COMPOSITIO MATHEMATICA

RAJIV GUPTA
M. RAM MURTY

Primitive points on elliptic curves

Compositio Mathematica, tome 58, n° 1 (1986), p. 13-44.
<http://www.numdam.org/item?id=CM_1986__58_1_13_0>

Compositio Mathematica 58 (1986) 13–44

PRIMITIVE POINTS ON ELLIPTIC CURVES *

Rajiv Gupta and M. Ram Murty [1]

§1. Introduction

A classical conjecture of E. Artin predicts the density of primes p for which a given rational number is a primitive root modulo p. An analogous conjecture for elliptic curves was formulated by Lang and Trotter in [12]. For the sake of definiteness, let E be an elliptic curve defined over the rational numbers $\mathbb{Q}$. Let a be a rational point of infinite order. The problem is to determine the density of primes p for which $\overline{E}(\mathbb{F}_p)$ (the rational points of the curve E viewed over the finite field $\mathbb{F}_p$) is generated by $\bar{a}$, the reduction of a(modulo p). Such a point is called *primitive* for these primes. In [12] it was conjectured the density of primes p for which a is a primitive point always exists.

The purpose of this paper is to prove this conjecture under the assumption of a suitable generalized Riemann hypothesis (henceforth abbreviated GRH) in the case that E has complex multiplication (CM). For simplicity, we assume that E has CM by the entire ring of integers $\mathcal{O}_k$ of an imaginary quadratic field k. Our method deals only with those rational primes which split in k, the supersingular primes being intractible by our method.

The assumption of the GRH can be relaxed somewhat and the situation is analogous to Hooley [6], where the classical conjecture of Artin was settled under a similar hypothesis.

Let us denote by $N_a(x)$, the number of primes $p \leqslant x$, such that p splits in k *and* a is a primitive point (mod p). We shall prove:

THEOREM 1: *Let E be an elliptic curve defined over $\mathbb{Q}$ with complex multiplication by $\mathcal{O}_k$ and let a be a rational point of infinite order. Under the GRH,*

$$N_a(x) = C_E(a)\frac{x}{\log x} + O\left(\frac{x \log\log x}{(\log x)^2}\right),$$

as $x \to \infty$.

[1] Supported in part by NSERC grant #U0237.

* This work was done while the authors were visiting the Institute for Advanced Study.

It would be of interest to determine when $C_E(a) > 0$. We are able to prove:

THEOREM 2: *If* 2 *and* 3 *are inert in* k *or* $k = \mathbb{Q}(\sqrt{-11})$, *then* $C_E(a) > 0$; *hence, on the GRH,*

$$N_a(x) \gg \frac{x}{\log x}$$

in these cases.

REMARK: Clearly, $C_E(a) = 0$ if all the 2-division points of E are rational.

In [12], Lang and Trotter formulated a condition for a prime q to divide the index $|\bar{E}(\mathbb{F}_p)\colon \langle \bar{a} \rangle|$, which we shall denote as $i(p)$. Indeed, let E_q denote the q-division points of E and consider the extension

$$T_q = \mathbb{Q}\left(E_q,\ q^{-1}a\right).$$

These fields are analogous to the splitting fields of $x^q - a = 0$ which occur in the classical Artin conjecture. The Galois group G_q of $T_q/\mathbb{Q}$ is a semidirect product of subgroups of $GL_2(\mathbb{F}_q)$ and E_q. Therefore, one can view elements of the Galois group as pairs of certain elements (γ, τ) with $\gamma \in GL_2(\mathbb{F}_q)$ and $\tau \in E_q$. For primes p not dividing the discriminant of $T_q/\mathbb{Q}$, let $\sigma_p = (\gamma_p, \tau_p)$ be the Frobenius element. It is then easy to show that q divides $i(p)$ if and only if $\sigma_p \in \overline{S_q}$, where $\overline{S_q}$ consists of all pairs (γ, τ) such that

i) $\gamma = 1$

or

ii) γ has eigenvalue 1, $\ker((\gamma - 1)\colon E_q \to E_q)$ is cyclic, and $\tau \in (\gamma - 1)E_q$.

It is easy to see that

$$|\overline{S_q}| \gg q^2$$

in the case that E has complex multiplication and

$$|\overline{S_q}| \gg q^4$$

if E has no complex multiplication. This was the source of difficulties in [12] in trying to prove the conjecture in line with Hooley's work for the Artin case. Our approach is different. We begin by considering the splitting fields of p in T_q. These extensions have degree $O(q^2)$ and we reformulate the above criterion in terms of these extensions. In doing this, we confine ourselves to primes p which split in k. This situation then becomes analogous to Hooley [6].

The case when E has no complex multiplication presents numerous difficulties. If instead of considering an infinite cyclic group generated by a, we consider a free subgroup Γ of rational points then it is indeed true that the primes p such that the image of $\Gamma(\text{mod } p)$ generates $\bar{E}(\mathbb{F}_p)$ have a density, *provided* that the rank of Γ is sufficiently large. In fact, this general situation was also formulated in [12].

Denote by $N_\Gamma(x)$ the number of primes $p \leqslant x$ such that $\bar{E}(\mathbb{F}_p) = \Gamma_p$, where Γ_p is the reduction of Γ mod p. We shall prove:

THEOREM 3: *Suppose that E has no complex multiplication and* $\text{rank}(\Gamma) \geqslant 18$. *Then, under GRH, there is a constant* $C_E(\Gamma)$ *such that*

$$N_\Gamma(x) = C_E(\Gamma)x/\log x + o(x/\log x)$$

as $x \to \infty$.

REMARK: At present, no curves are known with rank $\geqslant 13$. Nevertheless, it is believed that there are curves of arbitrary rank. One can also prove an analogous result in the CM case if $\text{rank}(\Gamma) \geqslant 10$.

In the case that E has CM, the assumption of GRH can be relaxed somewhat. A zero free region of $\text{Re}(s) > \frac{1}{2}$ for the zeta functions under consideration is not necessary. If we assume an $\alpha - \text{GRH}$, that is, a zero-free region of $\text{Re}(s) > \alpha$, then we can obtain an asymptotic formula for $\tilde{N}_\Gamma(x)$, consisting of those primes contributing to $N_\Gamma(x)$ and which split in k. The rank however has to increase correspondingly with the assumed zero-free region. The precise relationship is given in

THEOREM 4: *Suppose that E has CM by an order in k and that rank of* $\Gamma = r$. *Assuming an* $(r/r+1) - GRH$, *we have*

$$\tilde{N}_\Gamma(x) = \tilde{C}_E(\Gamma)x/\log x + o(x/\log x)$$

as $x \to \infty$.

REMARK: An analogous result can be formulated in the non-CM case also.

We can eliminate the GRH or any modified version of it if we resort to the lower bound sieve method. This however has the disadvantage that it does not produce a positive proportion of the primes with the desired property. Nevertheless, we do obtain an infinitude of such primes.

THEOREM 5: *If E has CM, and rank of* $\Gamma \geqslant 6$, *then*

$$N_\Gamma(x) \gg \frac{x}{(\log x)^2}.$$

Again, if the rank of Γ is sufficiently large, a similar result holds in the non-CM case.

The above result has the following curious corollary.

COROLLARY: *There is a finite set S which can be given explicitly, such that for some $a \in S$, $\bar{E}(\mathbb{F}_p) = \langle \bar{a} \rangle$ for infinitely many primes p, provided rank of $E(\mathbb{Q}) \geq 6$.*

§2. Divisibility criterion for the index

Throughout, we shall suppose that E is an elliptic curve defined over $\mathbb{Q}$, with complex multiplication by the integers $\mathcal{O}_k$ of an imaginary quadratic field k. In this section, we shall derive a criterion for the index $i(p)$ to be divisible by a prime q. This is essential for further analysis since $\langle \bar{a} \rangle = \bar{E}(\mathbb{F}_p)$ if and only if $q \nmid i(p)$ for any prime q.

Now suppose that E has good reduction at p and that $p \nmid \Delta$, where Δ denotes the discriminant of E. Let $\bar{E}$ be the reduction of E(modulo p). We would like to determine a criterion for a prime q to divide $i(p)$. First suppose that $q \neq p$. If the q-division points $\bar{E}[q]$ are contained in $\bar{E}(\mathbb{F}_p)$ then clearly $q \mid i(p)$, as $\bar{E}[q]$ is an elementary abelian group of type (q, q). If the q-division points are not contained in $\bar{E}(\mathbb{F}_p)$, then the q-primary part of $\bar{E}(\mathbb{F}_p)$ is cyclic. As q divides the index, there is a $\bar{b} \in \bar{E}(\mathbb{F}_p)$ such that $q \cdot \bar{b} = \bar{a}$. This essentially proves:

LEMMA 1: *Suppose that $p \nmid \Delta$ and $q \neq p$. Then $q \mid i(p)$ if and only if either*
(a) *$\bar{E}(\mathbb{F}_p) \supseteq \bar{E}[q]$ or*
(b) *the q-primary part of $\bar{E}(\mathbb{F}_p)$ is non-trivial and cyclic and there is a $\bar{b} \in \bar{E}(\mathbb{F}_p)$ such that $q \cdot \bar{b} = \bar{a}$.*

If $q = p$ and $p \mid i(p)$, then $a_p = 1$, for $p > 5$.

PROOF: For the first part of the lemma, the implication follows from the previous discussion and the converse is clear. For the second part, we have $p + 1 - a_p \equiv 0 (\mathrm{mod}\ p)$ and hence $a_p \equiv 1 (\mathrm{mod}\ p)$. But since $|a_p| \leq 2\sqrt{p}$, we must have $a_p = 1$ for $p > 5$. This completes the proof.

REMARK: The prime divisors of Δ introduce only an error of $O(1)$ in the final enumeration. Moreover, if $p \mid i(p)$, then $a_p = 1$ for $p > 5$ and hence by Serre [15], the number of such primes is $o(x/\log x)$. In fact, as we are in the complex multiplication case, the contribution is even less. Indeed, if $a_p = 1$, then as $2\pi_p = -a_p \pm \sqrt{a_p^2 - 4p}$, we must have $a_p^2 - 4p = Dn^2$ for some n. Here D is the discriminant of k. If $a_p = 1$, then p is in a quadratic progression. Clearly then if $p \leq x$ we must have $n = O(\sqrt{x})$, and therefore the contribution from such primes does not exceed $O(\sqrt{x})$.

It is possible by an elementary sieve method to improve this error term to $O(\sqrt{x}/\log x)$.

We now formulate this condition in terms of the Frobenius automorphism acting on certain number fields. For $\mathfrak{a}$ an ideal of k, we let $\mathfrak{a}^{-1}a$ denote a point $b \in E(\mathbb{C})$ such that $\alpha \cdot b = a$, where $\mathfrak{a} = (\alpha)$ (recall E is defined over $\mathbb{Q}$ so $\mathcal{O}_k$ has class number one). Note that $\mathfrak{a}^{-1}a$ is uniquely determined only up to translation by an $\mathfrak{a}$-division point and, because of the choice of α, complex multiplication by a unit in $\mathcal{O}_k$. For $\mathfrak{q}$ a first degree prime ideal of k, define

$$L_{\mathfrak{q}} = k\big(E[\mathfrak{q}],\ \mathfrak{q}^{-1}a\big),$$

where $E[\mathfrak{q}]$ denotes the $\mathfrak{q}$-division points of E. Then $L_{\mathfrak{q}}$ is independent of the choice of $\mathfrak{q}^{-1}a$ and is a normal extension of k. If q is a rational prime, set

$$K_q = k\big(E[q]\big),$$

the field obtained from k by adjoining the q-division points of E.

We begin by translating Lemma 1 in terms of fields over $\mathbb{Q}$.

LEMMA 2: *Suppose that $p \nmid q\Delta$. Then $q \mid i(p)$ if and only if p splits completely in $\mathbb{Q}(E[q])$ or the q-primary part of $\bar{E}(\mathbb{F}_p)$ is a non-trivial cyclic group and p has a first-degree prime factor in $\mathbb{Q}(q^{-1}a)$.*

PROOF: The first assertion follows by noting that p splits completely in $\mathbb{Q}(E[q])$ if and only if the Frobenius endomorphism of $\bar{E}$ acts trivially on the q-division points. The second assertion follows by noting that part (b) of Lemma 1 implies the solvability of

$$q \cdot x \equiv \bar{a} (\mathrm{mod}\ p)$$

and hence, p has a first-degree factor in $\mathbb{Q}(q^{-1}a)$.

We now deduce a divisibility criterion in terms of behavior over k.

LEMMA 3: *Suppose that p splits in k and $p \nmid q\Delta$.*

(a) *If q is inert in k, then $q \mid i(p)$ if and only if p splits completely in K_q.*

(b) *If q ramifies or splits in k, let $q = \mathfrak{q}_1\mathfrak{q}_2$ be its factorization in k. Then $q \mid i(p)$ if and only if (π_p) splits completely in $L_{\mathfrak{q}_1}$ or $L_{\mathfrak{q}_2}$ or K_q.*

(Here π_p is chosen so that $p = \pi_p\bar{\pi}_p$, and multiplication by π_p gives the Frobenius endomorphism of $E (\mathrm{mod}\ \pi_p)$.)

PROOF: Let $|\bar{E}(\mathbb{F}_p)| = p + 1 - a_p$. We know that $p + 1 - a_p = N(\pi_p - 1)$ and hence $q \mid i(p)$ implies that

$$N(\pi_p - 1) \equiv 0 (\mathrm{mod}\ p).$$

If q is insert, then $\pi_p \equiv 1 (\mathrm{mod}\ q)$ and hence π_p acts trivially on the q-division points. Therefore, π_p splits completely in K_q. If q is split and unramified in k, we find

$$\pi_p \equiv 1 (\mathrm{mod}\ \mathfrak{q}_1) \quad \text{or} \quad \pi_p \equiv 1 (\mathrm{mod}\ \mathfrak{q}_2).$$

If both these congruences hold, then p splits completely in $k(E[q])$, which is the compositum of $k(E[\mathfrak{q}_1])$ and $k(E[\mathfrak{q}_2])$, as q is unramified in k. If only one of the congruences holds,

$$\pi_p \equiv 1 (\mathrm{mod}\ \mathfrak{q}_1) \quad \text{(say)},$$

then π_p splits completely in $k(E[\mathfrak{q}_1])$. By Lemma 2, p also has a first degree prime factor in $\mathbb{Q}(q^{-1}a)$. Therefore, π_p has a first degree prime factor in $k(\mathfrak{q}_1^{-1}a)$. Hence, π_p splits completely in the normal extension $L_{\mathfrak{q}_1}$. If q is ramified in k, then let us write $(q) = \mathfrak{q}^2$. The above congruence implies that π_p acts trivially on the $\mathfrak{q}$-division points. Now, two possibilities arise: either π_p acts trivially on the q-division points, in which case π_p splits completely in K_q, or π_p acts trivially only on the $\mathfrak{q}$-division points. But now, as before, π_p has a first degree prime factor in $k(\mathfrak{q}^{-1}a)$ and so π_p splits completely in $L_{\mathfrak{q}}$. This completes the proof of the lemma.

REMARK: It is also possible to prove Lemma 3 by specializing the Lang-Trotter condition [12] to our situation.

§3. The division polynomial

We begin by recalling certain well-known facts concerning the division polynomal. If E, given in Weierstrass normal form, has complex multiplication by an order $\mathcal{O}$ in k and $P = (x, y)$ is any point on the curve, then the first-co-ordinate of βP, for $\beta \in \mathcal{O}$ is given by

$$x(\beta P) = f_\beta(x)/g_\beta(x),$$

where f_β and g_β are polynomials of degree $N(\beta)$ and $N(\beta) - 1$ respectively. (Here $N(\beta)$ denotes the norm of β in k). The roots of $g_\beta(x)$ are the x-co-ordinates of the non-zero β-division points. Furthermore, we normalize by letting g_β have leading coefficient β^2. Then, f_β and g_β have coefficients in k.

LEMMA 4: *For any non-zero β-division point u,*

$$\wp(u) \ll N(\beta),$$

where $\wp$ denotes the Weierstrass $\wp$-function and the implied constant depends only on E.

PROOF: Let $\Omega = \omega_0 \mathcal{O}$ be the lattice associated to E. Then $u = \alpha\omega_0/\beta$ for some $\alpha \in \mathcal{O}$ not divisible by β. The distance from u to Ω is

$$\min_{\omega \in \Omega} |u - \omega| = \min_{\gamma \in \mathcal{O}} |\omega_0| \left| \frac{\alpha}{\beta} - \gamma \right| = |\omega_0| \min_{\gamma \in \mathcal{O}} \sqrt{\frac{N(\alpha - \beta\gamma)}{N(\beta)}}$$

$$\geqslant \frac{|\omega_0|}{\sqrt{N(\beta)}},$$

and the result follows easily from the definition of the Weierstrass $\wp$-function.

LEMMA 5: *With the above normalization, the coefficients of $g_\beta(x)$ are bounded by* $\exp(CN(\beta) \log N(\beta))$ *for some constant C depending only on E.*

PROOF: We have

$$g_\beta(x) = \beta^2 \prod_u (x - \wp(u))$$

where the product ranges over the non-zero β-division points. Clearly any coefficient of $g_\beta(x)$ is bounded by

$$N(\beta) \cdot 2^{N(\beta)} \prod_u \max(1, |\wp(u)|)$$

with a similar restriction on the product. The result now follows from Lemma 4.

§4. Estimates for the degrees

Let $\mathfrak{a}$ be a squarefree integral ideal in $\mathcal{O}$ which is only divisible by prime ideal factors of degree one and let s be a squarefree integer. Define

$$L_{\mathfrak{a}} = \prod_{\mathfrak{q} \mid \mathfrak{a}} L_{\mathfrak{q}}, \quad n(\mathfrak{a}) = [L_{\mathfrak{a}} : k].$$

We note that

$$L_{\mathfrak{a}} = k\left(E[\mathfrak{a}], \mathfrak{a}^{-1}a\right).$$

Moreover, as $\mathrm{Gal}(k(E[\mathfrak{a}]/k)$ is a subgroup of $(\mathcal{O}/\mathfrak{a})^*$, we have that $\mathrm{Gal}(L_\mathfrak{a}/k)$ is a subgroup of

$$\left\{\begin{pmatrix} 1 & * \\ 0 & * \end{pmatrix} \in GL_2(\mathcal{O}/\mathfrak{a})\right\}.$$

We also set

$$K_s = \prod_{q \mid s} K_q, \qquad m(s) = [K_s : k],$$

and also

$$L_{\mathfrak{a},s} = L_\mathfrak{a} \cdot K_s = k\left(E[\mathfrak{a}s],\ \mathfrak{a}^{-1}a\right)$$

and denote by $n(\mathfrak{a}, s)$, $d(\mathfrak{a}, s)$ the degree and discriminant of the extension $L_{\mathfrak{a},s}$ over k and over $\mathbb{Q}$ respectively.

LEMMA 6:

$$\log n(\mathfrak{a}, s) \ll \log N(\mathfrak{a}) + \log s.$$

PROOF: Clearly $n(\mathfrak{a}, s) \leqslant n(\mathfrak{a})m(s)$. It is classical that $m(s) \leqslant \phi(s\mathcal{O}_k)$, where ϕ denotes the phi function of k. Moreover, from the above remarks,

$$n(\mathfrak{a}) \leqslant \phi(\mathfrak{a})N(\mathfrak{a}).$$

The result now follows from this.

LEMMA 7:

$$\frac{\log |d(\mathfrak{a}, s)|}{n(\mathfrak{a}, s)} \ll \log N(\mathfrak{a}) + \log s.$$

PROOF: It is a result of Hensel (see [15]) that if $L/\mathbb{Q}$ is a normal extension of degree n and ramified only at the primes $p_1, \ldots, p_m$, then

$$\frac{1}{n} \log |d_{L/\mathbb{Q}}| \leqslant \log n + \sum_{j=1}^{m} \log p_j,$$

where $d_{L/\mathbb{Q}}$ is the discriminant of $L/\mathbb{Q}$. In view of Lemma 6, it suffices to determine the ramified primes of the extensions $\mathbb{Q}(E[m], m^{-1}a)$, as the extensions under consideration are certainly contained in extensions

of this type for a suitable m, namely $m = N(\mathfrak{a})s$. It is well-known that the latter extensions are ramified only at primes dividing m and the discriminant of E (see [2]). We therefore deduce the result from Hensel's bound.

LEMMA 8: *If* $\mathfrak{a}$ *and* s *are coprime to* 6Δ, *where* Δ *is the discriminant of* E, *then*

$$n(\mathfrak{a}, s) = \frac{n(\mathfrak{a})m(s)}{\phi(\mathfrak{a}, s)}$$

where $(\mathfrak{a}, s)$ *denotes the gcd of* $\mathfrak{a}$ *and* s.

PROOF: Let $\mathfrak{b} = \operatorname{lcm}(\mathfrak{a}, s)$ so that

$$k(E[\mathfrak{a}])k(E[s]) = k(E[\mathfrak{b}]).$$

Since $(\mathfrak{b}, 6\Delta) = 1$, the Galois group $\operatorname{Gal}(k(E[\mathfrak{b}])/k)$ is equal to the full group $(\mathcal{O}/\mathfrak{b})^*$. This follows for example from the fact (see [2] or [4]) that for a prime $\mathfrak{p} \nmid 6\Delta$, the extension $k(E[\mathfrak{p}])/k$ is unramified outside of $6\mathfrak{p}\Delta$ but totally ramified at $\mathfrak{p}$ and has Galois group $(\mathcal{O}/\mathfrak{p})^*$. Thus,

$$[k(E[\mathfrak{b}]: k] = \phi(\mathfrak{b}) = \frac{[k(E[\mathfrak{a}]): k][k(E[s]): k]}{\phi(\mathfrak{a}, s)}.$$

Lemma 8 now follows (with $\mathfrak{c} = 1$) from the following fact.

LEMMA 9: *Suppose* $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$ *are squarefree*, $\mathfrak{a}$ *and* $\mathfrak{c}$ *are products of first-degree primes, and that* $(\mathfrak{a}, 6\Delta) = 1$, $\mathfrak{a} \mid \mathfrak{b}$, $\mathfrak{c} \mid \mathfrak{b}$, *and* $(N(\mathfrak{a}), N(\mathfrak{c})) = 1$. *Then*

$$[k(E[\mathfrak{b}], \mathfrak{a}^{-1}\mathfrak{c}^{-1}a): k(E[\mathfrak{b}], \mathfrak{c}^{-1}a)] = [L_{\mathfrak{a}}: k(E[\mathfrak{a}])].$$

PROOF: The Galois group $\operatorname{Gal}(k(E[\mathfrak{b}], \mathfrak{a}^{-1}\mathfrak{c}^{-1}a)/k)$ can be identified with a subgroup G_1 of

$$\left\{\begin{pmatrix} 1 & \alpha \\ 0 & \beta \end{pmatrix}: \alpha \in \mathcal{O}/\mathfrak{a}\mathfrak{c},\ \beta \in (\mathcal{O}/\mathfrak{b})^*\right\}$$

and $\operatorname{Gal}(L_{\mathfrak{a}}/k)$ with a subgroup G_2 of

$$\left\{\begin{pmatrix} 1 & \alpha \\ 0 & \beta \end{pmatrix}: \alpha \in \mathcal{O}/\mathfrak{a},\ \beta \in (\mathcal{O}/\mathfrak{a})^*\right\}.$$

The subfields $k(E[\mathfrak{b}], \mathfrak{c}^{-1}a)$ and $k(E[\mathfrak{a}])$ correspond to subgroups I_1 and I_2 of $\mathcal{O}/\mathfrak{a}\mathfrak{c}$ and $\mathcal{O}/\mathfrak{a}$ respectively, where

$$I_1 = \left\{\alpha: \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \in G_1,\ \alpha \equiv 0 (\mathrm{mod}\ \mathfrak{c})\right\}$$

and

$$I_2 = \left\{\alpha: \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \in G_2\right\}.$$

We need to show $|I_1| = |I_2|$. It will suffice to show that for each $p \mid N(\mathfrak{a})$, the projections

$$\phi_1 : I_1 \to \mathcal{O}/(\mathfrak{a},\ p)$$

and

$$\phi_2 : I_2 \to \mathcal{O}/(\mathfrak{a},\ p)$$

have the same image. Suppose $p \| N(\mathfrak{a})$, so that $(\mathfrak{a},\ p) = \mathfrak{p}$ with $N(\mathfrak{p}) = p$. Then $\mathrm{Im}(\phi_i) = 0$ or $\mathcal{O}/\mathfrak{p}$ for $i = 1, 2$. Note that $\mathrm{Im}(\phi_i) = 0$ if and only if $\mathfrak{p}^{-1}a \in k(E[\mathfrak{b}], \mathfrak{c}^{-1}a)$ or $k(E[\mathfrak{a}])$ for $i = 1, 2$ respectively. Clearly, if $\mathfrak{p}^{-1}a \in k(E[\mathfrak{a}])$, then $\mathfrak{p}^{-1}a \in k(E[\mathfrak{b}], \mathfrak{c}^{-1}a)$. Conversely, if $\mathrm{Im}(\phi_1) = 0$, then the projection

$$\left\{\alpha: \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \in G_1\right\} \to \mathcal{O}/\mathfrak{p}$$

has trivial image and $\mathfrak{p}^{-1}a \in k(E[\mathfrak{b}])$. This implies $\mathfrak{p}^{-1}a \in k(E[\mathfrak{a}])$ since otherwise the non-abelian extension $k(E[\mathfrak{a}], \mathfrak{p}^{-1}a)$ would be contained in the abelian extension $k(E[\mathfrak{b}])$. Thus, $\mathrm{Im}(\phi_1) = \mathrm{Im}(\phi_2)$.

Now suppose $p^2 \| N(\mathfrak{a})$ so $(\mathfrak{a},\ p) = \mathfrak{p}_1\mathfrak{p}_2$ (say). Since $\mathrm{Gal}(k(E[p])/k) \simeq (\mathcal{O}/p)^*$, we have for any $\delta \in (\mathcal{O}/p)^*$, some $\beta \in (\mathcal{O}/\mathfrak{a})^*$ and $\gamma \in \mathcal{O}/\mathfrak{a}$ with $\beta \equiv \delta (\mathrm{mod}\ p)$ and

$$\begin{pmatrix} 1 & \gamma \\ 0 & \beta \end{pmatrix} \in G_2.$$

Then for any $\alpha \in I_2$,

$$\begin{pmatrix} 1 & \gamma \\ 0 & \beta \end{pmatrix}^{-1} \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \gamma \\ 0 & \beta \end{pmatrix} = \begin{pmatrix} 1 & \alpha\beta \\ 0 & 1 \end{pmatrix} \in G_2.$$

This shows that $\mathrm{Im}(\phi_2)$ is an *ideal* in $\mathcal{O}/p$. Similarly, $\mathrm{Im}(\phi_1)$ is an ideal. Letting $\phi_i^{(j)}$ be the projection of I_i on $\mathcal{O}/\mathfrak{p}_j$, we have

$$\mathrm{Im}(\phi_i) \simeq \mathrm{Im}\ \phi_i^{(1)} \times \mathrm{Im}\ \phi_i^{(2)}$$

for $i = 1, 2$. Arguing as before shows that $\operatorname{Im} \phi_1^{(j)} = \operatorname{Im} \phi_2^{(j)}$ for $j = 1, 2$ and hence $\operatorname{Im}(\phi_1) = \operatorname{Im}(\phi_2)$. This completes the proof of Lemmas 8 and 9.

§5. The asymptotic formula

Denote by $N(x, y)$ the number of primes of k which are of first degree and norm $\leqslant x$ which do not split completely in any $L_{\mathfrak{q}}$ or K_q for $q \leqslant y$ and $N(\mathfrak{q}) \leqslant y$. It is then clear that

$$N_a(x) \leqslant \tfrac{1}{2} N(x, y).$$

If π_p splits completely in $L_{\mathfrak{q}}$ or K_q, then as $q \mid (p + 1 - a_p)$, we must have $q \leqslant 2p \leqslant 2x$. Letting $M(y_1, y_2)$ denote the number of primes $p \leqslant x$ such that π_p splits completely in $L_{\mathfrak{q}}$ or K_q for some q or $\mathfrak{q}$ satisfying $y_1 < q < y_2$, $y_1 < N(\mathfrak{q}) < y_2$, we find that

$$N_a(x) \geqslant \tfrac{1}{2} N(x, y) - M(y, 2x).$$

Hence

$$N_a(x) = \tfrac{1}{2} N(x, y) + \mathrm{O}(M(y, 2x)).$$

We choose $y = \frac{1}{12} \log x$ and let $\pi(x, \mathfrak{a}, s)$ denote the number of first degree primes of k of norm $\leqslant x$ which split completely in $L_{\mathfrak{a},s}$. By the inclusion-exclusion principle,

$$N(x, y) = \sum_{\mathfrak{a},s}{}' \mu(\mathfrak{a}) \mu(s) \pi(x, \mathfrak{a}, s)$$

where the dash on the summation indicates that any prime ideal factor of $\mathfrak{a}$ has norm $\leqslant y$ and any prime factor of s is $\leqslant y$. If we assume that the Dedekind zeta function of $L_{\mathfrak{a},s}$ satisfies the Riemann hypothesis, then one can give an asymptotic formula for $\pi(x, \mathfrak{a}, s)$ with a good error term.

LEMMA 10: *Lagarias-Odlyzko* [19]). *Let L/K be a normal extension of degree n, and discriminant $d = \operatorname{disc}(L/\mathbb{Q})$. Let $\pi_C(x, L)$ be the number of prime ideals of first degree of K whose Frobenius automorphism lies in a given conjugacy class C of* $\operatorname{Gal}(L/K)$. *If the Dedekind zeta function of L satisfies the Riemann hypothesis, then*

$$\left| \pi_C(x, L) - \frac{|C|}{n} \operatorname{li} x \right| \ll |C| x^{1/2} (\log x + \delta(L))$$

where the implies constant depends only on K and

$$\delta(L) = \frac{\log |d|}{n}.$$

(li x *is as usual the logarithmic integral of* x.)

We apply this in the case $K = k$, $L = L_{\mathfrak{a},s}$ and $C = \{1\}$. Then,

$$\left| N(x, y) - \sum_{\mathfrak{a},s}{}' \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)} \operatorname{li} x \right| \ll x^{1/2} \sum_{\mathfrak{a},s}{}' (\log x + \delta(\mathfrak{a}, s))$$

where $\delta(\mathfrak{a}, s) = n(\mathfrak{a}, s)^{-1} \log |d(\mathfrak{a}, s)|$. By Lemma 7, the error is

$$\ll x^{1/2} \sum_{\mathfrak{a},s}{}' (\log x + \log N(\mathfrak{a}) + \log s).$$

Any ideal $\mathfrak{a}$ in the range of summation above satisfies

$$N(\mathfrak{a}) \leqslant \prod_{N(\mathfrak{a}) \leqslant y} N(\mathfrak{q})$$

and hence

$$\log N(\mathfrak{a}) \ll y.$$

A similar estimate holds true for $\log s$. The number of pairs $(\mathfrak{a}, s)$ occuring in the sum is at most 2^{3y} by an elementary computation. The error term is therefore,

$$\ll x^{1-\epsilon}$$

for any $\epsilon > 0$ for the choice $y = \frac{1}{12} \log x$. This proves that

$$N(x, y) = \sum_{\mathfrak{a},s}{}' \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)} \operatorname{li} x + O(x^{1-\epsilon}).$$

We shall show that if the above series is allowed to run over all such $\mathfrak{a}$, s, then the series is absolutely convergent. Indeed, by Lemma 8,

$$\sum_{\mathfrak{a},s} \frac{1}{n(\mathfrak{a}, s)} \ll \sum_{\mathfrak{a},s} \frac{\phi(\mathfrak{a}, s)}{n(\mathfrak{a}) m(s)},$$

where the summation is over all squarefree numbers s and squarefree ideals $\mathfrak{a}$ of $\mathcal{O}_k$ composed only of first degree prime ideals. The constant implied above depends on the number of divisors of 6Δ and we have

accordingly decomposed the initial sum according to the $\gcd(\mathfrak{a}, s, 6\Delta)$ so that there are only finitely many such sums. As $\phi(\mathfrak{a}, s)$ is a multiplicative function in s for fixed $\mathfrak{a}$, we find

$$\sum_{\mathfrak{a},s} \frac{\phi(\mathfrak{a}, s)}{n(\mathfrak{a})m(s)} \ll \sum_{\mathfrak{a}} \frac{1}{n(\mathfrak{a})} \prod_{q} \left(1 + \frac{\phi(\mathfrak{a}, q)}{m(q)}\right).$$

Since the product

$$\prod_{q} \left(1 + \frac{1}{m(q)}\right)$$

converges, the above sum is

$$\ll \sum_{\mathfrak{a}} \frac{1}{n(\mathfrak{a})} \prod_{(\mathfrak{q}, \mathfrak{a}) \neq (1)} \left(1 + \frac{\phi(\mathfrak{a}, q)}{m(q)}\right)$$

$$\ll \sum_{\mathfrak{m}} \frac{2^{\nu(\mathfrak{a})}}{n(\mathfrak{a})},$$

where $\nu(\mathfrak{a})$ denotes the number of prime ideal factors of $\mathfrak{a}$. The latter series clearly converges, as $2^{\nu(\mathfrak{a})} = O(N(\mathfrak{a})^{\epsilon})$ and $n(\mathfrak{a}) \geqslant N(\mathfrak{a})^{3/2}$ for all $N(\mathfrak{a})$ sufficiently large.

We therefore set

$$\delta = \sum_{\mathfrak{a},s} \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)}$$

where the sum is now unrestricted. Note that

$$\left| \sum_{\mathfrak{a},s}{}' \frac{\mu(\mathfrak{a})\mu(s)}{n(\mathfrak{a}, s)} - \delta \right| \leqslant \sum_{\mathfrak{a},s}{}'' \frac{1}{n(\mathfrak{a}, s)},$$

the double dash in the sum indicating that either $N(\mathfrak{a}) \geqslant y$ or $s \geqslant y$. By an analysis similar to the above, we find

$$\sum_{\mathfrak{a},s}{}'' \frac{1}{n(\mathfrak{a}, s)} \ll \sum_{N(\mathfrak{a}) \geqslant y} \frac{1}{n(\mathfrak{a})} + \sum_{s \geqslant y} \frac{1}{n(s)}$$

Utilising elementary estimates for the ϕ-function, we find

$$\sum_{\mathfrak{a},s}{}'' \frac{1}{n(\mathfrak{a}, s)} \ll \frac{\log \log x}{\log x}$$

for our choice of y. This yields

$$N(x, y) = \delta \operatorname{li} x + O\left(\frac{x \log\log x}{\log^2 x}\right).$$

It now remains to estimate $M(y, 2x)$.

§6. Estimation of M(y, 2x)

Clearly,

$$M(y, 2x) \leqslant M(y, x^{1/2}/\log^2 x) + M(x^{1/2} \log^2 x, 2x).$$

Utilising Lemma 10, we find (on the GRH) that,

$$M(y, x^{1/2}/\log^2 x) \ll \sum_{q}\left(\frac{\operatorname{li} x}{m(q)} + O(x^{1/2} \log x)\right) + \sum_{\mathfrak{q}}\left(\frac{\operatorname{li} x}{n(\mathfrak{q})} + O(x^{1/2} \log x)\right)$$

where the summation over q and $\mathfrak{q}$ are in the restricted ranges stipulated by $M(y, x^{1/2}/\log^2 x)$. We therefore find that

$$M(y, x^{1/2}/\log^2 x) \ll \frac{x}{\log^2 x},$$

as $m(q) \gg q^2$ and $n(\mathfrak{q}) \gg N(\mathfrak{q})^2$.

We are therefore left with estimating $M(x^{1/2}/\log^2 x, 2x)$. We write

$$M(x^{1/2}/\log^2 x, 2x) \leqslant M(x^{1/2}/\log^2 x, x^{1/2} \log^2 x) + M(x^{1/2} \log^2 x, 2x).$$

To estimate $M(x^{1/2}/\log^2 x, x^{1/2} \log^2 x)$, we utilise the analogue of the Brun-Titchmarsh theorem for number fields, easily proved by an appropriate generalisation of the large sieve (see for example, Schaal [16]). For any ideal $\mathfrak{q}$, the number of primes π_p with $N(\pi_p) \leqslant x$ satisfying $\pi_p \equiv 1 (\mathrm{mod}\ \mathfrak{q})$ is

$$\ll \frac{x}{\phi(\mathfrak{q}) \log(x/N(\mathfrak{q}))}$$

provided $N(\mathfrak{q}) < x$. In our case, $N(\mathfrak{q}) < x^{1/2} \log^2 x$ and hence

$$\pi_1(x, L_{\mathfrak{q}}) \ll \frac{x}{N(\mathfrak{q}) \log x}.$$

As in [13], we easily find

$$\pi_1(x, K_q) \ll \frac{x}{q^2}.$$

Therefore,

$$M(x^{1/2}/\log^2 x, x^{1/2} \log^2 x) \ll \frac{x}{\log x} \sum \frac{1}{N(\mathfrak{q})} + O(x^{1/2} \log x).$$

As usual, in the above sum $N(\mathfrak{q})$ satisfies

$$x^{1/2}/\log^2 x < N(\mathfrak{q}) < x^{1/2} \log^2 x.$$

Since we know

$$\sum_{n(\mathfrak{q}) \leqslant z} \frac{1}{N(\mathfrak{q})} = \log \log z + c + O\left(\frac{1}{\log z}\right)$$

for a suitable constant c, we find that the above sum is

$$\ll \frac{x \log \log x}{\log^2 x}.$$

It therefore remains to deal with $M(x^{1/2} \log^2 x, 2x)$.

It is impossible for a prime π_p to split completely in K_q for q in the above range as $q^2 | (p + 1 - a_p)$ implies $q \leqslant 2\sqrt{x}$. We therefore need to consider only those primes π_p which split completely in $L_{\mathfrak{q}}$, for $N(\mathfrak{q})$ in the given range. If π_p splits completely in $L_{\mathfrak{q}}$, then

$$\pi_p \cdot \mathfrak{q}^{-1}\bar{a} \equiv \mathfrak{q}^{-1}\bar{a} (\mathrm{mod}\ \pi_p)$$

and hence

$$\left(\frac{\pi_p - 1}{\beta}\right) \cdot \bar{a} \equiv \bar{0} (\mathrm{mod}\ \pi_p),$$

where β generates $\mathfrak{q}$. Therefore,

$$g_\alpha(a) \equiv 0 (\mathrm{mod}\ \pi_p)$$

for $\alpha = (\pi_p - 1)/\beta$. We note that

$$N(\alpha) \leqslant \frac{2x^{1/2}}{\log^2 x}.$$

Therefore, $M(x^{1/2} \log^2 x, 2x)$ is bounded by the number of prime fac-

tors in the numerator of

$$\prod_{N(\alpha)\leqslant 2x^{1/2}/\log^2 x} g_\alpha(a) = R \quad \text{(say)}.$$

The total number of prime factors is bounded by

$$2\log|R| \ll \sum_{N(\alpha)\leqslant 2x^{1/2}/\log^2 x} N(\alpha)\log N(\alpha) \ll x/\log^3 x$$

by Lemma 5. This completes the estimation.

We have therefore proved that

$$N_a(x) = \frac{\delta}{2}\operatorname{li} x + O\left(\frac{x\log\log x}{\log^2 x}\right).$$

It remains to determine the nature of δ and this we take up in the next section.

§7. Calculation of the density

In view of Lemma 8, we should be able to decompose δ as an infinite product from which it will become apparent that under certain conditions, $\delta > 0$. We need the following fact.

LEMMA 11: *Let* $\mathfrak{a} = \mathfrak{a}_1\mathfrak{b}$, $s = s_1 b$ *where* $(\mathfrak{a}_1, 6\Delta) = (s_1, 6\Delta) = 1$ *and* $\mathfrak{b}$, $b \mid 6\Delta$. *Then*

$$n(\mathfrak{a}, s) = n(\mathfrak{a}_1, s_1)n(\mathfrak{b}, b).$$

PROOF: It suffices to show that

$$[L_{\mathfrak{a},s}: L_{\mathfrak{b},b}] = [L_{\mathfrak{a}_1,s_1}: k].$$

Recall that for $\mathfrak{p}[\operatorname{lcm}(\mathfrak{a}_1, s_1)$, $k(E[\mathfrak{p}])$ is an extension of k in which $\mathfrak{p}$ ramifies totally and primes not dividing $6\mathfrak{p}\Delta$ do not ramify. Since $\mathfrak{p}$ does not ramify in $L_{\mathfrak{b},b}$ (see [2]), it follows that

$$[k(E[\mathfrak{d}], \mathfrak{b}^{-1}a): L_{\mathfrak{b},b}] = [k(E[\mathfrak{c}]): k]$$

where $\mathfrak{d} = \operatorname{lcm}(\mathfrak{a}, s)$ and $\mathfrak{c} = \operatorname{lcm}(\mathfrak{a}_1, s_1)$. Moreover, by Lemma 9, we have

$$\begin{aligned}[L_{\mathfrak{a}_1}: k(E[\mathfrak{a}_1])] &= [L_{\mathfrak{a},s}: k(E[\mathfrak{d}], \mathfrak{b}^{-1}a)] \\ &= [L_{\mathfrak{a}_1,s_1}: k(E[\mathfrak{c}])]\end{aligned}$$

and Lemma 11 follows from this.

As the Möbius function is multiplicative and since $\mathfrak{a}$, s are squarefree, we find that

$$\delta = \sum_{\substack{\mathfrak{a}_1, s_1 \\ \mathfrak{b}, b}} \frac{\mu(\mathfrak{a}_1)\mu(s_1)}{n(\mathfrak{a}_1, s_1)} \cdot \frac{\mu(\mathfrak{b})\mu(b)}{n(\mathfrak{b}, b)}$$

utilising Lemma 11. In the above sum, $\mathfrak{a}_1$, s_1 are coprime to 6Δ, $\mathfrak{b}$ runs through the divisors formed from the first degree prime ideal factors of (6Δ) and b runs through the positive divisors of 6Δ. We therefore obtain

$$\delta = \sum_{\mathfrak{b}, b} \frac{\mu(\mathfrak{b})g(b)}{n(\mathfrak{b}, b)} \cdot \sum_{\mathfrak{a}_1, s_1} \frac{\mu(\mathfrak{a}_1)\mu(s_1)}{n(\mathfrak{a}_1, s_1)}$$

$$= \delta_0 \cdot \delta_1 \quad \text{(say)}.$$

Using Lemma 8, the second sum can be decomposed into an infinite product. Indeed,

$$\delta_1 = \sum_{\mathfrak{a}_1, s_1} \frac{\mu(\mathfrak{a}_1)\mu(s_1)}{n(\mathfrak{a}_1)m(s_1)} \phi(\mathfrak{a}_1, s_1)$$

$$= \sum_{s_1} \frac{\mu(s_1)}{m(s_1)} \prod_{\mathfrak{q}} \left(1 - \frac{\phi(\mathfrak{q}, s_1)}{n(\mathfrak{q})}\right)$$

where the product ranges over the first degree prime ideals of $\mathcal{O}$ coprime to 6Δ. As $\phi(\mathfrak{q}, s_1) = 1$ except when $\mathfrak{q} \mid s_1$, we find

$$\delta_1 = \prod_{\mathfrak{q}} \left(1 - \frac{1}{n(\mathfrak{q})}\right) \sum_{s_1} \frac{\mu(s)}{m(s_1)} \prod_{\mathfrak{q} \mid s_1} \left(1 - \frac{1}{N(\mathfrak{q})}\right)\left(1 - \frac{1}{n(\mathfrak{q})}\right)^{-1}$$

$$= \prod_{\substack{q \text{ inert} \\ \text{in } k \\ (q, 6\Delta)=1}} \left(1 - \frac{1}{q^2 - 1}\right)$$

$$\prod_{\substack{q \text{ split} \\ \text{in } k \\ (q, 6\Delta)=1}} \left(1 - \frac{2}{q(q-1)} - \frac{1}{(q-1)^2} + \frac{2}{q(q-1)^2}\right).$$

It will also be observed the density of primes not splitting in the fields attached to the prime q is the q-factor appearing in the above product. Here, we have assumed that $a \neq qb$ for any $b \in E(\mathbb{Q})$ and q which splits in k. In general, the q-factor above for finitely many split q needs to be

replaced by $(1-(q-1)^{-1})^2$. The prime factors which are ramified in k do not occur in δ_1 as they divide 6Δ, and so we find that $\delta_1 \neq 0$.

It remains to analyse δ_0. We first note that δ_0 represents the density of primes π_p which do not split completely in any $L_{\mathfrak{b},b}$, where $\mathfrak{b}$, b range over certain divisors of (6Δ) and 6Δ respectively. If θ represents the density of primes π_p not splitting completely in any of K_q (if q is second degree in k) or $k(E[\mathfrak{q}])$, (if $\mathfrak{q}$ is of first degree), then clearly, we have

$$\delta_0 \geqslant \theta.$$

We shall show that if 2 and 3 are inert in k (and hence $k \neq \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$), then $\theta \geqslant 0$.

The fields obtained by adjoining the $\mathfrak{q}$-division points to k are well-known to contain ray class fields. If $\mathfrak{a}$ is any ideal of k, then the ray class field $k(\mathfrak{a})$ has degree $\phi(\mathfrak{a})/w(\mathfrak{a})$ where $w(\mathfrak{a})$ denotes the number of inequivalent units mod $\mathfrak{a}$. We consider the fields

$$T_{\mathfrak{a}} = \prod_{\mathfrak{p} \mid \mathfrak{a}} k(\mathfrak{p})$$

where the product ranges over all prime ideal divisors of $\mathfrak{a}$. As the fields $k(\mathfrak{p})$ are disjoint as $\mathfrak{p}$ varies over the prime ideal divisors of $\mathfrak{a}$, we find $T_{\mathfrak{a}}$ has degree (over k)

$$\prod_{\mathfrak{p} \mid \mathfrak{a}} \frac{\phi(\mathfrak{p})}{w(\mathfrak{p})}.$$

Hence

$$\theta \geqslant \prod_{\mathfrak{p} \mid 6\Delta} \left(1 - \frac{w(\mathfrak{p})}{\phi(\mathfrak{p})}\right).$$

In our situation, $w(\mathfrak{p}) = 2$ except in the case $\mathfrak{p} = 2$, in which case $w(\mathfrak{p}) = 1$. It is now easily seen that if 2 and 3 are inert in k, then $\theta > 0$. This proves $\delta_0 > 0$ at least in these cases. That is, in the cases $k = \mathbb{Q}(\sqrt{-19})$, $\mathbb{Q}(\sqrt{-43})$, $\mathbb{Q}(\sqrt{-67})$, and $\mathbb{Q}(\sqrt{-163})$, we have shown $\delta_0 > 0$.

The case $k = \mathbb{Q}(\sqrt{-11})$ requires a litte more effort since 3 splits, say as $\mathfrak{p}_1\mathfrak{p}_2$, and the corresponding ray class fields are trivial. Instead of these class fields, consider instead the fields $k(E[\mathfrak{p}_1])$ and $k(E[\mathfrak{p}_2])$. Since one is the complex conjugate of the other and

$$\zeta_3 \in k(E[3]) = k(E[\mathfrak{p}_1])k(E[\mathfrak{p}_2]),$$

$k(E[\mathfrak{p}_1])$ and $k(E[\mathfrak{p}_2])$ are quadratic extensions of k in which $\mathfrak{p}_1$ or $\mathfrak{p}_2$ ramify. This implies that the fields $k[E[3])$, $k(\mathfrak{p})$ are disjoint as $\mathfrak{p}$ ranges

over the prime divisors of 6Δ other than $\mathfrak{p}_1$ and $\mathfrak{p}_2$. As before, we then see that $\delta_0 > 0$ in this case as well.

In case $k = \mathbb{Q}(\sqrt{-7})$ and E has CM by the maximal order, we see that 2 splits and hence the 2-division points are contained in k. Therefore, if p splits in k, $\bar{E}(\mathbb{F}_p)$ contains the 2-division points. Hence $\delta_0 = 0$ in this case.

We can also make some remarks in the case $k = \mathbb{Q}(\sqrt{-2})$. These remarks are based on

LEMMA 12: *Let K_i, $i \in I$, be a finite number of non-trivial disjoint normal extensions of k, and let L/k be normal of prime degree. Then*

(1) *either $L \not\subset \prod_{i \in I} K_i$ or there is a unique minimal subset I_L of I such that $L \subset \prod_{i \in I_L} K_i$.*

(2) *the density of first degree prime ideals which do not split completely in L or any K_i is zero if and only if $L \subset \prod_{i \in I} K_i$, $[L : k] = 2$, $|I_L|$ is even, and for each $i \in I_L$, $[K_i : k] = 2$.*

PROOF: For a subset J of I, let $K_J = \prod_{i \in J} K_i$. Since the K_i are disjoint, if $L \subset K_J$ and $L \subset K_{J'}$, then $L \subset K_{J \cap J'}$, whence (1) follows. For (2), first note that if $L \not\subset K_I$, then as $[L : k]$ is prime, L is disjoint from the K_i's so we have a positive density. Suppose therefore that $L \subset K_I$. Then the density of primes not splitting completely in L or any K_i is

$$\sum_{J \subset I} \frac{\mu(J)}{[K_J : k]} - \frac{1}{p} \sum_{\substack{J \subset I \\ J \not\supset I_L}} \frac{\mu(J)}{[K_J : k]} - \sum_{\substack{J \subset I \\ J \supset I_L}} \frac{\mu(J)}{[K_J : k]},$$

where $p = [L : k]$. Re-write this density as

$$\frac{p-1}{p} \left(\sum_{J \subset I} \frac{\mu(J)}{[K_J : k]} - \sum_{\substack{J \subset I \\ J \supset I_L}} \frac{\mu(J)}{[K_J : k]} \right)$$

and note that

$$\sum_{J \subset I} \frac{\mu(J)}{[K_J : k]} = \prod_{i \in I} \left(1 - \frac{1}{[K_i : k]} \right)$$

and

$$\sum_{\substack{J \subset I \\ J \supset I_L}} \frac{\mu(J)}{[K_J : k]} = \frac{\mu(I_L)}{[K_{I_L} : k]} \prod_{i \notin I_L} \left(1 - \frac{1}{[K_i : k]} \right).$$

Therefore, the density is zero if and only if

$$\prod_{i\in I_L}\left(1-\frac{1}{[K_i\colon k]}\right)=\frac{\mu(I_L)}{[K_{I_L}\colon k]}=\mu(I_L)\prod_{i\in I_L}\frac{1}{[K_i\colon k]}$$

and (2) follows.

We now apply this to the case $k=\mathbb{Q}(\sqrt{-2})$. Here, 3 splits as $\mathfrak{p}_1\mathfrak{p}_2$ say and 2 ramifies; the associated ray class fields are trivial. Nevertheless, $k(E[2])=k((\sqrt{-2})^2)$ (the ray class field mod $(\sqrt{-2})^2$) is a quadratic extension of k, and proceeding as for $\mathbb{Q}(\sqrt{-11})$, we see that the fields $k(E[2])$, $k(E[3])$, and $k(\mathfrak{p})$, where $\mathfrak{p}$ ranges over the prime divisors of 6Δ other than $\mathfrak{p}_1$, $\mathfrak{p}_2$, and $(\sqrt{-2})$, are non-trivial disjoint extensions of k. We let the K_i in Lemma 12 range over the fields $k(E[\mathfrak{p}_1])$, $k(E[\mathfrak{p}_2])$, $k(E[2])$, $k(\mathfrak{p})$, $\mathfrak{p}$ as above. Note that the only quadratic extensions of k in this list are the first three.

Now let $L=k((\sqrt{-2})^{-1}a)$. Then $L=k$ exactly when there is some $b\in E(k)$ with $a=\sqrt{-2}\,b$, and in this case $\delta_0=0$. Otherwise, L is a quadratic extension of k. Suppose moreover that $\mathfrak{p}_1$ and $\mathfrak{p}_2$ do not ramify in L. In this case, it is readily checked that if

$$L\subset k(E[\mathfrak{p}_1])k(E[\mathfrak{p}_2])k(E[2]),$$

then $L=k(E[2])$. Using Lemma 12, we then deduce that $\delta_0>0$.

If the point a corresponds to the point (x_0, y_0) (where x_0 is rational but y_0 need not be) on the canonical curve with CM by $\mathbb{Q}(\sqrt{-2})$,

$$y^2=4x^3-30x-28,$$

then L/k is obtained by solving

$$\frac{2x^2+4x+9}{4x+8}=-x_0.$$

The discriminant of the resulting quadratic is $8(2x_0^2-4x_0-7)$, and hence $L=k$ if and only if $-(2x_0^2-4x_0-7)$ is a square. Moreover, $\mathfrak{p}_1$ and $\mathfrak{p}_2$ do not ramify in L if $x_0\not\equiv 1(\mathrm{mod}\ 3)$. Thus, we have $\delta_0>0$ most of the time, when $k=\mathbb{Q}(\sqrt{-2})$.

§8. The higher rank case

We begin by considering the following situation. Suppose we have a free subgroup Γ of rational points. Let Γ_p be the reduction of $\Gamma(\mathrm{mod}\ p)$. Suppose that $q\,|\,(\bar{E}(\mathbb{F}_p)\colon \Gamma_p)$, and that $q>z$.

For primes $p\leqslant x$, this means that

$$|\,\Gamma_p\,|\leqslant\frac{x}{z}.$$

Therefore, if z is large, the image of $\Gamma(\text{mod } p)$ is small. If we can show that the number of primes for which $|\Gamma_p|$ satisfies the above inequality is small, then for almost all primes, the prime divisors of the index are $\leqslant z$. This is basically our strategy.

To begin with, let $P_1, \ldots, P_r$ be r independent generators of Γ, where $r =$ rank of Γ. We will make use of the canonical height pairing of Néron and Tate.

Recall, that this is a positive semidefinite, bilinear pairing on $E(\overline{\mathbb{Q}})$ with the property that $\langle P, P\rangle = 0$ if and only if P is a torsion point. In fact, this height pairing is related to the naive height in the following way. If $P = (a, b) \in E(\mathbb{Q})$ then writing $a = r/s$, r and s coprime, we define the a-height as

$$h_a(P) = \log \max(|r|, |s|).$$

If we let $H(P) = \langle P, P\rangle$, then for $P \in E(\mathbb{Q})$,

$$H(P) = h_a(P) + O(1),$$

where the implied constant depends only on E.

LEMMA 13: *The number of r-tuples of integers* $(n_1, \ldots, n_r)$ *satisfying*

$$H(n_1P_1 + \cdots + n_rP_r) \leqslant x$$

is

$$\frac{(\pi x)^{r/2}}{\sqrt{R}\,\Gamma\left(\frac{r}{2}+1\right)} + O(x^{(r-1)/2+\epsilon}),$$

where $R = \det(\langle P_i, P_j\rangle)$.

PROOF: We want to determine the integer solutions of

$$\left\langle \sum_{i=1}^{r} n_iP_i, \sum_{i=1}^{r} n_iP_i \right\rangle \leqslant x$$

which is the same as

$$\sum_{i,j} n_in_j\langle P_i, P_j\rangle \leqslant x.$$

This corresponds to counting lattice points in the r-dimensional ellipsoid determined by the above quadratic form. It is well known that the

number of lattice points is given by the above expression. (See [17].)

The following is of interest in its own right.

LEMMA 14: *The number of primes p satisfying*

$$|\Gamma_p| < y \quad \text{is} \quad O(y^{(r+2)/r}).$$

PROOF: Consider the set S of all r-tuples of integers $(n_1, \ldots, n_r)$ satisfying

$$H(n_1P_1 + \cdots + n_rP_r) \leqslant Cy^{2/r},$$

where C is any constant chosen so that

$$\frac{(C\pi)^{r/2}}{\sqrt{R}\,\Gamma\left(\frac{r}{2}+1\right)} > 1.$$

Since the number of elements of S is $> y$, by Lemma 13, and $|\Gamma_p| < y$, we must have for two *distinct* r-tuples $(n_1, \ldots, n_r)$ and $(m_1, \ldots, m_r)$ that

$$n_1P_1 + \cdots + n_rP_r \equiv m_1P_1 + \cdots + m_rP_r (\text{mod } P).$$

Therefore, the denominator of the non-zero point

$$\sum_{i=1}^{r} (n_i - m_i)P_i = Q,$$

is divisible by p. The number of such primes is clearly bounded by $h_a(Q)$ as any integer n has at most log n prime factors. Moreover, Q is *not* a torsion point as $P_1, \ldots, P_r$ are independent. Therefore

$$h_a(Q) \ll H(Q).$$

Moreover, $H(Q) \leqslant 2Cy^{2/r}$, and therefore, the number of such Q's is by Lemma 13, $O(y)$. As each Q gives rise to only $O(y^{2/r})$ prime factors, we get that the total number of prime factors satisfying $|\Gamma_p| < y$ is $O(y^{1+2/r})$, as desired.

These lemmas will be utilised in the proof of Theorem 3.

§9. Proof of Theorem 3

We shall now consider the extensions

$$M_q = \mathbb{Q}\left(E[q],\ q^{-1}P_1, \ldots, q^{-1}P_r\right).$$

These are normal extensions over $\mathbb{Q}$ and the Galois group over $\mathbb{Q}$ is a subgroup of the semi-direct product

$$GL_2(\mathbb{F}_q) \rtimes E[q]^r.$$

Ribet [14] has shown that for q sufficiently large, $\mathrm{Gal}(M_q/\mathbb{Q}(E[q]))$ is in fact isomorphic to $E[q]^r$ given by

$$\left(\frac{1}{q}P_1, \ldots, \frac{1}{q}P_r\right) \mapsto \left(\frac{1}{q}P_1 + a_1, \ldots, \frac{1}{q}P_r + a_r\right)$$

where $(a_1, \ldots, a_r) \in E[q]^r$.

We may view every element $\sigma = (\gamma, \tau)$ of $\mathrm{Gal}(M_q/\mathbb{Q})$ as above, with $\gamma \in GL_2(\mathbb{F}_q)$ and $\tau \in E[q]^r$. Then every element σ determines a homomorphism

$$\tau\colon \Gamma \to E[q].$$

Clearly $\tau(\Gamma)$ is the subgroup of $E[q]$ generated by $a_1, \ldots, a_r$.

As before, we shall view γ as an element of $GL_2(\mathbb{F}_q)$ operating on $E[q]$. Then Lang and Trotter proved in [12], the following criterion for the divisibility of the index $(\bar{E}(\mathbb{F}_p)\colon \Gamma_p)$ by q.

LEMMA 15: *Let S_q consist of elements $\sigma = (\gamma, \tau)$ of $\mathrm{Gal}(M_q/\mathbb{Q})$ such that*

(i) $\ker(\gamma - 1) = E[q]$ *and* $\operatorname{rank} \tau(\Gamma) = 0$ *or* 1

or

(ii) $\ker(\gamma - 1)$ *is a non-trivial cyclic group and* $\tau(\Gamma) \subset \mathrm{Im}(\gamma - 1)$. *For* $p \nmid q\Delta$, *we have* $q \mid (\bar{E}(\mathbb{F}_p)\colon \Gamma_p)$ *if and only if* $\sigma_p \in S_q$ (*where* σ_p *denotes the Frobenius element of* p *in* $\mathrm{Gal}(M_q/\mathbb{Q})$).

REMARK: The primes dividing Δ are only finite in number and hence they introduce an error of $O(1)$ in the enumeration, so that we may ignore these. If $p = q$ and $p \mid (\bar{E}(\mathbb{F}_p)\colon \Gamma_p)$ then $p + 1 - a_p \equiv 0 \pmod{p}$ so that $a_p = 1$ for $p > 5$, as before. It can be shown that the number of such primes $p \leqslant x$ is $o(x/\log x)$. (See Serre [15].)

The number of elements in S_q satisfying condition (i) in the above lemma is clearly $q^{r+1} + q^r - q$. The number of γ such that $\ker(\gamma - 1)$ is cyclic is $q + O(1)$ in the CM case and $q^3 + O(q^2)$ in the non-CM case. Hence, the number of elements satisfying (ii) is

$$q^{r+1} + O(q^r)$$

in the CM case and

$$q^{r+3} + O(q^{r+2})$$

in the non-CM case.

For each squarefree number s, we set

$$M_s = \prod_{q \mid s} M_q$$

and note that, as usual

$$N_\Gamma(x) = N_\Gamma(x, y) + O(M_\Gamma(y, 2x)),$$

where $N_\Gamma(x, y)$ denotes the number of primes $p \leqslant x$ such that $\sigma_p(M_q/\mathbb{Q}) \notin S_q$ for all $q < y$, and $M_\Gamma(y, 2x)$ denotes the number of those primes p satisfying $\sigma_p(M_q/\mathbb{Q}) \in S_q$ for some $y < q < 2x$.

The S_q's for $q \mid s$ determine a conjugacy class S_s in $\mathrm{Gal}(M_s/\mathbb{Q})$ and we let $\pi(x, s)$ be the number of primes $p \leqslant x$ such that $\sigma_p(M_s/\mathbb{Q}) \in S_s$. Let $G_s = \mathrm{Gal}(M_s/\mathbb{Q})$ and we set

$$\delta(s) = \frac{|S_s|}{|G_s|}.$$

The usual inclusion-exlusion principle yields that

$$N_\Gamma(x, y) = \sum_s{}' \mu(s)\pi(x, s)$$

where the dash on the summation indicates that $q \mid s$ implies $q \leqslant y$. We choose

$$y = \left(\tfrac{1}{4} \log x\right)^{1/(r+2)}.$$

Invoking Lemma 10, we have on the GRH,

$$N_\Gamma(x, y) = \sum_s{}' \mu(s)\delta(s) \operatorname{li} x + O(x^{1-\epsilon})$$

by any easy calculation similar to the one carried out in §5. As $\delta(s) = O(s^{-r-1})$, we find that

$$C_E(\Gamma) = \sum_s \mu(s)\delta(s)$$

is absolutely convergent. Therefore,

$$N_\Gamma(x, y) = C_E(\Gamma)x/\log x + o(x/\log x).$$

We now handle $M_\Gamma(y, 2x)$. Setting

$$V_q^{(\iota)} = \mathbb{Q}\left(E[q], q^{-1}P_\iota\right),$$

we find that if $\sigma_p(M_q/\mathbb{Q}) \in S_q$ then σ_p restricted to $V_q^{(i)}$ must satisfy the Lang-Trotter criterion of §1 for all $i = 1, 2, \ldots, r$. The image of S_q restricted to $V_q^{(i)}$ is therefore $O(q^2)$ for all i, if E has CM and $O(q^4)$ in the non-CM case. With obvious notation

$$M_\Gamma(y, x^\alpha) \leqslant \sum_{y<q<x^\alpha} \left(\frac{\operatorname{li} x}{q^2} + O(q^g x^{1/2} \log x) \right)$$

by Lemma 10. Here, we have set $g = 2$ if E has CM and $g = 4$ in non-CM case. The first term above is clearly $o(x/\log x)$ for our choice of y. The error term is

$$\ll x^{(g+1)\alpha + 1/2}.$$

We choose $x^{\alpha(g+1)} = x^{1/2}/\log^2 x$, so that for this choice of α, we have

$$M(y, x^\alpha) = o(x/\log x).$$

It remains to consider $M_\Gamma(x^\alpha, 2x)$. If $\sigma_p(M_q/\mathbb{Q}) \in S_q$ for $x^\alpha \log^A x < q < 2x$, where A shall be suitably chosen later, then

$$|\Gamma_p| < x^{1-\alpha} \log^{-A} x.$$

Hence, by Lemma 14,

$$M_\Gamma(x^\alpha \log^A x, 2x) \ll \{x^{1-\alpha} \log^{-A} x\}^{1+2/r}.$$

A simple calculation reveals that if $r \geqslant 4g + 2$ and A is sufficiently large, then

$$M_\Gamma(x^\alpha \log^A x, 2x) = o(x/\log x).$$

The remaining interval is handled as in §5. Indeed,

$$M_\Gamma(x^\alpha, x^\alpha \log^A x) \leqslant M(x^\alpha, x^\alpha \log^A x)$$

and this latter quantity is easily estimated by utilising the Brun-Titchmersh theorem. We find,

$$M(x^\alpha, x^\alpha \log^A x) = o(x/\log x).$$

This proves that if $r \geqslant 4g + 2$, then

$$N_\Gamma(x) = c_E(\Gamma) x/\log x + o(x/\log x).$$

This completes the proof of Theorem 3.

§10. Higher rank in the CM case

We suppose in this section that E has complex multiplication by an order $\mathcal{O}$ in k. We will establish the higher rank analogue of Theorem 1 for such curves assuming only a modified Riemann hypothesis.

We begin with a result analogous to Lemma 13.

LEMMA 16: *The number of r-tuples of algebraic integers* $(\alpha_1, \ldots, \alpha_r)$, $\alpha_i \in \mathcal{O}$ *satisfying*

$$H(\alpha_1 P_1 + \cdots + \alpha_r P_r) \leqslant x$$

is

$$\gg x^r$$

where the implies constant depends only on E.

PROOF: For the sake of simplicity, we shall take $\mathcal{O}$ to be the full ring of integers of k, the general case being analogous. Moreover, as we are interested in a lower bound only, we may count only those α of the form $m + n\sqrt{-D}$, where D is squarefree and $k = \mathbb{Q}(\sqrt{-D})$. We therefore find, for such $\alpha_i = m_i + n_i\sqrt{-D}$, that

$$H(\alpha_1 P_1 + \cdots + \alpha_r P_r) = \sum_{i,j} T(i, j),$$

where

$$T(i, j) = m_i m_j \langle P_i, P_j \rangle + 2m_i n_j \langle P_i, \sqrt{-D}\, P_j \rangle + n_i n_j \langle \sqrt{-D}\, P_i, \sqrt{-D}\, P_j \rangle.$$

This is a quadratic form in $2r$ variables corresponding to the symmetric matrix

$$\tilde{R} = \left(\begin{array}{c|c} \langle P_i, P_j \rangle & \langle \sqrt{-D}\, P_i, P_j \rangle \\ \hline \langle P_i, \sqrt{-D}\, P_j \rangle & \langle \sqrt{-D}\, P_i, \sqrt{-D}\, P_j \rangle \end{array} \right).$$

Hence, by a well-known fact (see [17]), the number of lattice points is given by

$$C_R \cdot x^r + O(x^{r-1})$$

for some constant C_R depending on R and r. This completes the proof.

We also have the analogue of Lemma 14. To this end, we denote by $\tilde{\Gamma}$ the $\mathcal{O}$-module generated by Γ. If p is a prime which splits in k, we can then consider the image $\tilde{\Gamma}_p$ of $\tilde{\Gamma}(\text{mod } \pi_p)$.

LEMMA 17: *Suppose E has complex multiplication by an order in k. The number of primes p which split in k and for which*

$$|\tilde{\Gamma}_p| < y$$

is $O(y^{1+1/r})$.

PROOF: The proof is entirely analogous to Lemma 14 except that now we make use of Lemma 16 instead of Lemma 13. We therefore omit the details.

For a prime p which splits in k, we let $\pi_p = c_p + d_p\omega$, where $1, \omega$ are a $\mathbb{Z}$-basis for $\mathcal{O}$, be such that $N(\pi_p) = p$ and π_p corresponds to the Frobenius element mod p.

LEMMA 18: *Let p split in k and suppose that q is a prime dividing the index $(\tilde{\Gamma}_p\colon \Gamma_p)$. Then $d_p \equiv 0(\text{mod } q)$.*

PROOF: $\tilde{\Gamma}_p = \Gamma_p + \omega\Gamma_p$ for all odd primes p splitting in k. But we know that π_p fixes Γ_p, and hence $d_p(\omega\Gamma_p) \subset \Gamma_p$. Therefore, the index $(\tilde{\Gamma}_p\colon \Gamma_p)$ divides d_p, so that $q \mid d_p$, as desired.

We can now prove Theorem 4.

PROOF OF THEOREM 4: As in the rank one case, we consider the analogous fields:

$$K_q = k(E[q]),\ \tilde{L}_{\mathfrak{q}} = k\big(E[\mathfrak{q}],\ \mathfrak{q}^{-1}\Gamma\big),$$

the latter fields being defined for any first degree prime ideal $\mathfrak{q}$ of k. For a rational prime p which splits in k, we have $\overline{E}(\mathbb{F}_p) = \Gamma_p$ if π_p does not split completely in any K_q or $\tilde{L}_{\mathfrak{q}}$. This is used to handle error terms in the proof.

The method of derivation is entirely analogous to the case $r = 1$ except for some small variations. We shall therefore be brief in our outline of the proof except for the estimation of the $M(y, x)$ term, where the situation is different.

With obvious notation, we have

$$\tilde{N}_\Gamma(x) = \tilde{N}_\Gamma(x, y) + O\big(\tilde{M}_\Gamma(y, 2x)\big),$$

where we choose $y = (1/6(r+1)) \log x$. Assuming an $(r/(r+1)) - $GRH, we easily find for the above choice of y,

$$\tilde{N}_\Gamma(x, y) = \tilde{C}_E(\Gamma) x/\log x + o(x/\log x)$$

and so it remains to estimate $\tilde{M}_\Gamma(y, 2x)$. Again on the $(r/(r+1))-$GRH, we find

$$\tilde{M}_\Gamma(y, x^{1/(r+1)} \log^{-2} x) = o(x/\log x).$$

Utilising the Brun-Titchmarsh theorem as in §6, we find

$$M(x^{1/(r+1)} \log^{-2} x, x^{1/(r+1)} \log^2 x) = o(x/\log x).$$

Now, if for $N(\mathfrak{q})$ or q satisfying

$$x^{1/(r+1)} \log^2 x \leqslant q, \qquad N(\mathfrak{q}) \leqslant 2x,$$

$q \mid (\overline{E}(\mathbb{F}_p)\colon \Gamma_p)$, then either $q \mid (\overline{E}(\mathbb{F}_p)\colon \tilde{\Gamma}_p)$ or $q \mid (\tilde{\Gamma}_p, \Gamma_p)$. In the former case, we find

$$|\tilde{\Gamma}_p| \leqslant x^{r/(r+1)} \log^{-2} x$$

and so by Lemma 17, the number of such primes is

$$o(x/\log x).$$

In the latter case, we have $q \mid (\tilde{\Gamma}_p\colon \Gamma_p)$ and so by Lemma 18, $d_p \equiv 0 (\mathrm{mod}\ q)$. Hence, $\pi_p \equiv 1 (\mathrm{mod}\ q)$. Therefore, π_p splits completely in K_q. The number of such primes is easily seen to be $O(x/q^2)$ by an elementary estimation (see for example [13]). Hence, the number of primes arising in the latter case is

$$\ll \sum_{q > x^{1/(r+1)}} \frac{x}{q^2} = O(x^{1/(r+1)}).$$

We therefore find,

$$\tilde{M}_\Gamma(x^{1/(r+1)} \log^2 x, 2x) = o(x/\log x),$$

as desired. This completes the proof of Theorem 4.

§11. A lower bound for $N_\Gamma(x)$

If the rank of Γ is $\geqslant 6$, we derive a lower bound for $N_\Gamma(x)$ in the CM case.

For the sake of simplicity, let us first suppose that all the 2-division points of E are rational and that $\mathbb{Q}(\frac{1}{2}\Gamma)$ is a proper extension of $\mathbb{Q}$. Note that it is necessarily abelian because of our assumption. We consider the supersingular primes and so $a_p = 0$. The following lemma is a familiar consequence of the lower bound sieve method.

LEMMA 19: *Let $S_\alpha(x)$ denote the number of primes $p \leqslant x$ which are inert in k, do not split in $\mathbb{Q}(\frac{1}{2}\Gamma)$, and are such that $q \mid (p+1)$, q prime, implies $q = 2$ or $q > x^\alpha$. For $\alpha = \frac{1}{4} + \epsilon$,*

$$S_\alpha(x) \gg \frac{x}{\log^2 x}.$$

PROOF: As the proof is standard, we only indicate the highlights. Indeed, the fact that p does not split in k or $\mathbb{Q}(\frac{1}{2}\Gamma)$ just imposes additional congruence conditions on p. Then utilising the lower bound sieve as developed either by Bombieri [1], or Iwaniec [9] yields a lower bound with an appropriate α. The key ingredient in both derivations is the Bombieri-Vinogradov theorem for primes in arithmetic progression. The former method yields our result for $\alpha = \frac{1}{6} - \epsilon$ while the latter gives it for $\alpha = \frac{1}{4} - \epsilon$. The recent result of Fouvry-Iwaniec [3], where a variant of the Bombieri-Vinogradov theorem is proved for an extended range, enables us to deduce the lower bound for S_α for $\alpha = \frac{1}{4} + \epsilon$.

REMARK: The simplest derivation of the lower bound sieve is given in Bombieri [1]. Utilising a "twisted" version of the Bombieri-Vinogradov theorem, one can remove the restriction that all the 2-division points be rational. That is, if we impose certain non-abelian conditions corresponding to a fixed extension of k, this results in twisting the Dirichlet characters by appropriate non-abelian characters of k. Then, a Bombieri-Vinogradov theorem can still be established for these "twisted" progressions.

PROOF OF THEOREM 5: With $\alpha = \frac{1}{4} + \epsilon$, we find from Lemma 19, that each prime p enumerated by $S_\alpha(x)$ has the property that if

$$q \mid \left(\bar{E}(\mathbb{F}_p) : \Gamma_p\right)$$

then $q > x^\alpha$ and hence $|\Gamma_p| < x^{1-\alpha}$. By Lemma 14, the number of such primes is

$$\ll (x^{1-\alpha})^{1+2/r} = O(x^{1-\epsilon})$$

for $r \geqslant 6$. Hence, apart from $O(x^{1-\epsilon})$ primes enumerated by $S_\alpha(x)$, we have that $\bar{E}(\mathbb{F}_p) = \Gamma_p$. Therefore, if $\operatorname{rank}(\Gamma) \geqslant 6$, then

$$N_\Gamma(x) \gg \frac{x}{\log^2 x}.$$

It is possible to show a corresponding result for primes which split in k. Indeed, the method is analogous to Bombieri [1] where we invoke the analogous theorems for number fields. In particular, the Bombieri-Vinogradov theorem for k as proved in Huxley [8] and the k-analogue of Theorem 18 in [1] suffice to yield: for $\operatorname{rank}(\Gamma) \geqslant 6$,

$$\tilde{N}_\Gamma(x) \gg \frac{x}{\log^3 x}$$

whenever 2 and 3 are inert in k. The $\log^3 x$-term comes from the fact that we consider the ray class fields $k(\mathfrak{q})$ in place of the cyclotomic extensions and these have degree

$$\frac{\phi(\mathfrak{q})}{2}$$

which yields a corresponding factor of

$$\prod_{N(\mathfrak{q}) < z} \left(1 - \frac{2}{N(\mathfrak{q}) - 1}\right)$$

in the lower bound sieve. We omit the details as it is entirely analogous to [1] where a similar result is proved for $\alpha = \frac{1}{6} - \epsilon$. Certainly, an analogue of the Fouvry-Iwaniec theorem in k would yield a corresponding result for $rk(\Gamma) \geqslant 4$.

The interest in these results lies in the fact that they are the first unconditional statements concerning $N_\Gamma(x)$. They also stress the importance of the sieve method in problems of this kind. Indeed, the lack of the analogue of the Bombieri-Vinogradov theorem is the main obstackle in obtaining a lower bound in the non-CM case.

PROOF OF THE COROLLARY: We consider the primes enumerated by $S_\alpha(x)$, by Lemma 19, with $\alpha = \frac{1}{4} + \epsilon$. We have shown above that apart from $O(x^{1-\epsilon})$ primes of $S_\alpha(x)$, $\bar{E}(\mathbb{F}_p)$ is generated by Γ_p provided rank of $\Gamma \geqslant 6$. Moreover, if $\bar{E}(\mathbb{F}_p)$ is not cyclic for these primes, then it contains a (q, q) group, where $q > x^{(1/4)+\epsilon}$. The number of such primes is clearly

$$\leqslant \sum_{q > x^{1/4+\epsilon}} \frac{x}{q^2} = O(x^{3/4-\epsilon})$$

as $q^2 | (p+1)$. Hence, apart from $O(x^{1-\epsilon})$ primes enumerated by $S_\alpha(x)$, we have that $\bar{E}(\mathbb{F}_p)$ is cyclic and generated by Γ_p, when rank of $\Gamma \geqslant 6$. Let $\Gamma = \{P_1, \ldots, P_6\}$. We want to produce a single generator

$$P = \sum_{i=1}^{6} n_i P_i$$

with $0 \leqslant n_i \leqslant A$. Let Q be a generator of $\bar{E}(\mathbb{F}_p)$ and let us write $P_i \equiv a_i Q (\mathrm{mod}\ p)$. As Γ_p generates $\bar{E}(\mathbb{F}_p)$, we must have $\gcd(a_1, \ldots, a_6, p+1) = 1$. The total number of possibilities for $(n_1, \ldots, n_6)$ is $(A+1)^6$. Of these, the number satisfying

$$\sum_{i=1}^{6} n_i a_i \equiv 0 (\mathrm{mod}\ 2)$$

it is most $(A+2)(A+1)^5/2$. As $p+1$ has odd prime divisors $q_1, q_2, q_3 > x^{(1/4)+\epsilon}$, we find that for each of these, there at most $(A+1)^5$ 6-tuples $(n_1, \ldots, n_6)$ satisfying

$$\sum_{i=1}^{6} n_i a_i \equiv 0 (\mathrm{mod}\ q_i)$$

because of the coprime condition.

Therefore, if

$$(A+1)^6 - \tfrac{1}{2}(A+2)(A+1)^5 - 3(A+1)^5 > 0,$$

we can find $(n_1, \ldots, n_6)$ such that $\sum_{i=1}^{6} n_i a_i$ is coprime to $(p+1)$ which serves to produce the single generator P of $\bar{E}(\mathbb{F}_p)$. We find that $A = 7$ gives the desired result.

REMARK: The analogue of this result in the classical case is new and is of interest in its own right. We therefore treat it in [5].

§12. Concluding remarks

Our first remark concerns the use of GRH in Theorem 1. It is well-known that to treat the $N(x, y)$ term, we do not need GRH provided y is chosen as a sufficiently small function of x tending to infinity as $x \to \infty$. The GRH is not necessary to deduce $N_\Gamma(x) \to \infty$. A zero free region of $\mathrm{Re}(s) > \frac{4}{5}$ allows us to deduce this result in line with Hooley's remark in the classical case [7]. This is effected by invoking a "twisted" Bombieri-Vinogradov theorem in the place of the GRH.

The use of the GRH in handling the $M(y, x^{1/2})$ term can be eliminated if we had an analogue of the Brun-Titchmarsh theorem for

non-abelian extensions. As such a theorem exists for the extensions K_q, the GRH need not be applied to handle the error term arising from these fields. In the case of L_q, such an upper bound seems to be very difficult to establish unconditionally.

References

[1] E. Bombieri: Le grand crible dans la théorie analytique des nombres. Société mathematique de France. *Asterisque* 18 (1974).
[2] J. Coates and A. Wiles: On the conjecture of Birch and Swinnerton-Dyer, *Inv. Math.* 39 (1977) 223–251.
[3] E. Fouvry and H. Iwaniec: Primes in arithmetic progressions. *Acta Arithmetica* 42 (1983) 197–218.
[4] R. Gupta: Fields of division points of elliptic curves related to Coates-Wiles, *Ph.D. Thesis, M.I.T.* (1983).
[5] R. Gupta and M. Ram Murty: A remark on Artin's conjecture *Inv. Math.* 78 (1984) 127–130.
[6] C. Hooley: On Artin's conjecture. *J. reine angew. Math.* 225 (1967) 209–220.
[7] C. Hooley: *Applications of sieve Methods to the Theory of Numbers*. Cambridge Univ. Press, London (1976).
[8] M. Huxley: The large sieve inequality for algebraic number fields III, Zero density results. *J. London Math. Soc.* 3 (1971) 233–240.
[9] H. Iwaniec: Rosser's sieve. Acta Arith. 36 (1980) 171–202.
[10]' J. Lagarias and A. Odlyzko: Effective versions of the Cebotarev density theorem. In: A. Frolich (ed.), *Algebraic Number Fields*. Proceedings of the 1975 Durham Symposium, Academic Press, London and New York (1977).
[11] S. Lang: *Elliptic Curves and diophantine Analysis*. Springer-Verlag (1978).
[12] S. Lang and H. Trotter: Primitive points on elliptic curves. *Bull. Amer. Math. Soc.* 83 (1977) 289–292.
[13] M. Ram Murty: On Artin's conjecture. *J. Number Theory* 16 (1983) 147–168.
[14] K. Ribet: Dividing rational points on abelian varieties of CM type. *Comp. Math.* 33 (1976) 69–74.
[15] J.P. Serre: Quelques applications du théorème de densité de Chebotarev. *Publ. Math. I.H.E.S.* 54 (1982) 123–201.
[16] W. Schaal: On the large sieve method in algebraic number fields. *J. Number Theory* 2 (1970) 249–270.
[17] A. Walfisz: Über Gitterpunkte in mehrdimensionalen Ellipsoiden III. *Akh. Math. Zietschr.* 27 (1978) S. 245–268.

(Oblatum 19-IV-1984)

Rajiv Gupta
Department of Mathematics
University of British Columbia
Vancouver, B.C. V6T 1Y4
Canada

M. Ram Murty
Department of Mathematics
McGill University
805 Sherbrooke St. W.
Montreal, P.Q. H3A 2K6
Canada