) = \sum_{\vec{n} \in \mathcal{S} \setminus \mathcal{G}} v_{\vec{n}} R(A\vec{m}_1) Q(A\vec{n}) + \sum_{\vec{n} \in \mathcal{S} \cap \mathcal{G}} v_{\vec{n}} R(A\vec{m}_1) Q(A\vec{n})$$

where $\vec{m}_1 = \vec{n} + \vec{m} - \vec{u} \in \mathbb{Z}^4$. By using (89) and (94), we obtain

$$\sum_{\vec{n} \in \mathcal{S}} v_{\vec{n}} \hat{B}(A\vec{n}) = \sum_{\vec{n} \in \mathcal{S} \cap \mathcal{G}} v_{\vec{n}} R(A\vec{m}_1) Q(A\vec{n}) = v_{\vec{u}} R(A\vec{m}) Q(A\vec{u}) = v_{\vec{u}} R(A\vec{m}) \neq 0.$$

Therefore, we find a *nonzero* polynomial of three complex variables z_1, z_2 and z_3

$$\begin{aligned}
&\hat{B}(z_1, z_2, z_3) \\
&= Q(z)R(z - A(\vec{u} - \vec{m})) \\
&= Q(z) \sum_{\alpha_1=0}^{b_1} \sum_{\alpha_2=0}^{b_2} \sum_{\alpha_3=0}^{b_3} \hat{r}_{(\alpha_1,\alpha_2,\alpha_3)} (z_1 - s_1)^{\alpha_1} (z_2 - s_2)^{\alpha_2} (z_3 - s_3)^{\alpha_3} \\
&= \sum_{\alpha_1=0}^{T_1} \sum_{\alpha_2=0}^{T_2} \sum_{\alpha_3=0}^{T_3} \hat{c}_{(\alpha_1,\alpha_2,\alpha_3)} z_1^{\alpha_1} z_2^{\alpha_2} z_3^{\alpha_3}
\end{aligned}$$

with the shift $A(\vec{u} - \vec{m}) = (s_1, s_2, s_3)^\top$, which satisfies

$$\sum_{\vec{n} \in \mathcal{S}} v_{\vec{n}} \hat{B}(A\vec{n}) \neq 0.$$

Thus, the proof of Lemma 7 is complete. □

References

[1] G. E. Andrews, The fifth and seventh order mock theta functions, *Trans. Amer. Math. Soc.*, **293** no. 1 (1986), 113–134.

[2] T. M. Apostol, *Introduction to Analytic Number Theory*, New York, NY: Springer, 1976.

[3] P. T. Bateman, On the representations of a number as the sum of three squares, *Transactions of the American Mathematical Society*, **71** no. 1 (1951), 70–101.

[4] C. Carathéodory Über den variabilitätsbereich der fourier'schen konstanten von positiven harmonischen funktionen, *Rendiconti del Circolo Matematico di Palermo*, **32** (1911), 193–217.

[5] H. Cohen, *Number Theory Volume I: Tools and Diophantine Equations*, Graduate Texts in Math. 239, New York, NY: Springer, 2007.

[6] K. Conrad, Ostrowski's theorem for number fields, *Expository Papers*, Online available: https://kconrad.math.uconn.edu/blurbs

[7] J. B. Conrey and K. Soundararajan, Real zeros of quadratic Dirichlet L-functions, *Invent. Math.*, **150** no. 1 (2002), 1–44.

[8] R. E. Crandall, New representations for the Madelung constant, *Exp. Math.*, **8** (1999), 367–379.

[9] H. Davenport, *Multiplicative Number Theory*, 2nd Edition, Graduate Texts in Math. 74, New York, NY: Springer, 1980.

[10] A. S. Elsenhans, J. Klüners, and F. Nicolae, Imaginary quadratic number fields with class groups of small exponent, *Acta Arith.*, **193** no. 3 (2020), 217–233.

[11] L. Euler, De formulis speciei $mxx + nyy$ ad numeros primos explorandos idoneis earumque mirabilibus proprietatibus (Presented 16 March 1778), *Nova acta acad. scien. Petropolitonae* **12** (1794), 1801, 22–46 = Leonhardi Euleri Opera Omnia I, **4** (1916), 269–289.

[12] G. Frei, Leonhard Euler's convenient numbers, *Math. Intell.*, **7** no. 3 (1985), 55–58, 64.

[13] J. B. Friedlander and H. Iwaniec, A note on Dirichlet L-functions, *Expo. Math.*, **36** (2018), 343–350.

[14] C. F. Gauss, *Disquisitiones Arithmeticae*, Translated by A. A. Clarke, 1966. New York, NY: Springer-Verlag, 1986.

[15] E. Grosswald, *Representations of Integers as Sums of Squares*, New York, NY: Springer, 1985.

[16] F. Grube, Ueber einige Euler'sche S̈atze aus der Theorie der quadratischen Formen, *Zeitschrift Math. Physik*, **19** (1874), 492–519.

[17] G. H. Hardy and J. E. Littlewood, Some problems of "partitio numerorum" (V): A further contribution to the study of Goldbach's problem, *Proceedings of the London Mathematical Society*, **s2–22** (1924), 46–56.

[18] E. Hecke, in the paper by E. Landau, Über die Klassenzahl imaginärquadratischer Zahlkörper, *Göttinger Nachrichlen*, **1918** (1918), 285–295.

[19] J. Hoffstein, On the Siegel–Tatuzawa theorem, *Acta Arith.*, **38** (1980), 167–174.

[20] T. W. Hungerford, *Algebra*, Graduate Texts in Math. 73, New York, NY: Springer, 1974.

[21] A. E. Ingham, *The Distribution of Prime Numbers*, Cambridge, U.K., 1934.

[22] E. Kani, Idoneal numbers and some generalizations, *Ann. Sci. Math. Québec*, **35** no. 2 (2011), 197–227.

[23] H. W. Lenstra, Codes from algebraic number fields, in M. Hazewinkel, J. K. Lenstra, and L. G. L. T. Meertens (eds), *Mathematics and Computer Science II, Fundamental Contributions in the Netherlands since 1945*, CWI Monograph 4, Amsterdam, Netherlands: North-Holland, 1986, pp. 95–104.

[24] X. B. Liang, The q-ary Gilbert–Varshamov bound can be improved for all but finitely many positive integers q, arXiv:2403.08727, March 2024.

[25] X. B. Liang, A recurrent neural network for nonlinear continuously differentiable optimization over a compact convex subset, *IEEE Transactions on Neural Networks*, **12** no. 6 (2001), 1487–1490.

[26] K. Mahler, On Hecke's theorem on the real zeros of the L-functions and the class number of quadratic fields, *Journal of the London Mathematical Society*, **s1-9** no. 4 (1934), 298–302.

[27] H. L. Montgomery and R. C. Vaughan, *Multiplicative Number Theory I. Classical Theory*, Cambridge Studies in Advanced Mathematics 97, Cambridge, U.K.: Cambridge University Press, 2006.

[28] L. J. Mordell, On the number of solutions in positive integers of the equation $yz + zx + xy = n$, *Amer. J. Math.*, **45** (1923), 1–4.

[29] E. T. Mortenson, A Kronecker-type identity and the representations of a number as a sum of three squares, *Bull. London Math. Soc.*, **49** (2017), 770–783.

[30] A. S. Mosunov and M. J. Jacobson, Unconditional class group tabulation of imaginary quadratic fields to $|\Delta| < 240$, *Mathematics of Computation*, **85** (2016), 1983–2009.

[31] J. Neukirch, *Algebraic Number Theory*, Berlin, Germany: Springer, 1999.

[32] OpenAI, Uniform exclusion of Landau–Siegel zeros, *Manuscript*, Oct. 1 (2026), 1–9.

[33] A. Ostrowski, Über einige lösungen der funktionalgleichung $\varphi(x) \cdot \varphi(x) = \varphi(xy)$, *Acta Math.*, **41** (1916), 271–284.

[34] C. D. Pan and C. B. Pan, *Fundamentals of Analytic Number Theory*, Beijing: Science Press, 1991 (in Chinese).

[35] H. Rademacher, On the Phragmén–Lindelöf theorem and some applications, *Mathematische Zeitschrift*, **72** (1959), 192–204.

[36] J. B. Rosser, Explicit bounds for some functions of prime numbers, *Amer. J. Math.*, **63** (1941), 211–232.

[37] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois J. Math.*, **6** no. 1 (1962), 64–94.

[38] J. Sherman and W. Morrison, Adjustment of an inverse matrix corresponding to a change in one element of a given matrix, *Annals of Mathematical Statistics*, **21** no. 1 (1950), 124–127.

[39] C. L. Siegel, Über die Classenzahl quadratischer Zahlkörper, *Acta Arith.*, **1** (1935), 83–86.

[40] H. M. Stark, Some effective cases of the Brauer–Siegel theorem, *Invent. Math.*, **23** (1974), 135–152.

[41] H. M. Stark, The analytic theory of algebraic numbers, *Bulletin of the American Mathematical Society*, **81** no. 6 (1975), 961–972.

[42] I. Stewart and D. Tall, *Algebraic Number Theory and Fermat's Last Theorem*, 3rd Edition, Natick, MA: A. K. Peters, 2002.

[43] T. Tatuzawa, On Siegel's theorem, *Japan. J. Math.*, **21** (1951), 163–178.

[44] I. M. Vinogradov, Representation of an odd number as a sum of three primes, *Dokl. Akad. Nauk SSSR*, **15** (1937), 291–294.

[45] A. Walfisz, Zur additiven Zahlentheorie. II., *Mathematische Zeitschrift*, **40** (1936), 592–607.

[46] M. Watkins, Real zeros of real odd Dirichlet L-functions, *Math. Comp.*, **73** no. 245 (2004), 415–423.

[47] A. Weil, *Number Theory: An approach through history*, Boston: Birkhäuser, 1964.

[48] P. Weinberger, Exponents of the class groups of complex quadratic fields, *Acta Arith.*, **22** (1973), 117–124.

[49] K. S. Williams, Integers of biquadratic fields, *Canadian Mathematical Bulletin*, **13** no. 4 (1970), 519–526.

Louisiana State University, Baton Rouge, LA 70803
E-mail: xbliang@lsu.edu