

ANALYTIC PROBLEMS FOR ELLIPTIC CURVES

E. KOWALSKI

ABSTRACT. We consider some problems of analytic number theory for elliptic curves which can be considered as analogues of classical questions around the distribution of primes in arithmetic progressions to large moduli, and to the question of twin primes. This leads to some local results on the distribution of the group structures of elliptic curves defined over a prime finite field, exhibiting an interesting dichotomy for the occurrence of the possible groups.

CONTENTS

1. Introduction	1
2. Some local invariants for elliptic curves	2
3. Totally split primes	7
4. Elliptic twins	21
5. Curves with complex multiplication	25
6. Local study of totally split primes	41
7. Numerical examples	57
8. Conclusion	63
References	64

1. INTRODUCTION

This paper introduces and discusses some problems of analytic number theory which are related to the arithmetic of elliptic curves over number fields. One can see them as analogues of some very classical problems about the distribution of prime numbers, especially primes in arithmetic progressions to large moduli. The motivation comes both from these analogies and from the conjecture of Birch and Swinnerton-Dyer.

To explain this, consider an elliptic curve E defined over \mathbf{Q} , given by a (minimal) Weierstrass equation ([Si-1, VII-1])

$$(1.1) \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in \mathbf{Z}$. For all primes p we can consider the reduced curve E_p modulo p , which for almost all p will be an elliptic curve over the finite field $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. We wish to study the behavior of sums of the type

$$(1.2) \quad \sum_{p \leq X} \iota_E(p)$$

as $X \rightarrow +\infty$, where $\iota_E(p)$ is some invariant attached to the reduced curve E_p and to its finite group of \mathbf{F}_p -rational points in particular. For example, taking

$$\iota_E(p) = \frac{|E_p(\mathbf{F}_p)|}{p}$$

1991 *Mathematics Subject Classification*. Primary 11N99; Secondary 11G05, 11G20, 11F99.

Key words and phrases. Elliptic curves, sieves, trace formula for Hecke operators, Chebotarev density theorem.

one gets the sum

$$\sum_{p \leq X} \frac{|E_p(\mathbf{F}_p)|}{p}$$

which should be related to the behavior of the logarithmic derivative of the Hasse-Weil zeta function of E at $s = 1$, and so conjecturally to a global invariant of E/\mathbf{Q} , the rank of its Mordell-Weil group $E(\mathbf{Q})$.

We wish to consider other sums of type (1.2) which are natural from the point of view of analytic number theory. The hope is to get precise enough asymptotics where global invariants of E would enter, to gain an understanding of the local-global principles which the Birch and Swinnerton-Dyer conjecture postulates.

The plan of this paper is as follows: in the first section we state basic facts on elliptic curves that we will use and introduce some natural invariants $\iota_E(p)$. In Section 3, we show how the study of the sum (1.2) for one of them brings about questions involving the equidistribution of Frobenius elements (in the extensions of \mathbf{Q} generated by the torsion points of E) to uniform and large moduli, especially on totally split primes in such extensions. We analyze this problem on GRH and discuss the new difficulties which arise in comparison with the case of primes in arithmetic progressions. There are several remarks here which may be of interest. One of the new phenomenon (primes splitting completely in fields generated by d torsion points with d very large) leads us to a notion of elliptic twins, analogues of the classical twin primes that we again discuss in general terms. At long last, non-trivial results are obtained in the next two sections: for CM curves, in Section 5, sieve techniques in quadratic fields can be usefully applied, and in Section 6 the subject of totally split primes is viewed from a different angle: now, given a prime p , and $d \geq 1$, we ask whether or not there exists *some* curve E with p totally split in $\mathbf{Q}(E[d])$. This is done in two ways, adapting results of Deuring, Waterhouse, Schoof, and using the trace formula and modular curves. Finally, since the problems are amenable to experimentation, we present in Section 7 some numerical data and further remarks.

Most of the results presented here are not very strong and the overall situation remains rather unsatisfactory. The excuse for this is that the problems seem genuinely difficult. On the other hand, to the author at least, their interest is very obvious.

Notation. The symbols $O()$ and $o()$ are used in the sense of (for example) Bourbaki, so $f(x) = O(g(x))$ as $x \rightarrow x_0$ means that for x in some neighborhood U of x_0 we have $|f(x)| \leq Cg(x)$ for some $C \geq 0$ (depending on U). On the other hand $f \ll g$ is used in the sense that there exists $C \geq 0$ such that for all x (in some set to be described explicitly or implicitly) we have $|f(x)| \leq Cg(x)$. The dependence of C on other parameters is indicated by subscripts \ll_ε , etc.

For notational convenience¹ it is sometimes useful to use another symbol $\underline{O}()$ such that $f = \underline{O}(g)$ is equivalent to $f \ll g$.

It will be convenient in a number of places to use the following notation: for every real number x , we let

$$(1.3) \quad x^- = (\sqrt{x} - 1)^2, \quad x^+ = (\sqrt{x} + 1)^2.$$

(defined for $x \geq 1$, $x \geq -1$, respectively). Note that

$$(x^+)^- = (x^-)^+ = x, \quad \text{and} \quad x^+ - x^- = 4\sqrt{x}.$$

2. SOME LOCAL INVARIANTS FOR ELLIPTIC CURVES

In this section we want to define some of the invariants that are of interest. First we recall some important facts about elliptic curves.

¹Many papers in analytic number theory actually use the notation $O()$ in this sense, and correspondingly speak of “hidden constants”, as for \ll .

2.1. Elliptic curves. Let E/K be an elliptic curve defined over a field K . We will mostly use “old-fashioned” language, identifying E with its set of \bar{K} -valued points, where \bar{K} is a fixed algebraic closure of K .

The endomorphism ring of E over K is denoted by $\text{End}(E)$, and the endomorphism ring of E over \bar{K} by $\text{End}_{\bar{K}}(E)$. The ring $\text{End}(E)$ contains the subring \mathbf{Z} corresponding to the morphisms $x \mapsto nx$ for $n \in \mathbf{Z}$. When $\text{End}(E)$ is strictly bigger than \mathbf{Z} , the curve is said to be CM, or to have complex multiplication.

To any $\varphi \in \text{End}(E)$ is associated its *dual* $\bar{\varphi} \in \text{End}(E)$ with the property that $\varphi \circ \bar{\varphi} = \bar{\varphi} \circ \varphi = [\text{deg}(\varphi)]$, the multiplication by the degree of φ , as a morphism of algebraic curves ([Si-1, III-6]).

The various possibilities for $\text{End}(E)$ have been studied extensively by Deuring [De]. We are concerned with two cases. Let $\mathcal{O} = \text{End}(E)$.

- If K is a finite field, E is always CM, and \mathcal{O} is either an order in an imaginary quadratic field, in which case E is said to be ordinary, or an order in a quaternion algebra, in which case E is said to be supersingular (see [Si-1, V-3]). There are only finitely many j -invariants $j \in \bar{K}$ corresponding to supersingular curves, all of degree ≤ 2 over the prime field.
- If K is a number field, either $\mathcal{O} = \mathbf{Z}$ or \mathcal{O} is an order in an imaginary quadratic field. In this case $j(E)$ is an algebraic integer. For fixed K , there are only finitely many possible values of $j \in K$ for which an elliptic curve over K with $j(E) = j$ has CM (see e.g. [Si-2, II, Pr. 1.2], and for instance [Si-2, App. A-3] for a list of all CM curves over \mathbf{Q}). The dual of an endomorphism σ is its (unique) conjugate over \mathbf{Q} .

Let E/K be an elliptic curve defined over a field K . For every integer $d \geq 1$, the d -torsion points of E form (depending on the point of view) either a finite subgroup or a finite subgroup scheme of E , denoted either $E[d]$ or $E[d](\bar{K})$ depending on the emphasis.

The structure of this group depends on the characteristic p of K and is given as follows ([Si-1, III-6.4]):

- If d_1 and d_2 are coprime, then

$$E[d_1 d_2](\bar{K}) = E[d_1](\bar{K}) \oplus E[d_2](\bar{K}).$$

- If $(d, p) = 1$ (in particular, if K is of characteristic 0), we have

$$E[d](\bar{K}) \simeq \mathbf{Z}/d\mathbf{Z} \oplus \mathbf{Z}/d\mathbf{Z}.$$

- If K is a finite field, $d = p^v$ with $v \geq 1$ and E is ordinary, then

$$E[d](\bar{K}) \simeq \mathbf{Z}/d\mathbf{Z}.$$

- If K is a finite field, $d = p^v$ with $v \geq 1$ and E is supersingular, then

$$E[d](\bar{K}) = 0.$$

In any case, $E[d]$ is a finite (and free) $\mathbf{Z}/d\mathbf{Z}$ -module, and the natural action of the Galois group $G_K = \text{Gal}(\bar{K}/K)$ induces a Galois representation

$$\rho_d(E) : G_K \longrightarrow \text{Aut}(E[d]).$$

Assume now that $(d, p) = 1$, then by choosing a basis we get 2-dimensional representations, well-defined up to conjugacy

$$\rho_d(E) : G_K \longrightarrow GL(2, \mathbf{Z}/d\mathbf{Z}).$$

Those are compatible, meaning that if $e \mid d$, then we have

$$\rho_e(E) = \rho_d(E) \pmod{e}$$

with obvious notations. In particular, taking a prime $\ell \neq p$ and $d = \ell^v$ for all $v \geq 0$, we obtain a projective system of representations into $GL(2, \mathbf{Z}/\ell^v\mathbf{Z})$ which can be put together into an integral ℓ -adic representation

$$\hat{\rho}_\ell : G_K \longrightarrow GL(2, \mathbf{Z}_\ell).$$

Let now $K = \mathbf{F}_q$ be a finite field with q elements, of characteristic p (this will be a standing convention). The group of \mathbf{F}_q -rational points on E is finite. We write

$$n(E) = |E(\mathbf{F}_q)|$$

for its order. The most important invariant of E/\mathbf{F}_q is the integer $a(E)$ such that

$$(2.1) \quad n(E) = |E(\mathbf{F}_q)| = q + 1 - a(E).$$

One knows that $a(E)$ characterizes the isogeny class of E over K (see [Si-1, Ex. 5.4]). Moreover, E is supersingular if and only if $p \mid a(E)$. In case $q = p$, this is equivalent with $a(E) = 0$ (see (2.6)), so there is a unique isogeny class of supersingular curves defined over the base field \mathbf{F}_p .

The integer $a(E)$ is also linked to $\text{End}(E)$. The Frobenius automorphism $\sigma : x \mapsto x^q$ of $\overline{\mathbf{F}}_q$ is an element of $\text{End}(E)$. We have ([Si-1, V])

$$(2.2) \quad a(E) = \text{Tr}(\sigma) = \sigma + \bar{\sigma}$$

$$(2.3) \quad n(E) = N(\sigma - 1) = (\sigma - 1)(\bar{\sigma} - 1).$$

For any integer d with $(d, p) = 1$, $a(E)$ is further related to the Galois representation $\rho_d(E)$ ([Si-1, V]) by

$$(2.4) \quad \det(\rho_d(\sigma)) = q \pmod{d} \quad \text{and} \quad \text{Tr}(\rho_d(\sigma)) = a(E) \pmod{d}.$$

Hence the ℓ -adic representation $\hat{\rho}_\ell$ satisfies the fundamental property

$$(2.5) \quad \det(\hat{\rho}_\ell(\sigma)) = q \quad \text{and} \quad \text{Tr}(\hat{\rho}_\ell(\sigma)) = a(E).$$

Hasse proved (the Riemann Hypothesis for elliptic curves over finite fields, see [Si-1, V-1.1]) that

$$(2.6) \quad |a(E)| \leq 2\sqrt{q}.$$

If K is a number field, then for any prime ideal \mathfrak{p} of K where E has good reduction, the above theory applies to the reduced curve $E_{\mathfrak{p}}$ modulo \mathfrak{p} . For instance, the Galois representation $\hat{\rho}_\ell(E)$ (for any ℓ not dividing \mathfrak{p}) satisfies

$$(2.7) \quad \det(\hat{\rho}_\ell(\sigma_{\mathfrak{p}})) = N\mathfrak{p} \quad \text{and} \quad \text{Tr}(\hat{\rho}_\ell(\sigma_{\mathfrak{p}})) = a_{\mathfrak{p}}(E)$$

where $\sigma_{\mathfrak{p}}$ is a Frobenius element at \mathfrak{p} and $a_{\mathfrak{p}} = a(E_{\mathfrak{p}})$.

For an elliptic curve E/K , and an integer $d \geq 1$, we let $K(E[d])$ denote the finite extension of K obtained by adjoining the coordinates of the d -torsion points of E , or in other words the smallest extension L/K such that $E[d](\bar{K}) \subset E(L)$. This is a Galois extension and in fact $K(E[d])$ is the extension of K corresponding to the closed subgroup $\ker(\rho_d)$ of G_K , i.e. $K(E[d]) = \bar{K}^{\ker \rho_d}$, so that there is a canonical isomorphism

$$(2.8) \quad \text{Gal}(K(E[d])/K) \simeq \text{Im } \rho_d \subset \text{Aut}(E[d]).$$

We will denote $G_d = \text{Gal}(K(E[d])/K)$ when E and K are clear in the context.

In the case $d = 2$, and K of characteristic $\neq 2$, and E/K is given by an equation

$$y^2 = f(x)$$

for some cubic polynomial $f \in K[X]$, the 2-division points of E are the origin, and the points $(\alpha, 0)$ where α runs over the three distinct roots of E in \bar{K} . In particular, $E[2] \subset E(K)$ if and only if f splits into linear factors in $K[X]$.

We let μ_d denote the group (scheme) of the d -th roots of unity. It is known ([Si-1, III-8.11]) that $K(\mu_d) \subset K(E[d])$ where $K(\mu_d)$ is the field obtained by adjoining all d -th roots of unity to K . In the case of number fields (resp. finite fields), this can be seen from (2.7) (resp. (2.4)): the determinant condition implies that primes totally split in $K(E[d])$ are totally split in $K(\mu_d)$, which implies that $K(E[d])$ contains $K(\mu_d)$ (see e.g. [Ne, V-6.8]).

If K is a number field and \mathfrak{p} is a prime ideal in K where E has good reduction, the residue field extension of $K(E[d])$ at \mathfrak{p} is isomorphic to $\mathbf{F}_{\mathfrak{p}}(E_{\mathfrak{p}}[d])$. Indeed the reduction map $E[d](\bar{K}_{\mathfrak{p}}) \rightarrow$

$E_{\mathfrak{p}}[d](\overline{\mathbf{F}}_{\mathfrak{p}})$ is surjective (see e.g. [Si-1, VII-3.1] if $(d, \mathfrak{p}) = 1$, which will be the case we need, and adapt [Si-1, Ex. IV-4.4] for the general case).

In this case of a number field, the Galois groups G_d are known “up to finite index”.

Theorem 2.1. *Let K be a number field, E/K an elliptic curve. Then*

1. (Deuring, see [Se-1, 4.5]) *If E has complex multiplication and $\mathcal{O} = \text{End}_{\overline{K}}(E)$, with $\mathcal{O} \subset K$, then ρ_d induces a group homomorphism*

$$\rho_d : G_K \rightarrow (\mathcal{O}/d\mathcal{O})^\times$$

with the property that as d ranges over all integers $d \geq 1$, the index of G_d in the finite group $(\mathcal{O}/d\mathcal{O})^\times$ is bounded by a constant $i(E)$.²

2. (Serre [Se-1]) *If E does not have complex multiplication, then the index of G_d in the finite group $\text{Aut}(E[d]) \simeq GL(2, \mathbf{Z}/d\mathbf{Z})$ is bounded by a constant $i(E)$.*

Note that

$$(2.9) \quad |GL(2, \mathbf{Z}/d\mathbf{Z})| = d\psi(d)\varphi(d)^2$$

where φ is Euler’s function and

$$(2.10) \quad \psi(d) = d \prod_{p|d} \left(1 + \frac{1}{p}\right).$$

Since \mathcal{O} is not a Dedekind ring in general, hence does not have unique factorization into ideals, the order of $(\mathcal{O}/d\mathcal{O})^\times$ is not a multiplicative function of d . If \mathcal{O} is the full ring of integers of its fraction field k , or if d is coprime with the discriminant of \mathcal{O} , then $|(\mathcal{O}/d\mathcal{O})^\times|$ is the analogue of the Euler function for ideals in k :

$$(2.11) \quad |(\mathcal{O}/d\mathcal{O})^\times| = d^2 \prod_{\mathfrak{p}|(d)} \left(1 - \frac{1}{N\mathfrak{p}}\right).$$

Informally, we say that in the CM case, $|G_d|$ is of order of magnitude d^2 , and in the non-CM case, $|G_d|$ is of order of magnitude d^4 . This difference will be important later on so we define the *Galois dimension* $g = g(E)$ of E to be 2 if E has CM and 4 if not (it is the dimension of the ℓ -adic Lie group $\text{Im}(\hat{\rho}_\ell(G_K)) \subset GL(2, \mathbf{Z}_\ell)$, or of its Lie algebra for ℓ large enough [Se-4]).

2.2. Local invariants. First we describe the group structure of the rational points of an elliptic curve defined over a finite field. This is well known.

Lemma 2.2. *Let E/\mathbf{F}_q be an elliptic curve defined over a finite field with q elements. There exist unique integers d_1 and d_2 such that*

$$(2.12) \quad E(\mathbf{F}_q) \simeq \mathbf{Z}/d_1\mathbf{Z} \oplus \mathbf{Z}/d_1d_2\mathbf{Z}.$$

Proof. The group $E(\mathbf{F}_q)$ is finite, hence of finite exponent, so for some $d \geq 1$ we have

$$E(\mathbf{F}_q) \subset E[d](\overline{\mathbf{F}}_q).$$

As we recalled in Section 2.1, the group on the right has a system of generators with at most two elements. By the structure theorem of finite abelian groups, the same is true for any subgroup, and they are all of the form stated. \square

The integers d_1, d_2 are very interesting invariants of E . We will denote them by $d_1(E)$ (resp. $d_2(E)$) or $d_1(\mathfrak{p})$ (resp. $d_2(\mathfrak{p})$) when E is obtained by reducing a curve over a number field modulo a prime ideal \mathfrak{p} .

²If K does not contain the endomorphism ring, G_d is at most an extension of $(\mathcal{O}/d\mathcal{O})^\times$ by $\mathbf{Z}/2\mathbf{Z}$.

Lemma 2.3. *Let E/\mathbf{F}_q be an elliptic curve over a finite field with q elements. Then*

(1) *We have*

$$d_1 = d_1(E) = \max\{d \geq 1 \mid (d, p) = 1 \text{ and } E[d](\overline{\mathbf{F}}_q) \subset E(\mathbf{F}_q)\}$$

i.e. $d_1(E)$ is the largest integer d prime to p for which all of the d -torsion is rational over \mathbf{F}_q . The max can be taken with respect to the order by divisibility or the “linear” order on \mathbf{Z} .

(2) *We have*

$$d_1(E)^2 d_2(E) = n(E) = q + 1 - a(E).$$

(3) *We have*

$$q + 1 - a(E) = 0 \pmod{d_1^2}, \quad q = 1 \pmod{d_1}, \quad a(E) = 2 \pmod{d_1}.$$

(4) *We have*

$$(2.13) \quad d_1(E) \leq \sqrt{q} + 1.$$

Proof. All this is easy from the structure of the d -torsion points. For (1), observe that the finite abelian group

$$\mathbf{Z}/d_1\mathbf{Z} \oplus \mathbf{Z}/d_1d_2\mathbf{Z}$$

contains d_1^2 points of order d_1 , namely $\mathbf{Z}/d_1\mathbf{Z} \oplus d_2\mathbf{Z}/d_1d_2\mathbf{Z}$. Since it is known a priori that $E(\overline{\mathbf{F}}_q)$ contains at most d^2 points of order d for any $d \geq 1$, all the d_1 -torsion is \mathbf{F}_q -rational. Moreover, if there exists $d > d_1$ for which $E[d](\overline{\mathbf{F}}_q) \subset E(\mathbf{F}_q)$, we can write $d = d_1d'$ for some $d' > 1$. Then d' must be of the form $d' = p^v$ for some $v \geq 1$, since otherwise there would be e^2 points of order e which are \mathbf{F}_q -rational, for some $e > d$, which the group structure (2.12) forbids.

The second point is obvious, and gives the first congruence in (3), while (2.4) gives the other congruences.

For (2.13), since $d_1^2 \mid q + 1 - a(E)$, and $q + 1 - a(E) > 0$, it follows that $d_1^2 \leq q + 1 - a(E) \leq (\sqrt{q} + 1)^2$ by (2.6). \square

Remark 2.4. The congruence $n(E) = 0 \pmod{d_1^2}$ can also be obtained from the Galois representations without referring to the points of the elliptic curve: let $\gamma = \rho(\sigma) \in GL(2, \mathbf{Z}/d_1^2\mathbf{Z})$. We know that $\gamma \equiv 1 \pmod{d_1}$ by definition. Now writing $\gamma = 1 + d_1\gamma'$ and expanding the trace and determinant, we obtain using (2.4) (both for $d = d_1$ and $d = d_1^2$)

$$2 + d \operatorname{Tr}(\gamma') = a(E) \pmod{d_1^2}, \quad 1 + d \operatorname{Tr}(\gamma') = p \pmod{d_1^2}.$$

Then observe that $\operatorname{Tr}(\gamma') = a(E) \pmod{d_1}$ and subtract to get $1 = a - p \pmod{d_1^2}$. (This remark is due to N. Katz).

Remark 2.5. If $q = p \geq 3$ the condition $(d, p) = 1$ in the characterization (1) of d_1 can be omitted unless either E is supersingular or $a(E) = 1$. In the first case, of course, $0 = E[p^n] \subset E(\mathbf{F}_p)$ for all $n \geq 1$, while in the second case we have $|E(\mathbf{F}_p)| = p$ so $E(\mathbf{F}_p)$ is cyclic of order p and must equal $E[p]$. Conversely, for E ordinary, if $d = p^ne$ with $(e, p) = 1$ and $E[d] \subset E(\mathbf{F}_p)$, we get $p^ne^2 \mid p + 1 - a(E)$ and by the Riemann Hypothesis (2.6) it follows immediately that $n = e = 1$.

Note that curves with $a(E) \equiv 1 \pmod{p}$ occur in other contexts. If E arises by reduction modulo p of a curve over \mathbf{Q} , the prime p is called *anomalous* [Ma]. When $p \geq 7$, $a(E) = 1$ is the same as $a(E) \equiv 1 \pmod{p}$, so those curves, and the supersingular curves, form two isogeny classes of curves over \mathbf{F}_p .

The next lemma is equally simple.

Lemma 2.6. *Let E/\mathbf{F}_q be an elliptic curve defined over a finite field and $d \geq 1$ an integer with $(d, p) = 1$. Then $E[d] \subset E(\mathbf{F}_q)$ if and only if $\sigma \equiv 1 \pmod{d}$ in $\operatorname{End}(E)$, where σ is the Frobenius endomorphism of E .*

Proof. Let $K = \text{End}(E) \otimes_{\mathbf{Z}} \mathbf{Q}$, which is either a quadratic field or a quaternion algebra over \mathbf{Q} , and let $\sigma' = (\sigma - 1)/d \in K$. The congruence in the statement of the Lemma means $\sigma' \in \text{End}(E)$; since d is central in K , there is no ambiguity in the side on which d^{-1} is put in the definition of σ' .

Now if $\sigma' \in \text{End}(E)$, we have $\sigma = 1 + d\sigma'$, so for any $x \in E[d]$ it follows that $\sigma(x) - x = \sigma'(dx) = 0$, hence x is \mathbf{F}_q -rational. Conversely, if $E[d] \subset E(\mathbf{F}_q)$, the \mathbf{F}_q -isogeny $\phi = \sigma - 1$ of E satisfies $\ker(d) \subset \ker(\phi)$; since $(d, p) = 1$, multiplication by d is separable, hence ([Si-1, III-4.11]) ϕ factorizes by $d : E \rightarrow E$, which means $\sigma \equiv 1 \pmod{d}$. \square

Here is the global interpretation of d_1 .

Lemma 2.7. *Let E/K be an elliptic curve over a number field, \mathfrak{p} a prime ideal such that E has good reduction modulo \mathfrak{p} . For any integer $d \geq 1$, we have $d \mid d_1(E_{\mathfrak{p}})$ if and only if \mathfrak{p} is totally split in the field $K(E[d])$.*

Proof. Both statements imply that $(d, \mathfrak{p}) = 1$: this is by definition for d_1 and because if \mathfrak{p} is totally split, it is unramified in $K(E[d])$, hence in $K(\mu_d)$, which implies $N\mathfrak{p} = 1 \pmod{d}$.

We know that the residue field extension of $K(E[d])$ at \mathfrak{p} is $\mathbf{F}_{\mathfrak{p}}(E_{\mathfrak{p}}[d])$. If \mathfrak{p} is totally split, this extension is trivial, so all the d -torsion is rational, i.e. $d \mid d_1(E_{\mathfrak{p}})$.

Conversely, if $d \mid d_1(E_{\mathfrak{p}})$, the condition $(d, \mathfrak{p}) = 1$ implies that \mathfrak{p} is unramified in $K(E[d])$ ([Si-1, 4.1]). Then the residue field extension being trivial means that \mathfrak{p} is totally split. \square

3. TOTALLY SPLIT PRIMES

3.1. The splitting problem for elliptic curves. Let E/K be an elliptic curve over a number field. Apart from the number of points $N\mathfrak{p} + 1 - a_{\mathfrak{p}}(E)$ on E modulo a prime ideal, one of the most natural invariant to insert in a sum (1.2) is $\iota(\mathfrak{p}) = d_1(\mathfrak{p})$. Thus we define for $X \geq 1$

$$(3.1) \quad S_E(X; d_1) = \sum_{N\mathfrak{p} \leq X} d_1(\mathfrak{p})$$

where as before $d_1(\mathfrak{p}) = d_1(E_{\mathfrak{p}})$ (we define, rather arbitrarily, $d_1(\mathfrak{p}) = 0$ for ramified primes).

Problem 3.1. *What is the asymptotic behavior of $S_E(X; d_1)$ as $X \rightarrow +\infty$?*

Because of the following link with primes totally split in division fields of E , we call this the *elliptic splitting problem* for E .

Lemma 3.2. *Let E/K be an elliptic curve over a number field. We have*

$$(3.2) \quad S_E(X; d_1) = \sum_{d \leq \sqrt{X+1}} \varphi(d) \pi_E(X; d, 1)$$

for $X \geq 1$, where

$$(3.3) \quad \pi_E(X; d, 1) = |\{\mathfrak{p} \mid N\mathfrak{p} \leq X, \text{ and } \mathfrak{p} \text{ is totally split in } K(E[d])\}|.$$

Proof. Using the convolution formula

$$n = \sum_{ab=n} \varphi(a)$$

and (2.13), we have

$$\begin{aligned} S_E(X; d_1) &= \sum_{N\mathfrak{p} \leq X} d_1(\mathfrak{p}) = \sum_{N\mathfrak{p} \leq X} \sum_{d \mid d_1(\mathfrak{p})} \varphi(d) = \sum_{d \leq \sqrt{X+1}} \varphi(d) \sum_{\substack{N\mathfrak{p} \leq X \\ d \mid d_1(\mathfrak{p})}} 1 \\ &= \sum_{d \leq \sqrt{X+1}} \varphi(d) \pi_E(X; d, 1), \quad \text{by Lemma 2.7.} \end{aligned}$$

\square

Remark 3.3. This lemma shows that the elliptic splitting problem is quite analogous to the classical *Titchmarsh divisor problem* (first considered in [Ti-1]) which concerns the asymptotic behavior of the sum

$$S(X, d) = \sum_{p \leq X} d(p-1)$$

where $d(n)$ is the number of (> 0) divisors of n . This was solved by Linnik³ (see [Li]):

Theorem 3.4. (*Linnik*) *We have*

$$(3.4) \quad S(X, d) \sim cx \quad \text{with } c = \prod_p \left(1 + \frac{1}{p(p-1)}\right) = \frac{\zeta(2)\zeta(3)}{\zeta(6)} = 1.943596\dots$$

as $X \rightarrow +\infty$.

Linnik proved this by a very difficult argument using the dispersion method, although now it is easy to derive from the Bombieri-Vinogradov theorem and the Brun-Titchmarsh theorem (see e.g. [HR, §3.5]; we will essentially redo this argument later on). Although this will not matter here, we mention that Bombieri, Friedlander, Iwaniec [BFI] and independently Fouvry [Fou], have proved a more precise formula, with a second term of magnitude $X/\log X$, using their deep results about primes in arithmetic progressions to moduli $d > \sqrt{X}$.

The first step in this proof is to write

$$(3.5) \quad \begin{aligned} d(n) &= \sum_{ab=n} 1 \\ &= 2 \sum_{\substack{d|n \\ d < \sqrt{n}}} 1 + \begin{cases} 1 & \text{if } n \text{ is a square,} \\ 0 & \text{otherwise} \end{cases} \quad (\text{Dirichlet's divisor-switching trick}) \end{aligned}$$

which leads immediately to

$$(3.6) \quad S(X, d) = \sum_{d \leq X} \pi(X; d, 1) = 2 \sum_{d < \sqrt{X}} (\pi(X; d, 1) - \pi(d^2 + 1; d, 1)) + \underline{O}\left(\frac{\sqrt{X}}{\log X}\right) + \underline{O}(1),$$

where for any integer a , $\pi(X; d, a)$ is the classical counting function for primes $p \equiv a \pmod{d}$. By the elementary theory of cyclotomic fields, this is also the number of primes $p \leq X$ such that the Frobenius at p acts on d -th roots of unity by $\zeta \mapsto \zeta^a$, so that $\pi(X; d, 1)$ is the number of $p \leq X$ totally split in the cyclotomic field generated by d -th roots of unity.

Theorem 3.4, via the formula (3.6), will actually be used in Section 6, reinforcing the connection between this classical result and Problem 3.1. We may also remark that another connection arises if one interprets $d(p-1)$ as the number of subgroups of the cyclic group $(\mathbf{Z}/p\mathbf{Z})^\times$. Indeed, the number of subgroups of the finite abelian group $E_p(\mathbf{F}_p)$ with

$$E_p(\mathbf{F}_p) \simeq \mathbf{Z}/d_1\mathbf{Z} \oplus \mathbf{Z}/d_1d_2\mathbf{Z}$$

is “essentially” dominated by d_1 (see Birkhoff’s description of the subgroups of a finite abelian group, [Bi, Th. 8.1], or [C-2, 4.1.10]), so $S_E(X; d_1)$ is closely related to the sum

$$\sum_{N\mathfrak{p} \leq X} T(\mathfrak{p})$$

where $T(\mathfrak{p})$ is the number of subgroups of $E_p(\mathbf{F}_p)$. The analogy between $S(X, d)$ and $S_E(X; d_1)$ seems however deeper using the Galois-theoretic interpretation.

More generally, for $\mathcal{C} \subset GL(2, \mathbf{Z}/d\mathbf{Z})$ a set of conjugacy classes, we will let

$$(3.7) \quad \pi_E(X; d, \mathcal{C}) = |\{\mathfrak{p} \mid N\mathfrak{p} \leq X, \text{ and } \sigma_{\mathfrak{p}} \pmod{d} \in \mathcal{C}\}|.$$

³Titchmarsh had shown the result on the Riemann Hypothesis (see also below).

It is also convenient in many situations to weigh primes by $\log p$, so we define also⁴

$$(3.8) \quad \theta_E(X; d, \mathcal{C}) = \sum_{\substack{N\mathfrak{p} \leq X \\ \sigma_{\mathfrak{p}} \in \mathcal{C}}} \log N\mathfrak{p}.$$

Since we deal with all fields $K(E[d])$ at the same time, we use the shorthand notation $\sigma_{\mathfrak{p}} \pmod{d}$ to denote a Frobenius element at \mathfrak{p} for the field $K(E[d])$, so $\sigma_{\mathfrak{p}} \in G_d$; by convention, writing this implies also that \mathfrak{p} is unramified in $K(E[d])$. This notation is compatible, in the case of the cyclotomic fields $\mathbf{Q}(\mu_d)$, with the usual meaning of congruences and the isomorphism $\text{Gal}(\mathbf{Q}(\mu_d)/\mathbf{Q}) \rightarrow (\mathbf{Z}/d\mathbf{Z})^\times$ which sends σ_p to $p \pmod{d}$.

We see that (3.6) and (3.2) are comparable in that both involve the average distribution of Frobenius elements in the extensions generated by d -torsion points of some algebraic group (either E or the multiplicative group), uniformly for d quite large. However, there are a number of important qualitative differences, as will be explained later on. Here we only mention that the factor $\varphi(d)$ in (3.2) makes it impossible to switch divisors there as in (3.5), making the contribution of the very large moduli very hard to handle.

The estimation of (3.2) seems to be a much harder problem than the Titchmarsh divisor problem.

Remark 3.5. I have not seen any mention of the problem of estimating $S_E(X; d_1)$ in the literature; however, there are a number of related works concerning the question of counting primes $p \leq X$ such that $E_p(\mathbf{F}_p)$ is cyclic (i.e. $d_1(E_p) = 1$) for an elliptic curve E/\mathbf{Q} (e.g. Serre studied this on GRH, R. Murty [Mu] proved the asymptotic formula for CM curves, R. Gupta and R. Murty [GM] proved $d_1(E_p) = 1$ infinitely often in all cases). Also Serre [Se-2], for counting supersingular primes $p \leq X$, uses the fields of ℓ -torsion with ℓ prime and quite large with respect to X ; however ℓ is fixed for a given X , so the question of uniformity with respect to the modulus occurs in somewhat attenuated form.

More recently, since the first version of this paper was written, there have been quite interesting work by Cojocaru [Co], Cojocaru and Duke [CD] and Cojocaru and Murty [CM] on similar topics.

3.2. Analysis of the elliptic splitting problem on GRH. For *fixed* $d \geq 1$, the asymptotic behavior of $\pi_E(X; d, 1)$ is given by the Chebotarev Density Theorem. Under GRH, it can be stated in a sharp form. First we introduce some notation. As before, E/K is an elliptic curve over a number field, $d \geq 1$ an integer, G_d is the Galois group of $K(E[d])$ over K . Let Δ_d be the absolute value of the discriminant of $K(E[d])/\mathbf{Q}$, n_1 the degree $[K : \mathbf{Q}]$, so $[K(E[d]) : \mathbf{Q}] = |G_d|n_1$. We let N_E be the norm of the conductor of E/K ([Si-2, IV-10]).

Proposition 3.6. *Assume GRH for the Artin L -functions. With the above notation, we have*

$$(3.9) \quad \pi_E(X; d, 1) = \frac{1}{|G_d|} \text{li}(X) + \underline{O}(\sqrt{X} \log(\Delta_1(d|G_d|N_EX)^{n_1}))$$

for $X \geq 2$, with an absolute implied constant, and

$$(3.10) \quad \theta_E(X; d, 1) = \frac{X}{|G_d|} + \underline{O}(\sqrt{X}(\log X)(\log(\Delta_1(d|G_d|N_EX)^{n_1}))).$$

for $X \geq 2$, with an absolute implied constant.

Proof. This is just making explicit the version given by Serre [Se-2], based on that of Lagarias–Odlyzko, and is well-known: we include the proof for completeness. Théorème 4 of [Se-2] reads in this case

$$\pi_E(X; C, 1) = \frac{1}{|G_d|} \text{li}(X) + r_E(X; d)$$

⁴It would be better to consider here the partial sum of coefficients of the logarithmic derivative of the Artin L -function associated to the character of G_d which has trace equal to the characteristic function of \mathcal{C} .

with the estimate

$$(3.11) \quad r_E(X; d) \ll \frac{1}{|G_d|} \sqrt{X} (\log(\Delta_d) + n_1 |G_d| \log X),$$

with an absolute implied constant. We have (see e.g. [Se-3, III])

$$\log \Delta_d = |G_d| \log \Delta_1 + \log N \mathfrak{d}_d$$

where \mathfrak{d}_d is the relative discriminant of $K(E[d])/K$. Then Proposition 5 of [Se-2] gives an upper bound

$$\log \Delta_d \leq |G_d| \log \Delta_1 + n_1 |G_d| \left(1 - \frac{1}{|G_d|}\right) \log P_d + n_1 |G_d| \log |G_d|,$$

where P_d is the product of the primes p which are residue characteristics of primes of K ramified in $K(E[d])$. If \mathfrak{p} is a prime of good reduction of E and $(d, \mathfrak{p}) = 1$, \mathfrak{p} is unramified in $K(E[d])$. It follows easily that

$$P_d \mid dN_E.$$

Thus we get

$$\frac{\log \Delta_d}{|G_d|} \leq \log \Delta_1 + n_1 \log dN_E + n_1 \log |G_d|.$$

The first term in (3.11) is thus

$$\frac{1}{|G_d|} \sqrt{X} \log(\Delta_d) \leq \sqrt{X} \log(\Delta_1 (d|G_d|N_E)^{n_1}),$$

so that we obtain

$$r_E(X; d) \ll \sqrt{X} \log(\Delta_1 (d|G_d|N_E X)^{n_1})$$

with an absolute implied constant.

The proof for θ_E is similar or deduced by partial summation. □

Remark 3.7. If $K = \mathbf{Q}$, this can be written

$$(3.12) \quad \pi_E(X; d, 1) = \frac{1}{|G_d|} \text{li}(X) + \underline{O}(\sqrt{X} \log(dN_E X)),$$

(with an absolute implied constant) by observing that $|G_d| \leq d^4$ (for example), and one can replace N_E by the absolute value of the discriminant of E , which it divides.

For comparison, it is classical that GRH for Dirichlet L -functions implies

$$(3.13) \quad \pi(X; d, a) = \frac{1}{\varphi(d)} \text{li}(X) + \underline{O}(\sqrt{X} \log(dX))$$

with an absolute implied constant.

Recall from Theorem 2.1 and the remark following, that as $d \rightarrow +\infty$ the order of G_d is comparable with d^g where $g = 2$ if E has CM and with $g = 4$ if not. Comparing the error term in (3.9) with $|G_d|$, it follows that (3.9) gives the asymptotic behavior

$$\pi_E(X; d, 1) \sim \frac{1}{|G_d|} \text{li}(X) \quad \text{as } X \rightarrow +\infty$$

uniformly for d up to $X^{1/(2g)-\varepsilon}$ for any $\varepsilon > 0$, whereas (3.13) implies the corresponding asymptotic for primes in arithmetic progression to moduli $d \leq X^{1/2-\varepsilon}$. Hence, since $1/(2g) = 1/4$ (in the CM case) or $= 1/8$ (otherwise), we see a great difference for the purpose of applying the estimates (3.9) or (3.13) to the sums (3.2) and (3.6). In the case of the Titchmarsh divisor problem, GRH provides an asymptotic formula valid for “almost all” the moduli d involved in (3.6), leaving only those d very close to $X^{1/2}$ to be dealt with; but for an elliptic curve, a whole range of d remains for which GRH does not give anything, namely

$$\begin{cases} X^{1/4-\varepsilon} \leq d \leq X^{1/2} + 1 & \text{if } E \text{ has CM} \\ X^{1/8-\varepsilon} \leq d \leq X^{1/2} + 1 & \text{if } E \text{ does not have CM.} \end{cases}$$

(it is certainly not surprising that the non-CM case appears superficially to be worse than the other, although whether it should really be is open to question...)

However, we can at least state what this gives for (3.2).

Proposition 3.8. *Let E/K be an elliptic curve over a number field. Assume GRH for Artin L -functions. Then we have*

$$(3.14) \quad \sum_{d \leq \frac{X^{1/4}}{\log X}} \varphi(d) \pi_E(X; d, 1) = c(E)X + O\left(\frac{X}{(\log X)^2} \log(\Delta_1 N_E^{n_1} X^{3n_1+1})\right) \quad \text{if } E \text{ has CM,}$$

$$(3.15) \quad \sum_{d \leq \frac{X^{1/4}}{(\log X)^2}} \varphi(d) \pi_E(X; d, 1) = c(E) \operatorname{li}(X) + O\left(\frac{X}{(\log X)^4} \log(\Delta_1 N_E^{n_1} X^{5n_1+1})\right) \quad \text{otherwise}$$

for $X \geq 2$, with absolute implied constants, where

$$(3.16) \quad c(E) = \operatorname{Res}_{s=0} \sum_{d \geq 1} \frac{\varphi(d)}{|G_d|} d^{-s} \quad \text{if } E \text{ has CM}$$

$$(3.17) \quad c(E) = \sum_{d \geq 1} \frac{\varphi(d)}{|G_d|} \quad \text{otherwise.}$$

Unconditionally, we have a lower bound

$$(3.18) \quad S_E(X; d_1) \gg_K \frac{X}{\log X}, \quad \text{and } S_E(X; d_1) \gg_K \frac{X \log \log X}{\log X} \quad \text{in the CM case.}$$

where the implied constant depends only on K .

Proof. This is an immediate corollary of Proposition 3.6. Take the non-CM case for example: we have

$$\frac{\varphi(d)}{|G_d|} \leq \frac{1}{d^2 \varphi(d)}$$

so the series defining $c(E)$ is absolutely convergent, and the main term of (3.9) gives

$$\operatorname{li}(X) \sum_{d \leq X^{1/4}/(\log X)} \frac{\varphi(d)}{|G_d|} = c(E) \operatorname{li}(X) + O_\varepsilon(X^{1/2+\varepsilon})$$

(for any $\varepsilon > 0$, say we take $\varepsilon = 1/4$), while for the error term we have

$$\sqrt{X} \sum_{d \leq X^{1/4}/(\log X)^2} \varphi(d) \log(\Delta_1 (d|G_d|N_E X)^{n_1}) \ll \frac{X}{(\log X)^4} \log(\Delta_1 N_E^{n_1} X^{5n_1+1})$$

by trivial summations (using $|G_d| \leq d^4$). The CM case is exactly similar, except that the series over d has logarithmic growth, hence the different formula for $c(E)$.

The first lower bound (3.18) is an immediate consequence of the Prime Ideal Theorem in K since by (3.2)

$$S_E(X; d_1) \geq \pi_E(X; 1, 1) = \pi_K(X) \gg_K \frac{X}{\log X}$$

where $\pi_K(X)$ is the number of prime ideals with norm $\leq X$; the second lower bound is explained in Remark 5.34. \square

Remark 3.9. Note that the restriction to $d \leq X^{1/4}$ comes from the occurrence of $\varphi(d)$ in (3.2). The exponent is thus independent of the Galois dimension of E , and so of the actual range where (3.9) gives an asymptotic formula for $\pi_E(X; d, 1)$. In other words, in the non-CM case, in part of the summation range in (3.15), the estimated term in the Chebotarev density theorem dominates over the main term.

Note that the constant c in (3.4) is also

$$c = \operatorname{Res}_{s=0} \sum_{d \geq 1} \frac{1}{\varphi(d)d^s}.$$

and the same argument gives

$$\sum_{d \leq \sqrt{X}/(\log X)} \pi(X; d, 1) \sim cX \quad \text{as } X \rightarrow +\infty,$$

leaving only the range $\sqrt{X}/(\log X) \leq d \leq \sqrt{X}$ to handle to solve (under GRH) the Titchmarsh divisor problem.

It is reasonable to expect that the sum in Proposition 3.8 could be extended to all $d \leq \sqrt{X}+1$, giving the desired asymptotic formula for the average of $d_1(\mathfrak{p})$ over \mathfrak{p} .

3.3. Computation of $c(E)$. In Section 7 below we perform numerical experiments for the elliptic splitting problem, and it is therefore useful to be able to explicitly evaluate the constant $c(E)$, at least for some elliptic curves E . This requires some knowledge of the Galois groups G_d , which is available in the case of what Lang-Trotter call *Serre curves* ([LT, I, §5-6-7]). Serre [Se-1, §5] has indeed given concrete examples of such curves, and we will use his examples in Section 7. Throughout this section, all curves are over \mathbf{Q} .

The difficulty in computing $|G_d|$, and hence $c(E)$, is that although the index between them is bounded, it is never the case that $G_d = GL(2, \mathbf{Z}/d\mathbf{Z})$ for all $d \geq 1$, as shown by Serre. More precisely, let $E[\infty]$ be the set of all torsion points of E , and

$$\rho_\infty : G_{\mathbf{Q}} \longrightarrow \operatorname{Aut}(E[\infty])$$

the natural Galois representation, so that $\rho_\infty(\bmod d) = \rho_d$ for all $d \geq 1$. Recall that

$$\operatorname{Aut}(E[\infty]) = \prod_{\ell} GL(2, \mathbf{Z}_\ell)$$

and the ℓ -th component of ρ_∞ is the ℓ -adic representation $\hat{\rho}_\ell$.

Define an index 2 subgroup H_E of $\operatorname{Aut}(E[\infty])$ as follows: let $\varepsilon : GL(2, \mathbf{Z}_2) \rightarrow \{\pm 1\}$ be the map given by composition

$$GL(2, \mathbf{Z}_2) \rightarrow GL(2, \mathbf{Z}/2\mathbf{Z}) \simeq \mathfrak{S}_3 \xrightarrow{\varepsilon} \{\pm 1\}$$

where ε is the signature on \mathfrak{S}_3 . Let χ be the Kronecker symbol of the quadratic extension $\mathbf{Q}(\sqrt{\Delta})$, where Δ is the discriminant of E , and m its conductor. The subgroup in question is defined by

$$H_E = \{g = (g_\ell) \in \operatorname{Aut}(E[\infty]) \mid \varepsilon(g_2) = \chi(g \bmod m)\}$$

Then the precise form of Serre's result ([Se-1, Prop. 22]) is:

Proposition 3.10. (*Serre*) *For any elliptic curve E/\mathbf{Q} we have $\rho_\infty(G_{\mathbf{Q}}) \subset H_E$.*

By definition, a *Serre curve* is an elliptic curve E/\mathbf{Q} such that $\rho_\infty(G_{\mathbf{Q}}) = H_E$ (see [LT, I, §5] for a more detailed discussion, Section 7 for concrete examples).

Proposition 3.11. *Let E/\mathbf{Q} be a Serre curve, and let m be as above. We have*

$$[GL(2, \mathbf{Z}/d\mathbf{Z}) : G_d] = \begin{cases} 2 & \text{if } 2m \mid d \\ 1 & \text{otherwise.} \end{cases}$$

Proof. Clearly we have

$$H_E = H_{2m} \times \prod_{(\ell, m)=1} GL(2, \mathbf{Z}_\ell),$$

where H_{2m} is the obvious subgroup (the definition of H_E only involves the components of g at $\ell \mid 2m$). Let $g = (g_\ell)$ be a representative of the non-trivial coset of H_{2m} . Correspondingly, if $d = d_1 d_2$ with $d_1 \mid (2m)^\infty$ and $(d_2, 2m) = 1$, we have

$$G_d = G_{d_1} \times GL(2, \mathbf{Z}/d_2\mathbf{Z}).$$

So it is enough to compute the index of G_{d_1} . Since H_E is of index 2 in $\text{Aut}(E[\infty])$, it is either 1 or 2. Now if $2m \mid d_1$, the reduction modulo d of g is an element in G_{d_1} which is not in $H_{2m} \pmod{d_1}$, so the index is 2 in this case.

Conversely, if $2m$ does not divide d_1 , let ℓ be a prime dividing $2m$ but not d_1 . For any $g \in GL(2, \mathbf{Z}/d_1\mathbf{Z})$, we can lift it to

$$\prod_{\ell' \mid d_1} GL(2, \mathbf{Z}_{\ell'})$$

and then change the component at ℓ so that the resulting \hat{g} is in H_{2m} ; this element reduces to g modulo d_1 , so the index of G_{d_1} is 1 in this case. \square

Lemma 3.12. *Let f and g be arithmetic functions with g multiplicative such that*

$$f(d) = \begin{cases} \alpha g(d) & \text{if } n \mid d \\ g(d) & \text{otherwise} \end{cases}$$

for some integer $n \geq 1$ and some $\alpha \in \mathbf{R}$. Assume moreover that

$$(3.19) \quad g(nd) = d^{-\kappa} g(n)$$

for all $d \mid n^\infty$ and some real number κ . Assume that the series $\sum g(d)$ converges absolutely. Then we have

$$\sum_{d \geq 1} f(d) = c \prod_p g_p$$

where

$$g_p = \sum_{k \geq 0} g(p^k),$$

and

$$c = 1 + (\alpha - 1)g(n) \prod_{p \mid n} g_p^{-1} (1 - p^{-\kappa})^{-1}.$$

Proof. We compute, from the assumption:

$$\begin{aligned} \sum_{d \geq 1} f(d) &= \alpha \sum_{n \mid d} g(d) + \sum_{n \nmid d} g(d) \\ &= \alpha \sum_{n \mid d} g(d) + \sum_{d \geq 1} g(d) - \sum_{n \mid d} g(d) \\ &= \sum_{g \geq 1} g(d) + (\alpha - 1) \sum_{n \mid d} g(d). \end{aligned}$$

By multiplicativity we have

$$\sum_{d \geq 1} g(d) = \prod_p g_p.$$

Factorizing uniquely $d = d_1 d_2$ with $d_1 \mid n^\infty$ and $(d_2, n) = 1$, we have further

$$\begin{aligned}
\sum_{n|d} g(d) &= \sum_{d \geq 1} g(nd) \\
&= \sum_{\substack{d_1 \mid n^\infty \\ (d_2, n) = 1}} g(nd_1 d_2) \\
&= \left(\sum_{(d_2, n) = 1} g(d_2) \right) \left(\sum_{d_1 \mid n^\infty} g(nd_1) \right) \\
&= g(n) \left(\prod_{(p, n) = 1} g_p \right) \left(\sum_{d_1 \mid n^\infty} d_1^{-\kappa} \right) \text{ (by multiplicativity and (3.19))} \\
&= g(n) \prod_{p|n} (1 - p^{-\kappa})^{-1} \prod_{(p, n) = 1} g_p,
\end{aligned}$$

whence the result follows. \square

Corollary 3.13. *Let E/\mathbf{Q} be a Serre curve. We have*

$$c(E) = \sum_{d \geq 1} \frac{\varphi(d)}{|G_d|} = c'(E) \zeta(2) \zeta(3) \prod_p (1 - p^{-2} + p^{-5})$$

with

$$c'(E) = 1 + \frac{1}{(2m)^3} \prod_{p|2m} (1 - p^{-2} + p^{-5})^{-1}.$$

Proof. In view of Proposition 3.11, we can apply Lemma 3.12 with $n = 2m$, $\alpha = 2$ and

$$\begin{aligned}
f(d) &= \frac{\varphi(d)}{|G_d|} \\
g(d) &= \frac{\varphi(d)}{|GL(2, \mathbf{Z}/d\mathbf{Z})|}.
\end{aligned}$$

Indeed (3.19) holds with $\kappa = 3$ since more generally we have by (2.9), (2.10)

$$g(dd_1) = (dd_1)^{-3} \prod_{p|dd_1} p^{-1} (1 - p^{-2})^{-1} = d_1^{-3} g(d)$$

if d_1 has no prime divisor outside d (this formula explains where functions satisfying (3.19) arise naturally).

We have by (2.9)

$$\begin{aligned}
g_p &= 1 + \sum_{k \geq 1} \frac{1}{p^{3k} (1 - p^{-1}) (1 + p^{-1})} \\
&= 1 + \frac{1}{p^3 (1 - p^{-2}) (1 - p^{-3})} \\
&= \frac{p^5 - p^3 + 1}{(p^2 - 1)(p^3 - 1)},
\end{aligned}$$

hence the result after some rearranging of terms. \square

Remark 3.14. Note that the correction factor $c'(E)$ is usually very close to 1, so the value of $c(E)$ for a Serre curve is close to

$$(3.20) \quad c_0 = \zeta(2) \zeta(3) \prod_p (1 - p^{-2} + p^{-5}) = 1.25845 \dots$$

This means in particular that if the expected asymptotic formula for $S_E(X; d_1)$ holds, by itself it does not carry much *global* information about E , except for distinguishing between CM curves and non-CM curves.

Remark 3.15. One may hope that this gives the “generic” value of $c(E)$. More precisely, recall that Duke [Du] has shown that for “almost all” elliptic curves over \mathbf{Q} (in the sense of almost all coefficients of Weierstrass equations), there are no “exceptional primes”, i.e. we have

$$G_p = GL(2, \mathbf{Z}/p\mathbf{Z})$$

for all primes p . It may be possible to refine this statement to show that almost all E/\mathbf{Q} (in the same sense) are Serre curves.

3.4. Outside primes. The simple-minded analysis based on GRH of the previous section points to a striking difference between the distribution of totally split primes in $K(E[d])$ for large modulus d and the case of arithmetic progressions. This is best made explicit using

$$\psi(X; d, 1) = \sum_{\substack{n \leq X \\ n \equiv a \pmod{d}}} \Lambda(n)$$

where $\Lambda(n)$ is the von Mangoldt function, equal to $\log p$ if $n = p^m$ for some prime p and $m \geq 1$, and to 0 otherwise. As for θ_E , we have on GRH

$$(3.21) \quad \psi(X; d, a) = \frac{X}{\varphi(d)} + O(\sqrt{X}(\log X)(\log dX))$$

for $X \geq 2$.

Now, consider the smallest prime $\equiv a$ modulo d , or the smallest X for which $\psi(X; d, a) > 0$. Since $p \equiv a \pmod{d}$ implies $d \leq p - a$, it follows that $p \geq d + a > d$, in particular the main term of (3.21) is > 1 , i.e. we have

$$\psi(X; d, 1) > 0 \Rightarrow X > d \Rightarrow \frac{X}{\varphi(d)} > 1.$$

We restate this as follows: all primes in arithmetic progression can be “accounted for” by the main term in the Chebotarev density theorem. Such is still the case of CM elliptic curves, since the *a priori* estimate (2.13) shows that

$$(3.22) \quad \theta_E(X; d, 1) > 0 \Rightarrow X \geq (d - 1)^2$$

which is (roughly) compatible with the density $1/|G_d| \geq 1/d^2$ in this case.

Non CM curves are different: the estimate (2.13) is the best general bound (as shown below), but now the density of totally split primes is roughly $1/d^g = 1/d^4$. If \mathfrak{p} splits in $K(E[d])$ with $N\mathfrak{p} < |G_d|$, the main term in the Chebotarev density theorem is < 1 , and this may be the case for values of d as large as $\sqrt{N\mathfrak{p}} + 1$. Such a prime is *not* accounted for by the main term of the Chebotarev density theorem.

Definition. Let E/K be a non-CM elliptic curve over a number field K . A prime ideal \mathfrak{p} which splits totally in $K(E[d])$ with $N\mathfrak{p} < |G_d|$ is called an outside prime of E . If \mathfrak{p} satisfies the weaker inequality $N\mathfrak{p} < d^4$, it is called a weak outside prime.

Equivalent formulations are $|G_{d_1(\mathfrak{p})}| > N\mathfrak{p}$ and $d_1(\mathfrak{p}) > (N\mathfrak{p})^{1/4}$ respectively.

The existence of outside primes is understandable: since the invariant $d_1(\mathfrak{p})$ only depends on the reduction of E modulo \mathfrak{p} , it follows that for given \mathfrak{p} , E being globally CM or not does not matter. The results on the possible group structures of elliptic curves over finite fields (see Section 6) show that the a priori bound (2.13) is always best possible.

We give here a simple illustrative example.

Example 3.16. Let A/\mathbf{Q} be the classical CM curve given by the Weierstrass equation

$$(3.23) \quad y^2 = x^3 - x$$

which has $j(A) = 1728$, conductor $N_A = 32$ and endomorphism ring $\text{End}_{\mathbf{Q}}(A) = \mathbf{Z}[i]$, the ring of Gaussian integers.

The determination of the local Frobenius endomorphism of A modulo p , up to conjugation, is classical (see e.g. [IR, 18.4]).

If $p \equiv 3 \pmod{4}$, A is supersingular at p and $a_p(A) = 0$. If $p \equiv 1 \pmod{4}$, on the other hand, p splits in $\mathbf{Q}(i)$, say $p = \pi\bar{\pi}$ for some prime element π , and the Frobenius at p is one of the elements $\pm\pi$, $\pm i\pi$, $\pm\bar{\pi}$, $\pm i\bar{\pi}$. Which one it is, up to conjugation, is settled by a congruence modulo $2(1+i)$, namely

$$(3.24) \quad \sigma_p \equiv 1 \pmod{2(1+i)}$$

(a Gaussian integer $z \equiv 1 \pmod{2(1+i)}$ is called primary). To see this, one can either express a_p in terms of Jacobsthal sums and reduce modulo $2(1+i)$ (see e.g. [I2, 8.2]) or observe that the $2(1+i)$ -torsion of A is rational over $\mathbf{Q}(i)$, hence over \mathbf{F}_p for p split in $\mathbf{Q}(i)$, so that (3.24) follows ($A[2(1+i)]$ is generated by the two-torsion points $(0,0)$, $(\pm 1,0)$ and by $(i, \pm(i-1))$; see e.g. [Ru, Ex. 12.3]).

Now if π is a Gaussian prime of the form $\pi = 1 + ni$ such that $\pi \equiv 1 \pmod{2(1+i)}$, then $p = n^2 + 1$ is prime and π is the Frobenius at p . But tautologically we have $\pi \equiv 1 \pmod{n}$ in $\text{End}(A_p)$, so that (Lemma 2.6) $d_1(A_p) = n$, and in fact, since $N(\pi-1) = n^2$, $A_p(\mathbf{F}_p) \simeq (\mathbf{Z}/n\mathbf{Z})^2$ (compare [Sc-1, 2.5]). Obviously $n = \lfloor \sqrt{p} + 1 \rfloor$.

In terms of p the condition is that $p = n^2 + 1$ and $4 \mid n$ (i.e. $p = 16n^2 + 1$). It is expected that there exist infinitely many primes p of this form, but this is not known (see [I1] for the best “almost prime” results). The first few are $p = 17, 257, 401, 577, \dots, 739601, \dots$

Now if p is a prime of this type, any curve E'/\mathbf{Q} with the same reduction modulo p as E will also have $d_1(E') = n$. For instance, take

$$E' : y^2 = x^3 - x - p$$

which for all p does not have CM and for $p = 16n^2 + 1$ will have $d_1(E'_p) = \lfloor \sqrt{p} + 1 \rfloor$ by construction.

Obviously, for the purpose of finding an asymptotic evaluation of (3.1), a few prime ideals with $d_1(\mathfrak{p})$ close to $\sqrt{N\mathfrak{p}}$ do not matter much. One might expect that, in general, outside primes are rare, and the presence of “too many” of them should mean that E has CM.

A partial clue in this direction is implicit in [Sc-1, p. 330]. We state the following simple result as an illustration: it shows that Example 3.16 is basically the only possibility in the most extreme case.

Proposition 3.17. *Let E/\mathbf{Q} be an elliptic curve with j -invariant j , $p \geq 11$ a prime of good reduction of E such that*

$$d_1(p) \geq \sqrt{\frac{p}{2}}.$$

Then $j \equiv j_0 \pmod{p}$, where

$$j_0 \in \mathcal{J} = \{0, 1728, -3375, 8000, -32768, 54000\}.$$

In particular, there are only finitely many such p unless $j \in \mathcal{J}$. In this case E is a CM curve.

Proof. First observe that the reduced curve E_p/\mathbf{F}_p is ordinary. Let $\pi \in \mathcal{O} = \text{End}_{\mathbf{F}_p}(E_p)$ be the Frobenius endomorphism. We have (Lemma 2.6) $\pi = 1 + d_1(E_p)\pi'$ for some $\pi' \in \mathcal{O}$, and

$$|E_p(\mathbf{F}_p)| = N(\pi - 1) = d_1(E_p)^2 N\pi'.$$

Moreover, since $\pi \notin \mathbf{Z}$, π' is not in \mathbf{Z} either. Let D be the discriminant of the quadratic imaginary order \mathcal{O} . For any $z \in \mathcal{O}$, $z \notin \mathbf{Z}$, we have

$$Nz \geq \frac{|D|}{4},$$

and applying this to π' we get

$$\begin{aligned} |D| &\leq 4 \frac{|E_p(\mathbf{F}_p)|}{d_1(E_p)^2} \\ &\leq 8 \frac{|E_p(\mathbf{F}_p)|}{p} \quad (\text{by assumption}) \\ &\leq 8 \left(1 + \frac{1}{\sqrt{p}}\right) < 15 \quad (\text{since } p \geq 11). \end{aligned}$$

But all quadratic imaginary orders of discriminant < 15 have class number one (see e.g. [Cox, Th. 7.30]). Now Deuring [De] has shown that an ordinary elliptic curve A over a finite field \mathbf{F}_q “lifts to characteristic 0”. This means that there exists a number field K , a prime ideal \mathfrak{p} of K with $\mathbf{F}_{\mathfrak{p}} = \mathbf{F}_q$, and an elliptic curve \tilde{A}/K with CM by $\text{End}(A)$ such that $\tilde{A}_{\mathfrak{p}} \simeq A$.

Let \tilde{E} be such a lift of E_p . It has CM by the order \mathcal{O} with class number one, hence (see e.g. [Si-2, II-2]) is defined over \mathbf{Q} , and actually a table such as that in [Cox, 12-C] or [Si-2, App. A-3], shows that $j(\tilde{E}) \in \mathcal{J} = \{0, 1728, -3375, 8000, -32768, 54000\}$. Since $\tilde{E}_{\mathfrak{p}} \simeq E_p$, we have $j \equiv j(\tilde{E}) \pmod{p}$. \square

Obviously this argument can be extended somewhat, but it seems hard to make interesting conclusions in greater generality. The difficulty is roughly as follows: say we want to estimate the number of \mathfrak{p} with $d_1(\mathfrak{p}) \geq N\mathfrak{p}^{\theta}$ for some $\theta > 0$ (for example, $\theta = 1/4$, corresponding essentially to outside primes). As above one derives

$$|D| \leq 8p^{1-2\theta}$$

where D is the discriminant of the quadratic order $\text{End}(\mathbf{F}_{\mathfrak{p}})$. This implies

$$j(E) \pmod{\mathfrak{p}} \in \Omega(\mathfrak{p})$$

for some finite set $\Omega(\mathfrak{p})$ with

$$|\Omega(\mathfrak{p})| \ll p^{1-2\theta}$$

for all such \mathfrak{p} . However since the cardinality of $\Omega(\mathfrak{p})$ is not bounded anymore, it is hard to go further.

Indeed, compare this to the analogous approach to the study of supersingular primes of E : if \mathfrak{p} is a prime of supersingular reduction, we have $j(E) \pmod{\mathfrak{p}} \in \Omega'(\mathfrak{p})$, where $\Omega'(\mathfrak{p})$ is the finite set of supersingular j -invariants. Lang and Trotter, who initiated the study of the set of supersingular primes of elliptic curves, explicitly mention this idea and state [LT, p. 7] that it doesn't seem to bring useful results.

We thus have the following problem:

Problem 3.18. *Let E/K be an elliptic curve without CM. What can one say about the distribution of outside primes of E ? Are there infinitely many of them? If yes, how many are there $\leq X$? Is it true that the series*

$$\sum_{\mathfrak{p}} \frac{1}{N\mathfrak{p}}$$

over outside primes of E converges?

The first guess, for E/\mathbf{Q} , might be that there are infinitely many outside primes. Heuristically from Proposition 6.43, one would expect that there are at most about $X^{1/4}$ outside primes $\leq X$. See Section 7 for some numerical data (showing that outside primes appear to be extremely scarce), and Section 4 below for a first idea.

Beyond the simple comparison with the main term of the Chebotarev density theorem, it may be worth recalling that GRH only implies that for a Galois extension L/K of number fields, with $[L : K] = m$, the smallest prime ideal \mathfrak{p} of K that is totally split in L satisfies

$$N\mathfrak{p} \ll (\log |D_{L/K}|)^2 \ll m^2(\log m)^2,$$

where the implied constants are absolute (see e.g. [Se-2, Th. 5]). For $K(E[d])/K$ this means GRH gives an upper bound of size roughly d^8 for the non-CM case.

Remark 3.19. Another seemingly simpler situation where “outside” primes can occur, which throws some light on the situation, is that of Kummer extensions. For simplicity, let $a \in \mathbf{Z}$ be a squarefree number. For $d \geq 1$, let $K_d = \mathbf{Q}(\mu_d, a^{1/d})$ be the Kummer extension generated by d -th roots of a . As is well-known, we have in this case an isomorphism

$$\text{Gal}(K_d/\mathbf{Q}) \simeq (\mathbf{Z}/d\mathbf{Z})^\times \rtimes (\mathbf{Z}/d\mathbf{Z}).$$

The order of the Galois group is thus $d\varphi(d)$, and one can define an *outside* prime for a to be p such that p splits completely in K_d with $p < d\varphi(d)$.

It is easy to see that, given p , the largest d for which p splits completely in K_d is $d = (p-1)/o_p$ where o_p is the multiplicative order of a modulo p : indeed we have $p \equiv 1 \pmod{d}$, and $a^{(p-1)/d} = a^{o_p} = 1 \pmod{p}$ so a is a d -th power modulo p .

Hence p is an outside prime if and only if

$$p < \frac{p-1}{o_p} \varphi\left(\frac{p-1}{o_p}\right).$$

Roughly speaking this is true if $o_p \ll \sqrt{p}$ (or equivalently if $p \mid a^j - 1$ with $j \ll \sqrt{p}$). Thus the question is clearly related to Artin’s conjecture about primitive roots and is currently much of a mystery. Getting non-trivial results seems extremely difficult, and one might expect the (non-CM) elliptic curve case to be also very hard.

3.5. Brun-Titchmarsh problems. In the study of the Titchmarsh divisor problem, to obtain a proof of (3.4) requires dealing with the large moduli $\sqrt{X}/(\log X) \leq d \leq \sqrt{X}$. Asymptotic formulae are not known in this range and do not follow from GRH (although they are conjectured to hold for $d \leq X^{1-\varepsilon}$, see e.g. [Gr]), but one can prove by sieve methods upper bounds of the correct order of magnitude which are sufficient to derive the asymptotic formula from that given by GRH (or, unconditionally, by the Bombieri-Vinogradov Theorem). This was first done by Titchmarsh [Ti-1]).

Theorem 3.20. *For all $d \geq 1$, all a with $(a, d) = 1$, and any $\varepsilon > 0$ we have*

$$(3.25) \quad \pi(X; d, a) \ll_\varepsilon \frac{X}{\varphi(d) \log X}$$

for $d \leq X^{1-\varepsilon}$, the implied constant depending only on ε .

A sharp version has been proved by Montgomery-Vaughan [MV]:

$$(3.26) \quad \pi(X; d, a) \leq \frac{2X}{\varphi(d) \log X/d}$$

for all $d < X$.

We recall for convenience how, using (3.25), one can now finish the proof of (3.4) on GRH from (3.6). Indeed, one has

$$(3.27) \quad \begin{aligned} \sum_{X^{1/2-\delta} \leq d \leq \sqrt{X}} \pi(X; d, 1) &\ll \frac{X}{\log X} \sum_{\sqrt{X}/(\log X) \leq d \leq X} \frac{1}{\varphi(d)} \\ &\ll \frac{X \log \log X}{\log X} \end{aligned}$$

for $X \geq 2$, and similarly

$$\sum_{d < \sqrt{X}} \pi(d^2 + 1; d, 1) \ll \sum_{d < \sqrt{X}} \frac{d^2}{\varphi(d) \log d} \ll \frac{X}{\log X},$$

for $X \geq 2$.

This naturally suggests the following problem:

Problem 3.21. Let E/K be an elliptic curve over a number field K . Is it true that for any $\varepsilon > 0$ there exists $C(E, \varepsilon) > 0$ such that

$$(3.28) \quad \pi_E(X; d, 1) \leq C(E, \varepsilon) \frac{X}{|G_d|(\log X)}$$

for all $d \leq X^{1/g-\varepsilon}$?

Note that the restriction to $d \leq X^{1/g}$ is certainly necessary, since for larger d the “main term” of the Chebotarev density theorem is < 1 (for X large enough). See below for further discussion of this point.

There’s a remark that arises in writing such an inequality: should one write $|G_d|$, in the denominator, or instead, assuming that E is non-CM, $|GL(2, \mathbf{Z}/d\mathbf{Z})|$? Both forms are equivalent, because of Serre’s result that the index of G_d in $GL(2, \mathbf{Z}/d\mathbf{Z})$ is bounded. But in fact an inequality

$$\pi_E(X; d, 1) \leq C(E, \varepsilon) \frac{X}{|GL(2, \mathbf{Z}/d\mathbf{Z})|(\log X)}$$

for $d \leq X^{1/g-\varepsilon}$ implies Serre’s result: fix d , take $\varepsilon = 1/(2g)$ (say), so for all $X \geq d^{2g}$ we have

$$\pi_E(X; d, 1) \leq C(E, (2g)^{-1}) \frac{X}{|GL(2, \mathbf{Z}/d\mathbf{Z})|(\log X)},$$

whereas by the Chebotarev density theorem

$$\pi_E(X; d, 1) \sim \frac{X}{|G_d|(\log X)}$$

as $X \rightarrow +\infty$. Comparing implies

$$[GL(2, \mathbf{Z}/d\mathbf{Z}) : G_d] \leq C(E, (2g)^{-1}).$$

Now it is interesting to note that the Brun-Titchmarsh inequality (3.25) is proved, with $\varphi(d)$ in the denominator, without any mention of cyclotomic fields! The same argument backwards then deduces from (3.25) that the index of the Galois group of $\mathbf{Q}(\mu_d)$ in $(\mathbf{Z}/d\mathbf{Z})^\times$ is bounded (by 2, using (3.26)). Of course, it is not hard to prove that it is 1 for all d (i.e. the cyclotomic polynomials are irreducible).⁵

Proposition 3.22. Let E/K be an elliptic curve over a number field. Assume that (3.28) holds for E in the range stated. Then we have

$$(3.29) \quad \sum_{d \leq X^{1/g-\varepsilon}} \varphi(d) \pi_E(X; d, 1) \ll X \quad (\text{if } E \text{ has CM})$$

$$(3.30) \quad \sum_{d \leq X^{1/g-\varepsilon}} \varphi(d) \pi_E(X; d, 1) \ll \frac{X}{\log X} \quad (\text{otherwise})$$

for any $\varepsilon > 0$ and any $X \geq 2$, the implied constant depending only on E and ε .

Note this is weaker than what GRH implies (Proposition 3.8), but it may be the case that (3.28) is easier to prove, as in the cyclotomic case. The proof is immediate, and the statement is given only for completeness.

It is clear that the Brun-Titchmarsh problem for $K(E[d])$ can be much generalized. Let us consider the following rather general context (compare [Se-2]): let K be a number field and K'/K an infinite Galois extension which is unramified outside a finite set of primes of K , and has Galois group $\text{Gal}(K'/K)$ which is (isomorphic to) a finite index subgroup of $G(\hat{\mathbf{Z}})$ for some

⁵Any constant < 2 in (3.25) would reprove this, but it is well-known (see references in [HR, p. 123]) that such a result would bring much richer rewards, as it would eliminate the possibility that the so-called Landau-Siegel zeros of quadratic Dirichlet L -functions exist.

smooth algebraic group G of finite type over \mathbf{Z} . For $d \geq 1$, let K_d/K be the fixed field of the kernel of the reduction modulo d map

$$\mathrm{Gal}(K'/K) \hookrightarrow G(\hat{\mathbf{Z}}) \twoheadrightarrow G(\mathbf{Z}/d\mathbf{Z}),$$

a Galois extension of K with $\mathrm{Gal}(K_d/K) = \mathrm{Gal}(K'/K) \pmod{d}$, with obvious notation. The Galois groups $\mathrm{Gal}(K_d/K)$ are, by the map above, subgroups of $G(\mathbf{Z}/d\mathbf{Z})$ with index bounded for $d \geq 1$. Let g be the (relative) dimension of G/\mathbf{Z} .

Definition. With notation as above, the field K' is a *Brun-Titchmarsh* field if and only if for any $\varepsilon > 0$ we have

$$(3.31) \quad \pi_{K'}(X; d, 1) \ll_{K', \varepsilon} \frac{1}{|G(\mathbf{Z}/d\mathbf{Z})|} \frac{X}{\log X}$$

if $d \leq X^{1/g-\varepsilon}$, the implied constant depending only on K' and ε , where $\pi_{K'}(X; d, 1)$ is the number of prime ideals of K with norm $\leq X$ which are totally split in K_d .

So the cyclotomic extension $\mathbf{Q}^{ab}/\mathbf{Q}$ is a Brun-Titchmarsh field, and Problem 3.21 can be rephrased as asking whether the field $K(E[\infty]) = \bigcup_d K(E[d])$ is a Brun-Titchmarsh field. Other examples arise naturally: for the same E/K , not CM, let $K' \subset K(E[\infty])$ be the subextension corresponding to the closed subgroup $Z(\hat{\mathbf{Z}}) \cap \mathrm{Gal}(K(E[\infty]))$, where Z is the center of $GL(2)$. It has Galois group G which is of finite index in $PGL(2, \hat{\mathbf{Z}})$, hence $g = 3$ in this case. If K'/K were a Brun-Titchmarsh field, and assuming GRH for Artin L -functions, the asymptotic formula

$$\sum_{d \leq X^{1/3-\varepsilon}} \varphi(d) \pi_E(X; d, 1) \sim c(E) \mathrm{li}(X)$$

(as $X \rightarrow +\infty$) would hold for any $\varepsilon > 0$. Indeed from (3.15), it suffices to estimate the sum over $X^{1/4}/(\log X) \leq d \leq X^{1/3-\varepsilon}$. This can be done using the Brun-Titchmarsh inequality (3.31) for K_d , since primes which are totally split in $K(E[d])$ must also be so in K_d :

$$\begin{aligned} \sum_{X^{1/4}/(\log X) \leq d \leq X^{1/3-\varepsilon}} \varphi(d) \pi_E(X; d, 1) &\ll_{\varepsilon} \frac{X}{\log X} \sum_d \frac{\varphi(d)}{|PGL(2, \mathbf{Z}/d\mathbf{Z})|} \\ &\ll_{\varepsilon} X^{3/4+\varepsilon}. \end{aligned}$$

One may ask similar questions with more general sets of conjugacy classes replacing the identity element; this is left to the reader to formulate, together with some potentially useful example for the elliptic splitting problem.

Besides the cyclotomic extension of \mathbf{Q} , it seems few Brun-Titchmarsh fields are known. We will see in Section 5.6 that the division fields of CM elliptic curves provide further examples. But all those correspond to (essentially) abelian Galois groups.

Problem 3.23. *Find a Brun-Titchmarsh extension K'/K corresponding to an algebraic group G/\mathbf{Z} of dimension > 0 with non-abelian connected component.*

The known proofs of the classical Brun-Titchmarsh inequality and of those for CM curves are based on sieve methods: one can use almost any form of ‘additive’ sieve (see [HR]) or a refined version of the large sieve (see [Bo, §3 or §4]). The latter may be generalized, to a certain extent using techniques as in [KM, Prop. 9] to handle Artin L -functions, but this requires to be useful that all irreducible representations of the finite groups $G(\mathbf{Z}/d\mathbf{Z})$ be of degree $\leq \gamma'$ for some $\gamma' > 0$ independent of d , which is equivalent to the connected component of G/\mathbf{Z} being abelian. However, this fails to give useful information for the Brun-Titchmarsh problem; this is because the required saving of the factor $1/|G(\mathbf{Z}/d\mathbf{Z})|$ comes, in the case of arithmetic progressions, from summing over integers $n \equiv 1 \pmod{d}$ by writing $n = md + 1$ and summing over m . This underlying regularity is of course non-existent in more complicated extensions.

This suggests another problem: prove (3.25) *without* appealing to the regularity of arithmetic progressions.

4. ELLIPTIC TWINS

4.1. Definition. The first step in the direction of Problem 3.18 introduces instead another interesting analytic problem. Let $K = \mathbf{Q}$ for simplicity. Fix $X \geq 1$ and an integer d such that $d^2 > 8X^{1/2}$. Let $\{p_1, \dots, p_k\}$ be the set of primes splitting completely in $\mathbf{Q}(E[d])$ (i.e. $d \mid d_1(E_{p_j})$) with $p_j \leq X$, and assume they are indexed in increasing order, so that $p_j < p_k$ if $j < k$.

Consider $p = p_j$ and $q = p_{j+1}$ for some j . Since

$$d^2 \mid d_1(p)^2 \mid n_p(E) = p + 1 - a_p(E) \text{ and also } d^2 \mid d_1(q)^2 \mid q + 1 - a_q(E)$$

we get by subtracting

$$d^2 \mid (q - p) + (a_p(E) - a_q(E)).$$

Therefore, if the right-hand side is non-zero, it follows that

$$q \geq p + (a_p(E) - a_q(E)) + d^2,$$

but by the Riemann Hypothesis for E_p and E_q , and the assumption $d^2 > 8X^{1/2} > 8q^{1/2}$, we have

$$|a_p(E) - a_q(E)| \leq 2(\sqrt{p} + \sqrt{q}) \leq \frac{d^2}{2},$$

hence we get a gap between p and q ,

$$q \geq p + \frac{d^2}{2},$$

which is stronger than the “trivial” gap imposed by the congruence $p \equiv q \equiv 1 \pmod{d}$.

However, this is subject to the condition that

$$(q - p) + (a_p(E) - a_q(E)) \neq 0$$

which is equivalent with

$$|E_p(\mathbf{F}_p)| \neq |E_q(\mathbf{F}_q)|.$$

There is no reason this should not occur, and this prompts the following general definition:

Definition. Let K be a number field and E/K an elliptic curve. Two distinct prime ideals \mathfrak{p} and \mathfrak{q} of K are called *elliptic twins* for E if

$$|E_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}})| = |E_{\mathfrak{q}}(\mathbf{F}_{\mathfrak{q}})|$$

i.e. E has as many points reduced modulo \mathfrak{p} and modulo \mathfrak{q} . We say that \mathfrak{p} has an E -twin, or simply a twin.

Remark 4.1. More generally, let C/K be an algebraic curve (or even an arbitrary algebraic variety) and fix $\mathcal{C}/\mathcal{O}_K[1/S]$ a model of C defined over the integers of K (minus a finite set S of primes). Two distinct prime ideals \mathfrak{p} and \mathfrak{q} of K which are not in S are called C -twins if

$$|C_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}})| = |C_{\mathfrak{q}}(\mathbf{F}_{\mathfrak{q}})|$$

We say that \mathfrak{p} has a C -twin. Note that except for finitely many pairs, this is independent of the choice of the model \mathcal{C} , but for definiteness one may choose one of the preferred models of C , or define twins for a variety defined over an open subset of $\text{Spec } \mathcal{O}_K$.⁶

N. Katz first suggested the following case, justifying the *rapprochement* with twin primes: instead of an elliptic curve, consider the affine conic $C : x^2 + y^2 = 1$ over \mathbf{Q} (equivalently, to stay with algebraic groups, the restriction of scalars from $\mathbf{Z}[i]$ to \mathbf{Z} of the kernel of the norm map $\mathbf{G}_{m/\mathbf{Z}[i]} \rightarrow \mathbf{G}_{m/\mathbf{Z}}$). This “is” a model over \mathbf{Z} , and we have (remember C is affine)

$$|C(\mathbf{F}_p)| = \begin{cases} p + 1 & \text{if } p \equiv 3 \pmod{4} \text{ (} p \text{ is inert in } \mathbf{Q}(i)\text{)} \\ p - 1 & \text{if } p \equiv 1 \pmod{4} \text{ (} p \text{ splits in } \mathbf{Q}(i)\text{)}. \end{cases}$$

Consequently, the condition $|C_p| = |C_q|$ means either $p = q$, or (1) $p \equiv 1 \pmod{4}$ and $p - 2$ is prime (it is then inert and $|C_{p-2}| = (p - 2) + 1 = p - 1 = |C_p|$), or (2) $p \equiv 3 \pmod{4}$ and $p + 2$

⁶Especially since no variety is known to have infinitely many twin pairs...

is prime, which is (1) with p and $p + 2$ exchanged. Hence the C -twins are “half” the ordinary twin primes, namely pairs $(p, p + 2)$ with $p \equiv 3 \pmod{4}$.

Note that it doesn’t seem to be possible to get the other half of all twin primes⁷ in this manner: using a conic one would need a quadratic field K with the property that p is split in K if and only if $p \equiv 3 \pmod{4}$. We ask:

Question 4.2. Is there an algebraic variety $\mathcal{X}/\mathbf{Z}[1/2]$ with the property that $p > 2$ and $q > p$ are \mathcal{X} -twins if and only if $q = p + 2$? Is there one such that p and q are \mathcal{X} -twins if and only if $q = p + 2$ and $p \equiv 1 \pmod{4}$?

The author’s guess is “No”.

The definition of elliptic twins certainly looks unnatural from a geometric viewpoint: we compare the reduction of a curve modulo two distinct primes. But in the absence of better ways of bounding the number of outside primes, and as analogues of the ordinary twin primes, they are worth investigating.

4.2. General facts. We now introduce some more notation. Fix an elliptic curve E/K defined over a number field. We define three arithmetic functions:

$$(4.1) \quad n_{\mathfrak{p}} = |E_{\mathfrak{p}}(\mathbf{F}_{\mathfrak{p}})|,$$

$$(4.2) \quad M(n) = |\{\mathfrak{p} \mid N\mathfrak{p} \leq X \text{ and } n_{\mathfrak{p}} = n\}|,$$

$$(4.3) \quad m(\mathfrak{p}) = M(n_{\mathfrak{p}}).$$

So $n_{\mathfrak{p}}$ and $m(\mathfrak{p})$ are supported on primes of K , and $M(n)$ is defined for all $n \geq 1$.

Of course \mathfrak{p} has an E -twin if and only if $m(\mathfrak{p}) > 1$. We’ll say that an $n \geq 1$ is a twin value if $M(n) > 1$, and call the primes \mathfrak{p} with $n_{\mathfrak{p}} = n$ the E -twins associated to n .

The main questions about elliptic twins concern the behavior of those three functions. In particular:

Question 4.3. What is the behavior of the function

$$(4.4) \quad j(X) = |\{n \leq X \mid n \text{ is a twin value}\}|$$

counting the twin values up to X , or of

$$(4.5) \quad J(X) = |\{\mathfrak{p} \mid N\mathfrak{p} \leq X \text{ and } \mathfrak{p} \text{ has an } E\text{-twin}\}|.$$

Question 4.4. What is the behavior of the sum

$$(4.6) \quad T(X) = \sum_{N\mathfrak{p} \leq X} m(\mathfrak{p})$$

as $X \rightarrow +\infty$?

Question 4.5. More generally, for fixed $k \geq 0$, what is the behavior of the moments of $m(\mathfrak{p})$ and $M(n)$

$$(4.7) \quad S_k(X) = \sum_{n \leq X} M(n)^k$$

$$(4.8) \quad T_k(X) = \sum_{N\mathfrak{p} \leq X} m(\mathfrak{p})^k.$$

Question 4.6. Differently formulated: what can be said about $M(n)$? How large can it be compared to n , and how does it behave as $n \rightarrow +\infty$?

⁷Numerical experiments (and standard conjectures) confirm that those “two-halves” are equidistributed, in an obvious sense.

Question 4.3 is the elliptic analogue of the classical twin-prime problem. On the other hand, because the analogue of the “multiplicity” $M(n)$ is simply the constant 2 for the twin-prime problem, Questions 4.4, 4.5 and 4.6 do not have a classical counterpart and are genuinely elliptic problems.

Also of interest is the dependence on E of all those quantities, in particular the “meta-question” is: what global arithmetic invariants of E can be extracted from information about the functions $M(n)$ and $m(n)$? (Recall that according to the Isogeny Theorem, the curve E/K is determined up to K -isogeny by the function $\mathfrak{p} \mapsto n_{\mathfrak{p}}$). We will see that it is likely that one can extract from the asymptotic of $j(X)$ whether E has CM or not. Recall the notation x^+ and x^- (1.3).

Lemma 4.7. *Let E/K be an elliptic curve over a number field. For any $n \geq 1$ we have*

$$(4.9) \quad n_{\mathfrak{p}} = n \Rightarrow n^- \leq N\mathfrak{p} \leq n^+,$$

$$(4.10) \quad \Rightarrow N\mathfrak{p}^- \leq n \leq N\mathfrak{p}^+.$$

and

$$(4.11) \quad M(n) \leq |\{\mathfrak{q} \mid \mathfrak{q} \text{ is prime and } n^- \leq N\mathfrak{q} \leq n^+\}| \ll [K : \mathbf{Q}] \frac{\sqrt{n}}{\log(n+1)},$$

the implied constant being absolute.

Proof. The implications (4.9) and (4.10) are just the Riemann Hypothesis (2.6) for $E_{\mathfrak{p}}$. The bound on $M(n)$ then follows trivially by definition; for the last inequality, observe that if \mathfrak{q} is prime and $n^- \leq N\mathfrak{q} \leq n^+$, $N\mathfrak{q}$ is a prime power in that range, of which the number is $\ll \sqrt{n}/(\log(n+1))$, with an absolute implied constant. Each prime power q^f can occur for at most $[K : \mathbf{Q}]$ prime ideals since \mathfrak{q} must be above q in K (compare (5.4) below). \square

Remark 4.8. The delicacy of the matter is indicated by the fact that the size (about \sqrt{n} ideals among n with $N\mathfrak{a} \leq n$) of this range is just such that, even on the Generalized Riemann Hypothesis, it is not possible to ensure that it contains at least one prime ideal \mathfrak{p} for all n large enough. Indeed, on GRH we have

$$\pi_K(X) = \text{li}(X) + \underline{O}(X^{1/2}(\log \Delta_K X))$$

(where Δ_K is the absolute value of the discriminant of K ; the implied constant is absolute, see [Se-2] for instance). This only implies

$$\pi_K(n^+) - \pi_K(n^-) \ll n^{1/2}(\log \Delta_K n)$$

which is worse than the trivial bound obtained by counting all integral ideals.

The “trivial” bound (4.11) is in a sense best possible, because it is possible to find curves over a finite prime field $\mathbf{Z}/p\mathbf{Z}$ with any value of a_E satisfying $|a_E| \leq 2\sqrt{p}$. We state more formally this easy fact:

Proposition 4.9. *Let $n \geq 1$ be an integer. There exists an elliptic curve E/\mathbf{Q} with good reduction at all primes p such that $n^- \leq p \leq n^+$, and with $n_p = n$ for all such primes.*

In contrast with the remark above, note that it is known that for “most” integers n the number of primes described is $\gg \sqrt{n}/(\log n)$ (see e.g. [Ha], where this is shown to hold for $n < p < n + n^\delta$ for any $\delta > 1/10$; the case $\delta = 1/2$ is much easier).

Proof. For p with $n^- \leq p \leq n^+$, let $b_p = p + 1 - n$, so by construction we have $|b_p| \leq 2\sqrt{p}$. By work of Deuring [De] (Honda-Tate theory for elliptic curves, see Theorem 6.8 below), there exists an elliptic curve E/\mathbf{F}_p with $a_E(p) = b_p$. Consider a Weierstrass equation

$$E_p/\mathbf{F}_p : y^2 + a_1(p)xy + a_3(p)y = x^3 + a_2(p)x^2 + a_4(p)x + a_6(p)$$

for such a curve. By the Chinese Remainder Theorem we can find $a_i \in \mathbf{Z}$, $i = 1, 2, 3, 4, 6$, reducing to $a_i(p)$ modulo p for all p with $n^- \leq p \leq n^+$. Then the curve

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

is an elliptic curve (since it reduces to a non-singular curve modulo those primes), and it has $n_p = n$ for all the primes p in question. \square

Of course, having constructed one n with $M(n) \gg \sqrt{n}/(\log n)$ does not tell anything about the asymptotic growth of $M(n)$ as $n \rightarrow +\infty$. The following trivial lemma shows (in particular) that on average $M(n)$ is much smaller.

Lemma 4.10. *Let E/K be an elliptic curve over a number field, $k \geq 1$ an integer. We have*

$$S_k(X) = \sum_{\substack{N\mathfrak{p} \leq X^+ \\ n_{\mathfrak{p}} \leq X}} m(\mathfrak{p})^{k-1}.$$

In particular

$$(4.12) \quad \sum_{n \leq X} M(n) = \pi_K(X) + \mathcal{O}_K(\sqrt{X}),$$

where $\pi_K(X)$ is the number of prime ideals of K with $N\mathfrak{p} \leq X$.

Note that $n_{\mathfrak{p}} \leq X$ implies $N\mathfrak{p} \leq X^+$, but this condition is included in the summation to recall how the size of $N\mathfrak{p}$ is controlled.

Proof. We have

$$\begin{aligned} \sum_{n \leq X} M(n)^k &= \sum_{n \leq X} M(n)^{k-1} \left(\sum_{n_{\mathfrak{p}}=n} 1 \right) = \sum_{n_{\mathfrak{p}} \leq X} M(n_{\mathfrak{p}})^{k-1} \\ &= \sum_{\substack{N\mathfrak{p} \leq X^+ \\ n_{\mathfrak{p}} \leq X}} m(\mathfrak{p})^{k-1}. \end{aligned}$$

Then (4.12) follows by taking $k = 1$ and noting that

$$\left| \sum_{\substack{N\mathfrak{p} \leq X^+ \\ n_{\mathfrak{p}} \leq X}} 1 - \sum_{N\mathfrak{p} \leq X} 1 \right| \leq \sum_{X^- \leq N\mathfrak{p} \leq X^+} 1 \ll_K \sqrt{X}.$$

\square

Question 4.11. Is it true that

$$(4.13) \quad M(n) = \mathcal{O}_{E,\varepsilon}(n^\varepsilon)$$

for all $\varepsilon > 0$?

We will see in Section 5 that this is true for CM curves (and we will give a more precise result). Heuristic and numerical evidence point to even stronger results, but note that because of Proposition 4.9, any progress requires using global properties of the elliptic curve.

If (4.13) holds, it follows that we have

$$(4.14) \quad S_k(X) = T_{k-1}(X) + \mathcal{O}_{E,\varepsilon,k}(X^{1/2+\varepsilon}), \text{ for any } \varepsilon > 0.$$

Finally we remark that the two functions $j(X)$ and $J(X)$ are somewhat different, since $J(X)$ counts the twins with multiplicity. For this reason (see Section 5), it is a little bit easier to deal with.

4.3. Heuristic. Here we consider an elliptic curve E/\mathbf{Q} which doesn't have CM, and we make some rough heuristics concerning elliptic twins. It should be possible to give somewhat more convincing arguments and more precise predictions using a probability model such as that used by Lang-Trotter [LT].

For a prime number p , there are about $4\sqrt{p}$ possible values of a_p , and according to the Sato-Tate conjecture, they should be such that the angle $\theta_p \in [0, \pi]$ satisfying

$$a_p = 2\sqrt{p} \cos \theta_p$$

is equidistributed with respect to the measure $d\mu = \frac{2}{\pi} \sin^2 \theta d\theta$.

Compared to the uniform measure, this measure is concentrated around 0, which should tend to limit the possibility of E -twins occurring, since a twin q must have $a_q = n_p - q - 1$, so q getting relatively large sends a_q towards the extreme, less probable, range of possible values. In particular, for heuristic purpose, assuming a_p to be uniformly distributed should bias the result towards *more* twins.

In a uniform situation, each possible prime q , $p^- \leq q \leq p^+$, has probability about $1/\sqrt{q}$ of being a twin of p . Since q must be prime, this makes a probability about

$$\approx \frac{1}{\sqrt{p}} \times \frac{\sqrt{p}}{(\log p)} \approx \frac{1}{\log p}$$

for p to have at least one twin. This is comparable to the situation with classical twin primes p , the probability of $p + 2$ being prime being about $1/(\log p)$. In particular we can ask

Question 4.12. Let E/\mathbf{Q} be an elliptic curve over \mathbf{Q} without CM. Prove or disprove that

$$(4.15) \quad j(X) \sim c \frac{X}{(\log X)^2}$$

for some $c > 0$ as $X \rightarrow +\infty$.

It is conjectured that the number $\pi_2(X)$ of twin primes $\leq X$ satisfies

$$\pi_2(X) \sim c_2 \frac{X}{(\log X)^2} \text{ with } c_2 = 2 \prod_{p \geq 3} \left(1 - \frac{1}{(p-1)^2}\right) = 1.3203\dots$$

In Section 5, we'll see it seems more plausible that for E with CM, we have

$$J(X) \sim c \frac{X}{\log X}, \quad j(X) \sim c \frac{X}{(\log X)^{3/2}}.$$

Concerning the multiplicity question, the same vague heuristic suggests that the probability that p has k twins is about $1/(\log p)^k$, and this would seem to imply that the maximal multiplicity is

$$(4.16) \quad m(p) = k \approx \frac{\log p}{\log \log p}.$$

Again, in the CM case, Section 5 suggests that $m(p)$ can be much larger, almost as large as a divisor-like function.

For numerical experiments, see Section 7 below.

5. CURVES WITH COMPLEX MULTIPLICATION

The analytic problems we have raised can be analyzed much further for CM curves. For elliptic twins, this will reveal some differences (so that, for instance, the behavior of $M(n)$, $m(\mathfrak{p})$ should distinguish between CM and non-CM curves) while highlighting in a different way the connexion with the classical twin primes. We will prove upper bounds for the moments of $M(n)$. Those upper bounds are such that general expectations about primes represented by polynomials lead us to believe that they are of the correct order of magnitude.

5.1. Preliminaries. We recall the basic facts of complex multiplication theory that describe the reductions of a CM curve and their Frobenius endomorphisms. The theory is basically due to Deuring; see for instance [Si-2, II] for a modern treatment.

Let E/H be an elliptic curve over a number field H with CM by an order \mathcal{O} in the ring of integers \mathcal{O}_K of a quadratic imaginary field K . *For simplicity, we will assume in this section that $K \subset H$, i.e. the defining field contains the CM field.* This excludes in particular the important case $H = \mathbf{Q}$, but the principle still applies in the general case, and we will extend the results for one curve over \mathbf{Q} in Section 7.3, so that a complete treatment could be easily obtained (recall that in any case the composite field HK is at most a quadratic extension of H , so the case $H = \mathbf{Q}$ is really “complementary” to the case $K \subset H$). For a given imaginary quadratic order

\mathcal{O} , it is known that all elliptic curves with CM by \mathcal{O} can be defined over the ring-class field associated to \mathcal{O} (e.g., if $\mathcal{O} = \mathcal{O}_K$, over the Hilbert class-field of K ; see e.g. [Si-2, II-Th.4.3] or [Sh-1, Th. 5.7]), but we do not need that here.

The following notation will be used: for an imaginary quadratic field K/\mathbf{Q} , we let $\chi = \chi_K$ denote the Kronecker symbol for K , i.e. the primitive quadratic Dirichlet character associated to K by class-field theory, and let $r(n)$ or $r_K(n)$ denote the arithmetic function

$$r(n) = r_K(n) = |\{\mathfrak{a} \subset \mathcal{O}_K \mid N\mathfrak{a} = n\}|$$

so that the Dedekind zeta function of K is given by

$$\begin{aligned} \zeta_K(s) &= \sum_{\mathfrak{a}} (N\mathfrak{a})^{-s} = \sum_{n \geq 1} r_K(n) n^{-s} \\ &= \prod_{\mathfrak{p}} (1 - (N\mathfrak{p})^{-s})^{-1} = \zeta(s) L(s, \chi_K). \end{aligned}$$

In particular,

$$(5.1) \quad r_K(n) = \sum_{d|n} \chi_K(d), \quad r_K(n) \leq d(n),$$

where $d(n)$ is the “number of divisors” function. It will be convenient to fix once and for all a basis $(1, \omega)$ of \mathcal{O}_K as a \mathbf{Z} -module.

The following result is that part of the theory of Complex Multiplication that will be needed; it says that the Frobenius modulo some prime of a CM curve can be lifted to characteristic 0.

Theorem 5.1. *With the above notation, there exists a map $\mathfrak{p} \mapsto \psi(\mathfrak{p}) \in \mathcal{O}$, defined from the set of prime ideals of H where E has good reduction, with the property that $\psi(\mathfrak{p})$, acting on the reduced curve $E_{\mathfrak{p}}$, is the Frobenius automorphism for $E_{\mathfrak{p}}/\mathbf{F}_{\mathfrak{p}}$.*

In fact, properly normalized, this map extends to the Grössencharakter of E (see e.g. [Si-2, Pr. 10.4] for curves with CM by the maximal order, [Sh-1, 7.8] for the general case), but we do not need this deeper fact.

We denote by $\Sigma(E)$ the image of ψ , i.e. the set of all Frobenius endomorphisms of E at primes of H .

By the properties of the Frobenius automorphism, if \mathfrak{p} is an unramified prime ideal of H , we have

$$(5.2) \quad N_{\mathbf{Q}}^H \mathfrak{p} = |\mathbf{F}_{\mathfrak{p}}| = N_{\mathbf{Q}}^K(\psi(\mathfrak{p})),$$

and

$$(5.3) \quad n_{\mathfrak{p}} = N_{\mathbf{Q}}^K(\psi(\mathfrak{p}) - 1).$$

We will reduce the problems about prime ideals in H to those of K using the following simple lemma:

Lemma 5.2. *With the same notation as before, for any prime ideal \mathfrak{p} in K , $\psi(\mathfrak{p})$ is divisible by a single prime p , and for any $z \in \mathcal{O}_K$ with this property*

$$|\{\mathfrak{p} \mid \psi(\mathfrak{p}) = z\}| \leq [H : \mathbf{Q}]$$

Proof. Equation (5.2) proves the first statement. Then for any \mathfrak{p} in H with $\psi(\mathfrak{p}) = z$, the prime p below \mathfrak{p} in \mathbf{Q} is independent of \mathfrak{p} : it is the unique p such that $N_{\mathbf{Q}}^K z = p^\nu$ for some $\nu \geq 1$. Hence the number of \mathfrak{p} is $\leq [H : \mathbf{Q}]$. \square

5.2. Elliptic twins. We apply now the theory of complex multiplication to elliptic twins. We keep the same notation and convention. First we can answer Question 4.11 for a CM curve.

Proposition 5.3. *Let E/H be a CM curve. We have for $n \geq 1$*

$$(5.4) \quad M(n) \leq [H : \mathbf{Q}]r_K(n),$$

and in particular for any $n \geq 1$ and any $\varepsilon > 0$,

$$(5.5) \quad M(n) = \underline{O}_{E,\varepsilon}(n^\varepsilon),$$

the implied constant depending only on E and ε .

Proof. By (5.3), for any \mathfrak{p} with $n_{\mathfrak{p}} = n$, the integer $z_{\mathfrak{p}} = \psi(\mathfrak{p}) - 1 \in \mathcal{O} \subset \mathcal{O}_K$ is a solution to the norm equation $N_{\mathbf{Q}}^K z = n$ in K . Moreover, if z is any solution of this equation, all prime ideals \mathfrak{p} with $z_{\mathfrak{p}} = z$ satisfy $\psi(\mathfrak{p}) = z + 1$. Thus by Lemma 5.2, for each z there are at most $[H : \mathbf{Q}]$ prime ideals \mathfrak{p} with $z_{\mathfrak{p}} = z$, hence (5.4) follows.

Now (5.5) is immediate since $r(n) \ll_{\varepsilon} n^{\varepsilon}$ (for instance, use (5.1)). \square

Our main result is the following theorem.

Theorem 5.4. *Let E/H be a CM elliptic curve as above. For any $\varepsilon > 0$, we have*

$$(5.6) \quad S_k(X) \ll X(\log X)^{\beta(k-1)+\varepsilon} \quad \text{for } k \geq 1$$

$$(5.7) \quad T_k(X) \ll X(\log X)^{\beta(k)+\varepsilon} \quad \text{for } k \geq 0,$$

for $X \geq 2$, where

$$(5.8) \quad \beta(k) = 2^k - k - 2.$$

The implied constants depend on k , K , H and ε .

Remark 5.5. One can probably put $\varepsilon = 0$; indeed, this is the case for $T_k(X)$ for $k = 0$, $k = 1$, and for all k the proof yields a stronger result with $(\log X)^{\varepsilon}$ replaced by a power of $\log \log X$; since I believe this is mistaken anyway (see the proof of Proposition 5.15), I prefer not to put this stronger statement.

For example,

$$\sum_{N_{\mathfrak{p}} \leq X} m(\mathfrak{p}) \ll_K \frac{X}{\log X}, \quad \sum_{N_{\mathfrak{p}} \leq X} m(\mathfrak{p})^2 \ll_K X.$$

Moreover, we'll see in the course of proving the theorem that standard conjectures about primes represented by polynomials imply that the estimates (5.7) and (5.6) are of the correct order of magnitude. For $T_0(X)$, this is just the Prime Ideal Theorem in K (and doesn't give any information about elliptic twins).

Before starting the proof, we remark that by Proposition 5.3 and (4.14), the bounds (5.6) and (5.7) are equivalent. We will work with $T_k(X)$ for $k \geq 1$, the case $k = 0$ being obvious.

5.3. Reduction to twin-prime-like counting. The strategy of the proof is to reduce to some counting of (principal) prime ideals in the ring \mathcal{O}_K , and to use (5.3) to put the counting into the shape of "parallel" twin-prime-like equations, for which upper bounds of the (conjectural) correct order of magnitude can be efficiently and uniformly obtained by a sieve method. In this case, we'll use Huxley's version of the large sieve in number fields [Hu].

A *prime element* in \mathcal{O}_K is an integer z such that (z) is a prime ideal. We first reduce to those \mathfrak{p} such that $\psi(\mathfrak{p})$ is a prime element.

Lemma 5.6. *Let E/H be as above. We have for any $k \geq 0$ and any $\varepsilon > 0$*

$$(5.9) \quad \sum_{\substack{N_{\mathfrak{p}} \leq X \\ f_{\mathfrak{p}} \geq 2}} m(\mathfrak{p})^k \ll_{\varepsilon, K, k} X^{1/2+\varepsilon}$$

the implied constant depending only on ε , K and k . In the sum, $f_{\mathfrak{p}}$ is the residual degree of \mathfrak{p} .

Proof. By (5.5), we have

$$\sum_{\substack{N\mathfrak{p} \leq X \\ f_{\mathfrak{p}} \geq 2}} m(\mathfrak{p})^k \ll_{\varepsilon, k} X^{\varepsilon} \sum_{\substack{N\mathfrak{p} \leq X \\ f_{\mathfrak{p}} \geq 2}} 1 \ll_{\varepsilon, k} X^{\varepsilon} \sum_{\substack{p^k \leq X \\ k \geq 2}} r_K(p^k) \ll_{\varepsilon, k, K} X^{1/2+\varepsilon}.$$

□

Henceforth we only consider prime ideals \mathfrak{p} of H which are of degree 1. In particular, by (5.2), $\psi(\mathfrak{p})$ is then a prime element of \mathcal{O}_K .

Next we deal with the parameterization of elliptic twins. Recall that an integer $z \in \mathcal{O}_K$ is *primitive* if it is not divisible by any $d \in \mathbf{Z}$, $d \neq \pm 1$; in terms of the basis $(1, \omega)$ of \mathcal{O}_K , if $z = a + b\omega$, this means that a and b are coprime. We let \mathcal{U} denote the set of primitive elements in \mathcal{O}_K modulo ± 1 . Note that any non-zero $z \in \mathcal{O}_K$ can be written $z = dv$ for some $d \in \mathbf{Z}$ and some $v \in \mathcal{U}$: if $z = a + b\omega$, $d = (a, b)$, $v = z/d$. The pair (d, v) is unique, up to simultaneous sign-change.

The norm Nu of an element $u \in \mathcal{U}$ is well-defined. So is the complex-conjugation (i.e. the action of the Galois group of K). In addition, for a k -tuple $\underline{u} = (u_1, \dots, u_k) \in \mathcal{U}^k$ we define the *discriminant* $\text{disc}(\underline{u})$ to be

$$(5.10) \quad \text{disc}(\underline{u}) = \prod_{1 \leq i < j \leq k} (u_i \bar{u}_j - \bar{u}_i u_j).$$

This is well-defined up to sign so it can be thought of as an integral ideal in K . Note that, by primitivity, $\text{disc}(\underline{u}) = 0$ if and only if there exist $i \neq j$ such that $u_i = u_j$ (in \mathcal{U}) (see the proof of the next lemma).

Lemma 5.7. *Let T be the set of $z \in K$ of norm 1. There exists a bijection*

$$\eta : \mathcal{U} \longrightarrow T$$

given by $u \mapsto \bar{u}/u$ for $u \in \mathcal{U}$.

Proof. Clearly η maps \mathcal{U} into T . Moreover, η is injective: if $\eta(v) = \eta(w)$ with $v, w \in \mathcal{U}$, we get $v/w \in \mathbf{Q}$ (because it is Galois-invariant), so we have $av = bw$ for some $a, b \in \mathbf{Q}$, $(a, b) = 1$. Because v and w are primitive, this implies that $|a| = |b| = 1$, so $v = \pm w$.

It remains to prove surjectivity. This amounts essentially to finding all pythagorean triples (when $K = \mathbf{Q}(i)$), but instead of doing it by hand, we can appeal to Hilbert's Theorem 90 for K/\mathbf{Q} (see e.g. [La, VIII-6]): for $z \in K^\times$, $Nz = 1$ is equivalent with $z = \bar{w}/w$ for some $w \in K^\times$. Writing $w = vd/e$ for some $v \in \mathcal{U}$ and $d, e \in \mathbf{Z}$, we have $z = \bar{v}/v = \eta(v)$. □

Note that one can write the discriminant $\text{disc}(\underline{u})$ as a Vandermonde determinant

$$\text{disc}(\underline{u}) = (u_1 \cdots u_k)^{k-1} \prod_{1 \leq i < j \leq k} (\eta(u_i) - \eta(u_j)) = (u_1 \cdots u_k)^{k-1} \prod_{i,j} |\eta(u_i)^{j-1}|_{i,j}.$$

Lemma 5.8. *Let K be an imaginary quadratic field. For integers $w, z \in \mathcal{O}_K$, we have*

$$(5.11) \quad N(w-1) = N(z-1)$$

if and only if there exists an $u \in \mathcal{U}$ such that $w = f_u(z)$, where f_u is the linear form

$$(5.12) \quad f_u(z) = \eta(u)(z-1) + 1 = \frac{\bar{u}}{u}(z-1) + 1.$$

Such an element $u \in \mathcal{U}$ is unique.

Proof. This is an immediate consequence of the previous lemma: (5.11) holds if and only if $N((w-1)/(z-1)) = 1$, therefore if and only if there exists a $u \in \mathcal{U}$ (which is unique) with

$$\frac{w-1}{z-1} = \eta(u) = \frac{\bar{u}}{u},$$

i.e. $w = \eta(u)(z-1) + 1 = f_u(z)$. □

Note that in this lemma we have $w = z$ if and only if $u = 1$ and $w = \bar{z}$ if and only if $u = z$.

By (5.3), it follows that if $n_{\mathfrak{p}} = n_{\mathfrak{q}}$, there exists $u \in \mathcal{U}$ such that $\psi(\mathfrak{p}) = f_u(\psi(\mathfrak{q}))$. For a given u , since $\psi(\mathfrak{p})$ is a prime element, this is similar to the classical twin-prime problem: the question is to find prime elements $\pi \in \mathcal{O}_K$ such that $f_u(\pi)$ is also prime (note that f_u can not be properly defined for prime *ideals*).

There are infinitely many $u \in \mathcal{U}$, but there is a (congruence) condition for $f_u(z)$ to be an integer when $z \in \mathcal{O}_K$, and this will restrict the values of u occurring in a sum like $T_k(X)$.

Lemma 5.9. *Let $\underline{u} = (u_1, \dots, u_k) \in \mathcal{U}^k$. For $z \in \mathcal{O}_K$, we have*

$$f_{u_i}(z) \in \mathcal{O}_K \text{ for all } i, 1 \leq i \leq k,$$

if and only if $z \equiv 1 \pmod{[\underline{u}]}$, where $[\underline{u}]$ is the (ideal) l.c.m of the elements u_1, \dots, u_k .

Proof. It suffices to treat the case $k = 1$, by definition of the l.c.m. Since

$$f_u(z) = \frac{\bar{u}}{u}(z - 1) + 1$$

we have $f_u(z) \in \mathcal{O}_K$ if and only if $\eta(u)(z - 1) \in \mathcal{O}_K$. Since u is primitive, u and \bar{u} are coprime, so this is equivalent with $z - 1 \in (u)$, i.e. $z \equiv 1 \pmod{u}$. \square

In other words, the ‘‘twin-prime problem’’ for f_u concerns only prime elements $\pi \in \mathcal{O}_K$ with $\pi \equiv 1 \pmod{u}$.

Corollary 5.10. *Let \mathfrak{p} be a prime ideal of H with $N\mathfrak{p} \leq X$. We have*

$$(5.13) \quad m(\mathfrak{p}) = \sum_{\substack{Nu \leq X^+ \\ f_u(\psi(\mathfrak{p})) \in \Sigma(E)}} 1.$$

Proof. By the above we get directly

$$(5.14) \quad m(\mathfrak{p}) = \sum_{\substack{u \in \mathcal{U} \\ f_u(\psi(\mathfrak{p})) \in \Sigma(E)}} 1.$$

Let $z \in \mathcal{O}_K$ be an integer with $Nz \leq X$ and $f_u(z) \in \mathcal{O}_K$. By Lemma 5.9, we can write

$$z = uv + 1 \text{ for some } v \in \mathcal{O}_K,$$

which implies $Nu \leq N(z - 1) \leq X^+$. Hence the result. \square

Corollary 5.11. *Let \mathfrak{p} be a prime ideal of degree 1 of H with no twin of degree ≥ 2 . We have*

$$(5.15) \quad m(\mathfrak{p}) \leq 2[H : \mathbf{Q}] \sum_{\substack{Nu \leq \sqrt{X}+1 \\ f_u(\psi(\mathfrak{p})) \text{ is prime}}} 1.$$

Proof. As in the proof of Proposition 5.3, to each prime element π of \mathcal{O}_K , there correspond at most $[H : \mathbf{Q}]$ prime ideals \mathfrak{p} of H with $\psi(\mathfrak{p}) = \pi$. Hence the previous corollary implies

$$(5.16) \quad m(\mathfrak{p}) \leq [H : \mathbf{Q}] \sum_{\substack{Nu \leq X^+ \\ f_u(\psi(\mathfrak{p})) \text{ is prime}}} 1.$$

Write $\pi = \psi(\mathfrak{p})$ for simplicity. For $z \in \mathcal{O}_K$ such that $Nz \leq X$ and $f_u(z) \in \mathcal{O}_K$ we have by Lemma 5.9

$$(5.17) \quad z = uv + 1 \text{ for some } v \in \mathcal{O}_K,$$

and

$$f_u(z) = \bar{u}v + 1.$$

We can use the classical trick of Dirichlet of switching divisors: remark that taking v instead of u in (5.17) leads to

$$f_v(z) = \bar{v}u + 1 = \overline{f_u(z)}.$$

In particular, if $f_u(z)$ is prime, so is $f_v(z)$, hence both u and v occur together in (5.16). Since one of them has norm $\leq \sqrt{X^+} = \sqrt{X} + 1$, the corollary follows. \square

We now rewrite the sum $T_k(X)$.

Lemma 5.12. *Let $k \geq 1$. We have*

$$T_k(X) = \sum_{\substack{\underline{u} \in \mathcal{U}^k \\ N u_i \leq X^+}} T_{\underline{u}}(X) + \underline{O}_{\varepsilon, k, K}(X^{1/2+\varepsilon})$$

for any $\varepsilon > 0$, where

$$T_{\underline{u}}(X) = |\{\mathfrak{p} \text{ degree 1 in } H \mid N\mathfrak{p} \leq X, f_{u_i}(\psi(\mathfrak{p})) \in \Sigma(E) \text{ for } 1 \leq i \leq k\}|$$

for $\underline{u} = (u_1, \dots, u_k)$.

Proof. By Corollary 5.10,

$$m(\mathfrak{p}) = \sum_{\substack{u \in \mathcal{U} \\ f_u(\psi(\mathfrak{p})) \in \Sigma(E)}} 1.$$

By Lemma 5.6 we can reduce to prime ideals of degree 1,

$$T_k(X) = \sum_{\substack{N\mathfrak{p} \leq X \\ f_{\mathfrak{p}}=1}} m(\mathfrak{p})^k + \underline{O}(X^{1/2+\varepsilon}).$$

Expanding the k -th power and changing the order of summation, the result follows. \square

Corollary 5.13. *Let $k \geq 1$. We have*

$$T_k(X) \ll \sum_{\substack{\underline{u} \in \mathcal{U}^k \\ N u_i \leq \sqrt{X}+1}} T_{(1, \underline{u})}^+(X) + \underline{O}_{\varepsilon, k, K}(X^{1/2+\varepsilon})$$

for any $\varepsilon > 0$, where $(1, \underline{u})$ is a $(k+1)$ -tuple, and for any k -tuple $\underline{v} = (v_1, \dots, v_k)$ we let

$$(5.18) \quad T_{\underline{v}}^+(X) = |\{z \in \mathcal{O}_K \mid Nz \leq X \text{ and } f_{v_i}(z) \text{ is prime for } 1 \leq i \leq k\}|.$$

The implied constant depends on ε , k and H .

Proof. Instead of Corollary 5.10, we use Corollary 5.11; note that it may well happen that \mathfrak{p} is of degree 1 but has a twin of degree ≥ 2 and such twins are not counted in (5.18), but the contribution of such twins is trivially $\ll X^{1/2+\varepsilon}$, by the same argument used in Lemma 5.6. \square

Note that $[v] = [u]$ if $v = (1, \underline{u})$.

Theorem 5.4 is a consequence of the following two propositions:

Proposition 5.14. *Let K/\mathbf{Q} be an imaginary quadratic field, $k \geq 1$ an integer and let $\underline{u} \in \mathcal{U}^k$ with $N[\underline{u}] \leq X$. Assume that $u_i \neq u_j$ for $i \neq j$ (in \mathcal{U}). Then we have*

$$T_{\underline{u}}^+(X) \ll_K \frac{\phi_k(\underline{u})}{N[\underline{u}]} \frac{X}{(\log(X/N[\underline{u}]))^k}$$

for $X \geq 2$, where

$$(5.19) \quad \phi_k(\underline{u}) = \prod_{\mathfrak{p} | N[\underline{u}]} \left(1 + \frac{k}{N\mathfrak{p}}\right).$$

The implied constant depends only on K and k .

Proposition 5.15. *Let K/\mathbf{Q} be an imaginary quadratic field, $k \geq 0$ an integer. For any $\varepsilon > 0$ we have*

$$\sum_{\substack{\underline{u} \in \mathcal{U}^k \\ N\underline{u}_i \leq X}} \frac{\phi_k(1, \underline{u})}{N[\underline{u}]} \ll_K (\log X)^{\gamma(k)+\varepsilon}$$

for $X \geq 2$, where $\gamma(k) = 2^k - 1$. The implied constant depends only on K , k and ε . For $k = 0$, we put, by convention, $\mathcal{U}^k = \{1\}$.

These will be proved in Section 5.4 and 5.5 respectively.

To finish the proof of Theorem 5.4, let

$$T_k^+(X) = \sum_{\substack{\underline{u} \in \mathcal{U}^k \\ N\underline{u}_i \leq \sqrt{X}+1}} T_{(1, \underline{u})}^+(X)$$

split the sum $T_k^+(X)$ into k subsums $T_{k,j}^+(X)$, $0 \leq j \leq k$, where $T_{k,j}^+(X)$ is the sum of the $T_{(1, \underline{u})}^+(X)$ for those $\underline{u} \in \mathcal{U}^k$ where there are $j+1$ values among the components of $(1, \underline{u})$ i.e. the set $\{1, u_i\}$ has $j+1$ elements.

By Lemma 5.13 and Proposition 5.14 (applied to the corresponding tuples $(1, \underline{i})$ for $(j+1)$ -tuples, we have

$$\begin{aligned} T_{k,j}^+(X) &\ll \sum_{\underline{u}} T_{(1, \underline{u})}^+(X) + X^{1/2+\varepsilon} \\ &\ll \sum_{\underline{u}} \frac{\phi_{j+1}(1, \underline{u})}{N[\underline{u}]} \frac{X}{(\log X)^{j+1}} + X^{1/2+\varepsilon} \\ &\ll \frac{X}{(\log X)^{j+1}} \sum_{\substack{\underline{v} \in \mathcal{U}^j \\ N\underline{v}_i \leq X}} \frac{\phi_{j+1}(1, \underline{v})}{N[\underline{v}]} \\ &\ll X(\log X)^{\gamma(j)-j-1+\varepsilon} \text{ for any } \varepsilon > 0 \text{ by Proposition 5.15.} \end{aligned}$$

In the next-to-last inequality, we used the fact that if the set $\{1, u_i\}$ has $j+1$ elements, $[\underline{u}] = [\underline{v}]$ where \underline{v} is any j -tuple whose components are the j elements of $\{u_i\}$, and applied Proposition 5.15 for j (there is a multiplicity for each \underline{v} , but it is a combinatorial function of j and k only).

Summing over $j \leq k$, the theorem follows, since $j \mapsto \gamma(j) - j - 1 = 2^j - j - 2$ is increasing for $j \geq 0$ ($0 \mapsto -1$, $1 \mapsto -1$, $2 \mapsto 0$, $3 \mapsto 3 \dots$). The implied constant depends on k , K , and H .

Remark 5.16. We conclude by justifying the assertion that Theorem 5.4 should provide the correct order of magnitude for $S_k(X)$ and $T_k(X)$ as $X \rightarrow +\infty$ (up to the $(\log X)^\varepsilon$ factor, see Remark 5.5). First, for $T_{\underline{u}}^+(X)$, we are counting integers z congruent to 1 modulo $[\underline{u}]$ such that the $k+1$ linear forms $f_{u_i}(z)$ take simultaneously prime values. For any $u \in \mathcal{U}$, we have $f_u(1) = 1$, hence there is no non-trivial common divisor to the values $f_u(z)$ for $z \in \mathcal{O}_K$, $z \equiv 1 \pmod{u}$. Also, if no two u_i coincide in \mathcal{U} , the condition that $f_{u_i}(z)$ be prime are ‘‘independent’’. Thus the usual heuristics predict that there should be infinitely many $z \equiv 1 \pmod{[\underline{u}]}$ for which the f_{u_i} take prime values, and moreover, each of those $k+1$ conditions should be satisfied with ‘‘probability’’ $1/(\log X)$ for $Nz \leq X$.

Since the congruence condition limits the values of z allowed, this justifies that Proposition 5.14 gives the asymptotic behavior, up to the arithmetic factor $\phi_k(\underline{u})$, which is very small; the asymptotic behavior should be

$$(5.20) \quad T_{\underline{u}}^+(X) \sim c(\underline{u}) \frac{X}{N[\underline{u}](\log X)^{k+1}}$$

as $X \rightarrow +\infty$, for some (more complicated) arithmetic function $c(\underline{u}) \leq \phi_k(\underline{u})$. Any other heuristic confirms this, of course; that based on cancellation in long averages involving the Möbius function could in theory provide a prediction for the value of $c(\underline{u})$ as an Euler product.

If it seems reasonable to expect that (5.20) holds, one may also expect that it does uniformly at least in a range $N[\underline{u}] \leq X^\delta$ for some $\delta > 0$, and this would provide a lower bound for $T^+(X)$ of the same order of magnitude.

The reader will easily convince herself that all other overcounting done in deriving Theorem 5.4 should have at most the effect of introducing a multiplicative constant: this includes the step from Frobenius elements $\Sigma(E)$ to all prime elements in K and the overcounting used in the proof of Proposition 5.15 (because of the logarithmic scaling of that sum).

5.4. Twin-primes in quadratic fields. In this section we prove Proposition 5.14. The argument is cleaner when the ideal $[\underline{u}]$ is principal: the reader may assume that it is so in a first reading.

Apart from the fact that we work over a quadratic field, the problem is quite standard, and the proof will be close to, for instance, the arguments in [Bo, §3].

We will use the large sieve for K , in the version given by Huxley [Hu, Th. 2]. First some notation: for an integral ideal \mathfrak{n} of K , we denote by $(\mathcal{O}_K/\mathfrak{n})^\vee$ the group of additive characters of $\mathcal{O}_K/\mathfrak{n}$. We write

$$\sum_{\psi}^* \alpha_{\psi}$$

for a sum over the *primitive* characters of $\mathcal{O}_K/\mathfrak{n}$, i.e. those which are not induced by a character modulo \mathfrak{m} for some \mathfrak{m} dividing \mathfrak{n} . Also we denote by

$$\sum_{\mathfrak{n}}^b \alpha_{\mathfrak{n}}$$

a sum over *squarefree* ideals \mathfrak{n} .

We define the height of $z \in \mathcal{O}_K$ by

$$h(z) = \max(|a|, |b|)$$

for $z = a + b\omega$. There exists a constant $\kappa > 0$ such that

$$(5.21) \quad Nz \leq X \text{ implies } h(z) \leq \kappa\sqrt{X} \text{ for } X > 0 \text{ and } z \in \mathcal{O}_K$$

(one can take $\kappa = 2$ for all K if the basis $(1, \omega)$ is the “canonical” one).

Theorem 5.17. (Huxley) *Let K/\mathbf{Q} be an imaginary quadratic field. We have*

$$(5.22) \quad \sum_{N\mathfrak{n} \leq Q} \sum_{\psi \in (\mathcal{O}_K/\mathfrak{n})^\vee}^* \left| \sum_{h(z) \leq X} a(z)\psi(z \bmod \mathfrak{n}) \right|^2 \ll (X^2 + Q^2) \sum_{h(z) \leq X} |a(z)|^2,$$

where $(a(z))$ is any sequence of complex numbers, Q and X are any real numbers ≥ 1 . The implied constant is absolute.

From this, proceeding as in [Bo, Th. 6], we derive an arithmetic sieve result: a *sieve* here is a pair (M, Ω) where

$$M = \{z \in \mathcal{O}_K \mid h(z) \leq X\}$$

for some $X \geq 1$ and Ω is a map which associates a subset $\Omega(\mathfrak{p}) \subset \mathcal{O}/\mathfrak{p}$ to prime ideals \mathfrak{p} with norm $N\mathfrak{p} \leq Q$. We denote $\omega(\mathfrak{p}) = |\Omega(\mathfrak{p})|$. The corresponding *sifted set* is

$$(5.23) \quad \mathcal{M} = \{z \mid h(z) \leq X \text{ and } z \pmod{\mathfrak{p}} \notin \Omega(\mathfrak{p}) \text{ for all } \mathfrak{p}\}.$$

Corollary 5.18. *Let K/\mathbf{Q} be an imaginary quadratic field and (M, Ω) a sieve. We have*

$$|\mathcal{M}| \ll \frac{X^2 + Q^2}{J}$$

where

$$J = \sum_{N\mathfrak{n} \leq Q}^b J(\mathfrak{n}), \text{ with } J(\mathfrak{n}) = \prod_{\mathfrak{p}|\mathfrak{n}} \frac{\omega(\mathfrak{p})}{N\mathfrak{p} - \omega(\mathfrak{p})}$$

for \mathfrak{n} squarefree. The implied constant is absolute.

We will apply Corollary 5.18 to the situation of Proposition 5.14.

To setup the situation, we use the ideal-class group of K . Let $\mathfrak{a} = [\underline{u}]$, let \mathfrak{b}_0 be an integral ideal of K with minimal norm in the ideal class inverse to that of \mathfrak{a} , say

$$\mathfrak{a}\mathfrak{b}_0 = (a_0) \text{ for some } a_0 \in \mathcal{O}_K.$$

If $z \in \mathcal{O}_K$ satisfies $z \equiv 1 \pmod{\mathfrak{a}}$, there exists an integral ideal \mathfrak{b} such that

$$(z - 1) = \mathfrak{a}\mathfrak{b}$$

and since $(z - 1)$ is principal, \mathfrak{b} and \mathfrak{b}_0 are in the same ideal class, i.e. there exists $b \in K^\times$ such that

$$(5.24) \quad \mathfrak{b} = b\mathfrak{b}_0, \text{ hence } (z - 1) = (a_0b).$$

Since \mathfrak{b} is integral, the denominator of b is bounded (by that of $N\mathfrak{b}_0$), i.e. there exists $d_0 \in \mathbf{Z}$, independent of z and with $d_0 \mid N\mathfrak{b}_0$, such that $b = c/d_0$ for some $c \in \mathcal{O}_K$.

Hence, using (5.24), there exists a unit $\varepsilon \in \mathcal{O}_K^\times$ (a finite group of order ≤ 6) such that

$$(5.25) \quad z = \varepsilon \frac{a_0c}{d_0} + 1.$$

Therefore

$$(5.26) \quad T_{\underline{u}}^+(X) \leq \sum_{\varepsilon \in \mathcal{O}_K^\times} |\{c \in \mathcal{O}_K \mid z = \varepsilon \frac{a_0c}{d_0} + 1 \text{ satisfies } N(z) \leq X \text{ and } f_{u_i}(z) \text{ is prime}\}|.$$

By (5.25) and the definition of a_0, d_0 , if $Nz \leq X$ we have

$$(5.27) \quad Nc \leq \frac{d_0^2}{Na_0} X^+ \leq \frac{X^+}{N\mathfrak{a}}.$$

For $\varepsilon \in \mathcal{O}_K^\times$, consider the sieving problem (M, Ω_ε) consisting in sieving the set

$$M = \{z \in \mathcal{O}_K \mid h(z) \leq \kappa(\sqrt{(X+1)/N\mathfrak{a}})\}$$

(where κ is as in (5.21)), by prime ideals \mathfrak{p} with $N\mathfrak{p} \leq \sqrt{X/N\mathfrak{a}}$, with $\Omega_\varepsilon(\mathfrak{p})$ defined as follows: let

$$(5.28) \quad \Omega^+(\mathfrak{p}) = \left\{ -\frac{u_i d_0}{\varepsilon \bar{u}_i a_0} \mid 1 \leq i \leq k \right\} \subset (\mathcal{O}_K/\mathfrak{p})$$

(with the convention that any ratio where the denominator is 0 modulo \mathfrak{p} is omitted), and define

$$\Omega_\varepsilon(\mathfrak{p}) = \begin{cases} \Omega^+(\mathfrak{p}) & \text{if } |\Omega^+(\mathfrak{p})| = k \\ \emptyset & \text{otherwise.} \end{cases}$$

Lemma 5.19. *Let \mathcal{M}_ε denote the sifted set for the sieving problem above. We have*

$$T_{\underline{u}}^+(X) \leq \sum_{\varepsilon} |\mathcal{M}_\varepsilon|.$$

This is an immediate consequence of the previous inequality (5.26), (5.21) and the definition of the sieve (one could of course be more precise and not disregard the primes \mathfrak{p} with $|\Omega^+(\mathfrak{p})| < k$).

Lemma 5.20. *We have $\omega_\varepsilon(\mathfrak{p}) = 0$ if and only if*

$$\mathfrak{p} \mid N[\underline{u}] \text{ disc}(\underline{u})$$

where the discriminant is defined in (5.10).

Proof. This is clear: the factor $N[\underline{u}] = N\mathfrak{a}$ arises from the possibility that the denominators in (5.28) are divisible by \mathfrak{p} , whereas the discriminant occurs from the possibility that

$$\frac{u_i}{\bar{u}_i} = \frac{u_j}{\bar{u}_j} \pmod{\mathfrak{p}} \text{ i.e. } u_i \bar{u}_j - \bar{u}_i u_j = 0 \pmod{\mathfrak{p}}$$

for some $i \neq j$. □

Note that $\text{disc}(\underline{u}) \neq 0$ in the application to Proposition 5.14 since no two u_i coincide.

By Corollary 5.18, we deduce that

$$(5.29) \quad T_{\underline{u}}^+(X) \ll \frac{1}{J} \frac{X}{N\mathfrak{a}}$$

for $X \geq 2$ with an absolute implied constant, where

$$J = \sum_{\substack{N\mathfrak{n} \leq \sqrt{X/N\mathfrak{a}+1} \\ (\mathfrak{n}, \text{disc}(\underline{u})N\mathfrak{a})=1}}^{\mathfrak{b}} J(\mathfrak{n}), \text{ with } J(\mathfrak{n}) = \prod_{\mathfrak{p}|\mathfrak{n}} \frac{k}{N\mathfrak{p} - k}.$$

Note that $\mathfrak{n} \mapsto J(\mathfrak{n})$ is an arithmetic function that depends only on k , not on \underline{u} .

It only remains to find a lower bound for J to get an upper bound for $T_{\underline{u}}^+(X)$; the only issue of note is the uniformity in \underline{u} . All the arguments below are standard (see e.g. [HR, Th. 2.4]), but by lack of a convenient reference, especially in the context of a number field, we give all details.

For \mathfrak{n} squarefree we have $J(\mathfrak{n}) \geq J^{\mathfrak{b}}(\mathfrak{n})$, where $J^{\mathfrak{b}}(\mathfrak{n})$ is the totally multiplicative arithmetic function on integral ideals of K such that

$$J^{\mathfrak{b}}(\mathfrak{p}) = \begin{cases} 0 & \text{if } N\mathfrak{p} \leq k^2 \\ k/N\mathfrak{p} & \text{otherwise.} \end{cases}$$

Therefore

$$(5.30) \quad J \geq \sum_{\substack{N\mathfrak{n} \leq \sqrt{X/N\mathfrak{a}+1} \\ (\mathfrak{n}, \text{disc}(\underline{u})N\mathfrak{a})=1}}^{\mathfrak{b}} J^{\mathfrak{b}}(\mathfrak{n}).$$

We consider the generating series

$$z(s) = \sum_{\mathfrak{n}}^{\mathfrak{b}} J^{\mathfrak{b}}(\mathfrak{n})(N\mathfrak{n})^{-s} = \prod_{N\mathfrak{p} > k^2} (1 + k(N\mathfrak{p})^{-s-1})$$

which converges absolutely⁸ for $\text{Re}(s) > 0$, and the closely related

$$w(s) = \sum_{\mathfrak{n}} J^{\mathfrak{b}}(\mathfrak{n})(N\mathfrak{n})^{-s} = \prod_{N\mathfrak{p} > k^2} (1 - k(N\mathfrak{p})^{-s-1})^{-1}$$

which also converges absolutely in the same region.

Lemma 5.21. *There exists a Dirichlet series*

$$y(s) = \sum_{\mathfrak{n}} Y(\mathfrak{n})(N\mathfrak{n})^{-s}$$

such that

$$(5.31) \quad z(s) = y(s)w(s),$$

and $y(s)$ converges absolutely for $\text{Re}(s) > -1/2$.

Proof. This is clear by comparing the Euler factors of $z(s)$ and $w(s)$, using the fact that the zeros of $1 - k(N\mathfrak{p})^{-s-1}$ have $\text{Re}(s) < -1/2$ for $N\mathfrak{p} > k^2$. \square

Lemma 5.22. *There exists a constant $c > 0$ such that*

$$\sum_{N\mathfrak{n} \leq Y}^{\mathfrak{b}} J^{\mathfrak{b}}(\mathfrak{n}) = c(\log Y)^k + \underline{O}((\log Y)^{k-1})$$

for $Y \geq 2$.

⁸In particular, has no zero.

Proof. This is obvious by comparison of $w(s)$ with $\zeta_K(s+1)^k$, which has a pole of order k at $s=0$, and contour integration: we have (as in Lemma 5.21)

$$w(s) = \zeta_K(s+1)w_1(s)$$

for some Dirichlet series $w_1(s)$ which converges absolutely in the region $\operatorname{Re}(s) > -1/2$. \square

Lemma 5.23. *Let $T(\mathfrak{n})$ be a completely multiplicative arithmetic function of integral ideals of K such that:*

(i) *There exists $A > 0$ such that*

$$T(\mathfrak{p}) \leq \frac{A}{N\mathfrak{p}}$$

for all prime ideals \mathfrak{p} .

(ii) *There exists $c > 0$ and $\gamma > 0$ such that*

$$\sum_{N\mathfrak{n} \leq Y} T(\mathfrak{n}) = c(\log Y)^\gamma + \underline{O}((\log Y)^{\gamma-1})$$

for $Y \geq 2$.

Fix an integer $B \geq 1$. Then for all $Y \geq 2$ and all non-zero integral ideals \mathfrak{q} such that $N\mathfrak{q} \leq Y^B$, we have

$$\sum_{\substack{N\mathfrak{n} \leq Y \\ (\mathfrak{n}, \mathfrak{q})=1}} T(\mathfrak{n}) = (\log Y)^\gamma \left(\sum_{\mathfrak{d}|\mathfrak{q}} \mu(\mathfrak{d})T(\mathfrak{d}) \right) + \underline{O}((\log Y)^{\gamma-1}(\log \log Y)^A),$$

the implied constant depending on A , B and γ .

In this statement and in the proof, we use $d(\mathfrak{n})$ (resp. $\mu(\mathfrak{n})$) to denote the divisor function (resp. Möbius) function for integral ideals. The latter is defined as usual (i.e. $\mu(\mathfrak{p}^k) = (-1)^k$ for any prime ideal \mathfrak{p} and $k \geq 0$, and μ multiplicative). The Möbius inversion formula holds:

$$\sum_{\mathfrak{d}|\mathfrak{n}} \mu(\mathfrak{d}) = \begin{cases} 1 & \text{if } \mathfrak{n} = 1 \\ 0 & \text{otherwise.} \end{cases}$$

We will use the following easy estimates

$$(5.32) \quad \prod_{\mathfrak{p}|\mathfrak{n}} \left(1 + \frac{A}{N\mathfrak{p}} \right) \ll (\log \log N\mathfrak{n})^A$$

for all non-zero integral ideals \mathfrak{n} . The implied constant depends only on A .

Proof. We have by Möbius inversion

$$\begin{aligned} \sum_{\substack{N\mathfrak{n} \leq Y \\ (\mathfrak{n}, \mathfrak{q})=1}} T(\mathfrak{n}) &= \sum_{\mathfrak{d}|\mathfrak{q}} \mu(\mathfrak{d}) \sum_{N\mathfrak{n} \leq Y/N\mathfrak{d}} T(\mathfrak{n}\mathfrak{d}) \\ &= \sum_{\substack{\mathfrak{d}|\mathfrak{q} \\ N\mathfrak{d} < Y^\delta}} \mu(\mathfrak{d})T(\mathfrak{d}) \sum_{N\mathfrak{n} \leq Y/N\mathfrak{d}} T(\mathfrak{n}) + \underline{O}(Y^{-\delta+\varepsilon}) \end{aligned}$$

for any (fixed) $\delta > 0$ and $\varepsilon < \delta$, having used the complete multiplicativity, and (i) and (ii) to estimate the remaining sum over large divisors of $N\mathfrak{q}$:

$$\begin{aligned} \sum_{\substack{\mathfrak{d}|\mathfrak{q} \\ N\mathfrak{d} \geq Y^\delta}} \mu(\mathfrak{d})T(\mathfrak{d}) \sum_{N\mathfrak{n} \leq Y/N\mathfrak{d}} T(\mathfrak{n}) &\ll \frac{(\log Y)^\gamma}{Y^\delta} \sum_{\mathfrak{d}|\mathfrak{q}} d(\mathfrak{d})^A \\ &\ll \frac{(\log Y)^\gamma}{Y^\delta} d(\mathfrak{q})^{A+1} \\ &\ll_{\varepsilon, B, A} Y^{-\delta+\varepsilon} \end{aligned}$$

(by the assumption $N\mathfrak{q} \leq Y^B$). The implied constant depends on ε , A , B and γ .

Using again (ii) we have

$$\begin{aligned} \sum_{\substack{\mathfrak{d}|\mathfrak{q} \\ N\mathfrak{d} < Y^\delta}} \mu(\mathfrak{d})T(\mathfrak{d}) \sum_{N\mathfrak{n} \leq Y/N\mathfrak{d}} T(\mathfrak{n}) &= c \sum_{\substack{\mathfrak{d}|\mathfrak{q} \\ N\mathfrak{d} < Y^\delta}} \mu(\mathfrak{d})T(\mathfrak{d}) \left(\left(\log \frac{Y}{N\mathfrak{d}} \right)^\gamma + \underline{O}((\log Y)^{\gamma-1}) \right) \\ &= c(\log Y)^\gamma \sum_{\substack{\mathfrak{d}|\mathfrak{q} \\ N\mathfrak{d} < Y^\delta}} \mu(\mathfrak{d})T(\mathfrak{d}) + \underline{O}((\log Y)^{\gamma-1}(\log \log Y)^A) \end{aligned}$$

by expanding the logarithm and estimating

$$\begin{aligned} (\log Y)^{\gamma-1} \left| \sum_{\substack{\mathfrak{d}|\mathfrak{q} \\ N\mathfrak{d} < Y^\delta}}^b \mu(\mathfrak{d})T(\mathfrak{d}) \right| &\leq (\log Y)^{\gamma-1} \prod_{\mathfrak{p}|\mathfrak{q}} (1 + T(\mathfrak{p})) \\ &\leq (\log Y)^{\gamma-1} \prod_{\mathfrak{p}|\mathfrak{q}} \left(1 + \frac{A}{N\mathfrak{p}} \right) \ll_A (\log \log N\mathfrak{q})^A \\ &\ll_{A,B} (\log \log Y)^A \end{aligned}$$

by (5.32).

It remains to get rid of δ , which is possible since

$$\sum_{\substack{\mathfrak{d}|\mathfrak{q} \\ N\mathfrak{d} \geq Y^\delta}} \mu(\mathfrak{d})T(\mathfrak{d}) \ll Y^{-\delta} \sum_{\mathfrak{d}|\mathfrak{q}} d(\mathfrak{d})^A \ll Y^{-\delta+\varepsilon}.$$

Choosing δ small enough and $\varepsilon < \delta$, the lemma follows. \square

We come back to (5.30) and write, using (5.31)

$$\sum_{\substack{N\mathfrak{n} \leq Y \\ (\mathfrak{n}, \text{disc}(\underline{u})N\mathfrak{a})=1}}^b J^b(\mathfrak{n}) = \sum_{\substack{N\mathfrak{m} \leq Y \\ (\mathfrak{m}, \text{disc}(\underline{u})N\mathfrak{a})=1}} Y(\mathfrak{m}) \sum_{\substack{N\mathfrak{n} \leq Y/N\mathfrak{m} \\ (\mathfrak{n}, \text{disc}(\underline{u})N\mathfrak{a})=1}} J^b(\mathfrak{n}).$$

To the inner sum we can apply Lemma 5.23 with $\mathfrak{q} = \text{disc}(\underline{u})N\mathfrak{a}$ and $\gamma = k$: the assumptions hold for some A, B and $\gamma = k$ by Lemma 5.22. Therefore

$$\begin{aligned} \sum_{\substack{N\mathfrak{n} \leq Y \\ (\mathfrak{n}, \text{disc}(\underline{u})N\mathfrak{a})=1}}^b J^b(\mathfrak{n}) &= c \sum_{\substack{N\mathfrak{m} \leq Y \\ (\mathfrak{m}, \text{disc}(\underline{u})N\mathfrak{a})=1}} Y(\mathfrak{m}) (\log(Y/N\mathfrak{a}))^k + \underline{O}((\log Y)^{k-1}(\log \log Y)^k) \\ (5.33) \quad &= c(\log Y)^k \left(\sum_{\mathfrak{d}|\text{disc}(\underline{u})N\mathfrak{a}} \mu(\mathfrak{d})J^b(\mathfrak{d}) \right) \sum_{\substack{N\mathfrak{m} \leq Y \\ (\mathfrak{m}, \text{disc}(\underline{u})N\mathfrak{a})=1}} Y(\mathfrak{m}) \\ &\quad + \underline{O}((\log Y)^{k-1}(\log \log Y)^k), \end{aligned}$$

by again expanding the logarithm, and using the fact that for any $B \geq 0$ the series

$$\sum_{\mathfrak{m}} Y(\mathfrak{m})(\log N\mathfrak{m})^B$$

is absolutely convergent. Now apply the following lemma to $Y(\mathfrak{m})$ and $\mathfrak{q} = \text{disc}(\underline{u})N\mathfrak{a}$:

Lemma 5.24. *Let $Y(\mathfrak{n})$ be a multiplicative arithmetic function, $y(s)$ its generating Dirichlet series. Assume that the Euler product for $y(s)$ converges absolutely for $\text{Re}(s) > -1/2$. Then for any non-zero integral ideal \mathfrak{q} we have*

$$\sum_{\substack{N\mathfrak{m} \leq X \\ (\mathfrak{m}, \mathfrak{q})=1}} Y(\mathfrak{m}) \gg 1$$

for $X \geq 2$, the implied constant depending only on the function Y .

Proof. By a standard application of contour integration and Perron's formula. The size of \mathfrak{q} does not matter here because the sum always involves $\mathfrak{m} = 1$, with a contribution = 1. In slightly more detail: it is well-known (see e.g. [Ti-2, p. 61]) that

$$\frac{1}{2i\pi} \int_{1-iT}^{1+iT} y^s \frac{ds}{s} = h(y) + \underline{O}\left(\frac{y}{T|\log y|}\right)$$

for all $y > 0$ and $T > 0$, where $h(y) = 1$ for $y > 1$, $h(y) = 0$ for $y < 1$ and $h(1) = 1/2$.

Let $y_{\mathfrak{q}}(s)$ be the generating Dirichlet series of $Y(\mathfrak{m})$ restricted to those \mathfrak{m} coprime to \mathfrak{q} . Choosing X of the form $1/2 + m$ for some integer m , as we may without loss of generality, we have

$$(5.34) \quad \frac{1}{2i\pi} \int_{1-iT}^{1+iT} y_{\mathfrak{q}}(s) X^s \frac{ds}{s} = \sum_{\substack{Nm \leq X \\ (\mathfrak{m}, \mathfrak{q})=1}} Y(\mathfrak{m}) + \underline{O}(XT^{-1})$$

since

$$\sum_{\mathfrak{m}} \frac{Y(\mathfrak{m})}{Nm |\log(X/N\mathfrak{m})|} < +\infty$$

(use the absolute convergence of $\sum Y(\mathfrak{m})$ and $|Nm(\log X/N\mathfrak{m})| \gg 1$).

On the other hand, by Cauchy's theorem we have

$$(5.35) \quad \frac{1}{2i\pi} \int_{\mathcal{C}} y_{\mathfrak{q}}(s) X^s \frac{ds}{s} = y_{\mathfrak{q}}(0)$$

where \mathcal{C} is the boundary of the rectangle $[-1/4, 1] \times [-T, T]$. By absolute convergence, the integral on the horizontal pieces and on the vertical line $\operatorname{Re}(s) = -1/4$ are

$$\begin{aligned} \frac{1}{2i\pi} \left\{ \int_{1/4-iT}^{1-iT} + \int_{1+iT}^{-1/4+iT} y_{\mathfrak{q}}(s) X^s \frac{ds}{s} \right\} &\ll XT^{-1} \\ \frac{1}{2i\pi} \int_{-1/4-iT}^{-1/4+it} y_{\mathfrak{q}}(s) X^s \frac{ds}{s} &\ll X^{-1/4} \end{aligned}$$

the implied constant depending only on Y . Hence (5.34) and (5.35) show that

$$\sum_{\substack{Nm \leq X \\ (\mathfrak{m}, \mathfrak{q})=1}} Y(\mathfrak{m}) = y_{\mathfrak{q}}(0) + \underline{O}(XT^{-1}) + \underline{O}(X^{-1/4}).$$

Taking $T = X^2$ for instance gives

$$\sum_{\substack{Nm \leq X \\ (\mathfrak{m}, \mathfrak{q})=1}} Y(\mathfrak{m}) \gg y_{\mathfrak{q}}(0)$$

the implied constant depending only on Y .

Since $y_{\mathfrak{q}}(0)$ is the same absolutely convergent Euler product as $y(0)$, except that primes dividing \mathfrak{q} are omitted, and any partial product of an absolutely convergent infinite product has a uniform lower bound, it follows that

$$y_{\mathfrak{q}}(0) \gg 1,$$

thereby proving the lemma. □

Since moreover

$$\sum_{\mathfrak{d}|\operatorname{disc}(\underline{u})N\mathfrak{a}} \mu(\mathfrak{d}) J^b(\mathfrak{d}) = \prod_{\mathfrak{p}|\operatorname{disc}(\underline{u})N\mathfrak{a}} (1 - J^b(\mathfrak{p})) > 0,$$

because $J^b(\mathfrak{p}) < 1$ for all \mathfrak{p} (this is why small primes had to be excluded), the inequality (5.33) proves that

$$(5.36) \quad J \gg \prod_{\mathfrak{p}|\operatorname{disc}(\underline{u})N\mathfrak{a}} (1 - J^b(\mathfrak{p}))$$

the implied constant depending on k and K only.

Lemma 5.25. *For all \mathfrak{p} we have*

$$1 - J^{\mathfrak{p}} \geq (1 - k^{-2}) \left(1 + \frac{k}{N\mathfrak{p}}\right).$$

Proof. This is obvious from the definition. □

Proposition 5.14 follows from (5.29), (5.36) and this lemma.

5.5. Proof of Proposition 5.15. In this section we prove Proposition 5.15. For $k = 0$, the result is obvious with no need of the factor $(\log X)^\varepsilon$, since the sum is reduced to $u = 1$. So we assume $k \geq 1$.

We have by (5.32)

$$\phi_k(1, \underline{u}) \ll (\log \log X)^k$$

with an absolute implied constant, hence by positivity

$$(5.37) \quad \sum_{\substack{\underline{u} \in \mathcal{U}^k \\ Nu_i \leq X}} \frac{\phi_k(1, \underline{u})}{N[\underline{u}]} \ll (\log \log X)^k \sum_{n \leq X^k} \frac{\rho(n)}{n}$$

for $X \geq 2$ (the constant depending only on k), where $\rho(n)$ is the arithmetic function defined by

$$(5.38) \quad \rho(n) = |\{(u_1, \dots, u_k) \text{ ideals in } \mathcal{O}_K \mid N[u_1, \dots, u_k] = n\}|.$$

Thus we drop the condition that the u_i be integers or primitive, and drop the size condition $Nu_i \leq X$ on the solutions of $N[\underline{u}] = n$, and this shouldn't change the order of magnitude because of the logarithmic weight.

The arithmetic function $\rho(n)$ is multiplicative.

Lemma 5.26. *Let $n \geq 1$ be an integer. We have*

$$\rho(n) \leq d(n)^{2k}$$

where $d(n)$ is the function “number of divisors”.

Proof. In (5.38), $Nu_i \mid n$ for all i , so there are at most $d(n)^k$ choices of (Nu_1, \dots, Nu_k) , and for each of those there are

$$r(Nu_1) \cdots r(Nu_k) \leq r(n)^k \leq d(n)^k$$

choices of (u_1, \dots, u_k) . □

Lemma 5.27. *Let p be a prime number. We have*

$$\rho(p) = (1 + \chi(p))(2^k - 1).$$

Proof. We have $N[u_1, \dots, u_k] = p$ if and only if

$$(5.39) \quad [u_1, \dots, u_k] = \pi$$

where π is an ideal such that $N\pi = p$.

For a given π , the solutions \underline{u} of $N\underline{u} = p$ correspond bijectively to k -tuples of integers (ν_1, \dots, ν_k) such that

$$u_i = \pi^{\nu_i},$$

with $0 \leq \nu_i \leq 1$ and at least one of the ν_i is $= 1$. The number of such tuples is equal to $2^k - 1$ (all tuples except $(0, \dots, 0)$).

The number of solutions of $N\pi = p$ is $1 + \chi(p)$ for all primes p , and the lemma follows. □

Proposition 5.15 is a consequence of (5.37) and Lemmas 5.26 and 5.27, applying to ρ the following very standard result (compare Section 5.4) applied with $\gamma = 2^k - 1$.

Lemma 5.28. *Let $\rho(n)$ be a multiplicative arithmetic function satisfying:*

(i) *There exists $A > 0$ such that*

$$(5.40) \quad \rho(n) \leq d(n)^A \text{ for all } n \geq 1,$$

(ii) *There exists an integer γ such that for all primes p we have $\rho(p) = \gamma(1 + \chi(p))$.*

Then there exists $c > 0$ such that

$$\sum_{n \leq X} \frac{\rho(n)}{n} \sim c(\log X)^\gamma$$

as $X \rightarrow +\infty$.

Proof. Let

$$z(s) = \sum_{n \geq 1} \rho(n)n^{-s}$$

be the Dirichlet generating series of ρ . By (i), the series converges and defines a holomorphic function for $\operatorname{Re}(s) > 1$. By multiplicativity, $z(s)$ has an absolutely convergent Euler product expansion

$$z(s) = \prod_{\chi(p)=1} (1 + 2\gamma p^{-s} + \rho(p^2)p^{-2s} + \dots) \prod_{\chi(p)=0} (1 + \gamma p^{-s} + \dots) \prod_{\chi(p)=-1} (1 + \rho(p^2)p^{-2s} + \dots).$$

Hypothesis (ii) implies that one can factorize

$$z(s) = \zeta_K(s)^\gamma z_1(s)$$

where $z_1(s)$, first defined by this equation for $\operatorname{Re}(s) > 1$, admits analytic continuation to a holomorphic function on $\operatorname{Re}(s) > 1/2$. Indeed one has

$$\zeta_K(s) = \prod_{\chi(p)=1} (1 - 2p^{-s} + p^{-2s})^{-1} \prod_{\chi(p)=-1} (1 - p^{-2s})^{-1},$$

so the products over split and inert primes already converge for $\operatorname{Re}(s) > 1/2$, while the coefficient of p^{-s} in the p -Euler factor for $z_1(s)$ vanishes.

Since $\zeta_K(s)$ has a simple pole at $s = 1$, it follows that $z(s)$ has a pole of order γ at $s = 1$, so a standard contour integration proves the lemma. \square

For $k = 1$, we can easily get rid of the annoying factor $\log \log X$, as mentioned in Remark 5.5.

Proposition 5.29. *We have*

$$\sum_{\substack{u \in \mathcal{U} \\ Nu \leq X}} \frac{\phi_1(1, u)}{Nu} \ll (\log X)$$

for $X \geq 2$, the implied constant depending only on K .

Proof. We allow ourself to be a little sketchy: we have

$$\phi_1(1, u) = \prod_{\mathfrak{p} | Nu(u-\bar{u})} (1 + (N\mathfrak{p})^{-1}).$$

Assume $K = \mathbf{Q}(\sqrt{-4D})$ with $4D$ a fundamental discriminant $4D \equiv 0 \pmod{4}$ so that $(1, \sqrt{-D})$ is a \mathbf{Z} -basis of \mathcal{O}_K (the remaining case being similarly treated) and $N(a + b\sqrt{-D}) = a^2 + Db^2$.

By trivial estimate, we have for $u = a + b\sqrt{-D}$

$$\phi_1(1, u) \leq \frac{\psi(2D)}{2D} \frac{\psi(a^2 + Db^2)}{a^2 + Db^2} \frac{\psi(b)}{b},$$

(recall ψ is defined in (2.10)). Hence

$$\sum_{\substack{u \in \mathcal{U} \\ Nu \leq X}} \frac{\phi_1(1, u)}{Nu} \leq 2 \sum_{d \leq X} \frac{\mu(d)^2}{d} \sum_{0 \leq |b| \leq (X/d)^{1/2}} \frac{\psi(b)}{b} \sum_{\substack{0 \leq a \leq \sqrt{X-Db^2} \\ d|a^2+Db^2}} \frac{1}{a^2 + Db^2}.$$

The contribution of $b = 0$ is $\ll 1$ (since $d \mid a^2$ and d squarefree imply $d \mid a$). For $|b| \geq 1$, in the inner sum we write $a = da_1 + \alpha$ for some α , $0 \leq \alpha < d$, such that $\alpha^2 = -Db^2 \pmod{d}$. For given α , by partial summation, the inner sum over a_1 is easily seen to be $\ll (bd\sqrt{D})^{-1}$, uniformly in α . The result then follows since the number of α for a given squarefree d is at most the number of divisors of d , and

$$\sum_{b \leq (X/D)^{1/2}} \frac{\psi(b)}{b^2} \ll \log X, \text{ and } \sum_{n \geq 1} \frac{d(n)\mu(n)^2}{n^2} < +\infty.$$

□

Extending this kind of argument for $k \geq 2$ might be possible although certainly cumbersome since the various u_i would become mixed up together. The issue is whether $\text{disc}(\underline{u})$ can have too often very small prime factors, and doesn't seem completely trivial.

5.6. The elliptic splitting problem. Because the condition $d \mid d_1(\mathfrak{p})$ is equivalent to the congruence $\sigma_{\mathfrak{p}} \equiv 1 \pmod{d}$ in the endomorphism ring of E , we can again apply sieve to obtain a Brun-Titchmarsh inequality for totally split primes in $K(E[d])$ for a CM curve. In particular, the extension $K(E[\infty])/K$ is a Brun-Titchmarsh field for a CM curve.

Theorem 5.30. *Let E/H be a CM curve with complex multiplication by an order \mathcal{O} of a quadratic field K/\mathbf{Q} , and $H' = H(E[\infty])$ its division field. Assume that H contains K . Then H'/H is a Brun-Titchmarsh field corresponding to the restriction of scalars $G = \text{Res}_{\mathcal{O}/\mathbf{Z}}(\mathbf{G}_m)$.*

First remark that the extension H'/H enters in the setup described in Section 3.5 for the general Brun-Titchmarsh problem, because of part 1 of Theorem 2.1 and the general ramification properties of $E[d]$.

Proposition 5.31. *Let H be a number field, E/H an elliptic curve with CM by an order $\mathcal{O} \subset K \subset H$ and let $d \geq 1$ be an integer. We have*

$$\pi_E(X; d, 1) \ll [H : \mathbf{Q}] \frac{X}{\varphi_{\mathcal{O}}(d)(\log X/d^2)}$$

for $d \leq X$, where the implied constant is absolute and $\varphi_{\mathcal{O}}(d) = |(\mathcal{O}/d\mathcal{O})^\times|$.

This proposition clearly implies the theorem since $\text{Gal}(H(E[d])/H)$ is of bounded index in $G(\mathbf{Z}/d\mathbf{Z}) = (\mathcal{O}/d\mathcal{O})^\times$. In turn, since \mathfrak{p} is split in $H(E[d])/H$ if and only if the Frobenius $\psi(\mathfrak{p})$ satisfies $\psi(\mathfrak{p}) \equiv 1 \pmod{d}$, it follows immediately from Lemma 5.2 and the next proposition:

Proposition 5.32. *Let K/\mathbf{Q} be an imaginary quadratic field. Then*

$$\pi_K(X; d, 1) \ll_K \frac{X}{\varphi_K(d)(\log X/d^2)}$$

the implied constant depending only on K .

Proof. This is almost a (simpler) special case of Proposition 5.14 (for $k = 1$ with d instead of u ; it is not included in that Proposition since the latter assumes $u \notin \mathbf{Z}$), so we can be very sketchy. One applies the large sieve, as in Section 5.4, to sieve

$$M = \{z \in \mathcal{O}_K \mid h(z) \leq \sqrt{X}/d\}$$

by primes \mathfrak{p} with $N\mathfrak{p} \leq \sqrt{X}/d = Q$, with $\Omega(\mathfrak{p}) = \{-1/d \pmod{\mathfrak{p}}\}$, if \mathfrak{p} does not divide d and $\Omega(\mathfrak{p}) = \emptyset$ otherwise. By Corollary 5.18 we derive

$$\pi_K(X; d, 1) \ll \frac{X}{d^2} \frac{1}{J}$$

with

$$J = \sum_{N\mathfrak{n} \leq Q}^b \prod_{\substack{\mathfrak{p} \mid \mathfrak{n} \\ (d, \mathfrak{p})=1}} \frac{1}{N\mathfrak{p} - 1}.$$

Evaluating this sum in the usual manner, the result follows. □

Note the following simple corollary of Theorem 5.30 for the elliptic splitting problem, which is still not very strong however (recall the expected order of magnitude is X).

Corollary 5.33. *Let E/H and K be as in the proposition. We have*

$$S_E(X; d_1) \ll_E X(\log X)^{1/2}$$

for $X \geq 2$.

Proof. We split the sum

$$S_E(X; d_1) = \sum_{d \leq \sqrt{X}+1} \varphi(d) \pi_E(X; d, 1)$$

in two ranges $d \leq B$ and $B < d \leq \sqrt{X} + 1$ where $B = (\sqrt{X} + 1)/A$ for some $A \geq 1$ to be chosen later. In the first range, applying the Brun-Titchmarsh inequality yields

$$\begin{aligned} \sum_{d \leq B} \varphi(d) \pi_E(X; d, 1) &\ll_E \frac{X}{\log X/B^2} \sum_{d \leq B} \frac{\varphi(d)}{\varphi_K(d)} \\ &\ll_E X \frac{\log(\sqrt{X}/A)}{\log A}. \end{aligned}$$

In the other range, we use instead the trivial bound coming from Lemma 5.2 and overcounting all integers $z \in \mathcal{O}_K$ instead of only prime elements, which gives

$$\pi_E(X; d, 1) \ll_K [H : \mathbf{Q}] |\{z \in \mathcal{O}_K \mid Nz \leq X \text{ and } z \equiv 1 \pmod{d}\}| \ll_K [H : \mathbf{Q}] \left(\frac{X}{d^2} + 1 \right).$$

Hence

$$\sum_{B < d \leq \sqrt{X}+1} \varphi(d) \pi_E(X; d, 1) \ll_K [H : \mathbf{Q}] X \sum_{B < d \leq \sqrt{X}+1} \frac{\varphi(d)}{d^2} \ll_K [H : \mathbf{Q}] X \log A.$$

We now choose $A = \exp(\sqrt{\log X})$ and it follows that

$$S_E(X; d_1) \ll_E X(\log X)^{1/2},$$

as desired. □

Remark 5.34. The Brun-Titchmarsh property and the Bombieri-Vinogradov Theorem in K can be used to prove a (weak) lower bound

$$S_E(X; d_1) \gg_E X \frac{\log \log X}{\log X}$$

(better than the trivial lower bound $X/\log X$ arising by taking the single term $d = 1$ in (3.2) only by $\log \log X$). The factor $\varphi(d)$ is the reason of the difficulties in the direction of lower bounds.

6. LOCAL STUDY OF TOTALLY SPLIT PRIMES

We now change the point of view, motivated by the considerations of the previous sections. We wish to understand, given $d \geq 1$, for which finite fields \mathbf{F}_q does there exist *some* elliptic curve E/\mathbf{F}_q with $d_1(E) = d$, or more generally with its d -torsion points rational over \mathbf{F}_q . In the cyclotomic case the answer is simple: \mathbf{F}_q contains all the d -th roots of unity if and only if $q \equiv 1 \pmod{d}$. And the analogue of d_1 is the largest d for which all d -th roots of unity are in \mathbf{F}_q , therefore it is simply $q - 1$.

We will first study this question using the methods introduced by Deuring [De]. The results can also be extracted from papers of Schoof [Sc-2], Howe [Ho], Tsfasman-Vladut [TV] (and maybe others I have not seen). But those are written with a slightly different emphasis. Then we recover similar results using modular curves and the trace formula, before giving some applications.

6.1. Results using endomorphism rings. We first deal quickly with the case of supersingular elliptic curves.

Proposition 6.1. *Let E/\mathbf{F}_q be a supersingular elliptic curve over a finite field with characteristic p . We have*

$$(6.1) \quad d_1(E) \leq 2$$

unless E satisfies $a(E)^2 = 4q$, in which case

$$(6.2) \quad d_1(E) = \begin{cases} \sqrt{q} + 1 & \text{if } a(E) = -2\sqrt{q} \\ \sqrt{q} - 1 & \text{if } a(E) = 2\sqrt{q}. \end{cases}$$

Proof. All this is contained in [Sc-2, Lemma 4.8] for instance, but most of it is easy to see. For instance, if $a(E)^2 = 4q$ (so q is a square) the Frobenius σ is a solution of the quadratic equation $X^2 - a(E)X + q = 0$, which has the double root $\pm\sqrt{q} \in \mathbf{Z}$ (with sign chosen as in the statement of the proposition). So $\sigma - 1 \in \mathbf{Z} \subset \text{End}(E)$, and Lemma 2.6 implies (6.2).

For the other cases, it is known that $a(E)^2 = q, 2q$ or $3q$, or $a(E) = 0$. If $a(E) = 0$ (the only possibility over \mathbf{F}_p), for instance, the congruence $a(E) \equiv 2 \pmod{d_1(E)}$ proves (6.1). Similarly in the other cases the congruences of Lemma 2.6 either prove (6.1), or a weaker bound like $d_1(E) \leq 4$, which will suffice here (see [Sc-2, Lemma 4.8] for complete details). \square

This has the following global corollary which shows that supersingular primes have a small contribution to (3.1).

Corollary 6.2. *Let E/\mathbf{Q} be an elliptic curve. We have*

$$(6.3) \quad \sum_{\substack{p \leq X \\ a_p(E)=0}} d_1(E) \ll_E \frac{X}{\log X} \quad \text{if } E \text{ has CM}$$

$$(6.4) \quad \sum_{\substack{p \leq X \\ a_p(E)=0}} d_1(E) \ll_E X^{3/4} \quad \text{otherwise.}$$

for all $X \geq 2$, the implied constant depending on E only.

Proof. If E has CM, the number of supersingular primes $p \leq X$ is well known to be (see e.g. [LT]) $\sim X/(2 \log X)$, while if E doesn't have CM, Elkies [El] has shown that the number of supersingular primes $p \leq X$ of E is $\ll_E X^{3/4}$. Since $d_1(p) \leq 2$ by Proposition 6.1, the result follows. \square

Remark 6.3. In the non-CM case, Serre's proof [Se-4] that the number of supersingular primes $\leq X$ is $o(X/\log X)$ suffices to show that

$$\sum_{\substack{p \leq X \\ a_p(E)=0}} d_1(E) = o\left(\frac{X}{\log X}\right)$$

as $X \rightarrow +\infty$.

From now on we assume that E/\mathbf{F}_q is an ordinary elliptic curve over a finite field with q elements. We let $\mathcal{O} = \text{End}(E)$, K the field of fractions of \mathcal{O} , \mathcal{O}_K the ring of integers of K . Let $\sigma \in \mathcal{O}$ be the Frobenius endomorphism of E . The main tool to find $d_1(E)$ is Lemma 2.6.

Lemma 6.4. *Let $d \geq 1$ be an integer. We have $d \mid \sigma - 1$ in \mathcal{O}_K if and only if $a(E) \equiv 2 \pmod{d}$ and $n(E) = q + 1 - a(E) \equiv 0 \pmod{d^2}$.*

Proof. Let $\sigma' = (\sigma - 1)/d \in K$, so $d \mid \sigma - 1$ in \mathcal{O}_K if and only if $\sigma' \in \mathcal{O}_K$. But since $\sigma' \notin \mathbf{Z}$, since E is ordinary, its minimal polynomial over \mathbf{Z} is

$$(X - \sigma')(X - \bar{\sigma}') = X^2 - \frac{a(E) - 2}{d}X + \frac{n(E)}{d^2}.$$

Hence the result since \mathcal{O}_K is the integral closure of \mathbf{Z} in K . \square

We can check that this gives back the other congruences.

Lemma 6.5. *Let $a, q \geq 2, d \geq 1$ be integers such that*

$$\begin{cases} a \equiv 2 \pmod{d} \\ q + 1 - a \equiv 0 \pmod{d^2}. \end{cases}$$

Then $q \equiv 1 \pmod{d}$ and $a^2 - 4q \equiv 0 \pmod{d^2}$.

Proof. We have modulo d

$$0 = q + 1 - a = q + 1 - 2 = q - 1$$

and modulo d^2

$$a^2 - 4q = (q + 1)^2 - 4q = (q - 1)^2 = 0.$$

□

Lemma 6.6. *Let E/\mathbf{F}_q as before. We have $d \mid \sigma - 1$ in \mathcal{O}_K if and only if $a^2 - 4q \equiv 0 \pmod{d^2}$ and $n(E) \equiv 0 \pmod{d^2}$.*

Proof. Let again $\sigma' = (\sigma - 1)/d \in K$. In terms of σ' , the two assumptions are

$$\begin{aligned} N(\sigma - 1) &= d^2 N \sigma' \equiv 0 \pmod{d^2} \\ (\sigma - \bar{\sigma})^2 &= d^2 (\sigma' - \bar{\sigma}')^2 \equiv 0 \pmod{d^2}, \end{aligned}$$

hence we see that $N \sigma' \in \mathbf{Z}$ and $(\sigma' - \bar{\sigma}')^2 \in \mathbf{Z}$.

The latter is also $(\sigma' + \bar{\sigma}')^2 - 4N \sigma'$, hence we deduce that $(\text{Tr } \sigma')^2 \in \mathbf{Z}$. Since $\text{Tr}(\sigma') \in \mathbf{Q}$, it must be an integer, hence the result. □

Those easy results give a good handle on the condition $d \mid \sigma - 1$ in \mathcal{O}_K . The problem is that \mathcal{O} is in general a proper order in \mathcal{O}_K . However, the necessary congruence conditions are also sufficient “up to isogeny”.

Proposition 6.7. *Let \mathbf{F}_q be a finite field with q elements, $d \geq 1$ an integer coprime with q .*

There exists an ordinary elliptic curve E/\mathbf{F}_q with $E[d] \subset E(\mathbf{F}_q)$, i.e. $d \mid d_1(E)$, if and only if there exists $a \in \mathbf{Z}$ such that

$$\begin{cases} |a| < 2\sqrt{q} \\ (a, q) = 1 \\ a \equiv 2 \pmod{d} \\ q + 1 - a \equiv 0 \pmod{d^2}. \end{cases}$$

For the proof we need some results which are part of Honda-Tate theory for elliptic curves (which goes back to Deuring), and others due to Waterhouse [Wa] concerning the endomorphism rings of elliptic curves over finite fields.

Theorem 6.8. *(Deuring, Honda, Tate) Let \mathbf{F}_q be a finite field with q elements. Given an integer a such that $|a| < 2\sqrt{q}$ and $(a, q) = 1$, there exists an ordinary elliptic curve E over \mathbf{F}_q with $a(E) = a$.*

See for instance [Wa, Th. 4.1].

Theorem 6.9. *(Deuring, Waterhouse) Let \mathbf{F}_q be a finite field with q elements, a an integer with $|a| < 2\sqrt{q}$ and $(a, q) = 1$. Let $K = \mathbf{Q}(\sqrt{a^2 - 4q})$ and let \mathcal{O} be an order of K . There exists an ordinary elliptic curve E/\mathbf{F}_q with $a(E) = a$ and $\text{End}(E) = \mathcal{O}$ if and only if \mathcal{O} contains the roots of*

$$X^2 - aX + q = 0.$$

See [Wa, Th. 4.2 (2)]. Note that this second result requires Tate’s Theorem identifying relating isogenies between elliptic curves with Galois-invariant maps between their ℓ -adic Tate modules, $(\ell, q) = 1$.

Proof of Proposition 6.7. The condition is necessary. Conversely, if a exists as described, Theorem 6.9 shows that there exists E/\mathbf{F}_q with $a(E) = a$ and $\text{End}(E) = \mathcal{O}_K$, where K is the imaginary quadratic field $K = \mathbf{Q}(\sqrt{a^2 - 4q})$.

The congruence conditions on $a(E)$ and $n(E)$ then mean (Lemma 6.4) that $d \mid \sigma - 1$ in $\mathcal{O}_K = \text{End}(E)$, hence $d \mid d_1(E)$. \square

Remark 6.10. If $q = p \geq 5$ is prime, one can remove the condition $(a, p) = 1$ on a from the statement of the proposition. Indeed, if $p \mid a$, we have $a = 0$, and since $a \equiv 2 \pmod{d}$, the only values of d occurring are $d = 1$ and $d = 2$. But those can be obtained from ordinary elliptic curves: $d = 1$ by any E , and $d = 2$ by a Legendre curve

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

(which always has $2 \mid d_1(E_\lambda)$) for some $\lambda \in \mathbf{F}_p - \{0, 1\}$. Indeed, the condition that E_λ be ordinary is equivalent (see e.g. [Si-1, V-4]) to $H_p(\lambda) \neq 0$, where H_p is the Hasse-Deuring polynomial

$$H_p = \sum_{j=0}^{(p-1)/2} \binom{(p-1)/2}{j} X^j \in \mathbf{F}_p[X].$$

Since $0 \leq \deg H_p = (p-1)/2 < p-2$, there is a $\lambda \in \mathbf{F}_p - \{0, 1\}$ which is not a root of H_p , hence a corresponding ordinary E_λ with $2 \mid d_1(E_\lambda)$.

On the other hand, if q is a square, let $d = \sqrt{q} + 1$. Then d satisfies all the assumptions of Proposition 6.7 with $a = -2\sqrt{q}$, except $(a, q) = 1$. But this is the only value of $a(E)$ for which one could have $d \mid d_1(E)$, and it corresponds to supersingular curves, so that in general $(a, q) = 1$ is a necessary assumption.

In applications, we are interested in the invariant $d_1(E)$, and $d = d_1(E)$ means not only $E[d] \subset E(\mathbf{F}_q)$, but also that no larger d (coprime with q) satisfies this. However, Proposition 6.7 remains true with $d = d_1(E)$ instead of $d \mid d_1(E)$ in the conclusion.

Proposition 6.11. *Let E/\mathbf{F}_q be an elliptic curve over a finite field with $d_1(E) = d$. For every $\delta \mid d$, there exists an elliptic curve E'/\mathbf{F}_q which is \mathbf{F}_q -isogenous to E and satisfies $d_1(E') = \delta$.*

Corollary 6.12. *Let \mathbf{F}_q and $d \geq 1$, $(d, q) = 1$, be as above. There exists an ordinary elliptic curve E/\mathbf{F}_q with $d_1(E) = d$ if and only if there exists $a \in \mathbf{Z}$ with $|a| < 2\sqrt{q}$, $(a, q) = 1$, and such that*

$$\begin{cases} a \equiv 2 \pmod{d} \\ q + 1 - a \equiv 0 \pmod{d^2}. \end{cases}$$

Proof of the proposition. Write $d = \delta\delta'$. We have, with the same notation as usual, $\sigma' = (\sigma - 1)/d \in \mathcal{O}$. It suffices to find a smaller order $\mathcal{O}' \subset \mathcal{O}$ with $\delta'\sigma' = (\sigma - 1)/\delta \in \mathcal{O}'$ but for which there is no $e > 1$ with $\delta'\sigma'/e \in \mathcal{O}'$. Then, since $\sigma \in \mathcal{O}'$, Theorem 6.9 shows that there exists E'/\mathbf{F}_q , isogenous to E (hence ordinary), with $\text{End}(E') = \mathcal{O}'$. Then $d_1(E') = \delta$ by construction (Lemma 2.6).

To construct \mathcal{O}' , we write $\mathcal{O} = \mathbf{Z} \oplus \omega\mathbf{Z}$ (see [Cox, 7-A]), and correspondingly $\sigma' = m + n\omega$, for some $m, n \in \mathbf{Z}$. So $\delta'\sigma' = \delta'm + \delta'n\omega$. Let \mathcal{O}' be the order $\mathbf{Z} \oplus c n \omega \mathbf{Z}$ of K . Then $\delta'\sigma' \in \mathcal{O}'$, but for any $e \geq 1$, we have

$$\frac{\delta'\sigma'}{e} = \frac{m\delta'}{e} + \frac{\delta'n\omega}{e}$$

and for this to be in \mathcal{O}' we must have $e = 1$, showing that \mathcal{O}' satisfies the conditions required. \square

Remark 6.13. Over the base field \mathbf{F}_p , it is again possible to remove the condition $(a, p) = 1$. Putting back supersingular curves, the following statement holds:

Let $d \geq 1$ be an integer. There exists an elliptic curve E over \mathbf{F}_p with $d_1(E) = d$ if and only if there exists a , $|a| < 2\sqrt{p}$, such that

$$\begin{cases} a \equiv 2 \pmod{d} \\ p + 1 - a \equiv 0 \pmod{d^2}. \end{cases}$$

In particular, this is always true for $d = 1$ and $d = 2$ (the latter for $p \geq 5$).

Remark 6.14. As a side remark and pretext to mention another interesting problem of analytic number theory, the case $d = 1$ can be studied purely analytically from Theorem 6.8 and the distribution of squarefree numbers in short intervals. Indeed, if $a \neq 0$ is such that $p + 1 - a$ is squarefree, any elliptic curve E/\mathbf{F}_p with $a(E) = a$ must have $d_1(E) = 1$. Hence the existence of such an E (for p large enough only, however) follows from any “non-trivial” estimate for error term in the asymptotic formula for the number of squarefree numbers $n \leq X$

$$\sum_{n \leq X} |\mu(n)| = \frac{1}{\zeta(2)} X + O(X^\theta)$$

as $X \rightarrow +\infty$, with $\theta < 1/2$, since this implies in particular

$$\sum_{|a| < 2\sqrt{p}} |\mu(p + 1 - a)| > 0.$$

The value $\theta = 1/2$ is easily obtained, any improvement requiring non-trivial cancellation in some exponential sums. See for instance [GK, p. 46] where it is shown that $\theta = 4/9 + \varepsilon$ is possible, for any $\varepsilon > 0$.

6.2. Results using the trace formula. The criterion obtained in Corollary 6.12 is quite convenient. However, from our point of view, it is more natural to fix a prime p (or prime power) and look for which $d \mid p - 1$ there exists E/\mathbf{F}_p with $d_1(E) = d$.

A criterion of that type arises naturally if we use, instead of endomorphism rings, the theory of modular curves and the Eichler-Selberg trace formula. Although Corollary 6.12 and Remark 6.13 would suffice for the applications in the next section, this approach is sufficiently independent and instructive to be included here.

Theorem 6.15. *Let p be a prime number, $d \mid p - 1$ an integer. Write $d = ef$ with $(e, 2) = 1$, $f \mid 2^\infty$. There exists E/\mathbf{F}_p with $d_1(E) = d$ if and only if there exists a with $|a| < 2\sqrt{p}$ such that*

- (1) *We have $e^2 \mid a^2 - 4p$;*
- (2) *If $f \neq 1$, there exists $\varepsilon = \pm 1 \pmod{f}$ such that $\varepsilon^2 - a\varepsilon + p = 0 \pmod{f^2}$.*

We need some geometric preliminaries. For any integer $d \geq 1$, there exists a smooth affine curve $Y(d)$ naturally defined over $\mathbf{Q}(\mu_d)$, with good reduction at all primes $p \nmid d$, which is a coarse moduli scheme for “elliptic curves with a d -level structure” (see [KaMa] or [DR]). Over \mathbf{C} , $Y(d)(\mathbf{C})$ is the “usual” quotient

$$\Gamma(d) \backslash \mathbf{H}$$

of the upper half-plane by the principal congruence subgroup

$$\Gamma(d) = \{g \in SL(2, \mathbf{Z}) \mid g \equiv 1 \pmod{d}\}.$$

Moreover, $Y(d)$ has an integral model over the ring of integers $\mathbf{Z}[\mu_d]$ of the cyclotomic field $\mathbf{Q}(\mu_d)$. Notice that $p \equiv 1 \pmod{d}$ means that the p is totally split in this field, hence $\mathbf{Z}[\mu_d]/(p) \simeq (\mathbf{F}_p)^{\varphi(d)}$. The above “moduli scheme” sentence implies in particular (see [DR, VI-3]) that for $p \equiv 1 \pmod{d}$, it is the same to give a point in $Y(d)(\mathbf{F}_p)$ as to give a pair $(E, (e_1, e_2))$ of an elliptic curve E/\mathbf{F}_p together with two \mathbf{F}_p -rational points e_1, e_2 of order d , such that the Weil pairing $\langle e_1, e_2 \rangle$ is equal to a fixed primitive d -th root of unity (these pairs taken up to isomorphism). In other words we have (see also [Ho] for a description of other modular curves over finite fields):

Lemma 6.16. *Let p be a prime number, $d \geq 1$ an integer such that $d \mid p - 1$. Then there exists E/\mathbf{F}_p with $E[d] \subset E(\mathbf{F}_p)$ if and only if $Y(d)(\mathbf{F}_p) \neq \emptyset$.*

We are thus reduced to finding points on the curve $Y(d)$ over the finite field \mathbf{F}_p .

The curve $Y(d)$ has a natural compactification $X(d)$, which over \mathbf{C} amounts to adding the cusps to \mathbf{H} before taking the quotient by $\Gamma(d)$. The projective curve $X(d)$ has also good

reduction at all p not dividing d (and a moduli description in terms of “generalized elliptic curves”).

For p a prime of good reduction, the local zeta function of $X(d)$

$$Z(X(d), p) = \exp\left(\sum_{n \geq 1} \frac{|X(d)(\mathbf{F}_{p^n})|}{n} T^n\right)$$

is, by general results (due to F.K. Schmidt in this case of curves over finite fields), a rational function of the form

$$Z(X(d), p) = \frac{P_d(T)}{(1-T)(1-pT)},$$

where $P_d(T)$ is a polynomial of degree $2g(d)$, $g(d)$ being the genus of $X(d)$. From this and the definition of $Z(X(d), p)$, one can deduce immediately that

$$|X(d)(\mathbf{F}_p)| = p + 1 - \sum_i \alpha_i$$

where

$$P_d = \prod_{i=1}^{2g(d)} (1 - \alpha_i T).$$

The point of using the compactified curve $X(d)$ is that we have the following consequence of the computation of the zeta functions of modular curves by Shimura ([Sh-1, §7.5]).

Theorem 6.17. *Let $d \geq 1$ be an integer, $p \equiv 1 \pmod{d}$ a prime number. We have*

$$|X(d)(\mathbf{F}_p)| = p + 1 - \text{Tr}(T_p | S_2(\Gamma(d))),$$

where the last term is the trace of the Hecke operator T_p acting on the space $S_2(\Gamma(d))$ of weight 2 holomorphic cusp forms for the congruence subgroup $\Gamma(d)$.

More precisely, Shimura’s result gives the zeta function for models of $X(d)$ over \mathbf{Q} , of which there exist several; but all give the same $X(d)$ over $\mathbf{Q}(\mu_d)$, hence the result since we consider p totally split in $\mathbf{Q}(\mu_d)$.

The Eichler-Selberg trace formula gives an expression for the trace, which one may use to find when $X(d)(\mathbf{F}_p) \neq \emptyset$; this idea is used by Jordan [Jo]. However, he works with Shimura curves, which are compact, and his main interest is at primes of bad reduction.

Here we have to take the cusps into account, since they do not correspond to elliptic curves. Over \mathbf{C} , the cusps of $X(d)$ are described in [Sh-1, Lemma 1.42]. We need to know which are rational over \mathbf{F}_p .

Let $\varphi^+(d)$ denote the number of even Dirichlet characters modulo d (i.e. $\chi(-1) = 1$). This is given by

$$(6.5) \quad \varphi^+(d) = \begin{cases} \frac{\varphi(d)}{2} & \text{if } d > 2 \\ \varphi(d) = 1 & \text{if } d = 2. \end{cases}$$

By orthogonality of characters, we have for any $x \in \mathbf{Z}$

$$(6.6) \quad \sum_{\chi \text{ even}} \chi(x) = \begin{cases} \varphi^+(d) & \text{if } x \equiv \pm 1 \pmod{d} \\ 0 & \text{otherwise.} \end{cases}$$

(This will be needed later on).

Lemma 6.18. *Let $d \geq 1$ be an integer, $p \equiv 1 \pmod{d}$ a prime number. All the cusps of $X(d)$ are \mathbf{F}_p -rational, and in particular*

$$|(X(d) - Y(d))(\mathbf{F}_p)| = \varphi^+(d)\psi(d) = \begin{cases} \frac{1}{2}\varphi(d)\psi(d) & \text{if } d > 2 \\ \varphi(d)\psi(d) & \text{if } d = 2. \end{cases}$$

Proof. This follows from Theorem 10.9.1 (3) of [KaMa] which says (in particular) that the cusps of $Y(d)/\mathbf{Z}[\mu_d]$ are rational over $\mathbf{Z}[\mu_d]$, and “do not vary” by base change to any $\mathbf{Z}[\mu_d]$ -algebra; heuristically, cusps rational over \mathbf{F}_p “correspond” to level d structures on the Tate curve $Tate(q)/\mathbf{F}_p((q))$ rational over $\mathbf{F}_p((q))$. Since the d -torsion of the latter is isomorphic as a Galois module ([Si-2, V-3]) to

$$\mathbf{Z}/d\mathbf{Z} \times \mu_d$$

and $d \mid p-1$ so $\mu_d \subset \mathbf{F}_p^\times$, it is visible that all level d structures on $Tate(q)$ are $\mathbf{F}_p((q))$ -rational.

The number of cusps over \mathbf{C} is found in [Sh-1, p. 22], or can be recomputed directly from the result in [KaMa] quoted above. \square

We will now state the trace formula in the form needed. A paper by Fomenko [Fom] should include it, but I have not been able to see it. On the other hand, the trace formula for $\Gamma(d)$ is not easily derived from general accounts: for instance, it does not correspond to an “Eichler order”, so the arguments in [Mi, Ch. 6], for instance, can not be adapted straightforwardly. We can circumvent these difficulties by reducing to the much better known case of Hecke congruence subgroups $\Gamma_0(N)$, for which we can quote for instance [Mi], [Se-5] or [Ha] (among many other non-conflicting sources).

Lemma 6.19. *Let $d \geq 1$ an integer and $p \equiv 1 \pmod{d}$ a prime number. There exists an isomorphism of vector spaces*

$$u : S_2(\Gamma(d)) \longrightarrow \bigoplus_{\chi \text{ even}} S_2(\Gamma_0(d^2), \chi)$$

where the direct sum is over all even Dirichlet characters modulo d , $S_2(\Gamma_0(d^2), \chi)$ is the space of weight 2 cusp forms for $\Gamma_0(d^2)$ with nebentypus χ , which satisfies

$$u \circ T_p = T_p \circ u,$$

where on the right T_p is the direct sum of Hecke operators acting on $S_2(\Gamma_0(d^2), \chi)$.

Proof. We first introduce the congruence subgroups

$$\Gamma_0(d, d) = \left\{ g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbf{Z}) \mid b = c = 0 \pmod{d} \right\}.$$

We have $\Gamma(d) \triangleleft \Gamma_0(d, d)$ with quotient $(\mathbf{Z}/d\mathbf{Z})^\times$.

The even Dirichlet characters modulo d are extended to characters of $\Gamma_0(d, d)$ by

$$\chi(g) = \chi(d).$$

Then the natural action of $\Gamma_0(d, d)/\Gamma(d)$ on $S_2(\Gamma(d))$ gives the direct sum decomposition

$$S_2(\Gamma(d)) = \bigoplus_{\chi \text{ even}} S_2(\Gamma_0(d, d), \chi)$$

(for odd χ , $S_2(\Gamma_0(d, d), \chi) = 0$).

Since $d \mid p-1$, we have $\chi(p) = 1$ for any character modulo d , and this implies that T_p acting on $S_2(\Gamma(d))$ is the direct sum of the T_p acting on $S_2(\Gamma_0(d, d), \chi)$ (see [Sh-1, 3.5.6]; it amounts to the fact that a $\chi(p)$ appears in the explicit formula for T_p acting on $S_2(\Gamma_0(d, d), \chi)$ but not for T_p on $S_2(\Gamma(d))$).

Moreover $\Gamma_0(d, d)$ is conjugate to $\Gamma_0(d^2)$ in $SL(2, \mathbf{R})$ by

$$g \mapsto \begin{pmatrix} d^{-1/2} & 0 \\ 0 & d^{1/2} \end{pmatrix} g \begin{pmatrix} d^{1/2} & 0 \\ 0 & d^{-1/2} \end{pmatrix}$$

This induces an isomorphism

$$(6.7) \quad S_2(\Gamma_0(d, d), \chi) \rightarrow S_2(\Gamma_0(d^2), \chi)$$

given by

$$f \mapsto f|_2 \begin{pmatrix} d^{1/2} & 0 \\ 0 & d^{-1/2} \end{pmatrix},$$

(where $\cdot|_2 \cdot$ denotes the usual weight 2 action of $SL(2, \mathbf{Z})$ on functions). Hence we have an isomorphism

$$u : S_2(\Gamma(d)) \rightarrow \bigoplus_{\chi \text{ even}} S_2(\Gamma_0(d^2), \chi).$$

Since T_p commutes with the isomorphism (6.7), as is well known (compare [Mi, 4.6.1]), u is also compatible. \square

Corollary 6.20. *Let $d \geq 1$ be an integer, $p \equiv 1 \pmod{d}$ a prime number. We have*

$$\mathrm{Tr} T_p | S_2(\Gamma(d)) = \sum_{\chi \text{ even}} \mathrm{Tr} T_p | S_2(\Gamma_0(d^2), \chi),$$

where the sum is over even Dirichlet characters modulo d .

To state the trace formula for $S_2(\Gamma_0(d^2), \chi)$, we require some further notation. Recall χ is an even character.

If \mathcal{O} is an order in an imaginary quadratic field, we let $H(\mathcal{O})$ denote its class number, divided by half the number of units (i.e. 1 unless $\mathcal{O} = \mathbf{Z}[i]$, where it's 2, or $\mathcal{O} = \mathbf{Z}[\mu_3]$, where it's 3). We denote by $\mathcal{O}(\delta)$ the order with discriminant $\delta < 0$, and let $H(\delta) = H(\mathcal{O}(\delta))$.

If $\mathcal{O} \subset \mathcal{O}(a^2 - 4p)$ is a sub-order with index f , and $N \geq 1$, we denote

$$(6.8) \quad \mu_\chi(\mathcal{O}, a, p, N) = \frac{\psi(N)}{\psi(N/(N, f))} \sum_{\substack{x \pmod{N} \\ x^2 - ax + p = 0 \pmod{N(N, f)}}} \chi(x)$$

(it makes sense).

Theorem 6.21. *Let $d \geq 1$ be an integer, χ an even Dirichlet character modulo d and $p \equiv 1 \pmod{d}$ a prime number. We have*

$$\mathrm{Tr} T_p | S_2(\Gamma_0(d^2), \chi) = t_d(\chi) - t_e(\chi) - t_h(\chi)$$

where

$$(6.9) \quad t_d(\chi) = \begin{cases} p + 1 & \text{if } \chi = 1 \\ 0 & \text{otherwise} \end{cases}$$

$$t_e(\chi) = \frac{1}{2} \sum_{\substack{a \in \mathbf{Z} \\ a^2 < 4p}} \sum_{\mathcal{O} \subset \mathcal{O}(a^2 - 4p)} H(\mathcal{O}) \mu_\chi(\mathcal{O}, a, p, d^2)$$

$$(6.10) \quad t_h(\chi) = \frac{1}{2} \sum_{b|p} \sum_{c|d^2} \varphi\left(\left(\frac{d^2}{c}, c\right)\right) \chi(y_c),$$

where y_c is an integer modulo $d^2 / ((d^2/c, c))$ such that

$$y_c \equiv b \pmod{c}$$

$$y_c \equiv p/b \pmod{d^2/c}.$$

Remark 6.22. The notation follows the genesis of these terms, for example in Shimura's formulation [Sh-2] of the trace formula as a kind of Lefschetz formula for correspondences: t_d refers to the "dual term", as it should be understood as coming from an H^2 , which is non-zero only for weight 2 and trivial character; t_e refers to the contribution of elliptic elements, and t_h to the contribution of hyperbolic elements. There is no parabolic contribution here because we are working with T_p and p is not a square.

Proof. Serre [Se-5, 4.1] quotes a general formula for all levels and characters. To deduce the form claimed, notice that the term denoted A_1 vanishes since p is not a square and the term

denoted A_4 gives directly t_d . The term $-A_3$, we claim, is the same as t_h . Indeed, we have from loc. cit.

$$-A_3 = \frac{1}{2} \sum_{b|p} \text{Inf}(b, p/b) \sum_c \varphi\left(\left(\frac{d^2}{c}, c\right)\right) \chi(y_c)$$

where the sum over c is restricted to divisors of d^2 such that

$$(6.11) \quad \left(\frac{d^2}{c}, c\right) \mid \frac{p}{b} - b$$

$$(6.12) \quad \left(\frac{d^2}{c}, c\right) \mid \frac{d^2}{d_\chi}$$

(d_χ is the conductor of χ). Now first for $b \mid p$ we have $\text{Inf}(b, p/b) = 1$, and also $p/b - b = \pm(p-1)$. Also, for all $c \mid d^2$, we have

$$(6.13) \quad \left(\frac{d^2}{c}, c\right) \mid d.$$

Indeed, proceeding locally at each prime ℓ , if $d = \ell^\nu$, and $c = \ell^\mu$ with $\mu \leq 2\nu$, the exponent of $(d^2/c, c)$ is $\text{Inf}(\mu, 2\nu - \mu) \leq \nu$.

Since $d_\chi \mid d$, and $d \mid p-1$, this shows that the two restrictions (6.11) and (6.12) on c are satisfied for all $c \mid d^2$.

Similarly, the term $-A_2$ in loc. cit. is the same as t_e (recall the weight is 2). \square

Corollary 6.23. *Let $d \geq 1$ an integer, $p \equiv 1 \pmod{d}$ a prime number. We have*

$$\text{Tr } T_p | S_2(\Gamma(d)) = p + 1 - t_e - t_h$$

where

$$t_e = \sum_{\chi \text{ even}} t_e(\chi)$$

$$t_h = \sum_{\chi \text{ even}} t_h(\chi).$$

The next observation is elementary but crucial.

Proposition 6.24. *Let $d \geq 1$ an integer, $p \equiv 1 \pmod{d}$ a prime number. Then t_h is equal to the number of \mathbf{F}_p -rational cusps of $X(d)$, i.e. $\varphi^+(d)\psi(d)$.*

Proof. The point is that the integer y_c in (6.10) can be chosen, for $b \mid p$ and any $c \mid d^2$, to satisfy

$$(6.14) \quad y_c \equiv 1 \pmod{d},$$

and since the character χ is modulo d (not d^2), we have $\chi(y_c) = 1$ for any χ .

To see (6.14), we work locally at all primes ℓ as before. We have $b = 1$ or $b = p$: both situations are similar, so assume $b = 1$. Then writing ℓ^ν for the ℓ -component of d , ℓ^μ for that of c , $\mu \leq 2\nu$, the conditions on y_c are

$$\begin{cases} y_c \equiv 1 & \pmod{\ell^\mu} \\ y_c \equiv p & \pmod{\ell^{2\nu-\mu}}. \end{cases}$$

We have either $\mu \geq \nu$, in which case the first equation implies $y_c \equiv 1 \pmod{\ell^\nu}$, or $2\nu - \mu > \nu$, in which case the second implies $y_c \equiv p \equiv 1 \pmod{\ell^\nu}$, since $p \equiv 1 \pmod{d}$. Those local congruences patch, proving the claim for $b = 1$, and $b = p$ is symmetric.

Using (6.6), and the fact that $b = 1$ and $b = p$ have the same contribution, we can now write t_h as

$$t_h = \varphi^+(d) \sum_{c|d^2} \varphi\left(\left(\frac{d^2}{c}, c\right)\right).$$

We now use $\delta = (d^2/c, c)$ as new summation variable. Recall that $\delta \mid d$ (6.13). We get

$$(6.15) \quad t_h = \varphi^+(d) \sum_{\delta \mid d} \varphi(\delta) M(\delta)$$

where

$$M(\delta) = |\{c \mid d^2 \mid (d^2/c, c) = \delta\}|.$$

We work again at each prime ℓ separately, with ℓ^ν the component of d , ℓ^ρ that of δ . The ℓ -component ℓ^μ of c must therefore satisfy

$$\text{Inf}(\mu, 2\nu - \mu) = \rho.$$

Given ρ , there are two choices of μ , namely $\mu = \rho$ or $\mu = 2\nu - \rho$ (since $\rho \leq \nu$), *unless* $\rho = \nu$, since in this case they coincide.

It is clear that

$$f(d) = \sum_{\delta \mid d} \varphi(\delta) M(\delta)$$

is multiplicative. Now we compute the value at ℓ^ν using the above: we have

$$\begin{cases} M(\ell^\rho) = 2 & \text{if } \rho < \nu \\ M(\ell^\nu) = 1, \end{cases}$$

so

$$\begin{aligned} f(\ell^\nu) &= \sum_{\rho=0}^{\nu-1} 2\varphi(\ell^\rho) + \varphi(\ell^\nu) \\ &= 2\ell^{\nu-1} + \ell^\nu - \ell^{\nu-1} \\ &= \psi(\ell^\nu). \end{aligned}$$

Comparing this and (6.15) with Lemma 6.18, the proposition is proved. \square

Remark 6.25. I did not find mention in the literature of this fact that the hyperbolic terms in the trace formula “count the cusps”, although that must be well-known. This applies obviously to more general subgroups, with corresponding applications to elliptic curves over finite fields using their moduli interpretation. It would be interesting to see if there are higher-rank analogues, and their consequences.

Corollary 6.26. *Let $d \geq 1$ an integer, $p \equiv 1 \pmod{d}$ a prime number. We have*

$$|Y(d)(\mathbf{F}_p)| = t_e.$$

In particular, there exists an elliptic curve E/\mathbf{F}_p with $E[d] \subset E(\mathbf{F}_p)$ if and only if $t_e > 0$.

Proof. We have by Proposition 6.24

$$\begin{aligned} |Y(d)(\mathbf{F}_p)| &= |X(d)(\mathbf{F}_p)| - t_h \\ &= p + 1 - \text{Tr } T_p - t_h \quad (\text{by Theorem 6.17}) \\ &= p + 1 - (p + 1 - t_e - t_h) - t_h \\ &= t_e. \end{aligned}$$

\square

Because of the average over χ , t_e is a sum of terms each of which is obviously ≥ 0 . This makes it possible to find a criterion to have $Y(d)(\mathbf{F}_p) \neq \emptyset$ (compare [Jo]). If the formula for t_e involved any oscillatory sum, it would be much harder to exploit it.

For a quadratic imaginary order $\mathcal{O} \subset \mathcal{O}(a^2 - 4p)$ with index f we let

$$\mu(\mathcal{O}, a, p, d^2) = \sum_{\chi \text{ even}} \mu_\chi(\mathcal{O}, a, p, d^2),$$

and

$$\mu(a, p, d^2) = \mu(\mathcal{O}(a^2 - 4p), a, p, d^2).$$

From (6.9) we have

$$(6.16) \quad t_e = \frac{1}{2} \sum_{\substack{a \in \mathbf{Z} \\ a^2 < 4p}} \sum_{\mathcal{O} \subset \mathcal{O}(a^2 - 4p)} H(\mathcal{O}) \mu(\mathcal{O}, a, p, d^2).$$

Lemma 6.27. *We have for an order $\mathcal{O} \subset \mathcal{O}(a^2 - 4p)$ of index f*

$$\mu(\mathcal{O}, a, p, d^2) = \frac{\varphi^+(d)\psi(d^2)}{\psi(d^2/(d^2, f))} \mu_0(a, p, d, f)$$

where

$$\mu_0(a, p, d, f) = |\{x \pmod{d^2} \mid x = \pm 1 \pmod{d} \text{ and } x^2 - ax + p = 0 \pmod{d^2/(d^2, f)}\}|$$

This is simply the orthogonality relation (6.6). We let $\mu_0(a, p, d) = \mu_0(a, p, d, 1)$.

Corollary 6.28. *Let $d \geq 1$ be an integer and $p \equiv 1 \pmod{d}$ a prime number. We have $Y(d)(\mathbf{F}_p) \neq \emptyset$ if and only if there exists an integer a with $|a| < 2\sqrt{p}$ such that $\mu(a, p, d) > 0$, if and only if there exists a with $|a| < 2\sqrt{p}$ such that the equation $x^2 - ax + p = 0 \pmod{d^2}$ has a solution x with $x = \pm 1 \pmod{d}$.*

Proof. From (6.16), we have $t_e > 0$ if and only if there exists a and $\mathcal{O} \subset \mathcal{O}(a^2 - 4p)$ with $\mu(\mathcal{O}, a, p, d^2) > 0$. But if this condition holds, seeing from the definition that

$$\mu(a, p, d^2) \geq \mu(\mathcal{O}, a, p, d^2),$$

we have $\mu(a, p, d^2) > 0$ also.

The last statement is a rephrasing of this condition using Lemma 6.27. \square

We thus need to find a condition on a for the existence of a solution to the system

$$(6.17) \quad x = \pm 1 \pmod{d}$$

$$(6.18) \quad x^2 - ax + p = 0 \pmod{d^2}.$$

By the chinese remainder theorem, this admits a solution if and only if it does locally at every prime ℓ . So we find equivalent conditions for $d = \ell^\nu$. First we consider ℓ odd.

Lemma 6.29. *Let ℓ be an odd prime, $d = \ell^\nu$. The system above admits a solution if and only if $d^2 = \ell^{2\nu} \mid a^2 - 4p$.*

Proof. Let $\Delta = a^2 - 4p$ denote the discriminant of the quadratic equation (6.18). Completing the square to rewrite it as

$$(6.19) \quad \left(x - \frac{a}{2}\right)^2 - \Delta = 0 \pmod{d^2}$$

(since ℓ is odd) shows that there is a solution to (6.18) if and only if Δ is a square modulo d^2 .

First assume that $d^2 \mid \Delta$. Then reducing modulo d and using $p \equiv 1 \pmod{d}$ we see that

$$(6.20) \quad a^2 = 4 \pmod{\ell^\nu}$$

which implies $a = \pm 2 \pmod{\ell^\nu}$ since ℓ is odd. By (6.19), $x = a/2$ is thus a root of (6.18) satisfying $x \equiv \pm 1 \pmod{\ell^\nu}$.

Conversely, assume that the system has a solution x . Reducing (6.18) modulo d leads to $2 - ax \equiv 0 \pmod{d}$, i.e. $x = a/2 \pmod{d}$ (since $x = \pm 1 \pmod{d}$). Let $x = a/2 + dy$. Using (6.19), we have

$$\Delta = \left(x - \frac{a}{2}\right)^2 = d^2 y^2 = 0 \pmod{d^2}.$$

\square

We now do the same with $\ell = 2$.

Lemma 6.30. *Let $\ell = 2$, $d = \ell^\nu$. The system (6.18), (6.17) above admits a solution if and only if $a = 2b$ is even and for some $\varepsilon = \pm 1$ we have*

$$\begin{cases} b^2 - p = 2^{2\nu-2}y \pmod{2^{2\nu}} \text{ and } b - \varepsilon \equiv 2^{\nu-1}y \pmod{d}, \text{ with } y \equiv 0, 1 \pmod{4} & \text{if } \nu \geq 2 \\ p + 1 = 2b \pmod{4} & \text{if } \nu = 1. \end{cases}$$

Proof. This is similar to the previous one, although more tedious, and we leave it as an exercise, as it will not be used in the sequel. \square

Remark 6.31. If we write $x = 1 + dy$ in (6.18), we obtain the corresponding equation for y

$$p + 1 - a + dy(2 - a) = 0,$$

so if $d^2 \mid p + 1 - a$, $d \mid a - 2$, any y (in particular $x = 1$) is a solution (compare Proposition 6.7). However, for composite d other cases are possible. In other words, the a of Theorem 6.15 is not necessarily the same as the a of Proposition 6.7: for instance take $p = 241$, $d = 15$. Here $a = 8$ satisfies $d^2 \mid a^2 - 4p$, but $p + 1 - a = 234 \not\equiv 0 \pmod{225}$. On the other hand, $a = 17$ satisfies $a \equiv 2 \pmod{d}$ and $p + 1 - a \equiv 0 \pmod{d^2}$.

Theorem 6.15 is a consequence of Corollary 6.28 and Lemma 6.29, and also Proposition 6.11. One could incorporate Lemma 6.30 to the statement, instead of rephrasing the system of equations (6.17), (6.18) at 2, but it would be more complicated.

For d odd, one can further rederive, using (6.16), Theorem 4.9 (i) of [Sc-2], namely:

Proposition 6.32. *Let p be a prime number, $d \mid p - 1$ an odd integer. The number of isomorphism classes of elliptic curves E/\mathbf{F}_p with $d_1(E) \geq d$ is equal to*

$$\sum_{\substack{|a| < 2\sqrt{p} \\ a \equiv p+1 \pmod{d^2}}} H((a^2 - 4p)/d^2).$$

Remark 6.33. One can also tackle the question of finding points on $Y(d)$ over finite fields by using the Riemann Hypothesis for the curve $X(d)$, namely the inequality

$$|N_n - (p^n + 1)| \leq 2g(d)p^{n/2}$$

for $n \geq 1$, where $N_n = X(d)(\mathbf{F}_{p^n})$ and $g(d)$ is the genus of $X(d)$. This implies

$$|X(d)(\mathbf{F}_{p^n})| \geq p^n + 1 - 2g(d)p^{n/2},$$

and if p^n is large enough compared to d so that this lower bound exceeds the number of cusps, it follows that $Y(d)(\mathbf{F}_{p^n}) \neq \emptyset$.

This approach is developed, in greater generality, by Howe [Ho]. For our purpose, we are very interested in values of d large compared to p (and in the base field, $n = 1$). The inequality above is then not precise enough.

Indeed we have

$$g(d) = 1 + d\varphi^+(d)\psi(d)\frac{d-6}{12d}$$

(see e.g. [Sh-1, (1.6.4)]), of size about d^3 , while (Lemma 6.18) the number of cusps is $\varphi^+(d)\psi(d)$, of size about d^2 , so the condition to ensure $Y(d)(\mathbf{F}_p) \neq \emptyset$, namely

$$p + 1 - 2g(d)\sqrt{p} > \varphi^+(d)\psi(d)$$

is true roughly speaking for p of size at least d^6 . This is weaker than Lemma 6.36 below gives from Remark 6.13 or Theorem 6.15.

6.3. Applications. The previous sections give some rather simple criteria for the existence of an elliptic curve over a finite field with a given value of $d_1(E)$. We will deduce here some results about the possible values of $d_1(E)$ for all elliptic curves defined over a given finite field. Let

$$D_1(p) = \{d \geq 1 \mid d = d_1(E) \text{ for some } E/\mathbf{F}_p\}.$$

What can be said about $D_1(p)$?

We list some properties previously established:

- $D_1(p)$ is a subset of the set of divisors of $p - 1$, indeed (2.13) a subset of the set

$$\{d \mid p - 1 \mid d \leq \sqrt{p} + 1\}.$$

- $D_1(p)$ contains 1 and 2.
- $D_1(p)$ is inductive (i.e. if $d \in D_1(p)$ and $e \mid d$, we have $e \in D_1(p)$, by Proposition 6.11).

We now consider $D_1(p)$ on average over primes p , and will describe, in a certain sense, which divisors of $p - 1$ belong to $D_1(p)$. It is of particular interest to consider primes p such that $p - 1$ has some divisor $d > p^{1/4}$, and see which of those d are in $D_1(p)$.

First we count on average the divisors of $p - 1$ which are of a certain size. Let

$$(6.21) \quad d_\alpha(n) = |\{d \mid n \mid d < n^\alpha\}|$$

for $n \geq 1$ and $\alpha > 0$.

We recall the Bombieri-Vinogradov theorem, already mentioned before.

Theorem 6.34. *For any $A > 0$ there exists $B > 0$ such that*

$$\sum_{d \leq \sqrt{X}/(\log X)^B} \max_{(a,d)=1} \left| \pi(X; d, a) - \frac{\text{li}(X)}{\varphi(d)} \right| \ll_A \frac{X}{(\log X)^A},$$

the implied constant depending only on A .

For a proof, see e.g. [Bo, §7].

Lemma 6.35. *Let $\alpha > 0$ be a real number. We have*

$$\sum_{p \leq X} d_\alpha(p - 1) = f(\alpha)cX + O_\alpha\left(\frac{X}{\log X}\right)$$

where

$$f(\alpha) = \begin{cases} \alpha & \text{if } 0 < \alpha \leq 1/2 \\ (1 - \alpha) & \text{if } 1/2 \leq \alpha \leq 1 \\ 1 & \text{if } \alpha \geq 1 \end{cases}$$

and

$$c = \frac{\zeta(2)\zeta(3)}{\zeta(6)}.$$

The implied constant depends on α only. In particular,

$$\sum_{p \leq X} \sum_{\substack{d \mid p-1 \\ d \leq \sqrt{X}+1}} 1 \sim \frac{c}{2}X$$

as $X \rightarrow +\infty$.

Proof. This is a (simpler) variant of the proof of (3.4) using the Bombieri-Vinogradov theorem and the Brun-Titchmarsh inequality. Indeed, if $\alpha = \frac{1}{2}$, this is a stronger form of (3.4) with explicit error term (see for instance [Fou]; the proof in [HR, 3.5] gives a slightly worse error term $X(\log \log X)/(\log X)$).

If $\alpha < \frac{1}{2}$, we let $\beta = 1/\alpha > 2$ and write

$$\sum_{p \leq X} d_\alpha(p - 1) = \sum_{d < (X-1)^\alpha} (\pi(X; d, 1) - \pi(d^\beta + 1; d, 1)).$$

Since $\alpha < 1$, the Brun-Titchmarsh inequality yields

$$\sum_{d < (X-1)^\alpha} \pi(d^\beta + 1; d, 1) \ll \sum_{d < (X-1)^\alpha} \frac{d^\beta}{\varphi(d)(\log(d^\beta + 1))} \ll \frac{X}{\log X}.$$

Moreover, by the Bombieri-Vinogradov Theorem we have

$$\sum_{d < (X-1)^\alpha} \left| \pi(X; d, 1) - \frac{\text{li}(X)}{\varphi(d)} \right| \ll \frac{X}{(\log X)^A}$$

for any $A > 0$. Since

$$\sum_{d < (X-1)^\alpha} \frac{\text{li}(X)}{\varphi(d)} \sim \alpha c X \text{ as } X \rightarrow +\infty,$$

this proves the first part for $\alpha \leq \frac{1}{2}$.

If $\frac{1}{2} < \alpha < 1$, we use Dirichlet's trick to switch divisors

$$d_\alpha(n) = d_{1-\alpha}(n)$$

to reduce to $1 - \alpha$. Finally, for $\alpha \geq 1$, $d_\alpha(n) = d(n)$, and this is Linnik's theorem (3.4) again, with error term.

The last statement follows from the case $\alpha = \frac{1}{2}$, noting that

$$\sum_{p \leq X} |\{d \mid p-1 \mid \sqrt{X} \leq d \leq \sqrt{X} + 1\}| = O(\sqrt{X}).$$

□

Lemma 6.36. *Let $d \geq 1$ be an integer and $p \equiv 1 \pmod{d}$ a prime number. If*

$$d < 2p^{1/4}$$

we have $d \in D_1(p)$.

Proof. This follows from the criterion of Remark 6.13, for instance. The assumption means that $4\sqrt{p} > d^2$, hence all $a \in \mathbf{Z}/d^2\mathbf{Z}$ have a lift to \mathbf{Z} with $|a| < 2\sqrt{p}$. In particular, there is an a , $|a| < 2\sqrt{p}$, with $a \equiv p+1 \pmod{d^2}$. Since $p \equiv 1 \pmod{d}$, we have $a \equiv 2 \pmod{d}$, and by Remark 6.13, $d \in D_1(p)$.

For odd d , one can also appeal to Theorem 6.15 in the same way: $a^2 \pmod{d^2}$ runs over all squares modulo d^2 , and $4p$ is a square modulo d^2 (since $p \equiv 1 \pmod{d}$); indeed, if $p = 1 + md$, $4p \equiv (2 + md)^2 \pmod{d^2}$. So there exists a with $4p = a^2 \pmod{d^2}$, i.e. $d^2 \mid a^2 - 4p$. □

Remark 6.37. One can see from the proof that this lemma is essentially best possible, in the sense (for instance) that for any $\theta > 1/4$, there exist p and d with $d < p^\theta$ and $d \notin D_1(p)$. This confirms again that the condition that $d_1(E)$ be of size larger than $p^{1/4}$ reflects a critical threshold in this subject.

Proposition 6.38. *We have*

$$\sum_{p \leq X} |D_1(p)| = \frac{cX}{4} + O\left(\frac{X}{\log X}\right)$$

for $X \geq 2$, with an absolute implied constant.

Actually, we will prove a more precise result. As suggested by Lemma 6.36, we partition $D_1(p)$ in two subsets according to whether $d < 2p^{1/4}$ or $d > 2p^{1/4}$ (there can not be equality); call those subsets $D_s(p)$ and $D_\ell(p)$, respectively.

We then have:

Proposition 6.39. *We have*

$$\sum_{p \leq X} |D_s(p)| = \frac{cX}{4} + O\left(\frac{X}{\log X}\right)$$

for $X \geq 2$.

Proposition 6.40. *We have*

$$\sum_{p \leq X} |D_\ell(p)| \ll \frac{X}{\log X}$$

for $X \geq 2$.

Proposition 6.38 follows immediately.

Proof of Proposition 6.39. By Lemma 6.36, we have

$$D_s(p) = \{d \mid p-1 \mid d < 2p^{1/4}\}$$

so $|D_s(p)| = d_{1/4}(p-1) + \delta(p)$, where

$$\delta(p) = |\{d \mid p-1 \mid (p-1)^{1/4} \leq d < 2p^{1/4}\}|.$$

By Lemma 6.35, it suffices to show that

$$\sum_{p \leq X} \sum_{\substack{d \mid p-1 \\ (p-1)^{1/4} \leq d < 2p^{1/4}}} 1 \ll \frac{X}{\log X}.$$

This follows as before from the Brun-Titchmarsh inequality, writing

$$\sum_{p \leq X} \sum_{\substack{d \mid p-1 \\ (p-1)^{1/4} \leq d < 2p^{1/4}}} 1 = \sum_{d \leq 2X^{1/4}} (\pi(d^4 + 1; d, 1) - \pi(d^4/16; d, 1)).$$

Equivalently, one may simply adapt the proof of Lemma 6.35 for $\alpha = 1/4$. \square

Proof of Proposition 6.40. By Remark 6.13, we have $d \in D_1(p)$ if and only if there exists $a \in \mathbf{Z}$ with $|a| < 2\sqrt{p}$ such that

$$\begin{cases} a \equiv 2 \pmod{d} \\ a \equiv p+1 \pmod{d^2} \end{cases}$$

Notice that $p \equiv 1 \pmod{d}$ is equivalent with $a \equiv 2 \pmod{d}$ if the last congruence holds.

Now we remark that if $d \in D_\ell(p)$, then such an a is unique: indeed, if a_1 and a_2 satisfy the above conditions, we have $a_1 \equiv a_2 \pmod{d^2}$. Since $d^2 > 4\sqrt{p}$ and $|a_i| < 2\sqrt{p}$, this is possible only if $a_1 = a_2$.

Therefore we can write

$$\sum_{p \leq X} |D_\ell(p)| = \sum_{p \leq X} \sum_{|a| < 2\sqrt{p}} \sum_{\substack{d \mid p-1 \\ d^2 \mid p+1-a \\ d^2 > 4\sqrt{p}}} 1.$$

We exchange the order of summation, getting

$$\sum_{p \leq X} |D_\ell(p)| = \sum_{d \leq \sqrt{X}+1} \sum_{\substack{|a| < 2\sqrt{X} \\ a \equiv 2 \pmod{d}}} \sum_p 1$$

where the inner sum is over primes p satisfying the size conditions:

$$\begin{cases} p \leq X \\ p < d^4/16 \\ a^2/4 < p \end{cases}$$

and the congruence

$$p \equiv a - 1 \pmod{d^2},$$

in other words

$$\sum_{p \leq X} |D_\ell(p)| = \sum_{d \leq \sqrt{X}+1} \sum_{\substack{|a| < 2\sqrt{X} \\ a \equiv 2 \pmod{d} \\ 2|a| < d^2}} \left(\pi(\inf(\frac{d^4}{16}, X); d^2, a-1) - \pi(a^2/4; d^2, a-1) \right).$$

We drop the second term by positivity, and write

$$\begin{aligned} \sum_{p \leq X} |D_\ell(p)| &\leq \sum_{d < 2X^{1/4}} \sum_{\substack{2|a| < d^2 \\ a \equiv 2 \pmod{d}}} \pi(d^4/16; d^2, a-1) \\ &+ \sum_{2X^{1/4} \leq d \leq \sqrt{X}+1} \sum_{\substack{|a| < 2\sqrt{X} \\ a \equiv 2 \pmod{d}}} \pi(X; d^2, a-1). \end{aligned}$$

By the Brun-Titchmarsh inequality (3.25), the first term is

$$\begin{aligned} \sum_{d < 2X^{1/4}} \sum_{\substack{2|a| < d^2 \\ a \equiv 2 \pmod{d}}} \pi(d^4/16; d^2, a-1) &\ll \sum_{d < 2X^{1/4}} \sum_{\substack{2|a| < d^2 \\ a \equiv 2 \pmod{d}}} \frac{d^4}{\varphi(d^2) \log d} \\ &\ll \frac{X}{\log X}. \end{aligned}$$

For the second term, we further split the range of d into $2X^{1/4} \leq d \leq X^{1/2-\delta}$ and $X^{1/2-\delta} < d \leq \sqrt{X} + 1$, where $0 < \delta < 1/2$. For the second range, where d is very large, we simply overcount all integers $n \equiv a - 1 \pmod{d^2}$ instead of primes, getting

$$\begin{aligned} \sum_{X^{1/2-\delta} < d \leq \sqrt{X}+1} \sum_{\substack{|a| < 2\sqrt{X} \\ a \equiv 2 \pmod{d}}} \pi(X; d^2, a-1) &\ll \sum_{X^{1/2-\delta} < d \leq \sqrt{X}+1} \frac{\sqrt{X}}{d} \times \frac{X}{d^2} \\ &\ll X^{1/2+3\delta}, \end{aligned}$$

so if $\delta < 1/6$, this saves a power of X instead of merely $\log X$.

Finally, we have again by (3.25)

$$\begin{aligned} \sum_{2X^{1/4} \leq d \leq X^{1/2-\delta}} \sum_{\substack{|a| < 2\sqrt{X} \\ a \equiv 2 \pmod{d}}} \pi(X; d^2, a-1) &\ll \sum_{2X^{1/4} \leq d \leq X^{1/2-\delta}} \sum_{\substack{|a| < 2\sqrt{X} \\ a \equiv 2 \pmod{d}}} \frac{X}{\varphi(d^2) \log X} \\ &\ll \frac{X^{3/2}}{\log X} \sum_{2X^{1/4} \leq d \leq X^{1/2-\delta}} \frac{1}{d^2 \varphi(d)} \\ &\ll \frac{X}{\log X}. \end{aligned}$$

□

Remark 6.41. Here the criterion given by the trace formula could also have been used, but it would be slightly more complicated, mainly because of the possible multiplicity of a occurring for the same d .

As a variant, we mention, and leave as an exercise, what happens for elements of $D_1(p)$ larger than $p^{1/4+\theta}$ for some fixed $\theta > 0$.

Proposition 6.42. *Let $\theta > 0$ be a real number. We have*

$$\sum_{p \leq X} |\{d \in D_1(p) \mid d > p^{1/4+\theta}\}| \ll_{\theta} X^{1-2\theta}$$

for $X \geq 2$, the implied constant depending only on θ .

We also leave as an exercise the following estimate on the average number of isomorphism classes of E/\mathbf{F}_p with $d_1(E) \geq 2p^{1/4}$ (use Proposition 6.32 and the trivial estimate $H(\Delta) \ll \Delta^{1/2} \log \Delta$, see e.g. [Cox, Th. 7-24]).

Proposition 6.43. *We have*

$$\sum_{p \leq X} \sum_{\substack{d|p-1 \\ 2 \nmid d \\ d \geq 2p^{1/4}}} |\{E/\mathbf{F}_p \mid d_1(E) \geq d\}| \ll X^{5/4}.$$

For comparison, the total number of isomorphism classes of E/\mathbf{F}_p with $p \leq X$ is $\sim X^2$ (there are p possible j -invariants and, except for cubic and biquadratic twists for $j = 0$, 1728, two isomorphism classes for each j -invariant, see e.g. [Si-1, X-5]).

Remark 6.44. For heuristic purposes in trying to make guesses about the distribution of outside primes for elliptic curves, it is really a lower-bound for $|D_{\ell}(p)|$ that one would like to have on average, or more precisely for the quantity in Proposition 6.43. This looks like a fairly hard problem: one can see in the proof of Proposition 6.40 that it boils down to assertions about the equidistribution of primes $\leq Y$ to moduli which are $\gg Y^{1/2}$, and moreover with “initial term” $a - 1$ which vary. The latter constraint, in particular, seems currently incompatible with the methods developed by Bombieri, Friedlander and Iwaniec [BFI].

7. NUMERICAL EXAMPLES

The various problems we have considered lend themselves easily to numerical experimentation using computer packages for elliptic curves computations. We have used the PARI/GP system and written scripts to perform the following computations, for an elliptic curve E/\mathbf{Q} given by a Weierstrass equation:

- Compute the invariants $d_1(p)$, $d_2(p)$ at a prime p , and the sum $S_E(X; d_1)$. Also, find the weak outside primes of E which are $\leq X$, and if the order of the Galois groups G_d can be computed, the outside primes $\leq X$.
- Compute the multiplicity functions $M(n)$ or $m(p)$, the number of E -twins $\leq X$ and more generally the various moments $S_k(X)$, $T_k(X)$.

The numerical results can be compared to the predictions, when we have some. Especially if E is a Serre curve (Section 3.3), one can compare $S_E(X; d_1)$ with the conjectural asymptotic

$$S_E(X; d_1) \sim c(E) \operatorname{li}(X).$$

The PARI system does not implement (yet) the computation of $d_1(p)$ as a primitive function although, based on Cohen’s description of the Shanks-Mestre algorithm to compute a_p ([C-1, 7.4.3]), this should be almost as fast as computing a_p . However one can write a simple enough algorithm by computing the exponent (i.e. $d_1 d_2$) of $E_p(\mathbf{F}_p)$ by looking for an element of maximal order, either by “exhaustion” or more efficiently (as suggested by K. Belabas) by picking up a few “random” points on $E_p(\mathbf{F}_p)$ and taking the l.c.m of their orders.⁹ Moreover, for primes p with $|E_p(\mathbf{F}_p)|$ squarefree, one has $d_1(p) = 1$ without further computations, and this happens quite often if the curve has no non-trivial rational 2-torsion points.

⁹ In the computations below, this was done with 20 random points, so in theory the results might be off by a small amount. However, it is easy to repeat the computations for the primes yielding “large” values of $d_1(p)$, thus ensuring their correctness.

Computing elliptic twins is even simpler, and the computation of the sums

$$S_k(X) = \sum_{n \leq X} M(n)^k$$

can be performed using very little memory by operating by blocks of n . Numerically, $M(n)$ is always very small so $S_k(X)$ is very close to $T_{k-1}(X)$ (compare (4.14)). Also we computed the modified first moment

$$S'(X) = \sum_{\substack{n \leq X \\ n \text{ twin value}}} M(n).$$

Note that we have obviously

$$S'(X) = J(X) + \underline{O}(\sqrt{X}).$$

(see (4.5) for $J(X)$).

7.1. The test curves. We used two non-CM curves, which are Serre curves, and one CM curve. Here are their id-sheets:

Example 7.1. Consider the curve (see [Se-1, 5.9.2], [LT, I §7])

$$E : y^2 = x^3 + 6x - 2$$

with $j(E) = 2^9 3$, discriminant $-2^6 3^5$, conductor 1728. It has rank 0. By [LT, Th. 7.1], this curve is a Serre curve and $m = 3$ in this case.

Using Corollary 3.13, (3.20), we have

$$(7.1) \quad \begin{aligned} c'(E) &= \frac{5461}{5425} = 1.0066\dots \\ c(E) &= c'(E)c_0 = 1.2668\dots \end{aligned}$$

Example 7.2. Consider the curve (see [Se-1, 5.5.6])

$$F : y^2 + y = x^3 - x$$

with $j(F) = 2^{12} 3^3 / 37$, discriminant 37, conductor 37. It has rank 1, the point $(0, 0)$ being of infinite order. It is also a Serre curve and $m = 37$. (It is also studied by Mazur and Swinnerton-Dyer in [MSD]).

Using Corollary 3.13, we have

$$(7.2) \quad \begin{aligned} c'(F) &= \frac{1732338101}{1732332625} = 1.000003\dots \\ c(F) &= c'(F)c_0 = 1.2584\dots \end{aligned}$$

(the value of $c(F)$ differs from c_0 by less than 10^{-5}).

Example 7.3. The last curve is the CM curve (3.23) of Example 3.16, namely

$$A : y^2 = x^3 - x,$$

(with CM by $\mathbf{Z}[i]$). The expected behavior is now

$$S_A(X; d_1) \sim c(A)X$$

with $c(A)$ given by (3.16).

7.2. Numerical examples: the elliptic splitting problem. We now give a few examples of computations of averages of d_1 . Here are some experimental data for $p \leq 60,000,000$, for the curves E and F of Examples 7.1 and 7.2.

X	$\pi(X)$	$S_E(X; d_1)$	Ratio	$S_F(X; d_1)$	Ratio
100,000	9592	11945	1.24530	11944	1.24520
500,000	41538	52418	1.26192	51969	1.25111
1,000,000	78498	99144	1.26301	98465	1.25436

5,000,000	348513	440751	1.26466	438079	1.25699
10,000,000	664579	841232	1.26581	835662	1.25743
15,000,000	970704	1229075	1.26616	1220393	1.25722
20,000,000	1270607	1608929	1.26626	1597802	1.25751
30,000,000	1857859	2352704	1.26635	2336778	1.25778
40,000,000	2433654	3081940	1.26638	3061994	1.25818
50,000,000	3001134	3800076	1.26621	3775641	1.25807
60,000,000	3562115	4510928	1.26636	4480730	1.25788

The agreement with the expected behavior seems quite good, but it should be noticed that only values of d (in the sense of (3.2)) which are fairly small actually occur in this range. In accordance with (7.1) and (7.2), the sum for E tends to be slightly larger than that for F .

All outside primes $\leq 300,000,000$ were computed. It turns out that there are very few of them. Here is the complete list, indicating the prime p , the value of $d_1(p)$ and the order of the Galois group G_d

p	$d_1(E, p)$	$ G_d $
196561	140	92897280
4095037	162	76527504
13403893	114	17729280
30626899	106	46433088
53629561	184	410370048
54460963	258	480598272
76391737	172	320398848
132576571	127	258080256
138085949	143	345945600
145030393	312	966131712

There are 20 additional weak outside primes, for instance $p = 779761$ with $d_1(p) = 36 = p^\alpha$ with $\alpha = 0.26\dots$

The impact of the single very large value of d_1 at $p = 196561$ is quite noticeable: we have

X	$S_E(X; d_1)$	$\pi(X)$	Ratio
196560	22218	17700	1.2552
196561	22358	17701	1.2630

In another direction, here is a table listing, for those $d \leq 140$ for which at least one $p \leq 3,000,000$ splits completely in $\mathbf{Q}(E[d])$, how many do: $\pi_X(E; d, 1)$ is in the second row, the third is the ratio $\pi(X)/\pi_E(X; d, 1)$, for comparison with $|G_d|$.

d	2	3	4	5	6	7
Number	13032	1624	783	164	502	28
Ratio	6.0223	48.335	100.25	478.63	156.36	2803.4
$ G_d $	6	48	96	480	144	2016
d	8	9	10	11	12	13
Number	40	17	33	7	28	4
Ratio	1962.4	4617.4	2378.6	11213.	2803.4	19624.
$ G_d $	1536	3888	2880	13200	2304	26208
d	14	15	16	17	18	19
Number	6	2	1	1	8	1
Ratio	13082.	39248.	78496.	78496.	9812.0	78496
$ G_d $	12096	23040	24576	78336	11664	123120
d	20	21	23	24	28	30
Number	1	1	2	2	1	1
Ratio	78496.	78496.	39248.	39248.	78496.	78496.

$ G_d $	46080	96768	267168	36864	193536	69120
d	35	36	70	140		
Number	1	1	1	1		
Ratio	78496.	78496.	78496.	78496.		
$ G_d $	967680	186624	5806080	92897280		

As for F , here is the table listing the outside primes $\leq 300,000,000$.

p	$d_1(F, p)$	$ G_d $
8317	11	13200
63317	22	79200
657493	44	1267200
1258667	37	1822176
11019023	98	29042496

One can see again that those p for which $d_1(p)$ is large have an important effect; here we have

X	$S_F(X; d_1)$	$\pi(X)$	Ratio
63313	7849	6343	1.2374
63317	7871	6344	1.2407
657491	66953	53378	1.2543
657493	66997	53379	1.2551

Here is the table of the number of primes $p \leq 3,000,000$ which split in $\mathbf{Q}(F[d])$ for $2 \leq d \leq 44$ (those d for which no p splits are omitted):

d	2	3	4	5	6
Number	13034	1645	790	152	268
Ratio	6.0224	47.718	99.363	516.42	292.89
$ G_d $	6	48	96	480	288
d	7	8	9	10	11
Number	30	56	15	22	10
Ratio	2616.5	1401.7	5233.1	3568.0	7849.7
$ G_d $	2016	1536	3888	2880	13200
d	12	13	14	15	16
Number	16	2	4	2	4
Ratio	4906.0	39248.	19624.	39248.	19624.
$ G_d $	4608	26208	12096	23040	24576
d	21	22	24	44	
Number	1	3	2	1	
Ratio	78497.	26165.	39248.	78497.	
$ G_d $	96768	79200	73728	1267200	

For the CM curve A of Example 7.3, we get the following for $p \leq 30,000,000$, where we compare $S_A(X; d_1)$ with X in the last column:

X	$S_A(X; d_1)$	Ratio
10000	5410	0.5410
100000	55578	0.5558
500000	267450	0.5349
1000000	529742	0.5297
5000000	2633630	0.5267
10000000	5274876	0.5275
15000000	7839124	0.5226
20000000	10386178	0.5193
25000000	13027268	0.5211

30000000 | 15665348 | 0.5222

The expected linear growth of $S_G(X; d_1)$ seems also apparent.

7.3. Numerical examples: elliptic twins. Motivated by the rough heuristic of Section 4.3, for non-CM curves we compare $S'(X)$ with¹⁰

$$\text{li}_2(x) = \int_2^x \frac{dt}{(\log t)^2} = \text{li}(x) - \text{li}(2) - \frac{x}{\log x} + \frac{2}{\log 2}.$$

The first table lists some values of X , $S'(X)$ and $S'(X)/\text{li}_2(X)$ for the curves E and F , for $X \leq 10^8$.

X	$S'_E(X)$	$S'_E(X)/\text{li}_2(X)$	$S'_F(X)$	$S'_F(X)/\text{li}_2(X)$
1000	32	0.9226	29	0.8361
10000	133	0.8198	154	0.9492
100000	1110	1.1736	1062	1.1229
1000000	7364	1.1788	7349	1.1764
5000000	29583	1.2079	29045	1.1860
10000000	54036	1.2143	52734	1.1850
20000000	98582	1.2136	97226	1.1969
40000000	181587	1.2197	178934	1.2018
60000000	259489	1.2206	255478	1.2018
80000000	333974	1.2193	329150	1.2017
99980000	407033	1.2205	401293	1.2033

Next we list the multiplicities $M(n)$ occurring for twin values n : in this range, $M(n) \leq 5$, and the number of integers with a given $M(n) = k > 1$ is as follows:

k	2	3	4	5
E	194197	5982	167	5
F	191817	5685	146	4

The values of $n \leq 10^8$ with $M_E(n) = 5$ are

$$n \in \{13269240, 14469576, 20024896, 52472068, 64703760\}$$

and those with $M_F(n) = 5$ are

$$n \in \{5597128, 64220836, 85004608, 86998320\}.$$

To compare with (4.16), note that

$$\frac{\log x}{\log \log x} = \begin{cases} 5.7980 & \text{for } x = 10^7 \\ 6.3225 & \text{for } x = 10^8. \end{cases}$$

Because of the very small number of n with $M(n) > 2$, $j(X)$ (see (4.4)) is almost equal to $\frac{1}{2}S'(X)$. In particular, the numerical data seems to confirm (4.15) for E and F .

We now consider the CM curve A/\mathbf{Q} . Of course, the field of definition does not contain the CM field, as assumed in Section 5. However, it is very simple to adapt the arguments there to this case.

For supersingular p , i.e. $p \equiv 3 \pmod{4}$, we have $n_p = p + 1$; in particular if we write

$$M(n) = M_o(n) + M_s(n),$$

where $M_o(n)$ (resp. $M_s(n)$) is the number of ordinary primes p with $n_p = n$ (resp. supersingular primes), it follows that $M_s(n) = 0$ or 1 according to whether $n - 1$ is prime $\equiv 3 \pmod{4}$ or not (note that $n_p \equiv 0 \pmod{4}$ for all p since $A[2] \subset A(\mathbf{Q})$, so $n_p - 1 \equiv 3 \pmod{4}$ for all p).

¹⁰As usual, this gives a much better approximation than $X/(\log X)^2$.

We thus get the bound

$$(7.3) \quad M(n) \leq 1 + \frac{1}{2}r(n)$$

instead of (5.4).

To estimate $S_k(X)$, write

$$\begin{aligned} S_k(X) &= \sum_{n \leq X} (M_o(n) + M_s(n))^k \\ &= \sum_{j=0}^k \binom{k}{j} \sum_{n \leq X} M_s(n)^{k-j} M_o(n)^j \\ &\leq \sum_{j=0}^k \binom{k}{j} S_{o,j}(X) \end{aligned}$$

since $M_s(n)^{k-j} \leq 1$, where $S_{o,j}(X)$ is the j -th moment of $M_o(n)$. To the latter sum, we can clearly apply the arguments used in Section 5 verbatim, and deduce

$$S_{o,j}(X) \ll_j X (\log X)^{\beta(j-1)+\varepsilon} \text{ with } \beta(j) = 2^j - j - 2, \text{ for any } \varepsilon > 0$$

hence we have:

Proposition 7.4. *For all $k \geq 0$ and $X \geq 2$ we have*

$$S_k(X) \ll_\varepsilon X (\log X)^{\beta(k-1)+\varepsilon} \text{ for } k \geq 1$$

$$T_k(X) \ll_\varepsilon X (\log X)^{\beta(k)+\varepsilon},$$

with $\beta(k) = 2^k - k - 2$ for any $\varepsilon > 0$, the implied constant depending only on k and ε .

Computations were performed for $p \leq 20,000,000$. Here is a table with values of $j(X)$, $S'(X)$ and of the ratio $S'(X)/\text{li}(X)$:

X	$S'_A(X)$	$S'_A(X)/\text{li}(X)$	$j(X)$
1000	67	0.37723	27
10000	486	0.39000	187
100000	3693	0.38349	1430
1000000	29068	0.36969	11052
5000000	126445	0.36268	47674
7500000	182930	0.35975	68842
10000000	238563	0.35878	89693
12500000	292994	0.35778	110021
15000000	346590	0.35692	130095
17500000	399567	0.35624	149871
20000000	451562	0.35530	169294

Here is a table with values of $S_2(X)$ et $S_3(X)$, compared with $\text{li}(X)$ and X respectively:

X	$S_2(X)$	$S_2(X)/\text{li}(X)$	$S_3(X)$	$S_3(X)/X$
100000	16757	1.7401	43637	0.43637
500000	73154	1.7582	198966	0.39793
1000000	138492	1.7613	384224	0.38422
2500000	323992	1.7680	919320	0.36772
5000000	618660	1.7745	1786380	0.35727
7500000	902363	1.7746	2635021	0.35133
10000000	1180791	1.7758	3469855	0.34698

12500000	1454892	1.7766	4285228	0.34281
15000000	1724899	1.7763	5098883	0.33992
17500000	1992562	1.7765	5897698	0.33701
20000000	2258677	1.7772	6714287	0.33571

Here is the table of values > 1 taken by $M(n)$ in this range (those k for which no n satisfies $M(n) = k$ are omitted):

2	3	4	5	6	7	8	9	10	11
106007	37191	14291	6123	2835	1360	670	386	195	108
12	13	14	15	16	17	18	19	20	24
60	33	13	9	7	1	2	1	1	1

The n with $M(n) = 24$ is $n = 12818000$. Notice that $n = 2^4 \cdot 5^3 \cdot 13 \cdot 17 \cdot 29$, each prime $\neq 2$ being (of course) a sum of two squares. We have $r(n) = 32$ in this case. In practice, it is quite easy to find rather large multiplicities without constructing a complete table: take an integer n divisible by 4 (because $A[2] \subset A(\mathbf{Q})$) and with many prime factors $\equiv 1 \pmod{4}$ so that $r(n)$ is large, and look at the primes p , $n^- \leq p \leq n^+$, for those with $n_p = n$.

For comparison, the integers $n \leq 10^8$ with $M_E(n) = 5$ or $M_F(n) = 5$ factor as follows:

$$13269240 = 2^3 \cdot 3^2 \cdot 5 \cdot 29 \cdot 31 \cdot 41, \quad 14469576 = 2^3 \cdot 3 \cdot 11 \cdot 23 \cdot 2383,$$

$$20024896 = 2^6 \cdot 139 \cdot 2251, \quad 52472068 = 2^4 \cdot 11 \cdot 37 \cdot 167 \cdot 193,$$

$$64703760 = 2^4 \cdot 3 \cdot 5 \cdot 11 \cdot 24509, \quad 5597128 = 2^3 \cdot 699641,$$

$$64220836 = 2^2 \cdot 19 \cdot 491 \cdot 1721, \quad 85004608 = 2^6 \cdot 13 \cdot 71 \cdot 1439. \quad 86998320 = 2^4 \cdot 3^3 \cdot 5 \cdot 40277,$$

the prime factors exhibiting no obvious property (?).

8. CONCLUSION

The many questions raised in this paper seem very hard to attack, but on the other they seem to be very interesting from the point of view of analytic number theory. Given the extensive experience with the distribution of primes in arithmetic progressions to large moduli, and the (much more modest) first results for CM curves obtained here, one would like to have some kind of sieve method available for the non-CM curves: roughly speaking, sieve is powerful because it exploits the embedding of primes inside the integers, and because the divisibility of integers by a given $d \geq 1$ can be used to recover primes by inclusion-exclusion, so some of the regularity of the distribution of integers can be exploited.

For a non-CM curve E/\mathbf{Q} , the function $d_1(p)$ has no obvious interpretation as the restriction to primes of an arithmetic function defined for all n , whereas if E/\mathbf{Q} has CM, $d_1(p)$ is $b(\pi - 1)$, where π is the Frobenius at p and $b(a)$ is defined for any $a \in \text{End}(E)$ as the largest integer $b \in \mathbf{Z}$ with $(b) \mid (a)$.¹¹

Also, despite the fact that the modularity of elliptic curves would seem to provide a “dual view”, similar to that of Dirichlet characters instead of 1-dimensional Galois representations, it is really the Artin L -functions attached to the fields $K(E[d])/K$ which are of importance. Those can have rank as large as d (roughly), which makes all current analytic techniques incapable of dealing with them, individually or on average, even assuming the Artin conjecture, or that they are automorphic L -functions.

Thus it seems much work is required to understand those analytic problems. As for arithmetic progressions however, where the stumbling block of the Riemann Hypothesis has often been circumvented by startling new results (Linnik’s dispersion method, the Bombieri-Vinogradov

¹¹The results of Duke and Toth ([DT]) can be used to “lift” the Frobenius on E_p to a matrix in $M(2, \mathbf{Z})$, well-defined up to $GL(2)$ -conjugacy, which reduced modulo d gives the action of σ_p on $\mathbf{Q}(E[d])$ for any d (prime to the discriminant). But I do not see how to isolate the conjugacy classes of this type; the set of all matrices is too big to give information on a single elliptic curve.

theorem, the results of Bombieri-Friedlander-Iwaniec, etc...), one may hope that there is much to discover.

REFERENCES

- [Bi] Birkhoff, G.: *Subgroups of Abelian Groups*, Proc. London Math. Soc. (2) 38 (1935), 385–401.
- [Bo] Bombieri, E.: *Le grand crible dans la théorie analytique des nombres*, Astérisque 18, SMF (1974).
- [BFI] Bombieri, E., Friedlander, J. and Iwaniec, H.: *Primes in arithmetic progressions to large moduli*, Acta Math. 156 (1986), 203–251.
- [C-1] Cohen, H.: *A Course in Computational Algebraic Number Theory*, GTM 138, Springer-Verlag, 1993.
- [C-2] Cohen, H.: *Advanced Topics in Computational Number Theory*, GTM 193, Springer-Verlag, 2000.
- [Co] Cojocaru, A.: *Cyclicity of CM elliptic curves modulo p* , Trans. Amer. Math. Soc. 355 (2003), no. 7, 2651–2662.
- [CD] Cojocaru, A. and Duke, W.: *Reductions of an elliptic curve and their Tate-Shafarevich groups*, Math. Ann. 329 (2004), no. 3, 513–534.
- [CM] Cojocaru, A. and Murty, R.: *Cyclicity of elliptic curves modulo p and elliptic curve analogues of Linnik’s problem*, Math. Ann. 330 (2004), no. 3, 601–625.
- [Cox] Cox, D.: *Primes of the form $x^2 + ny^2$* , Wiley 1989.
- [De] Deuring, M.: *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Hamburg 14 (1941), 197–272.
- [DR] Deligne, P. and Rapoport, M.: *Les schémas de modules de courbes elliptiques*, Lecture Notes in Math. 349, Springer-Verlag (1973), 143–316.
- [Du] Duke, W.: *Elliptic curves with no exceptional primes*, C. R. Acad. Sci. Paris Sér. I Math. 325 (1997), no. 8, 813–818.
- [DT] Duke, W. and Toth, A.: *On the splitting of primes in division fields of elliptic curves*, Experiment. Math. 11 (2002), no. 4, 555–565 (2003).
- [El] Elkies, N.: *Distribution of supersingular primes*, Journées Arithmétiques 1989, Astérisque 198–200 (1991), 127–132.
- [Fom] Fomenko, O. M.: *A formula for the trace of Hecke’s operator in the space of parabolic forms relative to a principal congruence subgroup*, in russian, Izv. Akad. Nauk UzSSR Ser. Fiz.-Mat. Nauk 12 (1968), 26–28.
- [Fou] Fouvry, É.: *Sur le problème des diviseurs de Titchmarsh*, J. Reine angew. Math. 357 (1985), 51–76.
- [GK] Graham, S.W. and Kolesnik, G.: *Van der Corput’s Method of Exponential Sums*, L.M.S. Lecture Note 126, Cambridge Univ. Press, 1991.
- [Gr] Granville, A.: *Unexpected Irregularities in the Distribution of Prime Numbers*, Proc. ICM 1994 (Zürich), Birkhäuser 1995, 388–399.
- [GM] Gupta, R. and Murty, R.: *Cyclicity and generation of points mod p on elliptic curves*, Invent. math. 101 (1990), 225–235.
- [Ha] Harman, G.: *Primes in short intervals*, Math. Z. 180 (1982), no. 3, 335–348.
- [HR] Halberstam, H. and Richert, H-E.: *Sieve methods*, Academic Press 1974.
- [Ha] Hamer, C.: *A formula for the traces of the Hecke operators on certain spaces of newforms*, Arch. Math. (Basel) 70 (1998), 204–210.
- [Ho] Howe, E.: *On the Group Orders of Elliptic Curves over Finite Fields*, Compositio Math. 85 (1993), 229–247.
- [Hu] Huxley, M. N.: *The large sieve inequality for algebraic number fields*, Mathematika 15 (1968) 178–187.
- [IR] Ireland, K. and Rosen, M.: *A Classical Introduction to Modern Number Theory*, 2nd Edition, GTM 84, Springer-Verlag (1990).
- [I1] Iwaniec, H.: *Almost-primes represented by quadratic polynomials*, Invent. Math. 47 (1978), 171–188.
- [I2] Iwaniec, H.: *Topics in Classical Automorphic forms*, Grad. Studies in Math. 17, A.M.S (1997).
- [Jo] Jordan, B.: *p -adic points on Shimura curves*, Séminaire de Théorie des Nombres de Paris 1982–83, Progress in Math. 51, Birkhäuser, 1984.
- [KaMa] Katz, N. and Mazur, B.: *Arithmetic Moduli of Elliptic Curves*, Ann. of Math. Studies 108, Princeton 1985.
- [KM] Kowalski, E. and Michel, P.: *Zeros of families of automorphic L -functions close to 1*, Pacific J. Math. 207 (2002), no. 2, 411–431.
- [La] Lang, S.: *Algebra*, 2nd edition, Addison-Wesley 1984.
- [Li] Linnik, J. V.: *New versions and new uses of the dispersion methods in binary additive problems* (Russian) Dokl. Akad. Nauk SSSR 137 (1961) 1299–1302.
- [LT] Lang, S. and Trotter, H.: *Frobenius distribution in $GL(2)$ extensions*, Lecture Notes 504, Springer-Verlag 1976.
- [Ma] Mazur, B.: *Rational points of abelian varieties with values in towers of number fields*, Invent. math. 18 (1972), 183–266.

- [MSD] Mazur, B. and Swinnerton-Dyer, P.: *Arithmetic of Weil curves*, Invent. math. 25 (1974), 1–61.
- [Mi] Miyake, T.: *Elliptic Modular Forms*, Springer Verlag, 1989.
- [MV] Montgomery, H. L. and Vaughan, R. C.: *The large sieve*, Mathematika 20 (1973), 119–134.
- [Mu] R. Murty: *On Artin's conjecture*, J. Number Theory 16 (1983), no. 2, 147–168.
- [Ne] Neukirch, J.: *Class Field Theory*, Grundlehren der Mathematischen Wissenschaften 280, Springer-Verlag, Berlin, 1986.
- [Ru] Rubin, K.: *Elliptic curves with complex multiplication and the conjecture of Birch and Swinnerton-Dyer*, CIME Lecture Notes.
- [Sc-1] Schoof, R.: *The exponents of the group of points on the reductions of an elliptic curve*, in Arithmetic Algebraic Geometry (van der Geer, Oort, Steenbring editors), Progress in Math. 89, Birkhäuser, 325–335 (1991).
- [Sc-2] Schoof, R.: *Nonsingular Plane Cubic Curves over Finite Fields*, Jour. Combinat. Theory Series A 46 (1987), 183–211.
- [Se-1] Serre, J-P.: *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. 15 (1972), 259–331.
- [Se-2] Serre, J-P.: *Quelques applications du théorème de densité de Chebotarev*, Publ. Math. IHES 54 (1981), 323–401.
- [Se-3] Serre, J-P.: *Corps locaux*, 3rd edition, Hermann 1968.
- [Se-4] Serre, J-P.: *Abelian ℓ -adic Representations and Elliptic Curves*, 3d Edition, Research Notes in Mathematics 7, A K Peters, 1998.
- [Se-5] Serre, J-P.: *Répartition asymptotique des valeurs propres de l'opérateur de Hecke T_p* , J. Amer. Math. Soc. 10 (1997), 75–102.
- [Sh-1] Shimura, G.: *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press 1971.
- [Sh-2] Shimura, G.: *On the trace formula for Hecke operators*, Acta Math. 132 (1974), 245–281.
- [Si-1] Silverman, J.: *The Arithmetic of Elliptic Curves*, GTM 106, Springer-Verlag, 1986.
- [Si-2] Silverman, J.: *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer-Verlag, 1994.
- [Ti-1] Titchmarsh, E. C.: *A divisor problem*, Rend. Circ. Mat. Palermo 54 (1930), 414–429.
- [Ti-2] Titchmarsh, E. C.: *The theory of the Riemann Zeta-function*, Second edition (revised by D. R. Heath-Brown), Oxford University Press, 1986.
- [TV] Tsfasman, M. A. and Vlăduț, S. G.: *Asymptotic properties of zeta-functions*, Algebraic geometry, 7. J. Math. Sci. (New York) 84 (1997), no. 5, 1445–1467.
- [Wa] Waterhouse, W.: *Abelian Varieties over Finite Fields*, Ann. scient. Éc. Norm. Sup. 4ème série, 2 (1969), 521–560.

UNIVERSITÉ BORDEAUX I - A2X, 351, COURS DE LA LIBÉRATION, 33405 TALENCE CEDEX, FRANCE
E-mail address: `emmanuel.kowalski@math.u-bordeaux1.fr`