ASIAN J. MATH.
Vol. 4, No. 4, pp. 737–756, December 2000

ON A DENSITY PROBLEM FOR ELLIPTIC CURVES OVER FINITE FIELDS*

YEN-MEI J. CHEN† AND JING YU‡

Abstract. We prove an analogue of Artin's primitive root conjecture for two-dimensional tori $\mathrm{Res}_{K/\mathbb{Q}}\mathbb{G}_m$ under the Generalized Riemann Hypothesis, where K is an imaginary quadratic field. As a consequence, we are able to derive a precise density formula for a given elliptic curve E over a finite prime field. One adjoins coordinates of all ℓ-torsion points to the base field and asks for the density of the rational primes ℓ for which the resulting Galois extension over the base field has degree $\ell^2 - 1$. It turns out that the density in question is essentially independent of the curves, and unless in certain special cases, even independent of the characteristic p if $p \not\equiv 1 \pmod 4$.

1. Introduction. Given an elliptic curve $E_{/\mathbb{F}_p}$, one is interested in the Galois representations on ℓ-torsion $E[\ell] \subset E(\bar{\mathbb{F}}_p)$ for various rational prime numbers ℓ. Let $\mathbb{F}_p(E[\ell])$ be the Galois extension of $\mathbb{F}_p$ obtained by adjoining all coordinates of points in $E[\ell]$. A basic question is: how often the degree $[\mathbb{F}_p(E[\ell]) : \mathbb{F}_p]$ can be the largest possible, in other words, is equal to $\ell^2 - 1$?

If the given curve $E_{/\mathbb{F}_p}$ is supersingular, it is not difficult to deduce that for almost all ℓ, the degree of $\mathbb{F}_p(E[\ell])/\mathbb{F}_p$ is bounded by $2(\ell - 1)$. Thus for our purpose it suffices to consider non-supersingular elliptic curves. We want to study the following set associated to a given non-supersingular $E_{/\mathbb{F}_p}$:

$$M_E = \{\ell : \ \ell \text{ rational prime}, \ [\mathbb{F}_p(E[\ell]) : \mathbb{F}_p] = \ell^2 - 1\}.$$

Our main result is that, under the generalized Riemann Hypothesis (GRH), these sets M_E always have positive density. Furthermore the value of this density $\mathrm{den}(M_E)$ can be given precisely in terms of a universal constant C_2:

$$C_2 = \frac{1}{4} \prod_{q \neq 2 \text{ prime}} \left(1 - \frac{2}{q(q-1)}\right) = 0.133776\cdots.$$

If $p \not\equiv 1 \pmod 4$, then always $\mathrm{den}(M_E) = C_2$ unless in certain exceptional cases. Otherwise we have $\mathrm{den}(M_E) = (1 - \frac{2}{p(p-1)})^{-1} C_2$ (c.f. Theorem 4.3).

The approach of this paper is based on a variation of Artin's primitive root problem for a family of two-dimensional tori over $\mathbb{Q}$. Let End_E denote the endomorphism ring of the elliptic curve E and let $\alpha \in \mathrm{End}_E$ be the Frobenius endomorphism. If E is not supersingular, $\mathbb{Z}[\alpha] \subset \mathrm{End}_E$, and $\mathbb{Z}[\alpha]$ is identified with an order in an imaginary quadratic field $K = K_E$. Then $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$, the ring of integers in K. The torus in question is the one obtained from $\mathbb{G}_{m/K}$ via restriction of scalars : $\mathbb{T} = \mathrm{Res}_{K/\mathbb{Q}} \mathbb{G}_{m/K}$. This $\mathbb{T}$ is a two-dimensional torus defined over $\mathbb{Q}$. It comes with a canonical homomorphism $\pi : \mathbb{T} \to \mathbb{G}_m$ defined over K which is universal, in the sense that any map into $\mathbb{G}_m$ defined over K can be factored through a map into $\mathbb{T}$ that is defined over $\mathbb{Q}$. One identifies $\mathbb{T}(\mathbb{Q})$ with $\mathbb{G}_m(K) = K^\star$. Therefore the Frobenius endomorphism α is regarded here as a rational point in $\mathbb{T}(\mathbb{Q})$. One observes that powers of such a

* Received June 20, 2000; accepted for publication October 5, 2000. Research partially supported by National Science Council, Rep. of China.

† Department of Mathematics, Tamkang University, Tamshui, Taipei, Taiwan (ymjchen@mail.tku.edu.tw).

‡ Institute of Mathematics, Academia Sinica, Nankang, Taipei, Taiwan and National Center for Theoretical Sciences, Hsinchu, Taiwan (yu@math.sinica.edu.tw).

point can never be contained in any proper subtorus of $\mathbb{T}$. Hence it has a good chance to become "primitive" when reducing modulo rational primes ℓ, in the sense that α modulo ℓ generates $\mathbb{T}(\mathbb{F}_\ell)$.

In §**2**, we begin with the condition for given $\alpha \in \mathcal{O}_K$ to be primitive point modulo prime ℓ for the torus $\mathbb{T}_K$, where K is an arbitrary imaginary quadratic field and ℓ is a rational prime which remains prime in K. The set M_α consisting of all primes ℓ having this property with respect to a fixed α is then characterized algebraically via a family of Galois extensions constructed from α. In §**3** we prove that M_α always has a density (assuming GRH) which can be given precisely. An application to elliptic curves is given in §**4**. Our method works well for elliptic curve E over any finite field $\mathbb{F}_r$, and one can gather in this way information on the distributions of the degrees $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$ as ℓ ranges over all prime numbers.

2. Primitive Points for Certain Two Dimensional Tori. Let K be a fixed imaginary quadratic number field, with ring of integers $\mathcal{O}_K \subset K$. We use τ to denote the complex conjugation and in this section ℓ always stands for a rational prime number that stays prime in K. For $\alpha \in \mathcal{O}_K \setminus \{0\}$, $N(\alpha) = \alpha\alpha^\tau$ denotes its absolute norm, $\bar{\alpha}$ denotes the coset in $(\mathcal{O}_K/\ell\mathcal{O}_K)^*$ containing α if $\mathrm{ord}_\ell(\alpha) = 0$, and $o_\ell(\alpha)$ denotes the order of $\bar{\alpha}$ inside $(\mathcal{O}_K/\ell\mathcal{O}_K)^*$. The set of all rational prime numbers is denoted by $\mathbb{P}$. Given $\alpha \in \mathcal{O}_K \setminus \{0\}$, we set $u = u(\alpha) = \alpha^\tau/\alpha$. The following straightforward Proposition is the starting point:

PROPOSITION 2.1. *Let ℓ be a rational prime that is inert(stays prime) in K and $\mathrm{ord}_\ell(\alpha) = 0$. Then $o_\ell(\alpha) = \ell^2 - 1$ if and only if $o_\ell(N(\alpha)) = \ell - 1$ and $o_\ell(u) = \ell + 1$.*

Proof. Note that as ℓ is inert in K, $\alpha^\tau \equiv \alpha^\ell \pmod{\ell}$. Thus $N(\alpha) \equiv \alpha^{\ell+1}$ and $u \equiv \alpha^{\ell-1} \pmod{\ell}$. Suppose that $o_\ell(\alpha) = \ell^2-1$. Then clearly we have $o_\ell(N(\alpha)) = \ell-1$ and $o_\ell(u) = \ell+1$. Conversely, if $o_\ell(\alpha) \neq \ell^2 - 1$, then there exists a prime q such that $q \mid \ell^2 - 1$ and $\alpha^{\frac{\ell^2-1}{q}} \equiv 1 \pmod{\ell}$. If $q \mid \ell - 1$, then $N(\alpha)^{\frac{\ell-1}{q}} \equiv \alpha^{\frac{\ell^2-1}{q}} \equiv 1 \pmod{\ell}$; and if $q \mid \ell + 1$, then $u^{\frac{\ell+1}{q}} \equiv \alpha^{\frac{\ell^2-1}{q}} \equiv 1 \pmod{\ell}$. Therefore, $o_\ell(\alpha) \neq \ell^2 - 1$ implies either $o_\ell((N(\alpha)) \lneqq \ell - 1$ or $o_\ell(u) \lneqq \ell + 1$. □

Recall that $\mathbb{T} = \mathrm{Res}_{K/\mathbb{Q}}\mathbb{G}_{m/K}$ is the algebraic group over $\mathbb{Q}$ obtained from the multiplicative group $\mathbb{G}_m$ by restriction of scalars. We have $\alpha \in \mathcal{O}_K\setminus\{0\} \subset K^* = \mathbb{T}(\mathbb{Q})$ and we are interested in the following set of primes:

$$\begin{aligned} M_\alpha &= \{\ell : \ell \text{ rational prime that is inert in} K,\ \mathrm{ord}_\ell(\alpha) = 0,\ o_\ell(\alpha) = \ell^2 - 1\} \\ &= \{\ell : \ell \text{ rational prime that is inert in } K,\ \bar{\alpha} \text{ generate } \mathbb{T}(\mathbb{F}_\ell)\}. \end{aligned}$$

Notations: Let q, q' be rational primes with q' odd. We introduce the following Galois number fields:

$E_1 = \mathbb{Q}$, $F_1 = K$.

$E_q = \mathbb{Q}(\boldsymbol{\mu}_q, \sqrt[q]{N(\alpha)})$, where $\boldsymbol{\mu}_q$ is the group of q-th roots of unity.

$E_m =$ the compositum $\prod_{q|m} E_q$, for square free m.

$F_{q'} = K(\boldsymbol{\mu}_{q'}, \sqrt[q']{u})$.

$F_n =$ the compositum $\prod_{q'|n} F_{q'}$, for square free odd n.

$L_{m,n} =$ the compositum $E_m F_n$, for m, n square free and n is odd.

For Galois number fields E/F, $(\wp, E/F)$ will denote the Artin symbol whenever the prime $\wp$ in F is unramified in E. We shall allow τ to stand also for the complex conjugation on $\mathbb{Q}(\boldsymbol{\mu}_n)$, i.e. $\tau(\xi) = \xi^{-1}$ for any $\xi \in \boldsymbol{\mu}_n$. Given square free m, n, with n odd, we consider in particular the following subset of $\mathrm{Gal}(L_{m,n}/\mathbb{Q})$:

$$C_{m,n} = \{\sigma \in \mathrm{Gal}(L_{m,n}/\mathbb{Q}) : \sigma|_K = \tau,\ \sigma|_{E_m} = \mathrm{id}, \sigma|_{\mathbb{Q}(\boldsymbol{\mu}_n)} = \tau,\ \text{and } \sigma^2 = \mathrm{id}\}.$$

We have

LEMMA 2.2. *Let ℓ be a prime that is inert in $K/\mathbb{Q}$ and q be a prime. Suppose* $\mathrm{ord}_\ell(\alpha) = 0$. *Then the following conditions are equivalent:*

(1) *$q \mid (\ell - 1)$ and $\bar{\alpha}^{\frac{\ell^2-1}{q}} = 1$ in $(\mathcal{O}_K/\ell\mathcal{O}_K)^\star$.*
(2) *ℓ splits completely in $E_q/\mathbb{Q}$.*
(3) *ℓ is unramified in $L_{q,1}/\mathbb{Q}$ and $(\ell, L_{q,1}/\mathbb{Q}) \subseteq C_{q,1}$.*

Proof. It suffices to note that (1) amounts to $q \mid (\ell - 1)$ and $N(\alpha)^{\frac{\ell-1}{q}} \equiv 1 \pmod{\ell}$. This is equivalent to $q \mid (\ell - 1)$ and $x^q \equiv N(\alpha) \pmod{\ell}$ has a solution in $\mathbb{Z}$. Thus we have (1)$\Leftrightarrow$(2). The rest follows from the definitions. □

LEMMA 2.3. *Let ℓ be a prime that is inert in $K/\mathbb{Q}$ and q' be an odd prime. Suppose* $\mathrm{ord}_\ell(\alpha) = 0$. *Then the following conditions are equivalent:*

(1) *$q' \mid (\ell + 1)$ and $\bar{\alpha}^{\frac{\ell^2-1}{q'}} = 1$ in $(\mathcal{O}_K/\ell\mathcal{O}_K)^\star$.*
(2) *$q' \mid (\ell + 1)$ and $\ell\mathcal{O}_K$ splits completely in $F_{q'}/K$.*
(3) *ℓ is unramified in $L_{1,q'}/\mathbb{Q}$ and $(\ell, L_{1,q'}/\mathbb{Q}) \subseteq C_{1,q'}$.*

Proof. We first note that (1) $\Leftrightarrow$ $q' \mid \ell + 1$ and $\bar{u}^{\frac{\ell+1}{q'}} = 1$ in $(\mathcal{O}_K/\ell\mathcal{O}_K)^\star$. This is equivalent to $q' \mid (\ell + 1)$ and $x^{q'} \equiv \alpha \pmod{\ell}$ has a solution in $\mathcal{O}_K$, since $(\mathcal{O}_K/\ell\mathcal{O}_K)^\star$ is cyclic. Also it is equivalent to $q' \mid (\ell + 1)$ and $x^{q'} \equiv \alpha^{\ell-1} \equiv u \pmod{\ell}$ has a solution in $\mathcal{O}_K$, because $q' \nmid (\ell - 1)$. Hence we obtain (1) $\Leftrightarrow$ (2). On the other hand $q' | (\ell + 1)$ if and only if $(\ell, \mathbb{Q}(\boldsymbol{\mu}_{q'})/\mathbb{Q}) = \tau$. If (2) holds, then ℓ is clearly unramified in $L_{1,q'}/\mathbb{Q}$. Because $\ell\mathcal{O}_K$ splits completely in $L_{1,q'}/K$, we have $\sigma^2 = \mathrm{id}$, for all $\sigma \in (\ell, L_{1,q'}/\mathbb{Q})$. Thus (2) $\Rightarrow$ (3). Conversely, from $\sigma^2 = \mathrm{id}$ for all $\sigma \in (\ell, L_{1,q'}/\mathbb{Q})$, we obtain immediately that $\ell\mathcal{O}_K$ splits completely in $F_{q'}/K$. Hence (3) $\Rightarrow$ (2). □

Combining Lemmas 2.2, 2.3, we deduce the crucial:

COROLLARY 2.4. *Let ℓ be a rational prime which is inert in $K/\mathbb{Q}$ and* $\mathrm{ord}_\ell(\alpha) = 0$. *Then $\ell \in M_\alpha$ if and only if both the following two conditions hold: (1) For all prime q, if ℓ is unramified in $L_{q,1}$, then $(\ell, L_{q,1}/\mathbb{Q}) \nsubseteq C_{q,1}$.*
(2) For all odd prime q', if ℓ is unramified in $L_{1,q'}$, then $(\ell, L_{1,q'}/\mathbb{Q}) \nsubseteq C_{1,q'}$.

From now on we make the further assumption that α is not a root of unity and $\gcd(\alpha, \alpha^\tau) = 1$, i.e. $1 \in \alpha\mathcal{O}_K + \alpha^\tau\mathcal{O}_K$. The remaining part of this section is occupied by a detailed study of the Galois family $L_{m,n}$, together with the computation of $\#C_{m,n}$. All these are preliminaries needed for the main theorems of §**3**.

LEMMA 2.5. *Let m, n be square-free positive integers with n odd. Let s be the largest integer with the property that $N(\alpha) \in (\mathbb{Q}^\star)^s$, and let s' be the largest integer with the property that $u \in (K^\star)^{s'}$. Let $m_1 = m/\gcd(m, s)$ and $n_2 = n/\gcd(n, s')$. Suppose* $\gcd(s, 6) = 1$. *Then*

(a)

$$[E_m : \mathbb{Q}] = \frac{m_1\phi(m)}{[k_m \cap \mathbb{Q}(\mu_m) : \mathbb{Q}]},$$

where $k_m = \mathbb{Q}$ (resp. $\mathbb{Q}(\sqrt{N(\alpha)})$) if $2 \nmid m$ (resp. $2 \mid m$).

(b)

$$[F_n:\mathbb{Q}]=\begin{cases}\frac{2n_2\phi(n)}{3[K\cap\mathbb{Q}(\mu_n):\mathbb{Q}]} & \textit{if } K=\mathbb{Q}(\sqrt{-3}),\ 3\mid n,\ \textit{and } u\in\left(K(\boldsymbol{\mu}_n)^\star\right)^3,\\ \frac{2n_2\phi(n)}{[K\cap\mathbb{Q}(\mu_n):\mathbb{Q}]} & \textit{otherwise.}\end{cases}$$

Proof. Our argument is based on the following

SUBLEMMA. *Let F be a field, K_1 a finite abelian extension of F, and K_2 be a finite extension of F which is not Galois but with prime extension degree. Then K_1, K_2 are linearly disjoint over F and $[K_1K_2:K_1]=[K_2:F]$.*

(a) Suppose that $2\nmid m$. For $q\mid m$, let $E_{m,q}=\mathbb{Q}\left(\boldsymbol{\mu}_m,\sqrt[q]{N(\alpha)}\right)$. Note that $[\mathbb{Q}(\sqrt[q]{N(\alpha)}:\mathbb{Q}]=1$ or q depending on whether $N(\alpha)\in(\mathbb{Q}^\star)^q$. By the Sublemma, we have therefore

$$[E_{m,q}:\mathbb{Q}(\boldsymbol{\mu}_m)]=\begin{cases}1 & \text{if } N(\alpha)\in(\mathbb{Q}^\star)^q,\\ q & \text{otherwise.}\end{cases}$$

Thus $E_{m,q}$'s are linearly disjoint over $\mathbb{Q}(\boldsymbol{\mu}_m)$. Since E_m is the compositum of $E_{m,q}$'s, we have $[E_m:\mathbb{Q}]=[E_m:\mathbb{Q}(\boldsymbol{\mu}_m)][\mathbb{Q}(\boldsymbol{\mu}_m):\mathbb{Q}]=m_1\phi(m)$.

Suppose that $2\mid m$, write $m=2m'$. Then $m_1=m/\gcd(m,s)=2\cdot m'/\gcd(m',s)=2m_1'$ and $E_m=E_2E_{m'}$. For $q'\mid m'$, let $E_{m,q'}=E_2\left(\boldsymbol{\mu}_{m'},\sqrt[q']{N(\alpha)}\right)$. Here one also has $[E_2(\sqrt[q']{N(\alpha)}):E_2]=1$ or q' depending on whether $N(\alpha)\in(\mathbb{Q}^\star)^{q'}$. Consequently,

$$[E_{m,q'}:E_2(\boldsymbol{\mu}_{m'})]=\begin{cases}1 & \text{if } N(\alpha)\in(\mathbb{Q}^\star)^{q'},\\ q & \text{otherwise.}\end{cases}$$

The $E_{m,q'}$'s are linearly disjoint over $E_2(\boldsymbol{\mu}_{m'})$ and we have

$$\begin{aligned}[E_m:\mathbb{Q}]&=[E_m:E_2(\boldsymbol{\mu}_{m'})][E_2(\boldsymbol{\mu}_{m'}):\mathbb{Q}]\\&=\frac{m_1}{2}\frac{[E_2:\mathbb{Q}][\mathbb{Q}(\boldsymbol{\mu}_{m'}):\mathbb{Q}]}{[E_2\cap\mathbb{Q}(\mu_{m'}):\mathbb{Q}]}\\&=\frac{m_1\phi(m)}{[E_2\cap\mathbb{Q}(\mu_m):\mathbb{Q}]}.\end{aligned}$$

(b) For $q'\mid n$, let $F_{n,q'}=K(\boldsymbol{\mu}_n,\sqrt[q']{u})$. Note that if $q'\nmid s'$, then $K(\sqrt[q']{u})$ is not Galois over K except that $K=\mathbb{Q}(\sqrt{-3})$ and $q'=3$. Also one has that $[K(\sqrt[q']{u}):K]=1$ or q' depending on whether $u\in(K^\star)^{q'}$. By the Sublemma, we have $[F_{n,q'}:K(\boldsymbol{\mu}_n)]=q'/\gcd(q',s')$ except when $K=\mathbb{Q}(\sqrt{-3})$ and $q'=3$. If $K=\mathbb{Q}(\sqrt{-3})$ and $3\mid n$, then

$$[F_{n,3}:K(\boldsymbol{\mu}_n)]=\begin{cases}1 & \text{if } u\in\left(K(\boldsymbol{\mu}_n)^\star\right)^3,\\ 3 & \text{if } u\notin\left(K(\boldsymbol{\mu}_n)^\star\right)^3.\end{cases}$$

Thus the $F_{n,q'}$'s are linearly disjoint over $K(\boldsymbol{\mu}_n)$ and we have:

$$[F_n:K(\boldsymbol{\mu}_n)]=\begin{cases}\frac{n_2}{3} & \text{if } K=\mathbb{Q}(\sqrt{-3}),\ 3\mid n,\ \text{and } u\in\left(K(\boldsymbol{\mu}_n)^\star\right)^3,\\ n_2 & \text{otherwise.}\end{cases}$$

Therefore,

$$\begin{aligned}[F_n:\mathbb{Q}]&=[F_n:K(\boldsymbol{\mu}_n)][K(\boldsymbol{\mu}_n):\mathbb{Q}]\\&=\begin{cases}\frac{2n_2\phi(n)}{3[K\cap\mathbb{Q}(\boldsymbol{\mu}_n):\mathbb{Q}]} & \text{if } K=\mathbb{Q}(\sqrt{-3}),\ 3\mid n,\ \text{and } u\in\left(K(\boldsymbol{\mu}_n)^\star\right)^3,\\ \frac{2n_2\phi(n)}{[K\cap\mathbb{Q}(\boldsymbol{\mu}_n):\mathbb{Q}]} & \text{otherwise.}\end{cases}\end{aligned}$$

□

LEMMA 2.6. *Let m, n be square-free positive integers with n odd and* $\gcd(m,n) = 1$. *Suppose further that α satisfies all the conditions in Lemma 2.5. If $K = \mathbb{Q}(\sqrt{-3})$, $3 \mid n$ and $u \in \left(K(\boldsymbol{\mu}_{mn})^\star\right)^3 \setminus \left(K(\boldsymbol{\mu}_n)^\star\right)^3$, then $E_m \cap F_n = k_m(\boldsymbol{\mu}_m) \cap K(\boldsymbol{\mu}_n, \sqrt[3]{u})$ and*

$$[E_m \cap F_n : \mathbb{Q}] = \frac{3[Kk_m \cap \mathbb{Q}(\boldsymbol{\mu}_{mn}) : \mathbb{Q}]}{[k_m \cap \mathbb{Q}(\boldsymbol{\mu}_m) : \mathbb{Q}][K \cap \mathbb{Q}(\boldsymbol{\mu}_n) : \mathbb{Q}]}.$$

Otherwise, $E_m \cap F_n = k_m(\boldsymbol{\mu}_m) \cap K(\boldsymbol{\mu}_n)$ and

$$[E_m \cap F_n : \mathbb{Q}] = \frac{[Kk_m \cap \mathbb{Q}(\boldsymbol{\mu}_{mn}) : \mathbb{Q}]}{[k_m \cap \mathbb{Q}(\boldsymbol{\mu}_m) : \mathbb{Q}][K \cap \mathbb{Q}(\boldsymbol{\mu}_n) : \mathbb{Q}]}.$$

(Recall that $k_m = \mathbb{Q}$ (resp. $\mathbb{Q}(\sqrt{N(\alpha)})$) if $2 \nmid m$ (resp. $2 \mid m$).)

Proof. First we contend that $E_m \cap Kk_m(\boldsymbol{\mu}_{mn}) = k_m(\boldsymbol{\mu}_m)$. Also that $F_n \cap Kk_m(\boldsymbol{\mu}_{mn}) = K(\boldsymbol{\mu}_n)$ except when $K = \mathbb{Q}(\sqrt{-3})$, $3 \mid n$, $u \in \left(K(\boldsymbol{\mu}_{mn})^\star\right)^3$ but $u \notin \left(K(\boldsymbol{\mu}_n)^\star\right)^3$.

Since $\gcd(m,n) = 1$, $Kk_m\left(\boldsymbol{\mu}_{mn}, \sqrt[m]{N(\alpha)}\right)$ and $Kk_m(\boldsymbol{\mu}_{mn}, \sqrt[n]{u})$ are linearly disjoint over $Kk_m(\boldsymbol{\mu}_{mn})$. Observe that $E_m \subset Kk_m\left(\boldsymbol{\mu}_{mn}, \sqrt[m]{N(\alpha)}\right)$ and $F_n \subset Kk_m(\boldsymbol{\mu}_{mn}, \sqrt[n]{u})$. Hence

$$E_m \cap F_n \subseteq Kk_m\left(\boldsymbol{\mu}_{mn}, \sqrt[m]{N(\alpha)}\right) \cap Kk_m(\boldsymbol{\mu}_{mn}, \sqrt[n]{u}) = Kk_m(\boldsymbol{\mu}_{mn}).$$

Note that for odd prime q, $N(\alpha) \in (\mathbb{Q}^\star)^q$ if and only if $N(\alpha) \in \left((Kk_m)^\star\right)^q$. Similar to the proof of Lemma 2.5(a), one has

$$[Kk_m\left(\boldsymbol{\mu}_{mn}, \sqrt[m]{N(\alpha)}\right) : Kk_m(\boldsymbol{\mu}_{mn})] = \frac{m_1}{\gcd(2,m)} = [E_m : k_m(\boldsymbol{\mu}_m)]$$

and therefore $E_m \cap Kk_m(\boldsymbol{\mu}_{mn}) = k_m(\boldsymbol{\mu}_m)$.

Similarly, because $N(\alpha)$ is divisible only by splitting primes, if $q' \nmid s'$, then $Kk_m(\sqrt[q']{u})$ is not Galois over Kk_m except when $K = \mathbb{Q}(\sqrt{-3})$ and $q' = 3$. Thus we have

$$[Kk_m(\boldsymbol{\mu}_{mn}, \sqrt[n]{u}) : Kk_m(\boldsymbol{\mu}_{mn})] = \begin{cases} \frac{n_2}{3} & \text{if } K = \mathbb{Q}(\sqrt{-3}),\ 3 \mid n,\ u \in \left(K(\boldsymbol{\mu}_{mn})^\star\right)^3, \\ n_2 & \text{otherwise.} \end{cases}$$

Therefore, $F_n \cap Kk_m(\boldsymbol{\mu}_{mn}) = K(\boldsymbol{\mu}_n)$ unless $K = \mathbb{Q}(\sqrt{-3})$, $3 \mid n$, and $u \in \left(K(\boldsymbol{\mu}_{mn})^\star\right)^3 \setminus \left(K(\boldsymbol{\mu}_n)^\star\right)^3$. In the last mentioned case, it is easy to check that $[F_n \cap Kk_m(\boldsymbol{\mu}_{mn}) : K(\boldsymbol{\mu}_n)] = 3$ and thus $F_n \cap Kk_m(\boldsymbol{\mu}_{mn}) = K(\boldsymbol{\mu}_n, \sqrt[3]{u})$.

If we are in the case $K = \mathbb{Q}(\sqrt{-3})$, $3 \mid n$, $u \in \left(K(\boldsymbol{\mu}_{mn})^\star\right)^3 \setminus \left(K(\boldsymbol{\mu}_n)^\star\right)^3$, what we obtain is

$$\begin{aligned}
[E_m \cap F_n : \mathbb{Q}] &= [(E_m \cap Kk_m(\boldsymbol{\mu}_{mn})) \cap (F_n \cap Kk_m(\boldsymbol{\mu}_{mn})) : \mathbb{Q})] \\
&= [k_m(\boldsymbol{\mu}_m) \cap K(\boldsymbol{\mu}_n, \sqrt[3]{u}) : \mathbb{Q}] = \frac{[k_m(\boldsymbol{\mu}_m) : \mathbb{Q}][K(\boldsymbol{\mu}_n, \sqrt[3]{u}) : \mathbb{Q}]}{[Kk_m(\boldsymbol{\mu}_{mn}, \sqrt[3]{u}) : \mathbb{Q}]} \\
&= \frac{3[k_m(\boldsymbol{\mu}_m) : \mathbb{Q}][K(\boldsymbol{\mu}_n) : \mathbb{Q}]}{[Kk_m(\boldsymbol{\mu}_{mn}) : \mathbb{Q}]} \\
&= 3 \cdot \frac{[k_m : \mathbb{Q}][\mathbb{Q}(\boldsymbol{\mu}_m) : \mathbb{Q}]}{[k_m \cap \mathbb{Q}(\boldsymbol{\mu}_m) : \mathbb{Q}]} \frac{[K : \mathbb{Q}][\mathbb{Q}(\boldsymbol{\mu}_n) : \mathbb{Q}]}{[K \cap \mathbb{Q}(\boldsymbol{\mu}_n) : \mathbb{Q}]} \frac{[Kk_m \cap \mathbb{Q}(\boldsymbol{\mu}_{mn}) : \mathbb{Q}]}{[Kk_m : \mathbb{Q}][\mathbb{Q}(\boldsymbol{\mu}_{mn}) : \mathbb{Q}]} \\
&= \frac{3[Kk_m \cap \mathbb{Q}(\boldsymbol{\mu}_{mn}) : \mathbb{Q}]}{[k_m \cap \mathbb{Q}(\boldsymbol{\mu}_m) : \mathbb{Q}][K \cap \mathbb{Q}(\boldsymbol{\mu}_n) : \mathbb{Q}]}.
\end{aligned}$$

On the other hand, in all other cases, we have

$$[E_m \cap F_n : \mathbb{Q}] = [k_m(\boldsymbol{\mu}_m) \cap K(\boldsymbol{\mu}_n) : \mathbb{Q}] = \frac{[k_m(\boldsymbol{\mu}_m) : \mathbb{Q}][K(\boldsymbol{\mu}_n) : \mathbb{Q}]}{[Kk_m(\boldsymbol{\mu}_{mn}) : \mathbb{Q}]}$$
$$= \frac{[k_m : \mathbb{Q}][\mathbb{Q}(\boldsymbol{\mu}_m) : \mathbb{Q}]}{[k_m \cap \mathbb{Q}(\boldsymbol{\mu}_m) : \mathbb{Q}]} \frac{[K : \mathbb{Q}][\mathbb{Q}(\boldsymbol{\mu}_n) : \mathbb{Q}]}{[K \cap \mathbb{Q}(\boldsymbol{\mu}_n) : \mathbb{Q}]} \frac{[Kk_m \cap \mathbb{Q}(\boldsymbol{\mu}_{mn}) : \mathbb{Q}]}{[Kk_m : \mathbb{Q}][\mathbb{Q}(\boldsymbol{\mu}_{mn}) : \mathbb{Q}]}$$
$$= \frac{[Kk_m \cap \mathbb{Q}(\boldsymbol{\mu}_{mn}) : \mathbb{Q}]}{[k_m \cap \mathbb{Q}(\boldsymbol{\mu}_m) : \mathbb{Q}][K \cap \mathbb{Q}(\boldsymbol{\mu}_n) : \mathbb{Q}]}. \qquad \square$$

LEMMA 2.7. *Let m, n be square-free positive integers with n odd. Suppose further that α satisfies all the conditions in Lemma 2.5. Let $c_{m,n} = \#C_{m,n}$. Then we have*

$$c_{m,n} = \begin{cases} 1 & \text{if } E_m \cap F_n \text{ is totally real,} \\ 0 & \text{otherwise.} \end{cases}$$

In particular, if $\gcd(m,n) \neq 1$, *then* $c_{m,n} = 0$.

Proof. Suppose that $E_m \cap F_n$ is not totally real. Then it is clear that $C_{m,n} = \emptyset$ and thus $c_{m,n} = 0$.

Now suppose that $E_m \cap F_n$ is totally real. Then $\gcd(m,n) = 1$. Note that $C_{m,n} \subseteq \mathrm{Gal}(L_{m,n}/E_m) \subseteq \mathrm{Gal}(L_{m,n}/E_m \cap F_n) \subseteq \mathrm{Gal}(L_{m,n}/\mathbb{Q})$. Recall that $L_{m,n}$ is the compositum of E_m, F_n and thus one has the following isomorphism

$$\mathrm{Gal}(L_{m,n}/E_m \cap F_n) \xrightarrow{\sim} \mathrm{Gal}(E_m/E_m \cap F_n) \times \mathrm{Gal}(F_n/E_m \cap F_n)$$
$$\sigma \mapsto (\sigma_1, \sigma_2) = (\sigma|_{E_m}, \sigma|_{F_n}).$$

Embedding F_n into $\mathbb{C}$, and restricting the complex conjugation τ to F_n, since $E_m \cap F_n$ is totally real, we may extend $\tau\,|_{F_n}$ to an element in $C_{m,n}$. It suffices to show that $\sigma \in C_{mn}$ if and only if $\sigma_2 = \tau|_{F_n}$. Suppose $\sigma \in C_{m,n}$. Then $\sigma_1 = \mathrm{id}$. Let ζ_n be a fixed primitive n-th root of unity. Suppose $\sigma_2(\sqrt[n]{u}) = \zeta_n^i \frac{1}{\sqrt[n]{u}}$ for some fixed i, $0 \leq i \leq n-1$. Then $\sqrt[n]{u} = \sigma_2^2(\sqrt[n]{u}) = \zeta_n^{-2i}\sqrt[n]{u}$. As n is odd, it follows that $i = 0$ and σ_2 is unique on F_n. $\square$

Let $d_{m,n}$ denote the extension degree of $L_{m,n}$ over $\mathbb{Q}$. Then we have

LEMMA 2.8. *Let m, n be square-free positive integers with n odd and* $\gcd(m,n) = 1$. *Suppose further that α satisfies all the conditions in Lemma 2.5. Then*

$$d_{m,n} = \begin{cases} \frac{2m_1n_2\phi(mn)}{3[Kk_m \cap \mathbb{Q}(\boldsymbol{\mu}_{mn}):\mathbb{Q}]} & \text{if } K = \mathbb{Q}(\sqrt{-3}),\ 3 \mid n, \text{ and } u \in \left(K(\boldsymbol{\mu}_{mn})^\star\right)^3, \\ \frac{2m_1n_2\phi(mn)}{[Kk_m \cap \mathbb{Q}(\mu_{mn}):\mathbb{Q}]} & \text{otherwise.} \end{cases}$$

Proof. Recall the fact that $L_{m,n}$ is the compositum of E_m and F_n. Combining Lemma 2.5 and Lemma 2.6, we have, if $K = \mathbb{Q}(\sqrt{-3})$, $3 \mid n$, and $u \in (K(\boldsymbol{\mu}_{mn})^\star)^3$, then

$$d_{m,n} = [L_{m,n} : \mathbb{Q}] = [E_m : \mathbb{Q}][F_n : \mathbb{Q}]/[E_m \cap F_n : \mathbb{Q}]$$
$$= \frac{2m_1n_2\phi(mn)}{3[Kk_m \cap \mathbb{Q}(\boldsymbol{\mu}_{mn}) : \mathbb{Q}]}.$$

Otherwise, $d_{m,n} = \dfrac{2m_1n_2\phi(mn)}{[Kk_m \cap \mathbb{Q}(\boldsymbol{\mu}_{mn}) : \mathbb{Q}]}$. $\square$

Let D_K denote the absolute value of the discriminant of the imaginary quadratic field K, and let $D_{m,n}$ denote the absolute value of the absolute discriminant of the number field $L_{m,n}$. Then we have

LEMMA 2.9. $D_{m,n} \mid D_K^{m_1 n_2 \phi(m)\phi(n)} \big(N(\alpha)mn\big)^{4m_1 n_2 \phi(m)\phi(n)}$.

Proof. It is routine to compute that the relative discriminant of $E_q/\mathbb{Q}$ and $F_{q'}/K$ divides $N(\alpha)^{[E_q:\mathbb{Q}]} q^{2[E_q:\mathbb{Q}]}$ and $N(\alpha)^{[F_{q'}:K]} q'^{2[F_{q'}:K]}$ respectively. Hence the relative discriminant of L_{mn}/K divides $\big(N(\alpha)mn\big)^{2m_1 n_2 \phi(m)\phi(n)}$. Consequently $D_{m,n} \mid D_K^{m_1 n_2 \phi(m)\phi(n)} \big(N(\alpha)mn\big)^{4m_1 n_2 \phi(m)\phi(n)}$. □

3. Existence and positivity of the density. Given a set $M \subset \mathbb{P}$, we are interested in the following limit:

$$\lim_{x\to\infty} \frac{\#\{\ell \in M : \ell \le x\}}{x/\log x}.$$

If this limit exists, its value is called the density of M, and will be denoted by den(M). We are going to prove that if $\alpha \in K$ satisfies certain conditions, then the set M_α introduced in §**2**, has a positive density. The structure of our proof follows that of Hooley[2], c.f. also Murty[4].

For pimes q, q' with q' odd, we define two sets

$$S_q = \{\ell \in \mathbb{P} : \ell \text{ is inert in } K,\ \ell\mathcal{O}_K \text{ is unramified in } L_{q,1}, \text{ and } (\ell, L_{q,1}) \in C_{q,1}.\},$$
$$T_{q'} = \{\ell \in \mathbb{P} : \ell \text{ is inert in } K,\ \ell\mathcal{O}_K \text{ is unramified in } L_{1,q'}, \text{ and } (\ell, L_{1,q'}) \in C_{1,q'}.\}.$$

Note that given a rational prime ℓ, there are only finitely many q's such that $\ell \in S_q$ and also there are only finitely many q''s such that $\ell \in T_{q'}$. We define $R(\ell)$ to be the compositum

$$R(\ell) = \prod_q L_{q,1} \cdot \prod_{q'} L_{1,q'},$$

where q runs through primes satisfying $\ell \in S_q$ and q' runs through odd primes satisfying $\ell \in T_{q'}$.

We are interested in the lattice of the fields $L_{m,n}{}'s$ where m, n are square-free positive integers with n odd, partially ordered by

$$L_{m,n} \preceq L_{m',n'} \text{ if and only if } m' \mid m \text{ and } n' \mid n.$$

This lattice will be denoted by $\mathcal{L}$. Given $L \in \mathcal{L}$, we also introduce the functions:

$$f(x, L) = \#\{\ell : \ell \in \mathbb{P},\ \ell \le x,\ \ell \text{ is inert in } K/\mathbb{Q}, \text{ and } R(\ell) = L\},$$
$$\pi_1(x, L) = \#\{\ell : \ell \in \mathbb{P},\ \ell \le x,\ \ell \text{ is inert in } K/\mathbb{Q}, \text{ and } R(\ell) \supseteq L\}.$$

For $L \in \mathcal{L}$, it is clear that $\pi_1(x, L) = \sum_{L' \preceq L} f(x, L')$. From Möbius inversion, we have $f(x, L) = \sum_{L' \preceq L} \mu(L', L)\pi_1(x, L')$ where $\mu(L', L)$ is the Möbius function of the lattice $\mathcal{L}$. (c.f. [5], Proposition 2.) In particular,

$$f(x, K) = \sum \mu(L_{m,n}, K)\pi_1(x, L_{m,n}) = \sum \mu(m)\mu(n)\pi_1(x, L_{m,n})$$

where m, n run through square-free positive integers with n odd.

We will use the following effective version of Chebotarev Density Theorem.

THEOREM 3.1. *Let $L/\mathbb{Q}$ be finite Galois extension with Galois group G, and C a union of conjugacy classes of G. Let $\pi_C(x, L/\mathbb{Q}) = \#\{p : p$ is a prime unramified in $L/\mathbb{Q}$, $p \le x$, and $(p, L/\mathbb{Q}) \subseteq C\}$. Assume GRH holds for the Dedekind zeta function* *of L. Then there exists a positive constant A_0 (independent of C, L) such that for every $x > 2$,*

$$|\pi_C(x, L/\mathbb{Q}) - \frac{\#C}{\#G}Li(x)| \leq A_0(\frac{\#C}{\#G}\sqrt{x}\log(D_L x^{[L:\mathbb{Q}]}))$$

where $Li(x)$ is the logarithmic integral $Li(x) = \int_2^x \frac{dt}{\log t} \sim \frac{x}{\log x}$ as $x \to \infty$.
(c.f. [6], Theorem 4.)

The existence of density for M_α is contained in the following

THEOREM 3.2. *Given $\alpha \in \mathcal{O}_K \setminus \mathcal{O}_K{}^*$ with $\gcd(\alpha, \alpha^\tau) = 1$. Let s be the largest integer such that $N(\alpha) \in (\mathbb{Q}^*)^s$. Assume that $\gcd(s, 6) = 1$ and furthermore GRH holds. Then $\operatorname{den}(M_\alpha)$ exists and is given by*

$$\operatorname{den}(M_\alpha) = \sum_{m,\, n} \frac{\mu(m)\mu(n)c_{m,n}}{d_{m,n}},$$

where in the sum m, n runs through all square free positive integers, n is required to be odd.

Remark. The condition $\gcd(s, 6) = 1$ in Theorem 3.2 is not essential. If $2 \mid s$ or $3 \mid s$, one can still prove such an identiy with both sides equal 0.

Proof of Theorem 3.2. First note that $\#\{\ell \in M_\alpha : \ell \leq x\} = f(x, K)$. Define $N(x, y) = \#\{\ell : \ell \in \mathbb{P},\ \ell \leq x,\ \ell \text{ is inert in } K,\ \ell \notin S_q \text{ and } \ell \notin T_{q'} \text{ for all } q, q' \leq y.\}$. Recall that for any $\sigma \in \operatorname{Gal}(L_{m,n}/\mathbb{Q})$,

$$\sigma \in C_{m,n} \Longleftrightarrow \sigma|_{L_{q,1}} \in C_{q,1} \text{ for all } q \mid m \text{ and } \sigma|_{L_{1,q'}} \in C_{1,q'} \text{ for all } q' \mid n.$$

Then it is clear that $f(x, K) \leq N(x, y)$ and

$$N(x, y) = \sum_{m,\, n}{}' \mu(m)\mu(n)\pi_1(x, L_{m,n})$$

where the dash on the sum indicates that all the prime divisors of mn are $\leq y$. Note that $\pi_1(x, L_{m,n}) = \pi_{C_{m,n}}(x, L_{m,n})$. Then applying Theorem 3.1 we can find a positive absolute constant A_0 such that for all $x > 2$,

$$|\pi_1(x, L_{m,n}) - \frac{c_{m,n}}{d_{m,n}}\mathrm{Li}(x)| \leq A_0(\frac{c_{m,n}}{d_{m,n}}\sqrt{x}\log(D_{m,n}x^{d_{m,n}})).$$

Now define $M(x, y_1, y_2) = \#\{\ell : \ell \in \mathbb{P},\ \ell \leq x,\ \ell \in S_q \text{ for some } q \in [y_1, y_2] \text{ or } \ell \in T_{q'} \text{ for some } q' \in [y_1, y_2].\}$. Then

$$(1) \quad f(x, K) \geq N(x, y) - M(x, y, x + 1).$$

Claim 1: $M(x, \frac{\sqrt{x}}{\log^2 x}, \sqrt{x}\log x) = o(\frac{x}{\log x})$.

Proof. The left-hand side is bounded by

$$\sum_{\sqrt{x}/\log^2 x < q < \sqrt{x}\log x} \pi_1(x, L_{q,1}) + \sum_{\sqrt{x}/\log^2 x < q' < \sqrt{x}\log x} \pi_1(x, L_{1,q'}).$$

If ℓ contributes a count of 1 to $\pi_1(x, L_{q,1})$ then $\ell \equiv 1 \pmod q$; if ℓ contributes a count of 1 to $\pi_1(x, L_{1,q'})$ then $\ell \equiv -1 \pmod{q'}$. Hence $\pi_1(x, L_{q,1})$ is bounded by $\#\{\ell : \ell \leq x,\ \ell \equiv 1 \pmod q\}$ and $\pi_1(x, L_{1,q'})$ is bounded by $\#\{\ell : \ell \leq x,\ \ell \equiv -1 \pmod{q'}\}$.

By the Brun-Titchmarsh theorem, for any $b \in \mathbb{Z}$, there is an absolute constant B such that for $q < x$,

$$\#\{\ell : \ell \leq x, \ell \equiv b \mod q\} \leq B\frac{x}{(q-1)\log(x/q)}.$$

Therefore we have

$$\begin{aligned} M(x, \tfrac{\sqrt{x}}{\log^2 x}, \sqrt{x}\log x) &\leq 2 \cdot \sum_{\sqrt{x}/\log^2 x < q < \sqrt{x}\log x} B\frac{x}{(q-1)\log(x/q)} \\ &\leq \frac{x}{\log x} \cdot O(\sum \frac{1}{q}) \\ &\leq \frac{x}{\log^2 x} \cdot O(\sum \frac{\log q}{q}) \\ &\leq O(\frac{x \log\log x}{\log^2 x}) = o(\frac{x}{\log x}). \end{aligned}$$

Claim 2: $M(x, \frac{\sqrt{x}}{\log^2 x}, x+1) = o(\frac{x}{\log x})$.

Proof. Note that one can write

$$M(x, \tfrac{\sqrt{x}}{\log^2 x}, x+1) = M(x, \tfrac{\sqrt{x}}{\log^2 x}, \sqrt{x}\log x) + M(x, \sqrt{x}\log x, x+1).$$

By Claim 1, it suffices to show that $M(x, \sqrt{x}\log x, x+1) = o(\frac{x}{\log x})$. Recall that if $\ell \in S_q$, then $\ell \equiv 1 \pmod q$ and $N(\alpha)^{\frac{\ell-1}{q}} \equiv 1 \pmod \ell$ in $\mathcal{O}_K$, which implies ℓ divides $N(\alpha)^{\frac{\ell-1}{q}} - 1$; similarly if $\ell \in T_{q'}$, then $\ell \equiv -1 \pmod{q'}$ and $u^{\frac{\ell+1}{q'}} \equiv 1 \pmod \ell$ in $\mathcal{O}_K$, which implies $\ell \mid (\alpha^{\frac{\ell+1}{q'}} - \alpha^{\tau\frac{\ell+1}{q'}})$. Since $\ell \leq x$ and $q, q' > \sqrt{x}\log x$, $(\ell-1)/q, (\ell+1)/q' < 2\sqrt{x}/\log x$. Let

$$R_1 = \prod_{k < 2\sqrt{x}/\log x} (N(\alpha)^k - 1) \quad \text{and} \quad R_2 = \prod_{k < 2\sqrt{x}/\log x} (\alpha^k - (\alpha^\tau)^k)^2.$$

Note that $R_1 \neq 0$ and $R_2 \neq 0$. Then it is easy to see that $\ell \in S_q$ implies $\ell \mid R_1$ and also that $\ell \in T_{q'}$ implies $\ell \mid R_2$. So $M(x, \sqrt{x}\log x, x+1)$ is bounded by the number of prime factors of R_1R_2, which is trivially $O(\log R_1 + \log R_2)$. Observe that

$$\log R_1 \leq \sum_{k < 2\sqrt{x}/\log x} k \log N(\alpha) = O(\tfrac{x}{\log^2 x}), \text{ and}$$

$$\log R_2 \leq \sum_{k < 2\sqrt{x}/\log x} k \log \sqrt{N(\alpha)} = O(\tfrac{x}{\log^2 x}).$$

Therefore $M(x, \sqrt{x}\log x, x+1) = o(\frac{x}{\log x})$.

Claim 3: $M(x, y, x+1)$ is $o(\frac{x}{\log x})$ provided $y = y(x) \to \infty$ as $x \to \infty$.

Proof. It suffices to show that $M(x, y, \frac{\sqrt{x}}{\log^2 x}) = o(\frac{x}{\log x})$. We have:

$$M(x, y, \frac{\sqrt{x}}{\log^2 x}) \leq \sum_{y < q < \frac{\sqrt{x}}{\log^2 x}} \pi_1(x, L_{q,1}) + \sum_{y < q' < \frac{\sqrt{x}}{\log^2 x}} \pi_1(x, L_{1,q'}),$$

$$\sum_{y<q<\frac{\sqrt{x}}{\log^2 x}} \pi_1(x, L_{q,1}) \leq \sum_{y<q<\frac{\sqrt{x}}{\log^2 x}} \frac{c_{q,1}}{d_{q,1}}\mathrm{Li}(x) + O(\frac{c_{q,1}}{d_{q,1}}\sqrt{x}\log D_{q,1}x^{d_{q,1}})$$
$$\leq \mathrm{Li}(x) \sum_{y<q<\frac{\sqrt{x}}{\log^2 x}} \frac{1}{q^2} + \sqrt{x}\cdot O(\sum_{y<q<\frac{\sqrt{x}}{\log^2 x}} \log q) + \sqrt{x}\log x \cdot O(\sum_{y<q<\frac{\sqrt{x}}{\log^2 x}} 1).$$

One also gets the same bound for the sum involving $\pi_1(x, L_{1,q'})$. Hence

$$M(x, y, \tfrac{\sqrt{x}}{\log^2 x}) \leq 2\cdot \mathrm{Li}(x) \sum_{y<q<\frac{\sqrt{x}}{\log^2 x}} \frac{1}{q^2} + 2\cdot\sqrt{x}\log x \cdot O(\sum_{y<q<\frac{\sqrt{x}}{\log^2 x}} 1)$$
$$= o(\frac{x}{\log x}) + O\big(\sqrt{x}\log x(\tfrac{\sqrt{x}}{\log^2 x}/\log\tfrac{\sqrt{x}}{\log^2 x})\big) = o(\frac{x}{\log x}).$$

Claim 4: If $y(x) = O(\log x)$, then

$$N(x,y) = \sideset{}{'}\sum_{m,n} \frac{\mu(m)\mu(n)c_{m,n}}{d_{m,n}}\frac{x}{\log x} + o(\frac{x}{\log x}).$$

Proof. Applying the effective Cebotarev Density Theorem to those fields $L_{m,n}$, and union of conjugacy classes $C_{m,n}$, with all prime divisors of mn bounded by y. Summing together the error terms, we have:

$$O(\sideset{}{'}\sum_{m,n}\frac{c_{m,n}}{d_{m,n}}\sqrt{x}\log D_{m,n}x^{d_{m,n}}) = O(\sqrt{x}\sideset{}{'}\sum_{m,n}\log mn) + O(\sqrt{x}\log x\sideset{}{'}\sum_{m,n}1)$$
$$= O(2^{2t}\sqrt{x}\log y + 2^{2t}\sqrt{x}\log x)$$
$$= O(2^{2t}\sqrt{x}\log x) = o(\frac{x}{\log x}),$$

where t is the number of rational primes $\leq y$, thus $t = O(\frac{y}{\log y})$.

Using Lemmas 2.7 and 2.8 we see that the series $\sum_{m,n}\frac{\mu(m)\mu(n)c_{m,n}}{d_{m,n}}$ is absolutely convergent. Now choose y properly ($y = O(\log x)$), combining (1), Claim 3 and Claim 4, we arrive at

$$f(x,K) = \sum_{m,n}\frac{\mu(m)\mu(n)c_{m,n}}{d_{m,n}}\frac{x}{\log x} + o(\frac{x}{\log x}).$$

Therefore we conclude that $\mathrm{den}(M_\alpha) = \sum_{m,n}\frac{\mu(m)\mu(n)c_{m,n}}{d_{m,n}}$. □

We are particularly interested in the case $N(\alpha) = p^s$, where p is a prime splitting in the imaginary quadratic field K. As in §**2**, the case $K = \mathbb{Q}(\sqrt{-3}) = K(\boldsymbol{\mu}_3)$ requires special attention. Suppose that $K = \mathbb{Q}(\sqrt{-3})$ and $\alpha \neq 0 \in \mathcal{O}_K$, $\gcd(\alpha, \alpha^\tau) = 1$, and $N(\alpha) = p^s$, with s an integer prime to 6. Then the principal ideal (α) is equal to $(\beta)^s$ for some primary prime of $\mathcal{O}_K$ lying above p. There is an unique integer $\delta(\alpha)$ modulo 6 with $\alpha = \zeta_6^{\delta(\alpha)}\beta^s$. From the classical theory of cubic Gauss sums (c.f. [3], Chap. 9), one knows that $p\beta \in K(\boldsymbol{\mu}_p)^{\star 3}$. Then it follows that for any square-free odd integer n, $u = \frac{\alpha^\tau}{\alpha} \in K(\boldsymbol{\mu}_n)^{\star 3}$ if and only if $3 \mid \delta(\alpha)$ and $p \mid n$. In the following we shall call an imaginary quadratic integer α exceptional if $\alpha \in K$, and $\alpha = \pm\beta^s$ with β primary prime. All other imaginary quadratic integers are called nonexceptional. From Lemma

2.6, we know that if α is nonexceptional then $E_m \cap F_n = k_m(\boldsymbol{\mu}_m) \cap K(\boldsymbol{\mu}_n)$ always holds for relatively prime square free positive integer m, n with n odd.

Let h denote the class number of K. For any positive integer n, let $f(n)$ denote the number of odd prime divisors of n. We are ready to derive a precise formula for the density.

THEOREM 3.3. *Assume GRH holds. Suppose* $\alpha \in \mathcal{O}_K \backslash \mathcal{O}_K{}^\star$, $\gcd(\alpha, \alpha^\tau) = 1$ *and* $N(\alpha) = p^s$, *where* p *is a prime splitting in* K, s *is an integer satisfying* $\gcd(6, s) = 1$ *and* $f(s) = f(\frac{s}{\gcd(s,h)})$. *Then* M_α *has positive density given by*

$$\mathrm{den}(M_\alpha) = \begin{cases} \frac{1}{4} \prod_{q|s,\, q\neq p} (1 - \frac{2}{(q-1)}) \prod_{q\geq 3,\, q\nmid ps} (1 - \frac{2}{q(q-1)}) & \textit{if } p \equiv 1 \pmod 4 \textit{ or } \alpha \textit{ is exceptional,} \\ \frac{1}{4} \prod_{q|s} (1 - \frac{2}{(q-1)}) \prod_{q\geq 3,\, q\nmid s} (1 - \frac{2}{q(q-1)}) & \textit{otherwise.} \end{cases}$$

Remark. 1. The condition $\gcd(6, s) = 1$ in Theorem 3.3 is essential.

2. It is possible to remove the condition $f(s) = f\big(\frac{s}{\gcd(s,h)}\big)$ from Theorem 3.3. In doing so, one has to modify the Euler factors in the infinite product which corresponds to primes dividing s. Writing $(\alpha) = \mathfrak{a}^s$, and let o be the order of the ideal class of $\mathfrak{a}$. The primes dividing $s' = s/o$ and those dividing o will give different contributions to the density, where s' is the largest integer with the property that $u \in (K^\star)^{s'}$.

Proof of Theorem 3.3. Since $f(s) = f(\frac{s}{\gcd(s,h)})$, one has $n_1 = n_2$ for all square free integer n.

First Case: Suppose that $p \equiv 1 \pmod 4$.
Case 1.1: $D_K \equiv 0 \pmod 4$.

By Lemma 2.6 for relatively prime square free positive integers m, n with n odd, we have

$$E_m \cap F_n = \begin{cases} \mathbb{Q}(\sqrt{p}) & \text{if } 2 \mid m \text{ and } p \mid n, \\ \mathbb{Q} & \text{otherwise,} \end{cases}$$

Then from Lemma 2.7 and 2.8, we obtain

$$c_{m,n} = 1 \text{ and } d_{m,n} = \begin{cases} m_1 n_1 \phi(mn) & \text{if } 2p \mid mn, \\ 2m_1 n_1 \phi(mn) & \text{otherwise.} \end{cases}$$

Applying Theorem 3.2, we have

$$\begin{aligned}
\mathrm{den}(M_\alpha) &= \sum_{\substack{m,\,n,\,2\nmid n\\ 2p\nmid mn}} \frac{\mu(mn)}{2m_1n_1\phi(mn)} + \sum_{\substack{m,\,n,\,2\nmid n\\ 2p\mid mn}} \frac{\mu(mn)}{m_1n_1\phi(mn)} \\
&= \sum_{2p\nmid c} \frac{2^{f(c)}\mu(c)}{2c_1\phi(c)} + \sum_{2p\mid c} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)} \\
&= \sum_{c} \frac{2^{f(c)}\mu(c)}{2c_1\phi(c)} + \sum_{2p\mid c} \frac{2^{f(c)}\mu(c)}{2c_1\phi(c)} \\
&= \frac{1}{4}\prod_{q\geq 3}(1-\frac{2}{q_1(q-1)}) + \frac{1}{2p_1(p-1)}\prod_{q\geq 3,\, q\neq p}(1-\frac{2}{q_1(q-1)}) \\
&= \frac{1}{4}\prod_{q\geq 3,\, q\neq p}(1-\frac{2}{q_1(q-1)}) \\
&= \frac{1}{4}\prod_{q\mid s,\, q\neq p}(1-\frac{2}{(q-1)})\prod_{q\geq 3,\, q\nmid ps}(1-\frac{2}{q(q-1)}) > 0.
\end{aligned}$$

Case 1.2: $-D_K \equiv 1 \pmod 4$, i.e. $K = \mathbb{Q}(\sqrt{-a}), a \equiv 3 \pmod 4$. Also the integer α is assumed to be nonexceptional.

By Lemma 2.6, for relatively prime square free positive integers m, n with n odd, we have that $E_m \cap F_n = k_m(\boldsymbol{\mu}_m) \cap K(\boldsymbol{\mu}_n)$ is totally real except when $a \mid mn$ with $\gcd(a,n) \equiv 1 \pmod 4$, in that case it contains the imaginary field $\mathbb{Q}(\sqrt{-a/\gcd(a,n)})$. From Lemmas 2.7 and 2.8, we get

$$c_{m,n} = \begin{cases} 0 & \text{if } a \mid mn \text{ and } \gcd(a,n) \equiv 1 \pmod 4, \\ 1 & \text{otherwise,} \end{cases}$$

$$d_{m,n} = \begin{cases} \frac{1}{2}m_1n_1\phi(mn) & \text{if } 2ap \mid mn, \\ m_1n_1\phi(mn) & \text{if either } a \mid mn \text{ or } 2p \mid mn, \text{ but not both,} \\ 2m_1n_1\phi(mn) & \text{otherwise.} \end{cases}$$

In order to compute $\mathrm{den}(M_\alpha)$ in this case, we first compute two sums S_1, S_2:

$$\begin{aligned} S_1 &= \sum_{\substack{m,\,n,\,2\nmid n \\ a\nmid mn,\,2p\nmid mn}} \frac{\mu(mn)}{2m_1n_1\phi(mn)} + \sum_{\substack{m,\,n,\,2\nmid n \\ a\nmid mn,\,2p\mid mn}} \frac{\mu(mn)}{m_1n_1\phi(mn)} \\ &= \sum_{a\nmid c,\,2p\nmid c} \frac{2^{f(c)}\mu(c)}{2c_1\phi(c)} + \sum_{a\nmid c,\,2p\mid c} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)} \\ &= \sum_{a\nmid c} \frac{2^{f(c)}\mu(c)}{2c_1\phi(c)} + \sum_{a\nmid c,\,2p\mid c} \frac{2^{f(c)}\mu(c)}{2c_1\phi(c)} \\ &= \sum_{c} \frac{2^{f(c)}\mu(c)}{2c_1\phi(c)} - \sum_{a\mid c} \frac{2^{f(c)}\mu(c)}{2c_1\phi(c)} + \sum_{2p\mid c} \frac{2^{f(c)}\mu(c)}{2c_1\phi(c)} - \sum_{2ap\mid c} \frac{2^{f(c)}\mu(c)}{2c_1\phi(c)} \\ &= \frac{1}{4}\prod_{q}(1-\frac{2}{q_1(q-1)}) - \frac{2^{f(a)}\mu(a)}{4a_1\phi(a)}\prod_{q\ge 3,\,q\nmid a}(1-\frac{2}{q_1(q-1)}) \\ &+ \frac{1}{2p_1(p-1)}\prod_{q\ge 3,\,q\ne p}(1-\frac{2}{q_1(q-1)}) - \frac{2^{f(a)}\mu(a)}{2p_1(p-1)a_1\phi(a)}\prod_{q\ge 3,\,q\nmid ap}(1-\frac{2}{q_1(q-1)}) \\ &= \frac{1}{4}(\prod_{q\mid a}(1-\frac{2}{q_1(q-1)}) - \frac{2^{f(a)}\mu(a)}{a_1\phi(a)})\prod_{q\ge 3,\,q\nmid ap}(1-\frac{2}{q_1(q-1)}). \end{aligned}$$

Next consider

$$S_2 = \sideset{}{'}\sum_{\substack{m,\,n,\,2\nmid n \\ a\mid mn,\,2p\nmid mn}} \frac{\mu(mn)}{m_1n_1\phi(mn)} + \sideset{}{'}\sum_{\substack{m,\,n,\,2\nmid n \\ a\mid mn,\,2p\mid mn}} \frac{2\mu(mn)}{m_1n_1\phi(mn)},$$

where the dash indicates that the sum runs through m, n with $\gcd(a,n) \equiv 3 \pmod 4$. Define for each integer r the function $f_r : \mathbb{Z}_{>0} \longrightarrow \mathbb{Z}$ by $f_r(n) = n/\gcd(n,r)$. Note that $n_1 = f_s(n)$ for every positive integer n. Let m and n be relatively prime integer, let a be a divisor of mn. Then one has $f_s(mn) = f_s(m)f_s(n)$, $mn = af_a(m)f_a(n)$, and

$$f_s(a)\cdot f_s\big(f_a(m)\big)f_s\big(f_a(n)\big) = f_s\big(af_a(m)f_a(n)\big) = f_s(mn) = f_s(m)f_s(n).$$

Thus

$$\frac{\mu(mn)}{m_1n_1\phi(mn)} = \frac{\mu(a)}{a_1\phi(a)}\frac{\mu\big(f_a(m)f_a(n)\big)}{f_a(m)_1f_a(n)_1\phi\big(f_a(m)f_a(n)\big)}.$$

For any positive integer n, let $g(n)$ denote the number of prime divisors of n that is congruent to 3 modulo 4. For each ordered-pair (m',n') with $\gcd(a,m'n') = 1$, the number of ordered pair (m,n) with $a \mid mn, n$ odd, and $g\big(\gcd(a,n)\big)$ odd satisfying $m' = f_a(m)$ and $n' = f_a(n)$ is equal to

$$\begin{aligned} &\left(\binom{g(a)}{1} + \binom{g(a)}{3} + \cdots \binom{g(a)}{g(a)}\right)\cdot 2^{f(a)-g(a)} \\ =&2^{g(a)-1}\cdot 2^{f(a)-g(a)} = 2^{f(a)-1}. \end{aligned}$$

Therefore,

$$
\begin{aligned}
S_2 &= \frac{2^{f(a)-1}\mu(a)}{a_1\phi(a)}\Big(\sum_{\substack{m,\,n,\,2\nmid n\\ 2p\nmid mn\,\gcd(a,mn)=1}} \frac{\mu(mn)}{m_1n_1\phi(mn)} + \sum_{\substack{m,\,n,\,2\nmid n\\ \gcd(a,mn)=1,\,2p\mid mn}} \frac{2\mu(mn)}{m_1n_1\phi(mn)}\Big)\\
&= \frac{2^{f(a)}\mu(a)}{2a_1\phi(a)}\Big(\sum_{\gcd(a,c)=1,\,2p\nmid c} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)} + \sum_{\gcd(a,c)=1,\,2p\mid c} \frac{2^{f(c)+1}\mu(c)}{c_1\phi(c)}\Big)\\
&= \frac{2^{f(a)}\mu(a)}{2a_1\phi(a)}\Big(\sum_{\gcd(a,c)=1} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)} + \sum_{\gcd(a,c)=1,\,2p\mid c} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)}\Big)\\
&= \frac{2^{f(a)}\mu(a)}{4a_1\phi(a)}\prod_{q\geq 3,\,q\nmid a}(1-\frac{2}{q_1(q-1)}) + \frac{2^{f(a)}\mu(a)}{2p_1(p-1)a_1\phi(a)}\prod_{q\geq 3,\,q\nmid ap}(1-\frac{2}{q_1(q-1)})\\
&= \frac{2^{f(a)}\mu(a)}{4a_1\phi(a)}\prod_{q\geq 3, q\nmid ap}(1-\frac{2}{q_1(q-1)}).
\end{aligned}
$$

Applying Theorem 3.2, we have

$$
\operatorname{den}(M_\alpha) = S_1 + S_2 = \frac{1}{4}\prod_{q\geq 3,\,q\neq p}(1-\frac{2}{q_1(q-1)}).
$$

Case 1.3: Suppose $K=\mathbb{Q}(\sqrt{-3})$ and α is exceptional

For square free m,n, n odd and $3\nmid m$, we compute $[E_m\cap F_n:\mathbb{Q}]$ using Lemma 2.6. If $\gcd(3p,n)=1$ and $2\nmid m$, we obtain $E_m\cap F_n=\mathbb{Q}$. If $p\mid m$ and $3\mid n$, then as in Case 3.1 $E_m\cap F_n = k_m(\boldsymbol{\mu}_m)\cap K(\boldsymbol{\mu}_n,\sqrt[3]{u})$ is cubic over $\mathbb{Q}$ no matter m is even or odd. When m is even, we also have $E_m\cap F_n=\mathbb{Q}$ if $\gcd(3p,n)=1$ or $p\nmid mn$. On the other hand, $E_m\cap F_n=\mathbb{Q}(\sqrt{p})$ if $p\mid n$. Therefore $E_m\cap F_n$ is always totally real, and

$$
c_{m,n} = \begin{cases} 0 & \text{if } 3\mid m,\\ 1 & \text{if } 3\nmid m.\end{cases}
$$

By Lemma 2.8, If $3\nmid m$ and $2\nmid m$, then

$$
d_{m,n} = \begin{cases} 2m_1n_1\phi(mn) & \text{if } 3\nmid n,\\ m_1n_1\phi(mn) & \text{if } 3\mid n \text{ and } p\nmid mn,\\ \frac{m_1n_1\phi(mn)}{3} & \text{if } 3\mid n \text{ and } p\mid mn.\end{cases}
$$

If $3\nmid m$ and $2\mid m$, then

$$
d_{m,n} = \begin{cases} 2m_1n_1\phi(mn) & \text{if } 3\nmid n \text{ and } p\nmid mn,\\ m_1n_1\phi(mn) & \text{if } 3\nmid n \text{ and } p\mid mn,\\ m_1n_1\phi(mn) & \text{if } 3\mid n \text{ and } p\nmid mn,\\ \frac{m_1n_1\phi(mn)}{6} & \text{if } 3\mid n \text{ and } p\mid mn.\end{cases}
$$

In order to compute $\mathrm{den}(M_\alpha)$, we first evaluate sums S_3, S_4 as follows:

$$S_3 = \sum_{\substack{m,\,n,\,2\nmid n\\ 3\nmid mn, 2\nmid m}} \frac{\mu(mn)}{2m_1n_1\phi(mn)} + \sum_{\substack{m,\,n,\,2\nmid n\\ 3\nmid mn, 2\mid m\\ p\nmid mn}} \frac{\mu(mn)}{2m_1n_1\phi(mn)} + \sum_{\substack{m,\,n,\,2\nmid n\\ 3\nmid mn, 2\mid m\\ p\mid mn}} \frac{\mu(mn)}{m_1n_1\phi(mn)}$$

$$= \sum_{\substack{m,\,n,\,2\nmid n\\ 3\nmid mn}} \frac{\mu(mn)}{2m_1n_1\phi(mn)} + \sum_{\substack{m,\,n,\,2\nmid n\\ 3\nmid mn, 2\mid m,\, p\mid mn}} \frac{\mu(mn)}{2m_1n_1\phi(mn)}$$

$$= \frac{1}{4} \sum_{\substack{m,\,n\\ \gcd(6,mn)=1}} \frac{\mu(mn)}{m_1n_1\phi(mn)} - \frac{1}{4} \sum_{\substack{m,\,n\\ \gcd(6,mn)=1,\, p\mid mn}} \frac{\mu(mn)}{m_1n_1\phi(mn)}$$

$$= \frac{1}{4} \sum_{\gcd(6,c)=1} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)} - \frac{1}{4} \sum_{\gcd(6,c)=1,\, p\mid c} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)} = \frac{1}{4} \sum_{\gcd(6p,c)=1} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)},$$

$$S_4 = \sum_{\substack{m,\,n,\,2\nmid n\\ 3\nmid m,\, 2\nmid m,\, 3\mid n,\, p\mid mn}} \frac{3\mu(mn)}{m_1n_1\phi(mn)} + \sum_{\substack{m,\,n,\,2\nmid n\\ 3\nmid m,\, 2\mid m,\, 3\mid n,\, p\mid mn}} \frac{6\mu(mn)}{m_1n_1\phi(mn)} = 0.$$

Applying Theorem 3.2, we have

$$\mathrm{den}(M_\alpha) = S_3 + S_4 + \sum_{\substack{m,\,n,\,2\nmid n\\ 3\nmid m,\, 3\mid n,\, p\nmid mn}} \frac{\mu(mn)}{m_1n_1\phi(mn)}$$

$$= \frac{1}{4} \sum_{\gcd(6p,c)=1} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)} - \frac{1}{12} \sum_{\gcd(6p,c)=1} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)}$$

$$= \frac{1}{6} \sum_{\gcd(6p,c)=1} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)} = \frac{1}{4} \prod_{q\mid s,\, q\neq p} (1 - \frac{2}{(q-1)}) \prod_{q\geq 3,\, q\nmid ps} (1 - \frac{2}{q(q-1)}).$$

Second Case: Suppose $p \not\equiv 1 \pmod 4$.

Case 2.1: $D_K \equiv 0 \pmod 4$. Then the possibility is $D_K \equiv 4 \pmod 8$ and $p \equiv 3 \pmod 4$.

By Lemmas 2.6, 2.7 and 2.8, for relatively prime square free positive integers m, n with n odd, we have

$$E_m \cap F_n = \mathbb{Q},\ c_{m,n} = 1, \text{ and } d_{m,n} = 2m_1n_1\phi(mn).$$

Then by Theorem 3.2, we have

$$\mathrm{den}(M_\alpha) = \sum_{m,\,n,\,2\nmid n} \frac{\mu(mn)}{2m_1n_1\phi(mn)} = \sum_c \frac{2^{f(c)}\mu(c)}{2c_1\phi(c)}$$

$$= \frac{1}{4}\prod_{q\geq 3}(1 - \frac{2}{q_1(q-1)})$$

$$= \frac{1}{4}\prod_{q\mid s}(1 - \frac{2}{(q-1)}) \prod_{q\geq 3,\, q\nmid s} (1 - \frac{2}{q(q-1)}) > 0.$$

Case 2.2: $-D_K \equiv 1 \pmod 4$, i.e. $a \equiv 3 \pmod 4$. The integer α is assumed to be nonexceptional. Note the case $p = 2$ is allowed here.

By Lemmas 2.6, 2.7 and 2.8, for relatively prime square free positive integers m, n with n odd, we have

$$E_m \cap F_n = \begin{cases} \mathbb{Q}(\sqrt{-a/\gcd(a,n)}) & \text{if } a \mid mn \text{ and } \gcd(a,n) \equiv 1 \pmod 4, \\ \mathbb{Q}(\sqrt{a/\gcd(a,n)}) & \text{if } a \mid mn \text{ and } \gcd(a,n) \equiv 3 \pmod 4, \\ \mathbb{Q} & \text{otherwise,} \end{cases}$$
$$c_{m,n} = \begin{cases} 0 & \text{if } a \mid mn \text{ and } \gcd(a,n) \equiv 1 \pmod 4, \\ 1 & \text{otherwise,} \end{cases}$$
$$d_{m,n} = \begin{cases} m_1 n_1 \phi(mn) & \text{if } a \mid mn, \\ 2m_1 n_1 \phi(mn) & \text{otherwise.} \end{cases}$$

We start with the sum

$$S_5 = \sum_{\substack{m,\,n,\,2\nmid n \\ a \mid mn}}{}' \frac{\mu(mn)}{m_1 n_1 \phi(mn)}.$$

where the dash indicates that the sum runs through m, n with $\gcd(a,n) \equiv 3 \pmod 4$. Similar to the computation of S_2, we have

$$S_5 = \frac{2^{f(a)}\mu(a)}{2a_1\phi(a)} \sum_{\gcd(a,c)=1} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)}.$$

Applying Theorem 3.2, we have

$$\begin{aligned} \operatorname{den}(M_\alpha) &= \sum_{\substack{m,\,n,\,2\nmid n \\ a\nmid mn}} \frac{\mu(mn)}{2m_1 n_1 \phi(mn)} + S_5 \\ &= \sum_{c} \frac{2^{f(c)}\mu(c)}{2c_1\phi(c)} = \frac{1}{4}\prod_{q\geq 3}(1 - \frac{2}{q_1(q-1)}). \end{aligned}$$

Case 2.3: Suppose $K = \mathbb{Q}(\sqrt{-3})$ and α is exceptional. Note that $p \equiv 3 \mod 4$.

Using Lemma 2.6, for square free m, n, n odd and $3 \nmid m$, we compute $E_m \cap F_n = \mathbb{Q}$ if $3 \nmid n$, or $p \nmid n$. On the other hand, if $p \mid m$ and $3 \mid n$, then $E_m \cap F_n = k_m(\boldsymbol{\mu}_m) \cap K(\boldsymbol{\mu}_n, \sqrt[3]{u})$ is a cubic extension of $\mathbb{Q}$. Thus $E_m \cap F_n$ is always totally real, and

$$c_{m,n} = \begin{cases} 0 & \text{if } 3 \mid m, \\ 1 & \text{if } 3 \nmid m. \end{cases}$$

From Lemma 2.8, we also obtain, for $3 \nmid m$:

$$d_{m,n} = \begin{cases} 2m_1 n_1 \phi(mn) & \text{if } 3 \nmid n, \\ m_1 n_1 \phi(mn) & \text{if } 3 \mid n \text{ and } p \nmid mn, \\ \frac{m_1 n_1 \phi(mn)}{3} & \text{if } 3 \mid n \text{ and } p \mid mn. \end{cases}$$

Applying Theorem 3.2, we see that the value of $\mathrm{den}(M_\alpha)$ is

$$\sum_{\substack{m,\,n,\,2\nmid n\\ 3\nmid mn}} \frac{\mu(mn)}{2m_1n_1\phi(mn)} + \sum_{\substack{m,\,n,\,2\nmid n\\ 3\nmid m,\,3|n,\,p\nmid mn}} \frac{\mu(mn)}{m_1n_1\phi(mn)} + \sum_{\substack{m,\,n,\,2\nmid n\\ 3\nmid m,\,3|n,\,p|mn}} \frac{3\mu(mn)}{m_1n_1\phi(mn)}$$

$$= \sum_{\substack{m,\,n\\ \gcd(6,mn)=1}} \frac{\mu(mn)}{4m_1n_1\phi(mn)} - \sum_{\substack{m,\,n\\ \gcd(6p,mn)=1}} \frac{\mu(mn)}{12m_1n_1\phi(mn)}$$

$$- \sum_{\substack{m,\,n\\ \gcd(6p,mn)=p}} \frac{\mu(mn)}{4m_1n_1\phi(mn)}$$

$$= \frac{1}{4}\sum_{\gcd(6,c)=1} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)} - \frac{1}{12}\sum_{\gcd(6p,c)=1} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)} - \frac{1}{4}\sum_{\gcd(6,c)=1,\,p|c} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)}$$

$$= \frac{1}{6}\sum_{\gcd(6p,c)=1} \frac{2^{f(c)}\mu(c)}{c_1\phi(c)} = \frac{1}{4}\prod_{q|s,\,q\neq p}(1-\frac{2}{(q-1)})\prod_{q\geq 3,\,q\nmid ps}(1-\frac{2}{q(q-1)}). \qquad \square$$

4. Applications to Elliptic Curves over Finite Fields. Let $\mathbb{F}_r$ denote a finite field of characteristic p with $r = p^s$ elements. Given an elliptic curve E defined over $\mathbb{F}_r$, we would like to know the size of the Galois extension of $\mathbb{F}_r$ obtained through adjoining coordinates of all ℓ-torsion points where ℓ is a prime. Let $E[\ell] \subset E(\bar{\mathbb{F}}_r)$ be the set of all these ℓ-torsion points. Let End_E denote the endomorphism ring of E and let $\alpha = \alpha_E \in \mathrm{End}_E$ be the Frobenius endomorphism which raises the coordinates of points on E to its r-th power. Then the size of the Galois extension in question is the degree $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$ which equals to the order of the Frobenius endomorphism acting on $E[\ell]$. If the curve E is not supersingular, a well-known theorem of Hasse asserts that $\mathbb{Z}[\alpha] \subset \mathrm{End}_E$ which can be identified with an order in an imaginary quadratic field $K = K_E$. If E is supersingular, it may happen that $\alpha_E \in \mathbb{Z}$, or else $\mathbb{Z}[\alpha]$ is still contained in an imaginary quadratic field $K = K_E$. We let $\mathrm{disc}(\alpha)$ be the discriminant of $\mathbb{Z}[\alpha]$. The following proposition bounds $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$ in the non-supersingular case:

PROPOSITION 4.1. *Given a non-supersingular elliptic curve $E_{/\mathbb{F}_r}$ with (geometric) Frobenius endomorphism α embedded in an imaginary quadratic field K. Let e_2 be the largest divisor of 24 such that $\alpha \in (K^\star)^{e_2}$, and $e_1 = 2$, or 1 according to whether α is a square in K. Suppose prime $\ell > 3$ and $\ell \nmid p\,\mathrm{disc}(\alpha)$. Then*

$$[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r] \leq \begin{cases} \frac{\ell^2-1}{e_2}, & \text{if } \ell \text{ is inert in } K/\mathbb{Q} \\ \frac{\ell-1}{e_1}, & \text{if } \ell \text{ splits in } K/\mathbb{Q} \end{cases}$$

Proof. The degree $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$ is exactly the order of the endomorphism α inside $(\mathrm{End}_E/\ell\,\mathrm{End}_E)^\star$. Since ℓ does not divide $\mathrm{disc}(\alpha)$, we have $\mathbb{Z}[\alpha]/\ell\mathbb{Z}[\alpha] \cong \mathrm{End}_E/\ell\,\mathrm{End}_E \cong \mathcal{O}_K/\ell\mathcal{O}_K$, hence $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$ equals the order of α inside the group $(\mathcal{O}_K/\ell\mathcal{O}_K)^\star$. If ℓ is inert in $K/\mathbb{Q}$, then we have $\#((\mathcal{O}_K/\ell\mathcal{O}_K)^\star) = \ell^2 - 1$ which is divisible by 24. On the other hand if ℓ splits in $K/\mathbb{Q}$, the group $(\mathcal{O}_K/\ell\mathcal{O}_K)^\star$ has exponent $\ell - 1$. The desired bound follows immediately from these observations. $\square$

We are interested in the distribution of the degrees $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$ as the prime number ℓ varies. In particular, how often the Galois extension degree $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$ can be the largest possible, in other words, is equal to $(\ell^2 - 1)/e_2$? We consider therefore the following set of primes:

$$M_E = \{\ell \mid \ell \in \mathbb{P},\ [\mathbb{F}_r(E[\ell]) : \mathbb{F}_r] = (\ell^2 - 1)/e_2\}.$$

The main theorem to be established is:

THEOREM 4.2. *Assume GRH holds, and suppose* $\gcd(s, 6) = 1$. *Let* $E_{/\mathbb{F}_r}$ *be any elliptic curve which is not supersingular . Then the set* M_E *always has positive density.*

Proof. Let $K = K_E$, with h equals to the class number of $\mathcal{O}_K$. First, we apply Theorem 3.2 to the Frobenius $\alpha = \alpha_E$. This shows that the set M_E has a density, since it differs from M_α only by a finite set. Next we can multiply s by suitable powers of those prime factors of h not dividing 6 so that s' and $s'/\gcd(s', h)$ has the same set of odd prime factors. Extending the base field to $\mathbb{F}_{p^{s'}}$, and replacing the curve E by E' which is the original E over $\mathbb{F}_{p^{s'}}$. Then the Frobenius $\alpha' = \alpha_{E'}$ satisfies the hypothesis of Theorem 3.3. It follows that the set $M_{E'}$ has positive density. To finish the proof, it suffices to show that $M_{\alpha'} \subseteq M_\alpha$. This follows from the fact that the order of α modulo ℓ is at least the order of α' modulo ℓ because α' is a power of α. □

For prime fields $\mathbb{F}_r = \mathbb{F}_p$, a precise value of the density can be given.

THEOREM 4.3. *Given an elliptic curve* $E_{/\mathbb{F}_p}$ *which is not supersingular. Suppose GRH holds. Then the density of* M_E *is :*

$$\mathrm{den}(M_E) = \begin{cases} (1 - \frac{2}{p(p-1)})^{-1} C_2 & \text{if } p \equiv 1 \pmod 4 \text{ or } \alpha \text{ is exceptional,} \\ C_2 & \text{otherwise,} \end{cases}$$

where C_2 *is the constant:*

$$C_2 = \frac{1}{4} \prod_{q \neq 2 \text{ prime}} (1 - \frac{2}{q(q-1)}) = 0.133776\cdots.$$

Proof. Since $\mathrm{den}(M_E) = \mathrm{den}(M_\alpha)$ in this case (s=1), the formula follows from Theorem 3.3 immediately. □

Let $t_E \in \mathbb{Z}$ denote the trace of the Frobenius endomorphism. If the curve E is supersingular, bounds on $[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r]$ are given by

PROPOSITION 4.4. *Suppose* $E_{/\mathbb{F}_r}$ *is supersingular and* ℓ *does not divide* $\mathrm{disc}(\alpha)$. *Then*

$$[\mathbb{F}_r(E[\ell]) : \mathbb{F}_r] \leq \begin{cases} (\ell - 1), & \text{if } t_E = \pm 2\sqrt{r}, \text{ and } s \text{ even} \\ 2(\ell - 1), & \text{if } t_E = 0 \\ 3(\ell - 1), & \text{if } t_E = \pm\sqrt{r}, \text{ and } s \text{ even} \\ 4(\ell - 1), & \text{if } t_E = \pm p^{(s+1)/2}, \ s \text{ odd, and } p = 2 \\ 6(\ell - 1), & \text{if } t_E = \pm p^{(s+1)/2}, \ s \text{ odd, and } p = 3 \end{cases}$$

Proof. Frobenius endomorphisms of all supersingular elliptic curves have been computed explicitly by Deuring (c.f.[7], Theorem 4.1). If $t_E = \pm 2\sqrt{r}$ and s is even, $\alpha_E \in \mathbb{Z}$. If $t_E = 0$, $\alpha_E = \pm\sqrt{-r}$, then $\alpha_E^2 \in \mathbb{Z}$. If $t_E = \pm\sqrt{r}$, and s is even, $\alpha_E = \pm p^{\frac{s}{2}} \frac{1 \pm \sqrt{-3}}{2}$, $\alpha_E^3 \in \mathbb{Z}$. If $t_E = \pm 2^{\frac{(s+1)}{2}}$ and s is odd, $\alpha_E = \pm 2^{\frac{s+1}{2}}(1 \pm \sqrt{-1})$, $\alpha_E^4 \in \mathbb{Z}$. If $t_E = \pm 3^{\frac{(s+1)}{2}}$ and s is odd, $\alpha_E = \pm 3^{\frac{s-1}{2}} \frac{3 \pm \sqrt{-3}}{2}$, $\alpha_E^6 \in \mathbb{Z}$. The proposition follows from this information immediately. □

Combining Theorem 4.3 with Proposition 4.4 we obtain the following characterization of supersingular elliptic curves:

COROLLARY 4.5. *Assume GRH holds. Then* $E_{/\mathbb{F}_p}$ *is supersingular if and only if* $[\mathbb{F}_p(E[\ell]) : \mathbb{F}_p] = O(\ell - 1)$ *as* ℓ *runs through the rational primes.*

In fact, in the supersingular case, it is not difficult to derive from Hooley's classical work on Artin's primitive roots conjecture (c.f. [2] or [4], the details are left to the reader) for the torus $\mathbb{G}_m$, the following result

THEOREM 4.6. *Assume GRH holds. Let $E_{/\mathbb{F}_p}$ be a supersingular elliptic curve. Then the set of primes ℓ satisfying $[\mathbb{F}_p(E[\ell]) : \mathbb{F}_p] = 2(\ell - 1)$ has a positive density.*

REFERENCES

[1] Y.-M. J. CHEN, *On primitive roots of one-dimensional tori*, Preprint, 2000.
[2] C. HOOLEY, *On Artin's conjecture*, J. reine angew Math., 225 (1967), pp. 209–220.
[3] K. IRELAND AND M. ROSEN, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, New York, 1982.
[4] M. R. MURTY, *On Artin's conjecture*, Journal of Number Theory, 16 (1983), pp. 147–168.
[5] G. ROTA, *On the foundations of combinatorial theory, I. theory of möbius functions*, Z. Wahrsch. Verw. Gebiete, 2 (1964), pp. 340–368.
[6] J.-P. SERRE, *Quelques applications du Théorème de densité de Chebotarev*, Publ. Math. IHES, 54 (1981), pp. 123–201.
[7] W. C. WATERHOUSE, *Abelian varieties over finite fields*, Ann. scient. EC. Norm. Sup., 2 (1969), pp. 521–560.