SCIENCE CHINA
Mathematics

• ARTICLES •

April 2017 Vol. 60 No. 4: 593–612
doi: 10.1007/s11425-015-0742-7

Congruent elliptic curves with non-trivial Shafarevich-Tate groups: Distribution part

WANG ZhangJie

Yau Mathematical Sciences Center, Tsinghua University, Beijing 100084*, China*
Email: zjwang@math.tsinghua.edu.cn

Received November 17, 2015; accepted June 8, 2016; published online December 21, 2016

Abstract Given a large positive number x and a positive integer k, we denote by $Q_k(x)$ the set of congruent elliptic curves $E^{(n)}: y^2 = z^3 - n^2 z$ with positive square-free integers $n \leqslant x$ congruent to one modulo eight, having k prime factors and each prime factor congruent to one modulo four. We obtain the asymptotic formula for the number of congruent elliptic curves $E^{(n)} \in Q_k(x)$ with Mordell-Weil ranks zero and 2-primary part of Shafarevich-Tate groups isomorphic to $(\mathbb{Z}/2\mathbb{Z})^2$. We also get a lower bound for the number of $E^{(n)} \in Q_k(x)$ with Mordell-Weil ranks zero and 2-primary part of Shafarevich-Tate groups isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$. The key ingredient of the proof of these results is an independence property of residue symbols. This property roughly says that the number of positive square-free integers $n \leqslant x$ with k prime factors and residue symbols (quadratic and quartic) among its prime factors being given compatible values does not depend on the actual values.

Keywords Shafarevich-Tate group, distribution, congruent elliptic curve, multiplicative number theory, number field, independence property, residue symbol

MSC(2010) 11G05, 11N99

Citation: Wang Z J. Congruent elliptic curves with non-trivial Shafarevich-Tate groups: Distribution part. Sci China Math, 2017, 60: 593–612, doi: 10.1007/s11425-015-0742-7

1 Introduction

A positive integer n is called a congruent number if it is the area of a right triangle with rational sides; or equivalently, if the elliptic curve $E^{(n)}: y^2 = z^3 - n^2 z$ has positive Mordell-Weil rank. Let E be the elliptic curve over $\mathbb{Q}$ defined by $y^2 = z^3 - z$. Then $E^{(n)}$ is a quadratic twist of E. We are interested in the behavior of arithmetic groups such as Mordell-Weil groups and Shafarevich-Tate groups in the quadratic twist family of E.

Goldfeld conjectured that for any elliptic curve over $\mathbb{Q}$ there are 50% elliptic curves with Mordell-Weil ranks zero and one respectively in its quadratic twist family. So far, this conjecture has not been verified for any single elliptic curve. The modular curve $X_0(19)$ has genus one and its cusp at ∞ is rational over $\mathbb{Q}$. For the elliptic curve $(X_0(19), [\infty])$, Vatsal [14] proved that a positive proportion of its quadratic twist family has Mordell-Weil ranks one (resp. ranks zero).

In this paper, we study the distribution of the number of congruent elliptic curves $E^{(n)}$ with Mordell-Weil ranks zero and 2-primary part of Shafarevich-Tate groups non-trivial. We first introduce some notation. Let $E^{(n)}(\mathbb{Q})$ be the Mordell-Weil group of $E^{(n)}$, and $Ш(E^{(n)}/\mathbb{Q})$ the Shafarevich-Tate group of $E^{(n)}$. For a positive integer k, we denote by Q_k the set of positive square-free integers n satisfying the following:

(1) $n \equiv 1 \pmod 8$ with exactly k prime factors, and

(2) any prime factor of n is congruent to 1 modulo 4.

Let $Q_k(x)$ be the set of integers $n \in Q_k$ with $n \leqslant x$. Denote by $C_k(x)$ the set of positive square-free integers $n \leqslant x$ with exactly k prime factors. Then a classical result implies that

$$\#C_k(x) \sim \frac{1}{(k-1)!} \cdot \frac{x}{\log x} (\log\log x)^{k-1}.$$

Here the symbol "$\sim$" means that the ratio of its two sides approaches the limit 1 as x goes to infinity.

Our main result in this paper is the following.

Theorem 1.1. *Let k be a positive integer. Denote by $P_k(x)$ those $n \in Q_k(x)$ such that*

$$\mathrm{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0 \quad \textit{and} \quad Ш(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^2.$$

Then

$$\#P_k(x) \sim 2^{-2-k}(u_k + (2^{-1} - 2^{-k})u_{k-1}) \cdot \#C_k(x).$$

Here $\{u_k = \prod_{i=1}^{\lfloor \frac{k}{2} \rfloor}(1 - 2^{1-2i}) \mid k \in \mathbb{N}\}$ is a decreasing sequence with limit $u \approx 0.419$, where $\lfloor \frac{k}{2} \rfloor$ is the maximal integer less than or equal to $k/2$.

Remark 1.2. The independence property of Legendre symbols of Rhoades [12] implies

$$\#Q_k(x) \sim \frac{1}{2^{k+1} \cdot (k-1)!} \cdot \frac{x}{\log x} \cdot (\log\log x)^{k-1}.$$

Hence, we have the density of $P_k(x)$ in $Q_k(x)$,

$$\lim_{x\to\infty} \frac{\#P_k(x)}{\#Q_k(x)} = \frac{1}{2}(u_k + (2^{-1} - 2^{-k})u_{k-1}).$$

Similar result for the congruent elliptic curves $E^{(n)}$ with $\mathrm{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0$ and $Ш(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^4$ is given in the following Theorem 1.3.

Theorem 1.3. *Denote by $\tilde{P}_k(x)$ those $n \in Q_k(x)$ with all prime factors congruent to 1 modulo 8 such that*

$$\mathrm{rank}_{\mathbb{Z}} E^{(n)}(\mathbb{Q}) = 0 \quad \textit{and} \quad Ш(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^4.$$

Then for any $k \geqslant 2$, $\#\tilde{P}_k(x)$ has a lower bound with main term

$$\sum_{l+l'=k} \frac{u_l u_{l'}}{2^{5+2k+ll'}} \cdot \binom{k}{l} \cdot \#C_k(x).$$

Here u_l is defined in Theorem 1.1 *and $\binom{k}{l}$ is the binomial coefficient.*

Now we explain the strategy for the proof of Theorem 1.1.

• By our previous paper [15], $n \in P_k(x)$ can be characterized by conditions of 4-rank and 8-rank of the ideal class group of $\mathbb{Q}(\sqrt{-n})$.

• The 4-rank condition gives rise to an $\mathbb{F}_2$-matrix related to quadratic residue symbols among prime factors of n, and the 8-rank condition is reduced to that for quartic residue symbols by Jung and Yue [10].

• By the independence property of residue symbols, namely Theorem 1.4, the number of those $n \leqslant x$ with prime factors in given residue classes modulo 16 and residue symbols among its prime factors being given compatible values can be estimated uniformly. Consequently, the proof of Theorem 1.1 is reduced to counting the number of certain $\mathbb{F}_2$-matrices.

To explain the independence property of residue symbols, we first introduce some notation. For $d \in Q_k$ and q an integer such that $(\frac{q}{p}) = 1$ for all prime divisors p of d, we denote by $(\frac{q}{d})_4$ the quartic residue symbol defined in Section 2.2. For an odd integer a, we define $[\frac{2}{a}] = 1$ if $a \equiv \pm 5 \pmod 8$ and $[\frac{2}{a}] = 0$ otherwise. Let k be a positive integer. Let $\alpha = (\alpha_1, \ldots, \alpha_k)$ with all $\alpha_l \in \{1, 5, 9, 13\}$ and $\prod_{l=1}^k \alpha_l \equiv 1 \pmod 8$. Assume that B is a $k \times k$ symmetric $\mathbb{F}_2$ matrix such that its rank is $k-1$ and the sum

of all elements of any of its given row is 0. If we view B as a linear transformation over $\mathbb{F}_2$, then $\mathfrak{b}=([\frac{2}{\alpha_1}],\dots,[\frac{2}{\alpha_k}])^{\mathrm{T}}$ lies in the image of B. Moreover, $By=\mathfrak{b}$ has two different solutions y and $y'\in\mathbb{F}_2^k$ with $y+y'=(1,\dots,1)^{\mathrm{T}}$. We assume that $z=(z_1,\dots,z_k)^{\mathrm{T}}$ is the one of y and y' such that $z_1=1$. Then we define $C_k(x,\alpha,B)$ to be all $n=p_1\cdots p_k\in C_k(x)$ with $p_1<\cdots<p_k$ such that

- $p_l\equiv\alpha_l \pmod{16}$ for $1\leqslant l\leqslant k$,
- the Legendre symbol $(\frac{p_l}{p_j})=(-1)^{B_{lj}}$ for all $1\leqslant l<j\leqslant k$, and
- $(\frac{2d}{n/d})_4(\frac{2n/d}{d})_4=(-1)^{\frac{n-1}{8}+\frac{d-5}{4}}$ with $d=\prod p_l^{z_l}$.

Now we state the independence property of residue symbols.

Theorem 1.4. *For k a positive integer, let $\alpha=(\alpha_1,\dots,\alpha_k)$ with $\alpha_l\in\{1,5,9,13\}$ and $\prod_{l=1}^k\alpha_l\equiv 1 \pmod 8$. If B is a $k\times k$ symmetric $\mathbb{F}_2$-matrix such that its rank is $k-1$ and the sum of all elements of any of its given row is 0, then*

$$\#C_k(x,\alpha,B)\sim\frac{1}{2^{3k+\binom{k}{2}+1}}\cdot\#C_k(x).$$

Rhoades [12] claimed a special case of the above theorem. Moreover, he proved an independence property of Legendre symbols by the method of Cremona and Odoni [2] over $\mathbb{Q}$. For Theorem 1.4, we have to extend the method of Cremona and Odoni [2] to $\mathbb{Q}(i)$ because of the quartic residue symbols.

Now we explain the ingredients of the proof of Theorem 1.4.

(1) We identify the set $C_k(x,\alpha,B)$ with a set $C'_k(x,\alpha,B)$ which counts certain integers of $\mathbb{Z}[i]$ with k prime factors.

(2) The method of Cremona and Odoni [2] reduces estimating $\#C'_k(x,\alpha,B)$ to a sum with every term counting primes in certain residue classes defined by residue symbols.

(3) To use Dirichet prime ideal theorem over $\mathbb{Z}[i]$, we transform a set counting primes of $\mathbb{Z}[i]$ into that counting prime ideals.

(4) The representation theory of finite abelian group is used to count the number of residue classes.

Since the main tool is analytic number theory, we will use many standard symbols in analytic number theory without definition, such as $\sim,o(\cdot),O(\cdot),\ll,\pi(x),\mathrm{Li}(x),\psi(x),\psi(x,\chi)$ and $\psi(x;a,q)$. These can be found in any book on analytic number theory, for example Iwaniec and Kowalski [9].

In the end of this introduction, we give the organization of this paper. We devote Section 2 to giving some preliminary results. Concretely, in Subsection 2.1 we summarize the method of Cremona and Odoni [2] in a simpler case; since many residue symbols are used, we give their definitions and prove some properties in Subsection 2.2; those analytic results over $\mathbb{Q}(i)$ are listed in Subsection 2.3. With these preparations, we prove Theorem 1.4 in Section 3; in particular, we separate out the case $k=1$ in Subsection 3.1 to make the ingredients (3) and (4) clearer and simpler. The distribution results are carried out in Section 4. Conclusions are presented in Section 5.

2 Preliminaries

2.1 Basic idea

Since the method of Cremona and Odoni [2] plays an important role in our proof of the independence property of residue symbols, we explain their basic idea in the following much simpler case

$$\#C_k(x)\sim\frac{1}{(k-1)!}\cdot\frac{x}{\log x}\cdot(\log\log x)^{k-1}.$$

Here $C_k(x)$ denotes the set of positive square-free integers $n\leqslant x$ with exactly k prime factors. For $k=1$, this follows from the prime number theorem. For $k\geqslant 2$, the key idea is to consider the induction map,

$$\varphi:C_k(x)\to C_{k-1}(x),\quad n\mapsto n/\tilde{n},$$

where $\tilde{n}$ is the maximal prime divisor of n. Note that $t \in C_{k-1}(x)$ is in the image of φ if and only if there is a prime p such that $\tilde{t} < p \leqslant xt^{-1}$. Thus we get

$$\#C_k(x) = \sum_{t \in C_{k-1}(x)} \#\{p \text{ prime} \,|\, \tilde{t} < p \leqslant xt^{-1}\}.$$

Then [2, Lemma 3.1] implies that only those $t \in (\mu, \nu] \cap C_{k-1}(x)$ contribute to the main term of $\#C_k(x)$, where $\mu = (\log x)^{100}$ and $\nu = \exp(\frac{\log x}{(\log\log x)^{100}})$. Hence we reduce to estimating

$$\sum_{\mu < t \leqslant \nu}^{*} \pi(xt^{-1}),$$

where

$$\sum_{a < t \leqslant b}^{*} f(t) := \sum_{t \in (a,b] \cap C_{k-1}(\infty)} f(t).$$

From the prime number theorem, we only need to estimate

$$\sum_{\mu < t \leqslant \nu}^{*} \mathrm{Li}(xt^{-1}).$$

[2, Lemma 3.1] and Section 1 give

$$\#C_k(x) \sim \frac{1}{(k-1)!} \cdot \frac{x}{\log x} (\log\log x)^{k-1}.$$

This is the key idea of Cremona and Odoni [2]. In that paper, they have to use $\psi(xt^{-1}; a, q)$ instead of $\pi(xt^{-1})$. This forces them to use the explicit formula of $\psi(x, \chi)$, which brings the additional difficulty in dealing with possible Siegel zeros in the error term. Due to Page theorem, the sum of all $\psi(xt^{-1}, \chi)$ with possible Siegel zeros contributes to an error term by the trivial estimation $\psi(xt^{-1})$ of $\psi(xt^{-1}, \chi)$.

Comparing with Cremona and Odoni [2], we have to deal with corresponding multiplicative number theory over $\mathbb{Q}(i)$.

2.2 Residue symbols

In this subsection, we will introduce several residue symbols that will be used in this paper.

Let λ be a prime element of the ring $\mathbb{Z}[i]$ of Gaussian integers coprime to $(1+i)$, and α be a Gaussian integer. Then the quartic residue symbol $(\frac{\alpha}{\lambda})_4$ is defined to be the unique element in $\{\pm 1, \pm i, 0\}$ such that

$$\alpha^{\frac{\lambda\bar{\lambda}-1}{4}} \equiv \left(\frac{\alpha}{\lambda}\right)_4 \pmod{\lambda}.$$

Here $\overline{\lambda}$ is the conjugate of λ. A reference for this is Ireland and Rosen [8].

We say a prime element λ of $\mathbb{Z}[i]$ Gaussian if it is not a rational prime. For two coprime Gaussian primes λ_1 and λ_2, we easily deduce that

$$\left(\frac{\lambda_1}{\lambda_2}\right)_4 \left(\frac{\bar{\lambda_1}}{\lambda_2}\right)_4 = 1.$$

Moreover, we have the quartic reciprocity law

$$\left(\frac{\lambda_1}{\lambda_2}\right)_4 = \left(\frac{\lambda_2}{\lambda_1}\right)_4 (-1)^{\frac{N\lambda_1-1}{4}\frac{N\lambda_2-1}{4}},$$

where N denotes the norm from $\mathbb{Q}(i)$ to $\mathbb{Q}$. If $\theta = \prod_{l=1}^{k} \lambda_l$ with λ_l prime element of $\mathbb{Z}[i]$ and coprime with $1+i$, we define

$$\left(\frac{\alpha}{\theta}\right)_4 = \prod_{l=1}^{k} \left(\frac{\alpha}{\lambda_l}\right)_4.$$

We say that an integer $\theta \in \mathbb{Z}[i]$ is primary if $\theta \equiv 1 \pmod{2+2i}$. Then any primary integer can be written uniquely as the product of primary primes. Since we will frequently consider $(\frac{2}{\theta})_4$, we compute it in the following proposition.

Proposition 2.1. *If $\theta = a + 2bi$ is a primary integer with $a, b \in \mathbb{Z}$, then $(\frac{2}{\theta})_4 = i^{-b}$.*

Proof. If θ has a rational prime factor p congruent to 3 (mod 4), then $(\frac{2}{-p})_4 = 1$ and there must be even many such prime factors counted with multiplicity. So their product n is congruent to 1 (mod 4) and $(\frac{2}{n})_4 = 1$. Hence we may assume that any prime factor of θ is Gaussian.

Now we induct on the number of prime factors of θ. If θ is a prime, then $(\frac{2}{\theta})_4 = i^{-b}$ by Iwaniec and Kowalski [9, p. 53]. If θ has $k \geqslant 2$ prime factors, then $\theta = \theta_1\theta_2$, where θ_l is a primary Gaussian integer having less than k prime factors for $l = 1, 2$. Hence if we denote $\theta_l = a_l + 2b_l i$ with $a_l, b_l \in \mathbb{Z}$, then Section 1 implies that

$$\left(\frac{2}{\theta_l}\right)_4 = i^{-b_l}.$$

Thus $(\frac{2}{\theta})_4 = i^{-(b_1+b_2)}$ by definition. On the other hand,

$$a + 2bi = \theta = \theta_1\theta_2 = a_1a_2 - 4b_1b_2 + 2(a_1b_2 + a_2b_1)i.$$

Therefore $b = a_1b_2 + a_2b_1$. Since θ_l is primary, we have $a_l - 2b_l \equiv 1 \pmod 4$. Consequently, $b \equiv (1+2b_1)b_2 + (1+2b_2)b_1 \equiv b_1 + b_2 \pmod 4$. So by Section 1, the proof is completed. □

For p a rational prime congruent to 1 modulo 4, there are exactly two primitive primes λ and $\bar{\lambda}$ lying above p with $p = \lambda\bar{\lambda}$. For q a rational integer with $(\frac{q}{p}) = 1$, the two quartic residue symbols $(\frac{q}{\lambda})_4 = (\frac{q}{\bar{\lambda}})_4 = \pm 1$. Then we use the symbol $(\frac{q}{p})_4$ to denote either $(\frac{q}{\lambda})_4$ or $(\frac{q}{\bar{\lambda}})_4$. The symbol $(\frac{q}{p})_4$ has the convenience that we do not need to choose which primary prime lies above p. Assume that d is a positive integer with all prime factors congruent to 1 (mod 4). If q is a rational integer such that $(\frac{q}{p}) = 1$ for any prime factor p of d, then

$$\left(\frac{q}{d}\right)_4 := \prod_{p|d} \left(\frac{q}{p}\right)_4^{v_p(d)},$$

where $v_p(d)$ denotes the p-adic valuation of d.

We introduce the general Legendre symbol over $\mathbb{Z}[i]$ as in [6, p. 196]. Let $\mathfrak{p}$ be a prime ideal of $\mathbb{Z}[i]$. If $\mathfrak{p}$ is coprime with $(1+i)$, then the general Legendre symbol $(\frac{\alpha}{\mathfrak{p}})$ is defined to be the unique element of $\{\pm 1, 0\}$ such that

$$\alpha^{\frac{N\mathfrak{p}-1}{2}} \equiv \left(\frac{\alpha}{\mathfrak{p}}\right) \pmod{\mathfrak{p}}.$$

If λ is the unique primary prime in $\mathfrak{p}$, we also denote

$$\left(\frac{\alpha}{\lambda}\right) = \left(\frac{\alpha}{\mathfrak{p}}\right).$$

If $\theta = \prod_{l=1}^{k} \lambda_l$ with λ_l primary prime, then we define

$$\left(\frac{\alpha}{\theta}\right) = \prod_{l=1}^{k} \left(\frac{\alpha}{\lambda_l}\right).$$

Another residue symbol is needed. For p an odd prime and a a rational integer coprime with p, the additive Legendre symbol $[\frac{a}{p}] = 1$ if the Legendre symbol $(\frac{a}{p}) = -1$ and $[\frac{a}{p}] = 0$ otherwise. Similarly, for d a positive odd integer and a a rational integer coprime with d, we define $[\frac{a}{d}] = 1$ if the Jacobi symbol $(\frac{a}{d}) = -1$ and $[\frac{a}{d}] = 0$ if $(\frac{a}{d}) = 1$.

2.3 Analytic results over number fields

Let K be a number field of degree n with discriminant Δ. Denote by $\mathcal{O}$ the ring of algebraic integers of K and N_K the norm from K to $\mathbb{Q}$. A non-zero element $\gamma \in K$ is called totally positive if it is positive under all real embeddings. If K has no real embedding, then γ is totally positive if and only if $\gamma \neq 0$. For an integral ideal $\dagger$ and $\gamma \in K$, the notation $\gamma \equiv 1 \pmod{\dagger}$ means that $\gamma \in \mathcal{O}_{\mathfrak{p}}$ and $\gamma \equiv 1 \pmod{\mathfrak{p}^{v_{\mathfrak{p}}(\dagger)}}$ if $\mathfrak{p} \mid \dagger$, where $\mathcal{O}_{\mathfrak{p}}$ is the integer ring of the $\mathfrak{p}$-adic completion of K. Let $P_{\dagger}$ be the group of principal fractional ideals (γ) with γ totally positive and $\gamma \equiv 1 \pmod{\dagger}$, and $I(\dagger)$ the group of all the fractional ideals that are coprime with $\dagger$. We say that χ is a character modulo an ideal $\dagger$ if χ is a character induced from $I(\dagger)/P_{\dagger}$. For a character χ modulo $\dagger$, we define $\chi(\mathfrak{a}) = 0$ if $\mathfrak{a}$ is not coprime with $\dagger$. Then $\psi(x, \chi)$ is defined to be

$$\psi(x, \chi) = \sum_{N_K \mathfrak{a} \leqslant x} \chi(\mathfrak{a}) \Lambda(\mathfrak{a}).$$

Here $\mathfrak{a}$ runs over all the integral ideals with norm no bigger than x, and $\Lambda(\mathfrak{a})$ is the Mangoldt function defined by

$$\begin{cases} \log N_K \mathfrak{p}, & \text{if } \mathfrak{a} = \mathfrak{p}^m \text{ with } m \geqslant 1\ , \\ 0, & \text{otherwise.} \end{cases}$$

Now we state the explicit formula of $\psi(x, \chi)$ (see [9, p. 114]).

Proposition 2.2. *If χ is a non-principal character mod $\dagger$ and $1 \leqslant T \leqslant x$, then*

$$\psi(x, \chi) = -\sum_{|\mathrm{Im}\rho| \leqslant T} \frac{x^{\rho} - 1}{\rho} + O(xT^{-1} \cdot \log x \cdot \log(x^n \cdot N_K \dagger)), \tag{2.1}$$

where ρ runs over all the zeros of $L(s, \chi)$ with $0 \leqslant \mathrm{Re}\rho \leqslant 1$ and $|\mathrm{Im}\rho| \leqslant T$, and the implied constant depends only on K.

For further application, we introduce Page theorem and Siegel theorem over K. For Page theorem over K (see Proposition 2.3(2)), we refer to Hoffstein and Ramakrishnan [7]; and for Siegel theorem over K (see Proposition 2.3(1)), we refer to Fogels [3–5].

Proposition 2.3. (1) *Let χ be a character modulo $\dagger$, and $D = |\Delta| N_K \dagger > D_0 > 1$.*

(i) *There is a positive constant c (which only depends on n) such that in the region*

$$\mathrm{Re}(s) > 1 - \frac{c}{\log D(1 + |\mathrm{Im}(s)|)} > \frac{3}{4}, \tag{$*$}$$

there is no zero of $L(s, \chi)$ with χ complex, for at most one real χ' there maybe a simple zero β' of $L(s, \chi')$.

(ii) *If β' is the exceptional zero corresponding to the exceptional character χ' modulo $\dagger$, then for any $\epsilon > 0$ there is a positive constant $c(n, \epsilon)$ such that*

$$1 - \beta' > c(n, \epsilon) D^{-\epsilon}.$$

(2) *For any $z \geqslant 2$ and c_0 a suitable constant, there is at most a real primitive character χ to a modulus $\dagger$ with $N_K \dagger \leqslant z$ such that $L(s, \chi)$ has a real zero β satisfying*

$$\beta > 1 - \frac{c_0}{\log z}.$$

For future purpose, the first term of (2.1) has to be estimated. Like the classical case, we get the following explicit formula:

$$\psi(x, \chi) = -\frac{x^{\beta'}}{\beta'} + R(x, T) \tag{2.2}$$

with

$$R(x, T) \ll x \cdot \log^2(x \cdot N_K \dagger) \cdot \exp\left(-\frac{c_1 \log x}{\log |T \cdot N_K \dagger|} \right) + xT^{-1} \log x \cdot \log |x^n \cdot N_K \dagger| + x^{\frac{1}{4}} \log x.$$

Here the term $-\frac{x^{\beta'}}{\beta'}$ occurs only if χ is a real character having a zero β' (then must be unique and simple) with

$$\beta' > 1 - \frac{c_2}{\log N_K\dagger},$$

where c_2 is a certain constant.

3 Independence property of residue symbols

To prove the independence property of residue symbols (see Theorem 1.4), we first identify $C_k(x,\alpha,B)$ with a set that counts certain integers in $\mathbb{Z}[i]$. For this purpose, we introduce some notation.

Denote by $\mathcal{P}$ the set of all primary primes in $\mathbb{Z}[i]$ with imaginary part positive. Let k be a positive integer, and $\alpha=(\alpha_1,\dots,\alpha_k)$ with all $\alpha_l\in\{1,5,9,13\}$ such that $\prod_{l=1}^k\alpha_l\equiv 1 \pmod 8$. Assume that $B=B_{k\times k}$ is a symmetric $\mathbb{F}_2$-matrix such that its rank is $k-1$ and the sum of all elements of any of its given row is 0. Then we define $C'_k(x,\alpha,B)$ to be all $\eta=\prod_1^k\lambda_l$ satisfying

- $N\eta\leqslant x$ and $N\lambda_1<\cdots<N\lambda_k$ with $\lambda_l\in\mathcal{P}$ for $1\leqslant l\leqslant k$,
- $N\lambda_l\equiv\alpha_l \pmod{16}$ and $(\frac{N\lambda_l}{N\lambda_j})=(-1)^{B_{lj}}$ for all $1\leqslant l\neq j\leqslant k$, and
- $(\frac{\theta'}{\theta})(\frac{2}{\eta})_4=(-1)^{\frac{\prod_1^k\alpha_j-1}{8}+\frac{\prod_1^k\alpha_j^{z_j}-5}{4}}$ with $\theta\theta'=\eta$ and $\theta=\prod_1^k\lambda_l^{z_l}$.

Here $z=(z_1,\dots,z_k)^{\mathrm{T}}\in\mathbb{F}_2^k$ satisfies $Bz=([\frac{2}{\alpha_1}],\dots,[\frac{2}{\alpha_k}])^{\mathrm{T}}$ and $z_1=1$.

Let $n=p_1\cdots p_k\in C_k(x,\alpha,B)$ such that $p_1<\cdots<p_k$. For $1\leqslant l\leqslant k$, we choose the unique $\lambda_l\in\mathcal{P}$ such that $p_l=\lambda_l\overline{\lambda_l}$. Then we claim that $\eta:=\prod_{l=1}^k\lambda_l\in C'_k(x,\alpha,B)$. Note that η obviously satisfies the first and second conditions in defining $C'_k(x,\alpha,B)$. Now we prove that η also satisfies the third. Considering the l-th row of both sides of $Bz=([\frac{2}{\alpha_1}],\dots,[\frac{2}{\alpha_k}])^{\mathrm{T}}$, we get

$$\sum_{j=1,j\neq l}^k z_jB_{lj}+z_l\sum_{j=1,j\neq l}^k B_{lj}=\left[\frac{2}{\alpha_l}\right],\quad B_{lj}=\left[\frac{p_j}{p_l}\right]\quad\text{if}\quad j\neq l,$$

since the sum of all elements of any of B's given row is 0. Thus $(\frac{2n/d}{p_l})=1$ if $z_l=1$ and $(\frac{2d}{p_l})=1$ if $z_l=0$. So the notations $(\frac{2n/d}{d})_4$ and $(\frac{2d}{n/d})_4$ are meaningful. In addition, according to their definitions we have

$$\begin{aligned}\left(\frac{2n/d}{d}\right)_4\left(\frac{2d}{n/d}\right)_4&=\left(\frac{2p_{t+1}\cdots p_k}{\lambda_1\cdots\lambda_t}\right)_4\left(\frac{2p_1\cdots p_t}{\lambda_{t+1}\cdots\lambda_k}\right)_4\\&=\left(\frac{2}{\eta}\right)_4\cdot\prod_{l=1}^t\prod_{j=t+1}^k\left(\frac{p_j}{\lambda_l}\right)_4\left(\frac{p_l}{\lambda_j}\right)_4\\&=\left(\frac{2}{\eta}\right)_4\cdot\prod_{l=1}^t\prod_{j=t+1}^k\left(\frac{\lambda_j}{\lambda_l}\right)_4\left(\frac{\overline{\lambda_j}}{\lambda_l}\right)_4\left(\frac{\lambda_l}{\lambda_j}\right)_4\left(\frac{\overline{\lambda_l}}{\lambda_j}\right)_4.\end{aligned}$$

Here we have assumed that $d=p_1\cdots p_t$ for notational simplicity. Using quartic reciprocity laws for $(\frac{\lambda_l}{\lambda_j})_4$ and $(\frac{\overline{\lambda_l}}{\lambda_j})_4$, we get

$$\left(\frac{\lambda_j}{\lambda_l}\right)_4\left(\frac{\overline{\lambda_j}}{\lambda_l}\right)_4\left(\frac{\lambda_l}{\lambda_j}\right)_4\left(\frac{\overline{\lambda_l}}{\lambda_j}\right)_4=\left(\frac{\lambda_j}{\lambda_l}\right)\left(\frac{\overline{\lambda_j}}{\lambda_l}\right)_4\left(\frac{\lambda_j}{\overline{\lambda_l}}\right)_4.$$

Note that $(\frac{\overline{\lambda_j}}{\lambda_l})_4(\frac{\lambda_j}{\overline{\lambda_l}})_4=1$. Then we obtain

$$\left(\frac{2n/d}{d}\right)_4\left(\frac{2d}{n/d}\right)_4=\left(\frac{2}{\eta}\right)_4\left(\frac{\theta'}{\theta}\right).\tag{3.1}$$

Thus $\eta\in C'_k(x,\alpha,B)$. From this we obtain a bijection

$$C_k(x,\alpha,B)\to C'_k(x,\alpha,B).\tag{3.2}$$

Now we divide the proof of Theorem 1.4 into two cases according to $k = 1$ or not in the following subsections.

3.1 The case $k = 1$

For the case $k = 1$, we have $\alpha_1 \in \{1, 9\}$. Moreover, only $B = 0_{1\times 1}$ has rank $k - 1 = 0$. So $C_1'(x, \alpha_1, 0)$ consists of all primary primes $\lambda \in \mathcal{P}$ such that

$$N\lambda \leqslant x, \quad N\lambda \equiv \alpha_1 \pmod{16}, \quad \left(\frac{2}{\lambda}\right)_4 = (-1)^{\frac{\alpha_1 - 9}{8}}.$$

We denote by A_{16} those primary classes a of $\mathbb{Z}[i]/16\mathbb{Z}[i]$ such that

(i) $Na \equiv \alpha_1 \pmod{16}$, and

(ii) $(\frac{2}{a})_4 = (-1)^{\frac{\alpha_1 - 9}{8}}$.

By Proposition 2.1, we obtain

$$\#C_1'(x, \alpha_1, 0) = \frac{1}{2}\pi'(x, A_{16}, 16). \tag{3.3}$$

Here $\pi'(y, A, \gamma)$ is the number of primes λ in $\mathbb{Z}[i]$ with $N\lambda \leqslant y$ and $\lambda \pmod{\gamma} \in A$, and the additional factor $\frac{1}{2}$ comes from $\lambda \in C_1'(x, \alpha, 0)$ with imaginary part positive.

Note that the Dirichlet prime ideal theorem over $\mathbb{Q}(i)$ involves prime ideals, while our estimation concerns prime elements. This can be solved as follows. Let $\mathfrak{c}$ be the ideal $16\mathbb{Z}[i]$. Then we define $I(\mathfrak{c})$ and $P(\mathfrak{c})$ as in Subsection 2.3. By [11, Theorem 6.1], we have the exact sequence

$$1 \to \mathbb{Z}[i]^\times \to (\mathbb{Z}[i]/\mathfrak{c})^\times \xrightarrow{f} I(\mathfrak{c})/P_{\mathfrak{c}} \to 1\ , \tag{3.4}$$

where f is induced from the map which sends every $\mathfrak{c}$-invertible Gauss integer a to the class of the ideal (a). In fact, the exactness of (3.4) can be verified directly for the class number of $\mathbb{Z}[i]$ is 1. Denote by $\pi(y, \mathfrak{A}, \mathfrak{a})$ those prime ideals $\mathfrak{p}$ with norm no greater than y such that $\mathfrak{p} \pmod{P_{\mathfrak{a}}} \in \mathfrak{A}$.

Now we transform the primes counted in $\pi'(x, A_{16}, 16)$ into prime ideals. Let $\mathfrak{A}_{16}$ be the image of A_{16} under f. For any prime ideal (λ) in a class of $\mathfrak{A}_{16}$, there are exactly four primes lying in (λ), but only one of them is primary. Then we get

$$\pi'(x, A_{16}, 16) = \pi(x, \mathfrak{A}_{16}, \mathfrak{c}) \tag{3.5}$$

and

$$\#\mathfrak{A}_{16} = \#A_{16}. \tag{3.6}$$

By Dirichlet prime ideal theorem over $\mathbb{Q}(i)$ (see the prime ideal theorem and Proposition 2.2), we get

$$\pi(x, \mathfrak{A}_{16}, \mathfrak{c}) \sim \frac{\#\mathfrak{A}_{16}}{\#I(\mathfrak{c})/P_{\mathfrak{c}}} \cdot \mathrm{Li}(x).$$

Let $\phi(16)$ be the number of $(\mathbb{Z}[i]/16\mathbb{Z}[i])^\times$. Then from the exact sequence (3.4), we have $\#I(\mathfrak{c})/P_{\mathfrak{c}} = \frac{\phi(16)}{4}$. Thus from (3.3) and (3.5), we obtain

$$\#C_1'(x, \alpha_1, 0) \sim \frac{2\#\mathfrak{A}_{16}}{\phi(16)} \cdot \mathrm{Li}(x).$$

According to Lemma 3.1, we get

$$\#C_1'(x, \alpha_1, 0) \sim \frac{1}{2^4} \cdot \mathrm{Li}(x).$$

Noting $\#C_1(x) \sim \mathrm{Li}(x)$ and the bijection (3.2), we finish the proof of Theorem 1.4 in the case $k = 1$.

Lemma 3.1. *The cardinality of A_{16} is $\phi(16)/2^5$.*

Proof. Let G be the set of the primitive residue classes $1+(2+2i)\mathbb{Z}[i]$ (mod 16). Then G is a subgroup of $(\mathbb{Z}[i]/16\mathbb{Z}[i])^\times$ and $\#G=\phi(16)/4$. By the definition of A_{16}, the condition that the class is primary selects the subgroup G from $(\mathbb{Z}[i]/16\mathbb{Z}[i])^\times$. To determine those elements of G selected by the conditions (i) and (ii), we introduce two characters on G defined by

$$\chi_1(g)=i^{\frac{Ng-1}{4}},\quad \chi_2(g)=\left(\frac{2}{g}\right)_4.$$

Hence we reduce to finding those $g\in G$ such that

$$\chi_1(g)=i^{\frac{\alpha_1-1}{4}},\quad \chi_2(g)=(-1)^{\frac{\alpha_1-9}{8}}. \tag{3.7}$$

This reminds us to study the behavior of χ_i on G. We can easily deduce that $\chi_j^2(g)=(\frac{2}{Ng})$ for $j=1,2$. Hence $\chi_1^2=\chi_2^2$. In addition, χ_1 and χ_2 are characters of order 4, since $\chi_j^2(-1+2i)=-1$. Moreover, we have $\chi_1(-1+2i)=i$ and $\chi_2(-1+2i)=i^{-1}$ by Lemma 2.1. Therefore $\chi_1\neq\chi_2$. So the character subgroup G' generated by χ_1 and χ_2 has 8 elements.

Now we show that G' is the dual group of $G/G_1\cap G_2$ with G_i the kernel of χ_i. It suffices to prove $\#G/G_1\cap G_2=8$. From the group isomorphism theorem, we only need to study G/G_1 and $G_1/G_1\cap G_2$. The former group $G/G_1\simeq\mu_4$ as χ_1 has order 4, where μ_4 is the group of units of order 4. For the latter group, we have the restriction map $\chi_2|_{G_1}: G_1/G_1\cap G_2\to\mu_4$. Because of $\chi_1\neq\chi_2$, we know that $\chi_2|_{G_1}$ is non-trivial. From $\chi_1^2=\chi_2^2$, we obtain

$$\chi_2(g_1)^2=\chi_1(g_1^2)=1,\quad g_1\in G_1.$$

Hence $\chi_2|_{G_1}$ has order 2 and $\#G_1/G_1\cap G_2=2$. Thus we get $\#G/G_1\cap G_2=8$. Therefore, G' is the dual group of $G/G_1\cap G_2$ by counting cardinality.

By finite abelian group representation theory (see [13, p. 62]), $G/G_1\cap G_2$ is also the dual of G'. Hence any $g\in G$ is a character of G', and we denote

$$g(\chi)=\chi(g)\quad\text{for any}\quad\chi\in G'.$$

Then for any integers x_1 and x_2, we claim that the following are equivalent:

(1) there is a $g\in G$ with $\chi_j(g)=i^{x_j}$ for $j=1,2$,

(2) $i^{2x_1}=i^{2x_2}$.

Note that (1) is equivalent to finding a character g on G' such that $g(\chi_1)=i^{x_1}$ and $g(\chi_2)=i^{x_2}$. Since G' is generated by χ_1 and χ_2 subjected to $\chi_1^2=\chi_2^2$, the existence of such g is equivalent to $g(\chi_1^2)=g(\chi_2^2)$. By $g(\chi_j^2)=\chi_j^2(g)=i^{2x_j}$, we know that (1) and (2) are equivalent.

Note that $i^{2\cdot\frac{\alpha_1-1}{4}}=(-1)^{2\cdot\frac{\alpha_1-9}{8}}=1$. Therefore there is a $g_0\in G$ such that (3.7) holds. Moreover, by transition of g_0, we know that all $g\in G$ satisfying (3.7) comprise the subset $g_0(G_1\cap G_2)$, which occupies an eighth of G. Hence we get

$$\#A_{16}=\frac{\phi(16)}{2^5}.$$

This completes the proof of the lemma. □

3.2 The case $k\geqslant 2$

In this subsection, we will use the method of Cremona and Odoni [2] to prove Theorem 1.4 in the case $k\geqslant 2$.

To define the similar map φ in Section 2, we define $T(x)$ to be all $n=p_1\cdots p_{k-1}\leqslant x$ with $p_1,\ldots,p_{k-1}$ strictly ascending such that

- $p_l\equiv\alpha_l\pmod{16}$ for $1\leqslant l\leqslant k-1$, and
- $(\frac{p_l}{p_j})=(-1)^{B_{lj}}$ for $1\leqslant l<j\leqslant k-1$.

From the independence property of Legendre symbols of Rhoades [12], we have

$$\#T(x)\sim 2^{-\binom{k}{2}-2k+2}\cdot\#C_{k-1}(x). \tag{3.8}$$

We identify $T(x)$ with a set $T'(x)$, similar to the identification of $C_k(x,\alpha,B)$. In addition, $T'(x)$ is defined to be all $\eta=\lambda_1\cdots\lambda_{k-1}$ with $N\eta\leqslant x$ and $N\lambda_1<\cdots<N\lambda_{k-1}$ such that

- $\lambda_j\in\mathcal{P}$ and $N\lambda_j\equiv\alpha_j \pmod{16}$ for $1\leqslant j\leqslant k-1$, and
- $(\frac{N\lambda_l}{N\lambda_j})=(-1)^{B_{lj}}$ for $1\leqslant l<j\leqslant k-1$.

Then we also have a bijection

$$T'(x)\to T(x),\quad \eta\mapsto N\eta. \tag{3.9}$$

Now we prove Theorem 1.4 with $k\geqslant 2$.

Proof of Theorem 1.4. Let $\tilde{\eta}$ be the primitive prime divisor of η with maximal norm and imaginary part positive. Then we define the map

$$\varphi: C'_k(x,\alpha,B)\to T'(x),\quad \eta\mapsto \eta/\tilde{\eta}.$$

Now we divide it into two cases according to $z_k=0$ or 1.

Now we assume that $z_k=0$. Let $\epsilon=\prod_1^{k-1}\lambda_j\in T'(x)$. Then ϵ lies in the image of φ if and only if there is a prime $\lambda\in\mathcal{P}$ with $N\tilde{\epsilon}<N\lambda\leqslant x/N\epsilon$ such that

(i) $N\lambda\equiv\alpha_k \pmod{16}$ and $(\frac{N\lambda}{N\lambda_j})=(-1)^{B_{jk}}$ with $1\leqslant j\leqslant k-1$, and

(ii) $(\frac{2}{\lambda})_4(\frac{\lambda}{\theta})=(\frac{2}{\epsilon})_4(\frac{\epsilon/\theta}{\theta})(-1)^{\frac{\prod_1^k\alpha_j-1}{8}+\frac{\prod_1^k\alpha_j^{z_j}-5}{4}}$ with $\theta=\prod_{l=1}^{k-1}\lambda_l^{z_l}$.

Here $\tilde{\epsilon}$ is the primitive prime divisor of ϵ with maximal norm and imaginary part positive. Thus from Proposition 2.1, there is a unique subset A_ϵ of invertible primary residue classes modulo 16ϵ such that the following holds: for a prime λ, the integer $\lambda\epsilon$ belongs to $C'_k(x,\alpha,B)$ if and only if λ lies in $\mathcal{P}$ and A_ϵ with norm in $(N\tilde{\epsilon},\ x/N\epsilon]$. Hence we obtain

$$\#C'_k(x,\alpha,B)=\sum_{\epsilon\in T'(x)}g(\epsilon) \tag{3.10}$$

with

$$g(\epsilon)=\#\{\lambda \text{ prime of } \mathbb{Z}[i]\mid \lambda\in\mathcal{P},\ \lambda\in A_\epsilon \pmod{16\epsilon},\ N\tilde{\epsilon}<N\lambda\leqslant x/N\epsilon\}.$$

As $\#A_\epsilon$ plays an important part in the main term, we list its value in the following lemma with proof postponed in the end of this subsection.

Lemma 3.2. *Let $\phi(16\epsilon)$ be the number of $(\mathbb{Z}[i]/16\epsilon\mathbb{Z}[i])^\times$. Then*

$$\#A_\epsilon=\frac{\phi(16\epsilon)}{2^{k+4}}.$$

Like Cremona and Odoni [2], we use the notation

$$\sum_{N\eta\in A}^{*}f(\eta)$$

to denote $\sum_{\eta\in T'(\infty),N\eta\in A}f(\eta)$ if A is a set consisting of positive integers. Let $\mu=(\log x)^{100}$ and $\nu=\exp(\frac{\log x}{(\log\log x)^{100}})$. Then the following Lemma 3.3 is parallel to [2, Lemma 3.1].

Lemma 3.3. *If either $m=20,n=\mu$ or $m=\nu,n=x^{\frac{k-1}{k}}$, then we have*

$$\sum_{m<N\eta\leqslant n}^{*}\mathrm{Li}(x/N\eta)=o\bigg(\frac{x\cdot(\log\log x)^{k-1}}{\log x}\bigg),$$

$$\sum_{\mu<N\eta\leqslant\nu}^{*}\mathrm{Li}(x/N\eta)\sim\frac{1}{k-1}\cdot\#T'(x)\cdot\log\log x.$$

Like [2, Lemma 3.1], this lemma can be proved by summation by parts.

Now we can estimate $\#C'_k(x,\alpha,B)$ in (3.10).

First, for $\epsilon \in T'(x)$ with $N\epsilon \leqslant 20$, we have $g(\epsilon) \leqslant \pi(x/N\epsilon)$, since every prime ideal corresponds to exactly one primitive prime element. Here

$$\pi(y) = \sum_{N\mathfrak{p}\leqslant y} 1 \sim \mathrm{Li}(y)$$

by the prime ideal theorem over $\mathbb{Q}(i)$. So all those ϵ with $N\epsilon \leqslant 20$ contribute $O(\frac{x}{\log x})$ to $\#C'_k(x,\alpha,B)$.

Second, for $\epsilon \in T'(x)$ with $20 < N\epsilon \leqslant \mu$, similarly we have $g(\epsilon) = O(\mathrm{Li}(x/N\epsilon))$. Hence these ϵ contribute

$$\sum_{20<N\epsilon\leqslant\mu} O(\mathrm{Li}(x/N\epsilon)) = O\bigg(\sum_{20<N\epsilon\leqslant\mu} \mathrm{Li}(x/N\epsilon)\bigg) = o\bigg(\frac{x}{\log x}\cdot(\log\log x)^{k-1}\bigg)$$

to $\#C'_k(x,\alpha,B)$ by Lemma 3.3.

Similarly, for those $\epsilon \in T'(x)$ with $N\epsilon$ belonging to $(\nu, x^{\frac{k-1}{k}}]$, they also contribute $o(\frac{x}{\log x}\cdot(\log\log x)^{k-1})$ to $\#C'_k(x,\alpha,B)$. While for those $N\epsilon > x^{\frac{k-1}{k}}$, they have no contribution. In fact, we have $N\tilde{\epsilon} > x^{\frac{1}{k}}$ in this case, but this contradicts that $N\tilde{\epsilon} < N\lambda \leqslant x/N\epsilon < x^{\frac{1}{k}}$.

Consequently we obtain

$$\#C'_k(x,\alpha,B) \sim \frac{1}{2}\sideset{}{^*}\sum_{\mu<N\epsilon\leqslant\nu} \pi'(x/N\epsilon, A_\epsilon, 16\epsilon) - \frac{1}{2}\sideset{}{^*}\sum_{\mu<N\epsilon\leqslant\nu} \pi'(N\tilde{\epsilon}, A_\epsilon, 16\epsilon)$$

with $\pi'(y,A,\gamma)$ defined under (3.3). The second sum of the above formula is bounded by

$$\sideset{}{^*}\sum_{\mu<N\epsilon\leqslant\nu} \pi'(N\tilde{\epsilon}, A_\epsilon, 16\epsilon) \leqslant \nu\cdot O\bigg(\frac{\nu}{\log\nu}\bigg) = O\bigg(\frac{\nu^2}{\log\nu}\bigg) = o\bigg(\frac{x}{\log x}\cdot(\log\log x)^{k-1}\bigg).$$

Therefore we have

$$\#C'_k(x,\alpha,B) \sim \frac{1}{2}\sideset{}{^*}\sum_{\mu<N\epsilon\leqslant\nu} \pi'(x/N\epsilon, A_\epsilon, 16\epsilon). \tag{3.11}$$

Like the case $k=1$, we transform from primes contributing to $\pi'(x/N\epsilon, A_\epsilon, 16\epsilon)$ to prime ideals as follows. We define $\mathfrak{c} = \mathfrak{c}_\epsilon$ to be the ideal generated by 16ϵ. Then we have the following exact sequence

$$1 \to \mathbb{Z}[i]^\times \to (\mathbb{Z}[i]/\mathfrak{c})^\times \xrightarrow{f} I(\mathfrak{c})/P_\mathfrak{c} \to 1\cdot \tag{3.12}$$

If we denote $\mathfrak{A}_\epsilon = f(A_\epsilon)$, then like (3.5) and (3.6) we get $\pi'(x, A_\epsilon, 16\epsilon) = \pi(x, \mathfrak{A}_\epsilon, \mathfrak{c})$ and

$$\#\mathfrak{A}_\epsilon = \#A_\epsilon, \tag{3.13}$$

where $\pi(x,\mathfrak{A}_\epsilon,\mathfrak{c})$ is defined under (3.4). Hence by (3.11), we reduce to estimating

$$\sideset{}{^*}\sum_{\mu<N\epsilon\leqslant\nu} \pi(x/N\epsilon, \mathfrak{A}_\epsilon, \mathfrak{c}).$$

Via the standard relation of $\pi(y,\mathfrak{A},\mathfrak{c})$ and $\psi(y,\mathfrak{A},\mathfrak{c})$, we only need to estimate

$$\sideset{}{^*}\sum_{\mu<N\epsilon\leqslant\nu} \psi(x/N\epsilon, \mathfrak{A}_\epsilon, \mathfrak{c}), \tag{3.14}$$

where

$$\psi(y,\mathfrak{A},\mathfrak{c}) := \sum_{\substack{N\mathfrak{a}\leqslant y\\ \mathfrak{a}\in\mathfrak{A}\bmod P_\mathfrak{c}}} \Lambda(\mathfrak{a}).$$

By the orthogonality of characters and the exact sequence (3.12), we have

$$\psi(y,\mathfrak{A}_\epsilon,\mathfrak{c})=\frac{4}{\phi(16\epsilon)}\sum_{\chi \bmod \mathfrak{c}_\epsilon}\psi(y,\chi)\sum_{[\mathfrak{a}]\in\mathfrak{A}_\epsilon}\overline{\chi(\mathfrak{a})}.$$

Here χ runs over all the characters of $I(\mathfrak{c})/P_{\mathfrak{c}}$, and

$$\psi(y,\chi):=\sum_{N\mathfrak{a}\leqslant y}\chi(\mathfrak{a})\Lambda(\mathfrak{a}).$$

Separating out all the principal characters $\chi_0 \bmod \mathfrak{c}_\epsilon$ from $\chi \bmod \mathfrak{c}_\epsilon$, we get

$$\sum_{\mu<N\epsilon\leqslant\nu}^{*}\psi(x/N\epsilon,\mathfrak{A}_\epsilon,\mathfrak{c})=(I)+\sum_{\mu<N\epsilon\leqslant\nu}^{*}\frac{4}{\phi(16\epsilon)}\sum_{\chi \bmod \mathfrak{c}_\epsilon}{}'\psi(x/N\epsilon,\chi)\sum_{[\mathfrak{a}]\in\mathfrak{A}_\epsilon}\overline{\chi(\mathfrak{a})}. \tag{3.15}$$

Here (I) is the main term given by

$$(\mathrm{I}):=\sum_{\mu<N\epsilon\leqslant\nu}^{*}\frac{4\cdot\#\mathfrak{A}_\epsilon}{\phi(16\epsilon)}\cdot\psi(x/N\epsilon,\chi_0)$$

and $\sum'$ denotes the sum over all non-principal characters of a fixed modulus.

To estimate the contribution of the non-principal characters in (3.15), we have to separate out those terms with possible Siegel zeros. To this purpose, let $\dagger_1$ be the conductor of the exceptional primitive character in Proposition 2.3(2) with $z=16^2\nu$. Separating out all the non-principal characters of modulus multiple of $\dagger_1$ in (3.15), we get

$$\sum_{\mu<N\epsilon\leqslant\nu}^{*}\psi(x/N\epsilon,\mathfrak{A}_\epsilon,\mathfrak{c})=:(\mathrm{I})+(\mathrm{II})+(\mathrm{III}).$$

Here

$$(\mathrm{II}):=\sum_{\substack{\mu<N\epsilon\leqslant\nu,\\ \dagger_1\mid\mathfrak{c}_\epsilon}}^{*}\frac{4}{\phi(16\epsilon)}\sum_{\chi \bmod \mathfrak{c}_\epsilon}{}'\psi(x/N\epsilon,\chi)\sum_{[\mathfrak{a}]\in\mathfrak{A}_\epsilon}\overline{\chi(\mathfrak{a})},$$

$$(\mathrm{III}):=\sum_{\substack{\mu<N\epsilon\leqslant\nu,\\ \dagger_1\nmid\mathfrak{c}_\epsilon}}^{*}\frac{4}{\phi(16\epsilon)}\sum_{\chi \bmod \mathfrak{c}_\epsilon}{}'\psi(x/N\epsilon,\chi)\sum_{[\mathfrak{a}]\in\mathfrak{A}_\epsilon}\overline{\chi(\mathfrak{a})}.$$

(I)–(III) are estimated in the following lemma.

Lemma 3.4. *We have the following estimations*:

$$(\mathrm{I})\sim\frac{1}{(k-1)\cdot 2^{k+2}}\cdot\#T'(x)\cdot\log x\cdot\log\log x,$$
$$(\mathrm{II})=O(x\log^{-99}\nu),$$
$$(\mathrm{III})=o\bigg(\frac{x}{\log x}\bigg).$$

We postpone the proof of this lemma. From this lemma and the bijection (3.9), we arrive at

$$\sum_{\mu<N\epsilon\leqslant\nu}^{*}\psi(x/N\epsilon,\mathfrak{A}_\epsilon,\mathfrak{c})\sim\frac{1}{(k-1)\cdot 2^{k+2}}\cdot\#T(x)\cdot\log x\cdot\log\log x.$$

Hence from the equations (3.8) and (3.11), we have

$$\#C_k'(x,\alpha,B)\sim\frac{1}{(k-1)\cdot 2^{k+3}}\cdot\#T(x)\cdot\log\log x$$

$$\sim \frac{1}{(k-1)\cdot 2^{\binom{k}{2}+3k+1}}\cdot \log\log x\cdot \#C_{k-1}(x)$$
$$\sim \frac{1}{2^{\binom{k}{2}+3k+1}}\cdot \#C_k(x).$$

For the case $z_k=1$, we can prove similarly. Thus from the bijection (3.2), we complete the proof of Theorem 1.4. □

Now we prove Lemma 3.4.

Proof of Lemma 3.4. Now we estimate the first sum (I). By (3.13) and Lemma 3.2, we have $\#\mathfrak{A}_\epsilon=\frac{\phi(16\epsilon)}{2^{k+4}}$. Then Lemma 3.3 implies that

$$\begin{aligned}(\mathrm{I})&=\frac{1}{2^{k+2}}\sideset{}{^*}\sum_{\mu<N\epsilon\leqslant\nu}\psi(x/N\epsilon)=\frac{1+o(1)}{2^{k+2}}\sideset{}{^*}\sum_{\mu<N\epsilon\leqslant\nu}\log(x/N\epsilon)\mathrm{Li}(x/N\epsilon)\\&=\frac{1+o(1)}{2^{k+2}}\cdot\log x\sideset{}{^*}\sum_{\mu<N\epsilon\leqslant\nu}\mathrm{Li}(x/N\epsilon)\\&\sim\frac{1}{(k-1)\cdot 2^{k+2}}\cdot\#T'(x)\cdot\log x\cdot\log\log x.\end{aligned}$$

Next, we prove the second estimation. The trivial estimation gives

$$(\mathrm{II})\ll\sideset{}{^*}\sum_{\substack{\mu<N\epsilon\leqslant\nu,\\ \dagger_1|\mathfrak{c}_\epsilon}}\psi(x/N\epsilon)\ll x\sideset{}{^*}\sum_{\substack{\mu<N\epsilon\leqslant\nu,\\ \dagger_1|\mathfrak{c}_\epsilon}}(N\epsilon)^{-1}.$$

For the last sum, we have

$$\sideset{}{^*}\sum_{\substack{\mu<N\epsilon\leqslant\nu,\\ \dagger_1|\mathfrak{c}_\epsilon}}(N\epsilon)^{-1}=\sum_{\substack{\mu<N\epsilon\leqslant\nu,\\ \dagger_1|\mathfrak{c}_\epsilon,\epsilon\in T'(\infty)}}(N\epsilon)^{-1}=\sum_{\mu<N\dagger_1 s\leqslant\nu}(N\dagger_1)^{-1}\cdot s^{-1}\sum_{\substack{\epsilon\in T'(\infty),\dagger_1|\mathfrak{c}_\epsilon\\ N\epsilon=N\dagger_1\cdot s}}1.$$

But for any s, the following holds:

$$\sum_{\substack{\epsilon\in T'(\infty),\dagger_1|\mathfrak{c}_\epsilon\\ N\epsilon=N\dagger_1\cdot s}}1\ll 1.$$

Therefore

$$(\mathrm{II})\ll xN\dagger_1^{-1}\sum_{\mu<sN\dagger_1\leqslant\nu}s^{-1}\leqslant xN\dagger_1^{-1}\cdot\log\nu. \tag{3.16}$$

To finish the estimation, we have to bound $N\dagger_1$ from below. By the Page theorem part of Proposition 2.3 with $z=16^2\nu$, the Siegel zero β of the primitive character with modulus $\dagger_1$ satisfies

$$\beta>1-\frac{c_0}{\log(16^2\nu)}.$$

By the Siegel theorem part of Proposition 2.3, for any $\epsilon_0>0$, there is a $c(\epsilon_0,2)$ such that

$$\beta\leqslant 1-c(\epsilon_0,2)D^{-\epsilon_0},$$

where $D=4N\dagger_1$. Thus if we choose $\epsilon_0=\frac{1}{200}$, then $N\dagger_1>\log^{100}\nu$. Hence (3.16) implies

$$(\mathrm{II})\ll x\log^{-99}\nu.$$

Finally, we estimate the third sum (III). There is no Siegel zero involved in the explicit formula (2.2). So for any $\psi(x/N\epsilon,\chi)$ in the sum (III), there exists a positive constant c such that

$$\psi(x/N\epsilon,\chi)\ll\frac{x}{N\epsilon}\cdot\log^2 x\cdot\exp\left(-\frac{c\log(x/N\epsilon)}{\log N\epsilon}\right)+\frac{x}{N\epsilon^5}\log^2 x+x^{\frac{1}{4}}N\epsilon^{-\frac{1}{4}}\log(x/N\epsilon),$$

where we have chosen $T = N\epsilon^4$ and used $N\dagger \leqslant 16^2 N\epsilon$ in (2.2). Corresponding to these three terms, (III) is divided into three subsums

$$(\mathrm{III}) = \Sigma_1 + \Sigma_2 + \Sigma_3.$$

They can be estimated as follows:

$$\begin{aligned}
\Sigma_1 &= x\log^2 x \sideset{}{^*}\sum_{\substack{\mu<N\epsilon\leqslant\nu,\\ \dagger_1\nmid\mathfrak{k}_\epsilon}} \frac{1}{N\epsilon}\cdot\exp\bigg(-c\frac{\log x/N\epsilon}{\log N\epsilon}\bigg)\\
&\ll x\log^2 x\cdot\exp(-c'(\log\log x)^{100})\cdot \sideset{}{^*}\sum_{\substack{\mu<N\epsilon\leqslant\nu,\\ \dagger_1\nmid\mathfrak{k}_\epsilon}} \frac{1}{N\epsilon}\\
&\ll x\log^3 x\cdot\exp(-c'(\log\log x)^{100}),\\
\Sigma_2 &= x\log^2 x \sideset{}{^*}\sum_{\substack{\mu<N\epsilon\leqslant\nu,\\ \dagger_1\nmid\mathfrak{k}_\epsilon}} N\epsilon^{-5} \ll x\log^2 x\cdot\mu^{-4}\ll x\log^{-200} x,\\
\Sigma_3 &\ll x^{\frac14}\log x \sideset{}{^*}\sum_{\substack{\mu<N\epsilon\leqslant\nu,\\ \dagger_1\nmid\mathfrak{k}_\epsilon}} N\epsilon^{-\frac14}\ll x^{\frac14}\log x\cdot\nu^{\frac34}\ll x^{\frac12}.
\end{aligned}$$

Therefore we arrive at

$$(\mathrm{III}) = o\bigg(\frac{x}{\log x}\bigg).$$

This completes the proof of Lemma 3.4. □

Now we prove Lemma 3.2.

Proof of Lemma 3.2. According to (i), (ii) and Lemma 2.1, we know that A_ϵ represents those primary classes $a \pmod{16\epsilon}$ such that

(i′) $Na \equiv \alpha_k \pmod{16}$ and $(\frac{Na}{N\lambda_j}) = (-1)^{B_{jk}}$ for $1\leqslant j\leqslant k-1$, and

(ii′) $(\frac{2}{a})_4(\frac{a}{\theta_1}) = (\frac{2}{\epsilon})_4(\frac{\epsilon/\theta_1}{\theta_1})(-1)^{\frac{\prod_1^k\alpha_j-1}{8}+\frac{\prod_1^k\alpha_j^{z_j}-5}{4}}$.

From Chinese Remainder Theorem, we have the following identification:

$$(\mathbb{Z}[i]/16\epsilon\mathbb{Z}[i])^\times \simeq (\mathbb{Z}[i]/16\mathbb{Z}[i])^\times\times\prod_{j=1}^{k-1}(\mathbb{Z}[i]/\lambda_j\mathbb{Z}[i])^\times$$

given by $a\mapsto(a_0,a_1,\ldots,a_{k-1})$, where a_j is the corresponding image of a modulo λ_j and $\lambda_0=16$. Then the residue symbol $(\frac{\cdot}{\theta_1})$ is trivial on those $(\mathbb{Z}[i]/\lambda_j\mathbb{Z}[i])^\times$-components with $\lambda_j\nmid\theta_1$, and other residue symbols have similar properties. As $p_j = N\lambda_j$ splits completely in $\mathbb{Z}[i]$ for $1\leqslant j\leqslant k-1$, the norm map induces an isomorphism $(\mathbb{Z}[i]/\lambda_j\mathbb{Z}[i])^\times\simeq(\mathbb{Z}/p_j\mathbb{Z})^\times$. Hence the condition $(\frac{Na_j}{N\lambda_j})=1$ selects a half of the $(\mathbb{Z}[i]/\lambda_j\mathbb{Z}[i])^\times$-component.

For the component of $(\mathbb{Z}[i]/16\mathbb{Z}[i])^\times$, we use the same notation as Lemma 3.1. Assume that $a_1,\ldots,a_{k-1}$ are chosen such that $(\frac{Na_j}{N\lambda_j})=1$ for $1\leqslant j\leqslant k-1$. Then the remaining conditions of (i′) and (ii′) are equivalent to finding $g\in G$ such that

$$\chi_1(g) = i^{\frac{\alpha_k-1}{4}},\quad \chi_2(g) = i^\delta. \tag{3.17}$$

Here,

$$i^\delta = \bigg(\frac{2}{\epsilon}\bigg)_4\bigg(\frac{\epsilon/\theta_1}{\theta_1}\bigg)\cdot\prod_{\lambda_j\mid\theta_1}\bigg(\frac{a_j}{\lambda_j}\bigg)\cdot(-1)^{\frac{\prod_1^k\alpha_j-1}{8}+\frac{\prod_1^k\alpha_j^{z_j}-5}{4}}.$$

By the equivalence of (1) and (2) of Lemma 3.1, the existence of $g\in G$ such that (3.17) holds is equivalent to $i^{2\cdot\frac{\alpha_k-1}{4}} = i^{2\delta}$. Now we verify this. Using $\prod_{j=1}^k\alpha_j\equiv1 \pmod 8$, we get

$$i^{2\delta} = \bigg(\frac{2^2}{\eta}\bigg)_4 = \bigg(\frac{2}{N\eta}\bigg) = \bigg(\frac{2}{\alpha_1\cdots\alpha_{k-1}}\bigg) = \bigg(\frac{2}{\alpha_k}\bigg),$$

while $i^{2\cdot\frac{\alpha_k-1}{4}}=(-1)^{\frac{\alpha_k-1}{4}}=(\frac{2}{\alpha_k})=i^{2\delta}$. (3.17) selects an eighth of G, similar to Lemma 3.1. Consequently,

$$\#A_\epsilon=\frac{\phi(16\epsilon)}{2^{k+4}}.$$

This completes the proof of the lemma. □

4 Distribution of congruent elliptic curves

In this section, we will prove the main results (see Theorems 1.1 and 1.3) of this paper.

4.1 Gauss genus theory

We first introduce some conceptions related to 4-rank of ideal class group. We refer to Section 3 of our previous paper [15]. Let $n=p_1\cdots p_k\equiv 1 \pmod 8$ in Q_k. Denote by $\mathcal{A}=\mathcal{A}_n$ the ideal class group of $\mathbb{Q}(\sqrt{-n})$. Assume that the group operation of $\mathcal{A}$ is written additively. Hence $2^j\mathcal{A}$ denotes the subgroup consisting of 2^j-powers of ideal classes of $\mathcal{A}$, where j is a positive integer. Then the 2^j-rank $h_{2^j}(n)$ of $\mathcal{A}$ is defined to be $\dim_{\mathbb{F}_2}2^{j-1}\mathcal{A}/2^j\mathcal{A}$. From this definition, we can easily get $h_4(n)=\dim_{\mathbb{F}_2}\mathcal{A}[2]\cap 2\mathcal{A}$, where $\mathcal{A}[2]$ denotes the subgroup consisting of ideal classes with square trivial. Gauss genus theory connects $\mathcal{A}[2]\cap 2\mathcal{A}$ with the kernel of the Rédei matrix R of $\mathbb{Q}(\sqrt{-n})$.

The definition of R is as follows. We assume that the prime divisors of n are arranged such that $p_1<\cdots<p_k$. Then the Rédei matrix $R=R_n$ is a $k\times(k+1)$ matrix over $\mathbb{F}_2$ given by $(A_n\mid\mathfrak{b})$. Here $A=A_n=(a_{ij})_{k\times k}$ and $\mathfrak{b}=([\frac{2}{p_1}],\ldots,[\frac{2}{p_k}])^{\mathrm{T}}$, where $a_{ii}=\sum_{l\neq i}a_{il}$ and $a_{ij}=[\frac{p_j}{p_i}]$ with $i\neq j$. Then Gauss genus theory implies that there is a two to one epimorphism

$$\{X\in\mathbb{F}_2^{k+1}\mid RX=0\}\to\mathcal{A}[2]\cap 2\mathcal{A} \tag{4.1}$$

with kernel $\{0,X_0\}$, where $X_0=(1,\ldots,1,0)^{\mathrm{T}}$. Thus we have $h_4(n)=k-\mathrm{rank}_{\mathbb{F}_2}R$.

Remark 4.1. The original definition of the Rédei matrix has no assumption on the magnitudes of prime factors of n. The purpose of this assumption is to get a unique Rédei matrix; the uniqueness makes the estimation of the number of certain elliptic curves more convenient.

There are two important properties of the matrix $A=A_n$. We first introduce a notion. For a matrix M over $\mathbb{F}_2$, we say that every row sum of M is 0 if the sum of all elements of any of M's given row is 0. Similarly, we can define that every column sum of M is 0. Then every row sum of A is 0 from its definition. In addition, A is symmetric by the quadratic reciprocity law. So from symmetry, every column sum of A is also 0.

4.2 Distribution of $Ш(E^{(n)}/\mathbb{Q})[2^\infty]\simeq(\mathbb{Z}/2\mathbb{Z})^2$

For $n\in Q_k$, [15, Theorem 1.1] characterizes that $n\in P_k$ if and only if

$$h_4(n)=1,\quad h_8(n)\equiv\frac{d-5}{4}\pmod 2, \tag{4.2}$$

where $d=\prod_{j=1}^k p_j^{x_j}$ with $X=(x_1,\ldots,x_k,x_{k+1})^{\mathrm{T}}$ a non-trivial solution to $RX=0$ such that $X\neq X_0$. Since $h_4(n)=1$, by Gauss genus theory (see the epimorphism (4.1)), there are two such choices X and X' with $X+X'=X_0$. Corresponding to X and X', we define d and d' as above. Then $X+X'=X_0$ implies that $d'd=n\equiv 1 \pmod 8$, so $\frac{d-1}{4}\equiv\frac{d'-1}{4} \pmod 2$. Hence either choice does not affect $\frac{d-1}{4}$ (mod 2). Like [15, Proof of Theorem 1.1], (4.2) can be divided into two cases according to rank$A$.

(i) The rank of A is $k-1$. Then $h_4(n)=1$. Let $x=(x_1,\ldots,x_k)^{\mathrm{T}}$ be a non-trivial solution to $Ax=\mathfrak{b}$ and $d=\prod_{j=1}^k p_j^{x_j}$. Then [10, Theorems 3.3(iii) and 3.3(iv)] imply that $h_8(n)=1$ if and only if

$$\left(\frac{2d}{d'}\right)_4\left(\frac{2d'}{d}\right)_4=(-1)^{\frac{n-1}{8}}$$

with $d'd=n$. Then by (3.1), this is equivalent to

$$\left(\frac{\theta'}{\theta}\right)\left(\frac{2}{n}\right)_4=(-1)^{\frac{n-1}{8}},$$

where θ (resp. θ') is the primary integer lying above d (resp. d') with every prime factor in $\mathcal{P}$.

(ii) The rank of A is $k-2$. Then $h_4(n)=1$ if and only if $\mathfrak{b}\notin \mathrm{Im}A$. Let $x=(x_1,\ldots,x_k)^{\mathrm{T}}\neq 0,(1,\ldots,1)^{\mathrm{T}}$ such that $Ax=0$. We define $d=\prod_{j=1}^k p_j^{x_j}$. Then $d\equiv 5 \pmod 8$ and [10, Theorem 3.3(ii)] implies that $h_8(n)=1$ if and only if

$$\left(\frac{d}{d'}\right)_4\left(\frac{d'}{d}\right)_4=-1,$$

where $d'd=n$.

Remark 4.2. We remark that there is a typo in [10, Theorem 3.3(iv)], which is corrected in (i).

Now we begin to prove Theorem 1.1. Recall that our strategy is to count $n\leqslant x$ with prime factors in given residue classes modulo 16 and residue symbols among its prime factors with given compatible values. The latter implies that the A_n-matrix of n is a given one over $\mathbb{F}_2$. From this and the two possibilities of rank$A$, we denote by $\mathcal{B}=\mathcal{B}_k$ the set of all the $k\times k$ symmetric $\mathbb{F}_2$ matrices with rank $k-1$ and every row sum 0; similarly we use $\mathcal{B}_*$ to denote those $k\times k$ symmetric $\mathbb{F}_2$ matrices with rank $k-2$ and every row sum 0. According to $A_n\in\mathcal{B}$ or $\mathcal{B}_*$, we can divide the proof into two parts.

First, we estimate the contribution of n with rank$A_n=k-1$ to $\#P_k(x)$. Let $\mathcal{I}$ denote the set of $\alpha=(\alpha_1,\ldots,\alpha_k)$ such that all $\alpha_j\in\{1,5,9,13\}$ and $\prod_{j=1}^k\alpha_j\equiv 1 \pmod 8$. Given any $\alpha\in\mathcal{I}$ and $B\in\mathcal{B}=\mathcal{B}_k$, the contribution of those $n=p_1\cdots p_k\leqslant x$ satisfying

- $p_1<\cdots<p_k$,
- $A_n=B$, and
- $p_j\equiv\alpha_j \pmod{16}$ for $1\leqslant j\leqslant k$

to $\#P_k(x)$ is $\#C_k(x,\alpha,B)$ by (i). If $B\neq\tilde{B}\in\mathcal{B}$ or $\alpha\neq\tilde{\alpha}\in\mathcal{I}$, then $C_k(x,\alpha,B)$ and $C_k(x,\tilde{\alpha},\tilde{B})$ are disjoint. Therefore the contribution of all those $n\in Q_k(x)$ with $A_n\in\mathcal{B}$ to $\#P_k(x)$ is

$$\Sigma_1=\sum_{B\in\mathcal{B}}\sum_{\alpha\in\mathcal{I}}\#C_k(x,\alpha,B).$$

By the independence property of residue symbols (see Theorem 1.4), this asymptotically equals

$$2^{-1-\binom{k}{2}-3k}\cdot\#C_k(x)\cdot\sum_{B\in\mathcal{B}}\sum_{\alpha\in\mathcal{I}}1=2^{-2-k-\binom{k}{2}}\cdot\#C_k(x)\cdot\#\mathcal{B},$$

where we have used $\#\mathcal{I}=2^{2k-1}$. So we reduce to computing $\#\mathcal{B}$, which can be accomplished by the following result of Brown et al. [1].

Proposition 4.3. *For non-negative integers $r\leqslant k$, let $\mathcal{B}_{k,r}$ denote all the $k\times k$ symmetric matrices over $\mathbb{F}_2$ with rank r. Then*

$$\#\mathcal{B}_{k,r}=2^{\binom{r+1}{2}}\cdot u_{r+1}\cdot\prod_{i=0}^{k-r-1}\frac{2^k-2^i}{2^{k-r}-2^i},$$

where u_r is defined in Theorem 1.1.

Given any $B\in\mathcal{B}$, we delete the last row and column of B. Then we get a $B'\in\mathcal{B}_{k-1,k-1}$. Since every row sum of B is 0 and B is symmetric, we obtain a one to one correspondence between $\mathcal{B}$ and $\mathcal{B}_{k-1,k-1}$. Hence Proposition 4.3 implies that

$$\#\mathcal{B}=\#\mathcal{B}_k=2^{\binom{k}{2}}\cdot u_k. \tag{4.3}$$

So we arrive at

$$\Sigma_1\sim 2^{-2-k}\cdot u_k\cdot\#C_k(x).$$

Second, we estimate the contribution of n with $A_n \in \mathcal{B}_*$ to $\#P_k(x)$. Then this implies that $k \geqslant 2$. Let $B \in \mathcal{B}_*$. We denote by $\mathcal{I}_B$ the set of $\alpha = (\alpha_1, \ldots, \alpha_k)$ with all $\alpha_j \in \{1, 5, 9, 13\}$ and $\prod_{j=1}^k \alpha_j \equiv 1 \pmod 8$ such that

$$\mathrm{rank}_{\mathbb{F}_2}(B \mid \mathfrak{b}_\alpha) = k - 1.$$

Here $\mathfrak{b}_\alpha = ([\frac{2}{\alpha_1}], \ldots, [\frac{2}{\alpha_k}])^{\mathrm{T}}$. Given $\alpha \in \mathcal{I}_B$, the contribution of those $n = p_1 \cdots p_k \leqslant x$ with

- $p_1 < \cdots < p_k$,
- $A_n = B$, and
- $p_j \equiv \alpha_j \pmod{16}$ for $1 \leqslant j \leqslant k$

to $\#P_k(x)$ is $\#C_k(x, \alpha, B)_*$. Here $C_k(x, \alpha, B)_*$ is defined to be all $n = p_1 \cdots p_k \in C_k(x)$ with $p_1 < \cdots < p_k$ satisfying

- $p_l \equiv \alpha_l \pmod{16}$ for $1 \leqslant l \leqslant k$,
- $(\frac{p_l}{p_j}) = (-1)^{B_{lj}}$ for $1 \leqslant l < j \leqslant k$, and
- $(\frac{d}{d'})_4 (\frac{d'}{d})_4 = -1$.

Here $d'd = n$ and $d = \prod_{j=1}^k p_j^{x_j}$ with $x = (x_1, \ldots, x_k)^{\mathrm{T}} \neq (1, \ldots, 1)^{\mathrm{T}}$ a non-trivial solution to $Ax = 0$. Like Theorem 1.4, we have the following independence property of residue symbols:

$$\#C_k(x, \alpha, B)_* \sim 2^{-1-3k-\binom{k}{2}} \cdot \#C_k(x). \tag{4.4}$$

Given $n = p_1 \cdots p_k \in Q_k(x)$ with $p_1 < \cdots < p_k$, we define $\alpha(n)$ to be the unique $\alpha \in \mathcal{I}$ (not $\mathcal{I}_{A_n}$) such that $\alpha_j \equiv p_j \pmod{16}$ for $1 \leqslant j \leqslant k$. Then the contribution of all $n \in Q_k(x)$ with $A_n \in \mathcal{B}_*$ and $\alpha(n) \in \mathcal{I}_{A_n}$ to $\#P_k(x)$ is

$$\Sigma_2 = \sum_{B \in \mathcal{B}_*} \sum_{\alpha \in \mathcal{I}_B} \#C_k(x, \alpha, B)_* \sim 2^{-1-3k-\binom{k}{2}} \sum_{B \in \mathcal{B}_*} \sum_{\alpha \in \mathcal{I}_B} \#C_k(x).$$

Therefore we reduce to counting $\#\mathcal{B}_*$ and $\#\mathcal{I}_B$.

Now we count $\#\mathcal{B}_*$. Performing the same operations on B as the case $B \in \mathcal{B}$, we obtain a $B' \in \mathcal{B}_{k-1,k-2}$. Moreover, we also get a one to one correspondence between $\mathcal{B}_*$ and $\mathcal{B}_{k-1,k-2}$. Thus from Proposition 4.3 we have

$$\#\mathcal{B}_* = 2^{\binom{k-1}{2}} \cdot u_{k-1} \cdot (2^{k-1} - 1). \tag{4.5}$$

Now we count $\#\mathcal{I}_B$ with $B \in \mathcal{B}_*$. We divide this into two steps.

First, we count the number of $\mathbb{F}_2$-matrix $\mathfrak{b} = \mathfrak{b}_{k\times 1}$ such that

(1) the sum of all elements of $\mathfrak{b}$ is 0, and

(2) $\mathrm{rank}_{\mathbb{F}_2}(B \mid \mathfrak{b}) = k - 1$.

Deleting the last element of $\mathfrak{b}$ and the last row and column of B, we know that $(B \mid \mathfrak{b})$ corresponds to $(B' \mid \mathfrak{b}')$. This correspondence is also one to one. As the rank of $(B' \mid \mathfrak{b}')$ is $k-1$ and that of B' is $k-2$, $\mathfrak{b}'$ is not in the image of B'. Thus there are exactly 2^{k-2} many such $\mathfrak{b}'$. Hence there are 2^{k-2} such $\mathfrak{b}$.

Next, we want to count the number of $\alpha \in \mathcal{I}_B$ such that $\mathfrak{b}_\alpha = \mathfrak{b}$, where $\mathfrak{b} = \mathfrak{b}_{k\times 1}$ is any given $\mathbb{F}_2$ matrix satisfying (1) and (2). Note that $b_{\alpha,j} = [\frac{2}{\alpha_j}] = b_j$ determines $\alpha_j \pmod 8$ for any $1 \leqslant j \leqslant k$. Then any α_j has exactly two choices. Therefore there are 2^k many $\alpha \in \mathcal{I}_B$ such that $\mathfrak{b}_\alpha = \mathfrak{b}$. Consequently, we have

$$\#\mathcal{I}_B = 2^{2k-2}. \tag{4.6}$$

Thus from (4.5) and (4.6), Σ_2 asymptotically equals

$$2^{-1-3k-\binom{k}{2}} \#\mathcal{B}_* \cdot 2^{2k-2} \cdot \#C_k(x) = 2^{-2-2k}(2^{k-1} - 1) u_{k-1} \cdot \#C_k(x).$$

From (i) and (ii), we know $\#P_k(x) = \Sigma_1 + \Sigma_2$. Therefore,

$$\#P_k(x) \sim 2^{-2-k}(u_k + (2^{-1} - 2^{-k}) u_{k-1}) \cdot \#C_k(x).$$

So we finish the proof of Theorem 1.1.

4.3 Distribution of $Ш(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^4$

In this subsection, we bound the number of congruent elliptic curves $E^{(n)}$ with $\mathrm{rank}_{\mathbb{Z}}E^{(n)}(\mathbb{Q}) = 0$ and $Ш(E^{(n)}/\mathbb{Q})[2^\infty] \simeq (\mathbb{Z}/2\mathbb{Z})^4$.

For a positive integer $k \geqslant 2$, we denote by $\tilde{Q}_k(x)$ the set of $n \in Q_k(x)$ with all prime factors congruent to 1 modulo 8. Let l and l' be positive integers. Assume that $n = dd' \in \tilde{Q}_{l+l'}(x)$ with $\omega(d) = l$ and $\omega(d') = l'$ such that

(i) $(\frac{p}{p'}) = 1$ for any prime divisor p of d and p' of d',

(ii) $h_4(d) = h_4(d') = 1$, and

(iii) $(\frac{2}{d})_4 = (-1)^{\frac{d-9}{8}}$, $(\frac{2}{d'})_4 = (-1)^{\frac{d'-9}{8}}$ and $(\frac{d}{d'})_4 = (\frac{d'}{d})_4 = 1$.

Here $\omega(d)$ is the number of prime factors of d. [15, Theorem 1.2 and Remark 4.7] imply that $n \in \tilde{P}_{l+l'}(x)$. In fact, [15, Theorem 4.5 and Corollary 4.6] give more general conditions such that $n \in \tilde{P}_{l+l'}(x)$. But for notational simplicity, we only consider (i)–(iii).

In order to count the number of those n satisfying (i)–(iii), we need some notation. Let $\sigma = \{\sigma_i\}_{i=1}^{l}$ be a strictly ascending subsequence of $1, \ldots, l+l'$. Then we denote by $\sigma' = \{\sigma'_i\}_{i=1}^{l'}$ the remained increasing subsequence of $1, \ldots, l+l'$ by deleting those elements of σ. Let $\mathcal{S}$ denote the set consisting of all the σ. Then $\#\mathcal{S} = \binom{l+l'}{l}$. Denote by $\mathcal{R}$ the set of $\alpha = (\alpha_1, \ldots, \alpha_{l+l'})$ with every $\alpha_j \in \{1, 9\}$. Then $\#\mathcal{R} = 2^{l+l'}$. Recall that $\mathcal{B}_l$ denotes all the $l \times l$ symmetric $\mathbb{F}_2$ matrices with rank $l-1$ and every row sum 0. In addition, A_n is the symmetric matrix occurred in the definition of the Rédei matrix of the ideal class group of $\mathbb{Q}(\sqrt{-n})$.

For $\alpha \in \mathcal{R}$, $B \in \mathcal{B}_l, B' \in \mathcal{B}_{l'}$ and $\sigma \in \mathcal{S}$, we denote by $C_{l,l'}(x, \alpha, B, B', \sigma)$ those $n = p_1 \cdots p_{l+l'} \in \tilde{Q}_{l+l'}(x)$ with $p_1 < \cdots < p_{l+l'}$ such that

- $p_j \equiv \alpha_j \pmod{16}$ for $1 \leqslant j \leqslant l+l'$,
- $A_d = B$ and $A_{d'} = B'$ with $d = \prod_{j=1}^{l} p_{\sigma_j}$ and $d' = \prod_{j=1}^{l'} p_{\sigma'_j}$,
- $(\frac{p}{p'}) = 1$ for any prime divisor p of d and p' of d',
- $(\frac{2}{d})_4 = (-1)^{\frac{\delta-9}{8}}$ and $(\frac{2}{d'})_4 = (-1)^{\frac{\delta'-9}{8}}$ with $\delta = \prod_{j=1}^{l} \alpha_{\sigma_j}$ and $\delta' = \prod_{j=1}^{l'} \alpha_{\sigma'_j}$, and
- $(\frac{d}{d'})_4 = (\frac{d'}{d})_4 = 1$.

Similarly to the independence property of residue symbols, namely Theorem 1.4, we have

$$\#C_{l,l'}(x, \alpha, B, B', \sigma) \sim \frac{1}{2^{4+3(l+l')+\binom{l+l'}{2}}} \cdot \#C_{l+l'}(x).$$

Moreover, from (i)–(iii) we know that $C_{l,l'}(x, \alpha, B, B', \sigma)$ is contained in $\tilde{P}_{l+l'}(x)$. The following lemma shows that the sets $C_{l,l'}(x, \alpha, B, B', \sigma)$ are mutually disjoint up to the trivial overlap $C_{l,l'}(x, \alpha, B, B', \sigma) = C_{l',l}(x, \alpha, B', B, \sigma')$.

Lemma 4.4. *For positive integers $\tilde{l}$ and $\tilde{l}'$ with $\tilde{l} + \tilde{l}' = l + l'$, we define $\tilde{\sigma}$ and $\tilde{\mathcal{S}}$ similarly. Assume that $\tilde{\alpha} \in \mathcal{R}, \tilde{B} \in \mathcal{B}_{\tilde{l}}, \tilde{B}' \in \mathcal{B}_{\tilde{l}'}$ and $\tilde{\sigma} \in \tilde{\mathcal{S}}$. If $(\tilde{\alpha}, \tilde{\sigma}, \tilde{B}, \tilde{B}') \neq (\alpha, \sigma, B, B')$ and (α, σ', B', B), then*

$$C_{l,l'}(x, \alpha, B, B', \sigma) \cap C_{\tilde{l},\tilde{l}'}(x, \tilde{\alpha}, \tilde{B}, \tilde{B}', \tilde{\sigma}) = \emptyset.$$

We postpone the proof of this lemma in the end of this subsection. Then the contribution of those $C_{l,l'}(x, \alpha, B, B', \sigma)$ with $\alpha \in \mathcal{R}$, $B \in \mathcal{B}_l, B' \in \mathcal{B}_{l'}, \sigma \in \mathcal{S}, 1 \leqslant l \leqslant k-1$ and $l + l' = k$ to $\#\tilde{P}_k(x)$ is

$$\begin{aligned}
&\frac{1}{2} \sum_{l+l'=k} \sum_{\alpha \in \mathcal{R}} \sum_{B \in \mathcal{B}_l} \sum_{B' \in \mathcal{B}_{l'}} \sum_{\sigma \in \mathcal{S}} \#C_{l,l'}(x, \alpha, B, B', \sigma) \\
&\quad \sim \frac{1}{2} \sum_{l+l'=k} \frac{\#\mathcal{R} \cdot \#\mathcal{B}_l \cdot \#\mathcal{B}_{l'} \cdot \#\mathcal{S}}{2^{4+3(l+l')+\binom{l+l'}{2}}} \cdot \#C_{l+l'}(x) \\
&\quad = \sum_{l+l'=k} \frac{u_l u_{l'} \cdot \binom{l+l'}{l} \cdot 2^{(l+l')+\binom{l}{2}+\binom{l'}{2}}}{2^{5+3(l+l')+\binom{l+l'}{2}}} \cdot \#C_k(x) \\
&\quad = \sum_{l+l'=k} \frac{u_l u_{l'} \cdot \binom{k}{l}}{2^{5+2k+ll'}} \cdot \#C_k(x).
\end{aligned}$$

Here we have used (4.3). This completes the proof of Theorem 1.3.

Now we prove Lemma 4.4.

Proof of Lemma 4.4. If n satisfies (i) and (ii), then $\mathrm{rank}_{\mathbb{F}_2} A_n = l + l' - 2 = \omega(n) - 2$ by Gauss genus theory in Subsection 4.1.

Note that if $\tilde{\alpha} \neq \alpha$. Then the lemma holds trivially. So we may assume that $\tilde{\alpha} = \alpha$.

If $\tilde{\sigma} \neq \sigma$ and σ', then at least three of the following increasing sequences are non-empty:

$$\sigma \cap \tilde{\sigma}, \quad \sigma \cap \tilde{\sigma}', \quad \sigma' \cap \tilde{\sigma}, \quad \sigma' \cap \tilde{\sigma}'.$$

Assume that $n \in C_{l,l'}(x, \alpha, B, B', \sigma) \cap C_{\tilde{l},\tilde{l}'}(x, \tilde{\alpha}, \tilde{B}, \tilde{B}', \tilde{\sigma})$. Then we denote by d_1 the product of those prime factors of n indexed by $\sigma \cap \tilde{\sigma}$. Similarly, d_2, d_3 and d_4 are the products of prime factors of n indexed by $\sigma \cap \tilde{\sigma}', \sigma' \cap \tilde{\sigma}$ and $\sigma' \cap \tilde{\sigma}'$, respectively. Then at least three of d_1, d_2, d_3 and d_4 are non-trivial. Since $n \in C_{l,l'}(x, \alpha, B, B', \sigma) \cap C_{\tilde{l},\tilde{l}'}(x, \tilde{\alpha}, \tilde{B}, \tilde{B}', \tilde{\sigma})$, we get

$$\left(\frac{p_{\sigma_i}}{p_{\sigma'_j}}\right) = 1, \quad \left(\frac{p_{\tilde{\sigma}_i}}{p_{\tilde{\sigma}'_j}}\right) = 1 \quad \text{for all } i \text{ and } j \text{ meaningful.}$$

Therefore for $i \neq j$,

$$\left(\frac{q_i}{q_j}\right) = 1$$

for any prime factor q_i of d_i and q_j of d_j. Switching certain rows and columns of A_n, we get a matrix

$$A' = \mathrm{diag}(A'_1, A'_2, A'_3, A'_4)$$

with A'_j an $\omega(d_j) \times \omega(d_j)$ matrix for $1 \leqslant j \leqslant 4$. Since every row sum of A_n is 0 and switching rows and columns does not change this property, every row sum of A' is 0. Thus every row sum of A'_j is also 0 for $1 \leqslant j \leqslant 4$. Hence if $d_j \neq 1$, then $\mathrm{rank}A'_j \leqslant \omega(d_j) - 1$. Therefore $\mathrm{rank}A' \leqslant \omega(n) - 3$. But A' is obtained from A_n by switching rows and columns, we get $\mathrm{rank}A_n = \mathrm{rank}A' \leqslant \omega(n) - 3$. This contradicts that $\mathrm{rank}A_n = \omega(n) - 2$. Consequently, we only need to prove the lemma with $\tilde{\sigma} = \sigma$ or σ'.

Now we assume that $\tilde{\sigma} = \sigma$. If $\tilde{B} \neq B$ or $\tilde{B}' \neq B'$, then

$$C_{l,l'}(x, \alpha, B, B', \sigma) \cap C_{\tilde{l},\tilde{l}'}(x, \tilde{\alpha}, \tilde{B}, \tilde{B}', \tilde{\sigma}) = \emptyset.$$

Now we assume that $\tilde{\sigma} = \sigma'$. Then $\tilde{l} = l'$. If $\tilde{B} \neq B'$ or $\tilde{B}' \neq B$, then

$$C_{l',l}(x, \alpha, B', B, \sigma') \cap C_{\tilde{l},\tilde{l}'}(x, \tilde{\alpha}, \tilde{B}, \tilde{B}', \tilde{\sigma}) = \emptyset.$$

Note that we obviously have

$$C_{l,l'}(x, \alpha, B, B', \sigma) = C_{l',l}(x, \alpha, B', B, \sigma').$$

So we complete the proof of the lemma. □

5 Conclusions

Due to the existence of quartic residue symbols in the characterization of Shafarevich-Tate groups, we use multiplicative number theory over $\mathbb{Q}(i)$ to derive an independence property of residue symbols. In fact, this method can be generalized to higher order residue symbols. This requires one to handle the ideal class group and unit group of certain number field in the estimation of integers counted by these symbols. Furthermore, we can predict that there may exist more complicated dependences among residue symbols.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 11501541). The author is greatly indebted to his advisor Professor Ye Tian for many instructions and suggestions. The author thanks Lvhao Yan for carefully reading the manuscript and giving valuable comments.

References

1 Brown M, Calkin N, James K, et al. Trivial Selmer groups and even partitions of a graph. Integers, 2006, 6: 1–17
2 Cremona J, Odoni R. Some density results for negative Pell equations: An application of graph theory. J Lond Math Soc (2), 1989, 39: 16–28
3 Fogels E. Über die Ausnahmenullstelle der Heckeschen L-Funktionen. Acta Arith, 1963, 8: 307–309
4 Fogels E. On the zeros of L-functions. Acta Arith, 1965, 11: 67–96
5 Fogels E. Corrigendum to the paper "On the zeros of L-functions" (Acta Arith, 1965, 11: 67–96). Acta Arith, 1968, 14: 435
6 Hecke E. Lectures on the Theory of Algebraic Numbers. Berlin: Springer-Verlag, 1981
7 Hoffstein J, Ramakrishnan D. Siegel zeros and cusp forms. Int Math Res Not IMRN, 1995, 6: 279–308
8 Ireland K, Rosen M. A Classical Introduction to Modern Number Theory. Berlin: Springer-Verlag, 1990
9 Iwaniec H, Kowalski E. Analytic Number Theory. Providence: Amer Math Soc, 2004
10 Jung H, Yue Q. 8-ranks of class groups of imaginary quadratic number fields and their densities. J Korean Math Soc, 2011, 48: 1249–1268
11 Lang S. Algebraic Number Theory. Berlin: Springer-Verlag, 1994
12 Rhoades R. 2-Selmer groups and the Birch-Swinnerton-Dyer conjecture for the congruent number curves. J Number Theory, 2009, 129: 1379–1391
13 Serre J. A Course in Arithmetic. Berlin: Springer-Verlag, 1973
14 Vatsal V. Rank-one twists of a certain elliptic curve. Math Ann, 1998, 311: 791–794
15 Wang Z J. Congruent elliptic curves with non-trivial Shafarevich-Tate groups. Sci China Math, 2016, 59: 2145–2166