Statistical properties of isogenies between elliptic curves over finite fields

Master thesis

Alexandre Benoist

Prepared at LORIA (Nancy), under the supervision of Jean Kieffer in the CARAMBA team

Sorbonne Université (Paris)
Master 2 - Fundamental mathematics
Academic year 2023-2024
Defense held on July 11, 2024

Table of notations

$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$	Usual sets of numbers
$\lvert C \rvert$	Cardinality of the set C
$\mathrm{GL}_2(R)$	General linear group of degree 2 over the ring R
$\mathrm{PGL}_2(R)$	Projective general linear group of degree 2 over the ring R
$\overline{k}$	Algebraic closure of the field k
$\mathrm{char}(k)$	Characteristic of the field k
$\mathbb{F}_q$	Finite field with q elements
$\mathbb{Z}_p$	Ring of p-adic integers
$\mathbb{Q}_p$	Field of p-adic numbers
$V(k)$	Set of k-points of the variety V
$\mathrm{Gal}(L/K)$	Galois group of the extension L/K
$\left(\frac{\cdot}{\cdot}\right)$	Jacobi symbol
li	Logarithmic integral function: $\mathrm{li}(x) = \int_0^x \frac{dt}{\log(t)}$
φ	Euler's totient function
$B(p)$	Bernoulli distribution of parameter p
$B(n,p)$	Binomial distribution of parameter p
$f(x) = O(g(x))$	There is some constant $C > 0$ and $A > 0$ such that $f(x) \leq Cg(x)$ for every $x > A$
$f(x) = o(g(x))$	There is some function h satisfying $h(x) \xrightarrow[x \to +\infty]{} 0$ and $A > 0$ such that $f(x) = h(x)g(x)$ for $x > A$
$f(x) \ll g(x)$	Equivalent to $f(x) = O(g(x))$
$\mathrm{End}(E)$	Endomorphism ring of the elliptic curve E
t_E	Trace of Frobenius of the elliptic curve E defined over a finite field
N_E	Conductor of the elliptic curve E defined over $\mathbb{Q}$
GRH	Generalised Riemann hypothesis
$\omega_L(n)$	Number of prime divisors of n in the interval $[L, 2L]$

Contents

1 Introduction

Elliptic curves play an important role in public-key cryptography. In many applications, it is necessary to determine efficiently the number of rational points of an elliptic curve defined over a finite field. For instance, the elliptic curve Diffie-Hellman protocol involves choosing an elliptic curve whose the number of points is a large prime (see [HMV04, § 4.1.5]). In order to do so, one often generates random elliptic curves and determines their number of points until finding a good one.

For fields of cryptographic size, the best method up to date for large characteristic is the Schoof-Elkies-Atkin algorithm [Sch95]. Its time complexity essentially depends on the distribution of Atkin and Elkies primes. Given an elliptic curve E defined over a finite field $\mathbb{F}_q$, a prime ℓ is said to be Elkies if there is an isogeny from E of degree ℓ defined over $\mathbb{F}_q$, otherwise it is said to be Atkin. The more Elkies primes smaller than $O(\log(q))$ there are, the more efficient the SEA algorithm is. The heuristic argument to determine the complexity of the algorithm is that there is roughly the same number of Atkin and Elkies primes. Theoretical results in this direction have been established by Shparlinski and Sutherland in the last decade in the papers [SS14],[SS15]. They correspond to Theorems 3.1 and 3.2 of this document. Both are results on average over a family of elliptic curves: the first one considers the elliptic curves defined over a fixed finite field $\mathbb{F}_q$ and the second one takes the reductions of a fixed elliptic curve defined over $\mathbb{Q}$. More precisely, the authors define a quantity which measures the difference between the expected value and the reality, analogous to moments in probability theory, and they give an asymptotic upper bound for it. The proofs mainly rely on ingredients about the distribution of elliptic curves and lemmas in analytic number theory.

In this Master thesis, we first present the proofs of Shparlinski and Sutherland's results. Then we carry out numerical experiments in order to confirm these results and to determine whether there are optimal or not. They suggest that the asymptotic upper bounds are not optimal. Moreover, we observe that the distribution of the number of Elkies or Atkin primes in a dyadic interval seems to converge (in some sense) to a Gaussian function. We are able to prove this claim for the reductions of an elliptic curve defined over $\mathbb{Q}$. This corresponds to Theorem 5.1, which is the main contribution of this thesis. We tried to make this document as self-contained as possible. When the proofs are very long or difficult to access, we refer the interested reader to another suitable reference.

In Section 2, we begin with quick reminders about elliptic curves defined over finite fields or number fields. Then we present important results about the distribution of elliptic curves according to their trace of Frobenius and Galois representations

attached to an elliptic curve. We also discuss Schoof's algorithm and the SEA algorithm, in order to motivate the need to understand the distribution of Elkies and Atkin primes. In Section 3, we provide the results from analytic number theory before proving the main theorems. In Section 4, we present our numerical experiments and key observations. Finally, we prove the result of convergence of the number of Elkies primes for reductions of an elliptic curve in Section 5.

2 Background on elliptic curves

In this section, we provide the material on elliptic curves that will be used to prove the results about the distribution of Atkin and Elkies primes. We start by recalling basic facts about elliptic curves, our main reference for this being Chapter III in Silverman's book [Sil09]. We assume some familiarity with algebraic varieties.

2.1 Elliptic curves over general fields

Let k be a perfect field and $\overline{k}$ an algebraic closure.

2.1.1 Definition and Weierstrass equations

We start by giving the formal definition of an elliptic curve.

Definition 2.1. An elliptic curve E over k is a smooth plane projective curve of degree 3 which is defined over k and equipped with a base point $O_E \in E(k)$.

One might only be interested in elliptic curves up to isomorphism. We say that two elliptic curves are isomorphic if there exists an isomorphism of algebraic varieties between them respecting the base points.

In fact, one can show that elliptic curves always come from Weierstrass equations. More precisely, there is an embedding $\iota : E \hookrightarrow \mathbb{P}^2$ mapping E to a curve defined by the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.1}$$

with coefficients in k such that $\iota(O_E) = (0 : 1 : 0)$ (thus, O_E is often called the point at infinity). The previous equation for E is not unique: the equation

$$y'^2 + a'_1x'y' + a'_3y' = x'^3 + a'_2x'^2 + a'_4x' + a'_6$$

defines an isomorphic elliptic curve (with the isomorphism defined over k) if and only if it can be obtained from (2.1) by applying the change of variables

$$\begin{cases} x &= u^2x' + r, \\ y &= u^3y' + su^2x' + t, \end{cases} \tag{2.2}$$

with $u \in k^*$ and $r, s, t \in k$. Conversely, if C is a smooth curve given by a Weierstrass equation of the form of (2.1), then C is an elliptic curve over k with base point $(0 : 1 : 0)$.

If $\mathrm{char}(k) \neq 2, 3$, an appropriate change of variables shows that E has a reduced Weierstrass equation of the form $y^2 = x^3 + Ax + B$ with $A, B \in k$. Among the changes of variables of the form (2.2), the only ones preserving this form of equation are $x = u^2 x'$ and $y = u^3 y'$ with $u \in k^*$. Thus, the coefficients of the new Weierstrass equation are $A' = u^{-4}A$ and $B' = u^{-6}B$, so the elliptic curve $E' : y'^2 = x'^3 + A'x' + B'$ is isomorphic to E over k if and only if there is an element $u \in k^*$ such that $A = u^4 A'$ and $B = u^6 B'$.

The discriminant is defined as $\Delta := -16(4A^3 + 27B^2)$ and the j-invariant is $j := -1728\frac{(4A)^3}{\Delta}$. If $A' = u^{-4}A$ and $B' = u^{-6}B$, then $\Delta' = u^{-12}\Delta$ and $j' = j$. A Weierstrass equation defines a nonsingular curve (and thus an elliptic curve) if and only if its discriminant is nonzero. Two elliptic curves are isomorphic over $\overline{k}$ if and only if they have the same j-invariant.

Remark 2.2. For $\mathrm{char}(k) = 2, 3$, it is also possible to define the discriminant and the j-invariant as polynomial expressions of the coefficients $a_1, ..., a_6$ of (2.1) (see the formulas in [Sil09, § III.1.]).

2.1.2 Group law

Elliptic curves are very special algebraic varities, because they are equipped with a group law. There are several ways to describe it. Here, we consider the geometric point of view.

Let E be an elliptic curve over k with base point $O_E \in E$. Let P and Q be two points of E (not necessarily distinct), and L be the projective line passing through these points (if $P = Q$, then L is the tangent line to E at P). By Bézout's theorem, there is a unique point R of E such that the intersection of E and L consists in the three points P, Q and R (points are counted with their multiplicity). Let L' be the line passing through R and O_E, which intersects E at a third point R'. Then, we define $P + Q = R'$.

This law is commutative, has neutral element O_E, and each element has an inverse. It is also associative, but this is more complicated to establish. For $m \in \mathbb{N}$, the point $\underbrace{P + \ldots + P}_{m \text{ terms}}$ will be denoted by $[m]P$. If $m < 0$, we set $[m]P = \underbrace{-P - \ldots - P}_{|m| \text{ terms}}$.

There are explicit formulas for this group law in terms of the coordinates of the points (see Silverman [Sil09, § III.2]). The coordinates of $P+Q$ are rational functions of the coordinates of P and Q.

2.1.3 Endomorphisms and isogenies

We now consider morphisms between elliptic curves. Let E_1 and E_2 be two elliptic curves.

Definition 2.3. A morphism of elliptic curves $\phi : E_1 \to E_2$ is a morphism of algebraic varieties which is also a morphism of groups.

Since a morphism of elliptic curves is a morphism of projective curves, it is either constant or surjective.

Definition 2.4. An isogeny $\phi : E_1 \to E_2$ is a surjective morphism of elliptic curves from E_1 to E_2.

The degree of an isogeny ϕ is its degree as a map of curves defined over k.

The set of morphisms of elliptic curves from E_1 to E_2 form a ring for the addition and the composition, denoted $\mathrm{Hom}(E_1, E_2)$. The neutral element for the addition is the constant morphism equal to O_{E_2}, which has degree 0. The endomorphism ring of an elliptic curve E is $\mathrm{End}(E) = \mathrm{Hom}(E, E)$. $\mathrm{Hom}_k(E_1, E_2)$ (resp. $\mathrm{End}_k(E)$) denotes the ring of isogenies (resp. endomorphisms) that are defined over k.

Example 2.5. Let m be an integer. Then, the multiplication by m

$$[m] : \begin{cases} E \to E \\ P \mapsto [m]P \end{cases}$$

defines an endomorphism of E defined over k. It has degree m^2.

We say that two elliptic curves E_1 and E_2 are *isogenous* if there exists a non-constant isogeny between them. Being isogenous is an equivalence relation: if $\phi : E_1 \to E_2$ is an isogeny of degree m, then there exists a unique isogeny $\hat{\phi} : E_2 \to E_1$ satisfying $\hat{\phi} \circ \phi = [m]$.

An isogeny always has a finite kernel. In fact, it is possible to construct isogenies from kernels. Given a subgroup C of an elliptic curve E, we say that C is defined over k if $(\sigma(x_P), \sigma(y_P)) \in C$ for every $P = (x_P, y_P)$ in C and $\sigma \in \mathrm{Gal}(\overline{k}/k)$.

Proposition 2.6. *Let E be an elliptic curve and C be a finite subgroup of E defined over k. Then, there exist a unique elliptic curve E' and a separable isogeny*

$$\phi : E \to E'$$

such that $\ker(\phi) = C$. *In particular,* $\deg(\phi) = |C|$. *Both E' and ϕ are defined over k.*

We refer the reader to Proposition III.4.12. in [Sil09] for the proof of this result.

We now consider the endomorphisms of an elliptic curve E. We already know that $\mathrm{End}(E)$ always contains a copy of $\mathbb{Z}$ corresponding to $\{[m] \ : \ m \in \mathbb{Z}\}$. We have a classification of the possible endomorphism rings for elliptic curves. If k is a finite field, then $\mathrm{End}(E)$ is either:

- an order in an imaginary quadratic number field. In this case, E is said to be ordinary.
- an order in a quaternion algebra. In this case, E is said to be supersingular.

If $\mathrm{char}(k) = 0$, then $\mathrm{End}(E)$ is either:

- $\mathbb{Z}$
- an order $\mathcal{O}$ in an imaginary quadratic number field. In this case, E is said to have complex multiplication (or CM) by $\mathcal{O}$.

We now focus on torsion points, which are the kernels of the endomorphisms $[m]$.

Definition 2.7. Let m be a positive integer. The group of m-torsion points of E is defined as

$$E[m] := \{P \in E(\overline{k}) \ : \ [m]P = O_E\}.$$

The group of torsion points of E is

$$E_{tors} := \bigcup_{m=1}^{+\infty} E[m].$$

One can show that the group $E[m]$ is finite. Moreover, if $\mathrm{char}(k) > 0$ and $\mathrm{char}(k) \nmid m$ or if $\mathrm{char}(k) = 0$, then

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}.$$

As we will see in subsection 2.3.3, the absolute Galois group $\mathrm{Gal}(\overline{k}/k)$ acts on $E[\ell]$, which defines a representation modulo ℓ. The Tate module is introduced to work with representations of characteristic 0, and it appears to be a useful tool for studying isogenies (we refer the reader to [Sil09, § III.7]).

Definition 2.8. Let ℓ be a prime. The ℓ-adic Tate module is the $\mathbb{Z}_\ell$-module

$$T_\ell(E) = \varprojlim_n E[\ell^n],$$

where the inverse limit is taken with respect to the multiplication-by-ℓ maps $[\ell]$ between $E[\ell^{n+1}]$ and $E[\ell^n]$.

Finally, we introduce division polynomials, which are an important tool for Schoof's algorithm. Let $y^2 = x^3 + Ax + B$ be a Weierstrass equation for E (we assume here that $\mathrm{char}(k) > 3$, but division polynomials can also be defined for $\mathrm{char}(k) = 2, 3$).

Definition 2.9. The divisions polynomials $\psi_n \in \mathbb{Z}[x, y, A, B]$ of E are recursively defined by:

- $\psi_1(x, y) = 1$,
- $\psi_2(x, y) = 2y$,
- $\psi_3(x, y) = 3x^4 + 6Ax^2 + 12Bx - A^2$,
- $\psi_4(x, y) = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - A^3 - 8B^2)$,
- $\forall n \geq 2,\ \psi_{2n+1} = \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3$,
- $\forall n \geq 3,\ \psi_{2n} = \frac{1}{2y}\psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$.

One can check by induction that ψ_n just depends on x if n is odd. For an odd prime ℓ, it has degree $\frac{\ell^2-1}{2}$ and ψ_ℓ just depends on x. If the point $P \in E(\overline{k})$ has coordinates (x_P, y_P), then

$$\psi_\ell(x_P, y_P) = 0 \iff P \in E[\ell].$$

For more about division polynomials, we refer the reader to [Was08, Section 3.2].

2.2 Elliptic curves over finite fields

In this subsection, we assume that k is a finite field $\mathbb{F}_q$ where $q = p^n$ is a prime power. Our goal is to introduce results on the distribution of elliptic curves.

2.2.1 The Frobenius endomorphism and isomorphism classes

An elliptic curve E over $\mathbb{F}_q$ always come with a special endomorphism: the Frobenius endomorphism. It is defined as follows:

$$\phi_q : \begin{cases} E \to E \\ (x, y) \mapsto (x^q, y^q). \end{cases}$$

It is defined over $\mathbb{F}_q$, has degree q and there is an integer t_E such that

$$\phi_q^2 - t_E \phi_q + q = 0.$$

This integer t_E is called the trace of Frobenius of E, and $X^2 - t_E X + q$ is called the characteristic polynomial of the endomorphism of Frobenius. Its discriminant $t_E^2 - 4q$ will be called the Frobenius discriminant of E.

The group of $\mathbb{F}_q$-rational points of E is exactly the set of points fixed by ϕ_q. It is well-known that the number of $\mathbb{F}_q$-rational points on E can be expressed in terms of the trace of Frobenius: we have

$$|E(\mathbb{F}_q)| = q + 1 - t_E.$$

Tate's theorem asserts that two elliptic curves over $\mathbb{F}_q$ are isogenous if and only if they have the same trace of Frobenius. Moreover, t_E satisifes the inequality

$$|t_E| \leq 2\sqrt{q}$$

which is known as the Hasse bound and E is supersingular if and only if $\mathrm{char}(\mathbb{F}_q)$ divides t_E. For an ordinary elliptic curve E defined over $\mathbb{F}_q$, the endomorphism ring $\mathrm{End}(E)$ is an order in an imaginary quadratic number field containing $\mathbb{Z}[\phi_q]$.

Remark 2.10. The elements of an order containing $\mathbb{Z}[\phi_q]$ all commute with the action of the Frobenius automorphism which generates $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$. Hence, all these elements are defined over $\mathbb{F}_q$, so $\mathrm{End}_{\overline{\mathbb{F}_q}}(E) = \mathrm{End}_{\mathbb{F}_q}(E)$.

For the two next propositions, our proofs will be inspired from Lenstra [LJ87].

Proposition 2.11. *Let $\mathcal{E}_q$ be a set of representatives of all isomorphism classes of elliptic curves defined over $\mathbb{F}_q$. Then, we have $|\mathcal{E}_q| = 2q + O(1)$.*

Proof. We will assume that $p = \mathrm{char}(\mathbb{F}_q)$ is greater than 3. For $p = 2, 3$, the ideas are the same, but we cannot reduce Weierstrass equations, so the computations are less easy (we refer the reader to [HMV04, Theorem 3.18] and [Jeo09]).

We have seen that isomorphims between two elliptic curves $E : y^2 = x^3 + Ax + B$ and $E' : y'^2 = x'^3 + A'x' + B'$ are all of the form $x \mapsto u^2x$ and $y \mapsto u^3y$ for some $u \in k^*$. Thus the set of automorphisms $\mathrm{Aut}(E)$ of E is identified with

$$\{u \in k^* \ : \ u^4A = A \text{ and } u^6B = B\},$$

and the number of short Weierstrass equations which define an elliptic curve in the isomorphism class of E is $\frac{|k^*|}{|\mathrm{Aut}(E)|} = \frac{q-1}{|\mathrm{Aut}(E)|}$. There are three possibilities for the cardinality of $\mathrm{Aut}(E)$:

- $A = 0$ and k^* contains an element of order 6: $|\mathrm{Aut}(E)| = 6$,
- $B = 0$ and k^* contains an element of order 4: $|\mathrm{Aut}(E)| = 4$,
- else $|\mathrm{Aut}(E)| = 2$.

The choice of a short Weierstrass equation over $\mathbb{F}_q$ consists in choosing (A, B) in $(\mathbb{F}_q)^2$ such that $\Delta = -16(4A^3 + 27B^2) \neq 0$. We have $4A^3 + 27B^2 = 0$ if and only if $A = -3C^2$ and $B = 2C^3$ for an element $C \in \mathbb{F}_q$, so there are q tuples (A, B) such that $4A^3 + 27B^2 = 0$. Therefore, there are $q^2 - q$ short nonsingular Weierstrass equations over $\mathbb{F}_q$. We deal precisely with the case $q \equiv 1 \bmod 12$, where $\mathbb{F}_q^*$ contains an element of order 6 and an element of order 4. In that case, if E is given by $y^2 = x^3 + Ax + B$ with $A = 0$, there are $\frac{q-1}{6}$ elliptic curves in the isomorphism class of E. If $B = 0$, there are $\frac{q-1}{4}$ elliptic curves in this class, and if $A, B \neq 0$, the class contains $\frac{q-1}{2}$ elliptic curves. Thus, the number of classes is

$$\underbrace{\frac{q-1}{(q-1)/6}}_{A=0} + \underbrace{\frac{q-1}{(q-1)/4}}_{B=0} + \underbrace{\frac{q^2-q-2(q-1)}{(q-1)/2}}_{A\neq 0, B\neq 0} = 6 + 4 + \frac{q^2-3q+2}{(q-1)/2} = 2q + 6.$$

Reasoning analogously, we find:

- $2q + 2$ classes if $q \equiv 5 \bmod 12$,
- $2q + 4$ classes if $q \equiv 7 \bmod 12$,
- $2q$ classes if $q \equiv 11 \bmod 12$. □

2.2.2 Structure of isogeny classes of ordinary elliptic curves

For an integer t, we write $f_q(t)$ for the number of isomorphism classes (with the isomorphism defined over $\mathbb{F}_q$) in the isogeny class of elliptic curves E over $\mathbb{F}_q$ such that $t_E = t$. Our goal is to get an estimate for $f_q(t)$. To do so, we will see what are the possible endomorphism rings (over $\mathbb{F}_q$) for elliptic curves of trace of Frobenius t, and then count how many isomorphism classes have a given endomorphism ring. We first recall some facts on discriminants.

For an order $\mathcal{O}$ in an imaginary quadratic field, we denote its discriminant by $\Delta(\mathcal{O})$. An integer Δ is said to be an imaginary quadratic discriminant if it occurs as the discriminant of an imaginary quadratic order $\mathcal{O}$. In fact, imaginary quadratic discriminants are exactly the negative integers congruent to 0 or 1 mod 4 and they are in one-to-one correspondence with orders: for a discriminant Δ, we write $\mathcal{O}(\Delta)$ for the order of discriminant Δ. An imaginary quadratic discriminant Δ is said to be a fundamental discriminant if it cannot be written $\Delta = m^2\Delta'$ where m is an integer greater than 1 and Δ' is another imaginary quadratic discriminant.

Let $\mathcal{O}$ be an imaginary quadratic order. Then, there is a unique way to write $\Delta(\mathcal{O}) = u^2\Delta_K$ where Δ_K is a fundamental discriminant. Moreover, Δ_K is the discriminant of the ring of integers $\mathcal{O}_K$ of $K = \mathbb{Q}(\sqrt{\Delta_K})$, we have $\mathcal{O} \subseteq \mathcal{O}_K$ and $u = [\mathcal{O}_K : \mathcal{O}]$. The integer u is often called the *conductor* of the order $\mathcal{O}$, and we have the following tower of orders indexed by the divisors v of u:

$$\mathcal{O} \subseteq \ldots \subseteq \mathcal{O}(v^2\Delta_K) \subseteq \ldots \subseteq \mathcal{O}_K.$$

We denote by $\mathrm{cl}(\mathcal{O})$ the ideal class group of $\mathcal{O}$ (invertible $\mathcal{O}$-ideals modulo invertible principal ideals) and by $h(\mathcal{O})$ its cardinality. Finally, we define

$$H(\Delta(\mathcal{O})) := \sum_{\mathcal{O}\subseteq\mathcal{O}'} h(\mathcal{O}'). \tag{2.3}$$

In the ordinary case and if $t^2 < 4q$, the quantity $f_q(t)$ can be expressed in terms of this function H. We also give the formulas for the other cases, but we will only sketch the proof for the first case (for the other cases, see [Sch87, Theorem 4.6]). We also assume that $p = \mathrm{char}(\mathbb{F}_q) > 3$ (we have similar expressions for $p = 2, 3$).

Proposition 2.12. *The number $f_q(t)$ is equal to:*

- $H(t^2 - 4q)$ *if* $t^2 < 4q$ *and* $p \nmid t$,
- $H(-4p)$ *if* $t = 0$ *and q is not a square,*

- $\frac{1}{12}\left(p+6-4\left(\frac{-3}{p}\right)-3\left(\frac{-4}{p}\right)\right)$ *if* $t^2=4q$ *and* q *is a square,*
- $1-\left(\frac{-3}{p}\right)$ *if* $t^2=q$ *and* q *is a square,*
- $1-\left(\frac{-4}{p}\right)$, *if* $t=0$ *and* q *is a square,*
- 0 *otherwise.*

Let t be an integer such that $t^2-4q\leq 0$ and $p\nmid t$, and E an elliptic curve of trace of Frobenius t. We have seen that $\mathrm{End}_{\mathbb{F}_q}(E)$ contains $\mathbb{Z}[\phi_q]\cong\mathcal{O}(t^2-4q)$. Waterhouse proved that all the orders containing $\mathcal{O}(t^2-4q)$ occur as the endomorphism ring of some elliptic curve with trace of Frobenius t (see [Wat69, Theorem 4.2]).

Let $\mathcal{O}$ be an imaginary quadratic order such that $\mathcal{O}(t^2-4q)\subseteq\mathcal{O}$. Denote by $\mathrm{Ell}_{\mathbb{F}_q}(\mathcal{O})$ the set of isomorphism classes of elliptic curves having $\mathcal{O}$ as their endomorphism ring. Then, we can define an action of the ideal class group of $\mathcal{O}$ on $\mathrm{Ell}_{\mathbb{F}_q}(\mathcal{O})$ as follows. Let E be an elliptic curve such that $\mathrm{End}_{\mathbb{F}_q}(E)\cong\mathcal{O}$ and $\mathfrak{a}$ be an ideal of $\mathcal{O}$. We define the $\mathfrak{a}$-torsion subgroup of E as

$$E[\mathfrak{a}]:=\{P\in E(\overline{\mathbb{F}_q})\ :\ \forall\alpha\in\mathfrak{a},\alpha(P)=O_E\}.$$

This is a finite subgroup of $E(\overline{\mathbb{F}_q})$ generalising $E[\ell]$. Therefore, there are a unique elliptic curve $E_{\mathfrak{a}}$ and an isogeny $\phi:E\to E_{\mathfrak{a}}$ such that $\ker(\phi)=E[\mathfrak{a}]$ by Proposition 2.6. One can show that $\mathrm{cl}(\mathcal{O})$ acts on $\mathrm{Ell}_{\mathbb{F}_q}(\mathcal{O})$ by

$$\begin{cases}\mathrm{cl}(\mathcal{O})\times\mathrm{Ell}_{\mathbb{F}_q}(\mathcal{O}) & \to & \mathrm{Ell}_{\mathbb{F}_q}(\mathcal{O})\\ (\mathfrak{a},E) & \mapsto & E_{\mathfrak{a}}\end{cases}$$

It can be shown that this action is free. In our case, this action has one orbit (in the supersingular case, this action can have two orbits, see [Sch87, Theorem 4.5]). Therefore, we have $|\mathrm{Ell}_{\mathbb{F}_q}(\mathcal{O})|=h(\mathcal{O})$.

This equality is also established in [Cox13, § 14.C], with a slightly different strategy. First, the author used the theory of complex multiplication over $\mathbb{C}$, where it is easier to show that the group action of the ideal class field of $\mathcal{O}$ is free and has one orbit, and then he reduced to the case of finite fields through the Deuring lifting theorem.

Hence, equation (2.3) shows that for $|t|\leq 2\sqrt{q}$,

$$f_q(t)=\sum_{\mathcal{O}(t^2-4q)\subseteq\mathcal{O}}|\mathrm{Ell}_{\mathbb{F}_q}(\mathcal{O})|=\sum_{\mathcal{O}(t^2-4q)\subseteq\mathcal{O}}h(\mathcal{O})=H(t^2-4q).$$

2.2.3 An upper bound on $f_q(t)$

We will now estimate $H(t^2-4q)$ by writing it as a special value of an L-function (up to some constant). Our goal is to prove the following:

Proposition 2.13. *We have* $f_q(t) \ll q^{1/2}\log(q)\log(\log(q))$.

For the expressions which don't involve H in Proposition 2.12, it is not hard to see that this estimate holds. We now estimate $H(\Delta)$ by analytic means for any discriminant Δ.

We write $\Delta = u^2\Delta_K$ where Δ_K is a fundamental discriminant. The Jacobi symbol is denoted by $\left(\frac{\cdot}{\cdot}\right)$ as usual.

Definition 2.14. The Kronecker symbol $\chi_\Delta : \mathbb{Z}_{>0} \to \{0,1,-1\}$ associated to Δ is the completely multiplicative character such that $\chi_\Delta(\ell) = \left(\frac{\Delta}{\ell}\right)$ if ℓ is an odd prime and $\chi_\Delta(2) = \begin{cases} 0 & \text{if } \Delta \equiv 0 \bmod 4, \\ 1 & \text{if } \Delta \equiv 1 \bmod 8, \\ -1 & \text{if } \Delta \equiv 5 \bmod 8. \end{cases}$

One can check that for a prime p, we have $\chi_\Delta(p) = \chi_{\Delta_K}(p)\chi_{u^2}(p)$. In particular, $\chi_\Delta(p) = 0$ if $p \mid u$, else $\chi_\Delta(p) = \chi_{\Delta_K}(p)$.

To the character χ_Δ, we associate the L-function $L(s,\chi_\Delta) = \sum_{n=1}^{+\infty} \frac{\chi_\Delta(n)}{n^s}$. The previous remark shows that we have

$$L(s,\chi_\Delta) = L(s,\chi_{\Delta_K}) \prod_{\substack{\ell \mid u \\ \ell \text{ prime}}} \left(1 - \frac{\chi_{\Delta_K}(\ell)}{\ell^s}\right)$$

and for a divisor d of u:

$$L(s,\chi_{\Delta/d^2}) = L(s,\chi_\Delta) \prod_{\substack{\ell \mid u \\ \ell \nmid \frac{u}{d}}} \frac{1}{\left(1 - \frac{\chi_{\Delta_K}(\ell)}{\ell^s}\right)}.$$

We recall Dirichlet's class number formula.

Proposition 2.15. *We have*

$$h(\Delta) = \frac{w_\Delta \sqrt{|\Delta|}}{2\pi} L(1,\chi_\Delta),$$

where $w_\Delta = \begin{cases} 2 & \text{if } \Delta < -4, \\ 4 & \text{if } \Delta = -4, \\ 6 & \text{if } \Delta = -3. \end{cases}$

Proof. See [Dav80, Chapter 6]. □

The next lemma gives an estimate for the special value $L(1, \chi_\Delta)$ which appears in the last formula.

Lemma 2.16. *We have* $L(1, \chi_\Delta) = O(\log(|\Delta|))$.

Proof. See for instance [Lou92]. □

We are now ready to prove that $H(\Delta) \ll |\Delta|^{1/2} \log(|\Delta|) \log(\log(|\Delta|))$ following McKee [McK99]. We write

$$\begin{aligned} H(\Delta) &= \sum_{\substack{d|u \\ d>0}} h\left(\frac{\Delta}{d^2}\right) \\ &= \sum_{d|u} \frac{w_{\Delta/d^2}\sqrt{|\Delta|}}{2\pi d} L(1, \chi_{\Delta/d^2}) \\ &= \sum_{d|u} \frac{w_{\Delta/d^2}\sqrt{|\Delta|} L(1, \chi_\Delta)}{2\pi d} \prod_{\substack{\ell|u \\ \ell\nmid \frac{u}{d}}} \left(1 - \frac{\chi_{\Delta_K}(\ell)}{\ell}\right)^{-1} \\ &\ll \sqrt{|\Delta|} L(1, \chi_\Delta) \underbrace{\sum_{d|u} \frac{1}{d} \prod_{\substack{\ell|u/d \\ \ell\nmid \frac{u}{d}}} \left(1 - \frac{\chi_{\Delta_K}(\ell)}{\ell}\right)^{-1}}_{\Psi(u)}. \end{aligned}$$

In the last line, we defined a function Ψ, which is multiplicative. Moreover, one can check that if p is prime and n is a positive integer,

$$\Psi(p^n) = \begin{cases} \frac{p - p^{-n}}{p-1} & \text{if } \chi_{\Delta_K}(\ell) = 0, \\ \frac{p - 2/(p^n + p^{n-1})}{p-1} & \text{if } \chi_{\Delta_K}(\ell) = -1, \\ \frac{p}{p-1} & \text{otherwise.} \end{cases}$$

By multiplicativity,

$$1 \le \Psi(u) \le \prod_{\ell|u} \frac{\ell}{\ell - 1} \le \frac{u}{\varphi(u)} \ll \log(\log(u))$$

where the last inequality is a consequence of the classical inequality $\frac{n}{\log(\log(n))} \ll \varphi(n)$ for Euler's totient function φ. Combining this with Lemma 2.16, we get

$$H(\Delta) \ll |\Delta|^{1/2} \log(|\Delta|) \log(\log(|\Delta|)).$$

Since $-4q < t^2 - 4q < 0$, we have

$$H(t^2 - 4q) \ll q^{1/2} \log(q) \log(\log(q)),$$

so Proposition 2.13 is proven.

2.3 Elliptic curves over $\mathbb{Q}$

The article [SS15] considers the case of an elliptic curve E defined over $\mathbb{Q}$, and its reductions modulo prime numbers p. In this subsection, we recall some facts about reductions of elliptic curves. We also introduce the conductor and Galois representations associated to an elliptic curve, which are the key ingredients to prove the lemmas of the paragraph 3.3.

2.3.1 Reminders of algebraic number theory

Let L be a Galois number field, p a prime number and $\mathfrak{p}$ a prime of L lying above p. We define the decomposition group of $\mathfrak{p}$ as $G_\mathfrak{p} := \{\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$. The fields L and $\mathbb{Q}$ are respectively dense in $L_\mathfrak{p}$ and $\mathbb{Q}_p$, so the decomposition subgroup $G_\mathfrak{p}$ is isomorphic to the Galois group $\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)$ (an element $\sigma \in G_\mathfrak{p}$ can be uniquely extended by continuity to an element of $\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)$). The inertia subgroup $I(L_\mathfrak{p}/\mathbb{Q}_p)$ of the extension $L_\mathfrak{p}/\mathbb{Q}_p$ is defined as as the subgroup of the elements of $G_\mathfrak{p}$ that act trivially on the residue field $\mathbb{F}_\mathfrak{p}$ of $L_\mathfrak{p}$. It is the kernel of the reduction map modulo $\mathfrak{p}$ denoted by $\pi(\mathfrak{p}/p)$. The absolute inertia group of $\mathbb{Q}_p$ denoted by $I(\overline{Q_p}/\mathbb{Q}_p)$ is defined as the subgroup pf elements of $\mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ that act trivially on $\overline{F_p}$. We have the following system of short exact sequences (see Wiese [Wie08]):

$$\begin{array}{ccccccccc} 1 & \longrightarrow & I(L_\mathfrak{p}/\mathbb{Q}_p) & \longrightarrow & \mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p) & \xrightarrow{\pi(\mathfrak{p}/p)} & \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p) & \longrightarrow & 1 \\ & & \uparrow\!\uparrow & & \uparrow\!\uparrow & & \uparrow\!\uparrow & & \\ 1 & \longrightarrow & I(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) & \longrightarrow & \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p) & \longrightarrow & 1. \end{array} \tag{2.4}$$

The order of $I(L_\mathfrak{p}/\mathbb{Q}_p)$ is actually the ramification index of the prime p in $L/\mathbb{Q}$ (in particular, p is unramified in $L/\mathbb{Q}$ if and only if $I(L_\mathfrak{p}/\mathbb{Q}_p)$ is trivial). We denote

by $\mathrm{Frob}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ the Frobenius element in $\mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ (the extension $\mathbb{F}_\mathfrak{p}/\mathbb{F}_p$ being an extension of finite fields of characteristic p). Assuming that p is unramified in $L/\mathbb{Q}$, the reduction map $\pi(\mathfrak{p}/p)$ is an isomorphism. The preimage of $\mathrm{Frob}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ in $\mathrm{Gal}(L_\mathfrak{p}/\mathbb{Q}_p)$ is called a Frobenius element of $L/\mathbb{Q}$ at p and we denote it by $\mathrm{Frob}_{\mathfrak{p}/p}$. If we take another prime $\mathfrak{P} = \sigma(\mathfrak{p})$ of L lying above p (with $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$), then

$$\mathrm{Frob}_{\mathfrak{P}/p} = \sigma \circ \mathrm{Frob}_{\mathfrak{p}/p} \circ \sigma^{-1}.$$

So, the Frobenius element at p of $L/\mathbb{Q}$ is in fact defined up to conjugation.

Now, let L/K be a finite Galois extension of local fields. We denote by v_L the normalised valuation of L and by R_L its ring of integers. For an integer $i \geq -1$, the i-th higher ramification group of L/K is

$$G_i(L/K) := \{\sigma \in \mathrm{Gal}(L/K) \ : \ \forall \alpha \in R_L, v_L(\sigma(\alpha) - \alpha) \geq i + 1\}$$

and we define $g_i(L/K) := |G_i(L/K)|$.

As for $\mathbb{Q}_p$, the absolute inertia group of K, denoted by $I(\overline{K}/K)$ is defined as the subgroup of elements of $\mathrm{Gal}(\overline{K}/K)$ that act trivially on the algebraic closure of the residue field of K.

2.3.2 Reductions of an elliptic curve

Let E be an elliptic curve defined over $\mathbb{Q}$ given by the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{2.5}$$

For a prime p, we denote the p-adic valuation by v_p. The change of variables

$$(x, y) \mapsto (p^{-2}x, p^{-3}y)$$

replaces the coefficients a_i by $p^i a_i$ for every $i \in \{1, 2, 3, 4, 5, 6\}$ in the previous equation. We now assume without loss of generality that $v_p(a_i) \geq 0$ for every i. Then, we have $v_p(\Delta) \geq 0$ and we say that the Weierstrass equation is minimal at p if the value of $v_p(\Delta)$ is minimal. According to [Sil09, Theorem VIII.8.3], there exists a Weierstrass equation that is minimal for every prime p. We call its discriminant Δ_E the minimal discriminant of the elliptic curve E.

It is possible to reduce the coefficients of a minimal equation of the form (2.5) modulo p to obtain a Weierstrass equation having coefficients in the field $\mathbb{F}_p$ and a curve E_p over $\mathbb{F}_p$. This curve is nonsingular if $v_p(\Delta_E) = 0$. Otherwise, the curve E_p has exactly one singular point P. We say that P is a *cusp* if the curve has one tangent direction at P, and that it is a *node* if it has two distinct tangent directions at P.

Definition 2.17. The elliptic curve E is said to have good reduction modulo p if the curve E_p is nonsingular (and thus an elliptic curve). Otherwise, it is said to have bad reduction modulo p. If the singular point is a cusp, we say that E has additive reduction and if it is a node, we say that E has multiplicative reduction.

Remark 2.18. Let ${E_p}^{ns}(\overline{\mathbb{F}_p})$ be the set of the nonsingular points of E_p over $\overline{\mathbb{F}_p}$. If E has multiplicative reduction, one can show that ${E_p}^{ns}(\overline{\mathbb{F}_p})$ is isomorphic to the multiplicative group $\overline{\mathbb{F}_p}^*$, and if E has additive reduction, then ${E_p}^{ns}(\overline{\mathbb{F}_p})$ is isomorphic to the additive group $\overline{\mathbb{F}_p}^+$. This explains the previous terminology.

Primes p of bad reduction are the prime divisors of the minimal discriminant. Thus, there are finitely many primes of bad reduction.

For more about reductions of elliptic curves, we refer the reader to [Sil09, Chapter VII].

2.3.3 Division fields and Galois representations

Let m be a positive integer and p be a prime. Let k be either $\mathbb{Q}_p$ or $\mathbb{Q}$. Since the elliptic curve E is defined over $\mathbb{Q}$, it can be seen as an elliptic curve over $\mathbb{Q}_p$. The field $k(E[m])$ is defined as the extension of k obtained by adding the coordinates of the points of $E[m]$. In the case $k = \mathbb{Q}$, it is called the m-th division field of E.

Proposition 2.19. *The extension $k(E[m])/k$ is Galois.*

Proof. We first prove that the coordinates of the elements of $E[m]$ are algebraic elements over $\mathbb{Q}$. Let $P = (x_P, y_P)$ be a point of $E[m]$ and let m' be the smallest positive integer such that $[m']P = 0$. Then, $[m'-1]P = -P$, and we know from the explicit formulas for the group law that the x-coordinate of $[m'-1]P$ and $-P$ are rational functions of x_P with rational coefficients. Thus, x_P is a root of a nonzero polynomial having rational coefficients: x_P is algebraic over k. It is also the case for y_P because $y_P^2 = x_P^3 + Ax_P + B$ where $y^2 = x^3 + Ax + B$ is a Weierstrass equation for E. Thus, $k(E[m])$ is an algebraic extension of k. To prove that it is Galois, it is enough to show that if $\sigma \in \mathrm{Hom}_k(k(E[m], \overline{k})$, then $\sigma(k(E[m])) \subseteq k(E[m])$. For a point $P \in E[m]$ different from the point at infinity O_E, we define $\widetilde{\sigma}(P) = (\sigma(x_P), \sigma(y_P))$, and $\widetilde{\sigma}(O_E) = O_E$. For $P \in E[m]$, $\widetilde{\sigma}(P)$ is also an element of $E[m]$. Thus, $\sigma(x_P)$ is in $k(E[m])$ and $\sigma(y_P)$ is in $k(E[m])$, which proves that $\sigma(k(E[m])) \subseteq k(E[m])$. □

Every element $\sigma \in \mathrm{Gal}(k(E[m])/k)$ acts on the points of E by

$$\sigma \cdot P = (\sigma(x_P), \sigma(y_P))$$

if $P = (x_P, y_P)$ is not the point at infinity O_E (and $\sigma \cdot O_E = O_E$). If P is an m-torsion point, then we also have $\sigma \cdot P \in E[m]$. Thus, this action defines a representation $\mathrm{Gal}(k(E[m])/k) \to \mathrm{Aut}(E[m])$. Setting $k = \mathbb{Q}$, we have seen that

$$E[m] \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

so $\mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$. We obtain an injective representation

$$\rho_m : \mathrm{Gal}(\mathbb{Q}(E[m])/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

We now ask when this representation is surjective. From now on, we assume that E doesn't have complex multiplication. A famous result from Serre, called Serre's open image theorem, says that there exists a finite set of primes $S(E)$ such that ρ_ℓ is surjective if $\ell \notin S(E)$. We define $A(E) = 2 \cdot 3 \cdot 5 \cdot \prod_{\ell \in S(E)} \ell$, which is sometimes called Serre's constant associated to E. It can be shown (see [Coj05, Appendix A]) that if $\gcd(m, A(E)) = 1$, then ρ_m is surjective. In that case, the extension $\mathbb{Q}(E[m])/\mathbb{Q}$ has Galois group $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$.

Serre asked if there is an absolute constant C independent of E such that the representation ρ_ℓ is bijective if $\ell > C$. This is still an open problem, but we have upper bounds for $A(E)$ in terms of the conductor of E, which will be introduced in the next paragraph.

In the proof of Lemma 3.16, we will have to consider a representation into $\mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})$ instead of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$, which we construct from ρ_m by projecting $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ into $\mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})$. We call $\overline{\rho_m}$ this new representation, it is no longer injective. Let $L_{m,E}$ be the subfield of $\mathbb{Q}(E[m])$ fixed by the nonzero scalar matrices. By Galois theory, we have $\mathrm{Gal}(L_{m,E}/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})$ and the representation

$$\overline{\rho_m} : \mathrm{Gal}(L_{m,E}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})$$

is bijective.

2.3.4 The conductor of an elliptic curve

We now give the definition of the exponent of the conductor of the elliptic curve E at a prime p. For a prime $\ell \neq p$, we write $V_\ell(E) = T_\ell(E) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell$ and $L_{p,\ell} = \mathbb{Q}_p(E[\ell])$. We denote by $V_\ell(E)^{I(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)}$ the subspace of $V_\ell(E)$ fixed by $I(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)$ and by $E[\ell]^{G_i(L_{p,\ell})/\mathbb{Q}_p}$ the subgroup of $E[\ell]$ fixed by $G_i(L_{p,\ell}/\mathbb{Q}_p)$. This following definition comes from a general formula for Galois representations.

Definition 2.20. The exponent $f_p(E)$ is defined as $f_p(E) = \varepsilon_p(E) + \delta_p(E)$, where

$$\begin{cases} \varepsilon_p(E) & = \dim_{\mathbb{Q}_\ell}(V_\ell(E)/V_\ell(E)^{I(\overline{\mathbb{Q}_p}/\mathbb{Q}_p)}), \\ \delta_p(E) & = \sum_{i=1}^{+\infty} \frac{g_i(L_{p,\ell}/\mathbb{Q}_p)}{g_0(L_{p,\ell}/\mathbb{Q}_p)} \dim_{\mathbb{F}_\ell} \left(E[\ell]/E[\ell]^{G_i(L_{p,\ell}/\mathbb{Q}_p)}\right). \end{cases}$$

The conductor of E is the integer $N_E = \prod_{p \text{ prime}} p^{f_p(E)}$.

In fact, it turns out that this definition is independent of ℓ. It seems unpractical for computing $\varepsilon_p(E)$ and $\delta_p(E)$, but we have the following criterion:

Proposition 2.21. *We have*

$$\varepsilon_p(E) = \begin{cases} 0 & \text{if } E \text{ has good reduction modulo } p, \\ 1 & \text{if } E \text{ has multiplicative reduction modulo } p, \\ 2 & \text{if } E \text{ has additive reduction modulo } p. \end{cases}$$

Moreover, if $p \geq 5$, $\delta_p(E) = 0$.

The primes which divide N_E are the primes of bad reduction. It has the same prime divisors as the minimal discriminant and it can be seen as a measurement of the arithmetic complexity of the curve.

We now give an upper bound for $A(E)$ in terms of the conductor (see Theorem 1 in [Coj05]).

Proposition 2.22. *Assuming the Generalised Riemann Hypothesis (GRH), there is a constant* $c > 0$ *such that* $A(E) \leq c \log(N_E) \log(\log(2N_E))^3$.

We denote by $\mathcal{P}(\mathbb{Q}(E[m]))$ the set of primes which ramify in $\mathbb{Q}(E[m])/\mathbb{Q}$.

Proposition 2.23. *The elements of* $\mathcal{P}(\mathbb{Q}(E[m]))$ *lie among the prime divisors of* $m \cdot N_E$.

Proof. In this proof, we will write $L = \mathbb{Q}(E[m])$ to ease notation. Let p be a prime which doesn't divide mN_E, and $\mathfrak{p}$ be a prime ideal of L above p.

By definition of L, we have the following diagram

$$\begin{array}{ccc} I(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \subseteq \mathrm{Gal}(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) & \longrightarrow & \mathrm{GL}(E[m]) \\ & \searrow \quad \nearrow & \\ & \mathrm{Gal}(L_{\mathfrak{p}}/\mathbb{Q}_p) & \end{array}$$

By using the diagram 2.4, we get

$$I(L_{\mathfrak{p}}/\mathbb{Q}_p) = \mathrm{Im}(I(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathrm{Gal}(L_{\mathfrak{p}}/\mathbb{Q}_p)) \cong \mathrm{Im}(I(\overline{\mathbb{Q}_p}/\mathbb{Q}_p) \to \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})).$$

According to the criterion of Néron-Ogg-Shafarevich (see [Sil09, § VII.7]), since p doesn't divide mN_E, the representation ρ_m is unramified at p, which means that the restriction of ρ_m to $I(\overline{\mathbb{Q}_p}/\mathbb{Q})$ is trivial. Therefore, $I(L_{\mathfrak{p}}/\mathbb{Q}_p)$ is trivial, which precisely means that p is unramified in $L/\mathbb{Q}$. □

The values of $\mathrm{tr}(\rho_m(\sigma_p))$ and $\det(\rho_m(\sigma_p)) \bmod m$ are known if $p \nmid mN_E$.

Proposition 2.24. *For $p \nmid mN_E$, we have*

$$\begin{cases} \mathrm{tr}(\rho_m(\sigma_p)) & \equiv t_{E_p} \bmod m \\ \det(\rho_m(\sigma_p)) & \equiv p \bmod m, \end{cases}$$

where σ_p is a Frobenius element at p in $\mathbb{Q}(E[m])/\mathbb{Q}$ and t_{E_p} is the trace of Frobenius of the reduction of E modulo p.

Proof. Again, we write $L = \mathbb{Q}(E[m])$. Let p be a prime which doesn't divide $m \cdot N_E$ and $\mathfrak{p}$ a prime of L lying above p. We denote by

$$\pi(\mathfrak{p}/p) : \mathrm{Gal}(L_{\mathfrak{p}}/\mathbb{Q}_p) \to \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$$

the reduction map modulo p. We will see $E[m]$ as a set of points of $L_{\mathfrak{p}}$, and we can consider the reduction map $\widetilde{\pi}(\mathfrak{p}/p) : E[m] \mapsto E_p[m]$. The Galois group $\mathrm{Gal}(L_{\mathfrak{p}}/\mathbb{Q}_p)$ (resp. $\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$) acts naturally on $E[m]$ (resp. $E_p[m]$). By definition of $\pi(\mathfrak{p}/p)$ and $\widetilde{\pi}(\mathfrak{p}/p)$, the following diagram is commutative:

$$\begin{array}{ccc} \mathrm{Gal}(L_{\mathfrak{p}}/\mathbb{Q}_p) & \xrightarrow{\pi(\mathfrak{p}/p)} & \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p) \\ \downarrow & & \downarrow \\ \mathrm{GL}(E[m]) & \xrightarrow{\widetilde{\pi}(\mathfrak{p}/p)} & \mathrm{GL}(E_p[m]) \end{array}$$

We denote by ϕ_p the Frobenius endomorphism of the elliptic curve E_p. Since $p \nmid m$, the group $E_p[m]$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. Then, the Frobenius endomorphism ϕ_p can be identified to an element of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ and by Proposition III.8.6 of [Sil09], we have $\mathrm{tr}(\phi_p) \equiv t_{E_p} \bmod m$ and $\det(\phi_p) \equiv p \bmod m$. The element $\mathrm{Frob}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p) \in \mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}/\mathbb{F}_p)$ acts naturally on $E_p[m]$ in the same way as ϕ_p.

We have seen that in $\mathrm{Gal}(L/\mathbb{Q})$, Frobenius elements are defined up to conjugation. It doesn't matter in our case, because the trace and the determinant are conjugacy-invariant. So, we consider here that σ_p is the element of the conjugacy class such

that $\sigma_p(\mathfrak{p}) = \mathfrak{p}$. Then, σ_p is the preimage of $\mathrm{Frob}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ by $\pi(\mathfrak{p}/p)$. Since the previous diagram is commutative, we have $\mathrm{tr}(\rho_m(\sigma_p)) \equiv \mathrm{tr}(\phi_p) \equiv t_{E_p} \bmod m$ and $\det(\rho_m(\sigma_p)) \equiv \det(\phi_p) \equiv p \bmod m$.

□

2.4 Counting points on elliptic curves

Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$. There are several methods and algorithms to determine $|E(\mathbb{F}_q)|$. A very naive one is to check whether (x, y) satisfies the Weierstrass equation defining E for every element $(x, y) \in (\mathbb{F}_q)^2$. However, the complexity of this method is $O(q^2)$, so it is unpractical in practice and especially for crypto-sized finite fields (for instance, $q \approx 2^{256}$). In this subsection, we present Schoof's algorithm and the SEA algorithm.

2.4.1 Schoof's algorithm

It was introduced by Schoof in 1985 in [Sch85]. The idea is to compute the trace of Frobenius t_E of E modulo ℓ for sufficiently small primes ℓ. Indeed, since $|t_E| \leq 2\sqrt{q}$, it suffices to consider primes $\ell \leq \ell_{max}$ such that $\prod_{\ell \leq \ell_{max}} \ell > 4\sqrt{q}$ and to reconstruct t_E through the Chinese Remainder Theorem.

Let ℓ be an odd prime and P be an ℓ-torsion point of E different from O_E (the point P is not required to be rational). Denote its coordinates by (x_P, y_P). Evaluating the characteristic equation of the Frobenius endomorphism ϕ_q at P gives

$$(x_P^{q^2}, y_P^{q^2}) - [t_E](x_P^q, y_P^q) + [q](x, y) = O_E.$$

Since P is ℓ-torsion, one can reduce t_E and q modulo ℓ in the previous equation:

$$(x_P^{q^2}, y_P^{q^2}) - [t_E \bmod \ell](x_P^q, y_P^q) + [q \bmod \ell](x_P, y_P) = 0.$$

In order to avoid working with polynomials of large degree, we perform the computations in the ring

$$R_\ell = \frac{\mathbb{F}_q[x, y]}{(y^2 - x^3 - ax - b, \psi_\ell(x))},$$

where ψ_ℓ is the ℓ-th division polynomial of E introduced in Definition 2.9. Its roots are the x-coordinates of the ℓ-torsion points. For $\ell \neq \mathrm{char}(\mathbb{F}_q)$, we recall that $|E[\ell]| = \ell^2$, so ψ_ℓ has degree $\frac{\ell^2-1}{2}$. Computing x^q, y^q, x^{q^2} and y^{q^2} in R_ℓ takes $\widetilde{O}(\ell^2 \log(q)^2)$ bit operations using exponentiation by squaring.

Chebyshev's theorem implies that

$$\sum_{\substack{\ell \leq x \\ \ell \text{ prime}}} \log(\ell) \sim x.$$

Therefore, $\ell_{max} \approx \log(4\sqrt{q})$. For instance, if $q \approx 2^{256}$ (a classical size for cryptography), then we get $\ell_{max} \approx 10^2$. Therefore, the primes ℓ considered are in $O(\log(q))$, so the computations in R_ℓ take $\widetilde{O}(\log(q)^4)$ bit operations. Since the number of primes ℓ is in $O(\log(q))$, the total complexity of Schoof's algorithm is $\widetilde{O}(\log(q)^5)$.

We describe Schoof's algorithm below in Algorithm 1.

Algorithm 1: Schoof's algorithm

Data: The elliptic curve E
Result: The trace of Frobenius of E

Pick a set of odd primes $\ell \leq \ell_{max}$ such that $\prod_{\ell \leq \ell_{max}} \ell > 4\sqrt{q}$
for $\ell \leq \ell_{max}$ **do**
  $n \leftarrow 0$
  Set $R_\ell = \frac{\mathbb{F}_q[x,y]}{(y^2 - x^3 - ax - b, \psi_\ell(x))}$
  $Q_0 \leftarrow (x^{q^2}, y^{q^2}) + [q](x, y)$
  $Q_1 \leftarrow (x^q, y^q)$
  $Q_2 \leftarrow O_E$
  while $Q_0 - [n]Q_1 \neq O_E$ **do**
    $n \leftarrow n + 1$
    $Q_2 \leftarrow Q_2 + Q_1$
  end
  $t_\ell \leftarrow n$
end
Find $t \in [-2\sqrt{q}, 2\sqrt{q}]$ such that $t \equiv t_\ell \bmod \ell$ for every ℓ with the Chinese Remainder theorem
Return t

2.4.2 The SEA algorithm

For fields of cryptographic size, Schoof's algorithm tends to be rather inefficient (according to Sutherland's lecture notes [Sut22], it might take one or two days to

compute $|E(\mathbb{F}_q)|$ when $q \approx 2^{256}$ with an implementation of the algorithm in *SageMath*). It received improvements by Elkies and Atkin in the nineties which led to the SEA (Schoof-Elkies-Atkin) algorithm. It is currently the best method for fields of large characteristic.

Remark 2.25. For "small" fields, some other algorithms such as baby-step giant-step are more efficient than SEA. In *SageMath*, for an elliptic curve E defined over a prime field $\mathbb{F}_p$, the SEA algorithm is used whenever $p > 10^{18}$, but different algorithms are used under this value of p.

We now link the existence of an isogeny of degree ℓ from E to an arithmetic condition on the discriminant of the characteristic polynomial of the endomorphism of Frobenius.

Proposition 2.26. *Let E be an elliptic curve defined over $\mathbb{F}_q$ and ℓ be a prime different from $p = \mathrm{char}(\mathbb{F}_q)$. Then, the three following statements are equivalent:*

(i) There is a separable isogeny $\varphi : E \to E'$ of degree ℓ defined over $\mathbb{F}_q$.

(ii) There is a subgroup $C \subseteq E[\ell]$ of order ℓ defined over $\mathbb{F}_q$.

(iii) $\left(\frac{t_E^2 - 4q}{\ell}\right) \neq -1$.

Proof. The statements (i) and (ii) are equivalent as a consequence of Proposition 2.6, so we just prove the equivalence between (ii) and (iii). We recall that the Frobenius endomorphism ϕ_q, seen as an endomorphism of the 2-dimensional $\mathbb{F}_\ell$-vector space $E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$, has characteristic polynomial

$$X^2 - (t_E \bmod \ell)X + q \bmod \ell$$

(see Proposition III.8.6. in [Sil09]). Its discriminant is $t_E^2 - 4q \bmod \ell$. Since the Frobenius endomorphism $x \mapsto x^q$ generates $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$, the existence of a subgroup $C \subseteq E[\ell]$ defined over $\mathbb{F}_q$ is equivalent to the existence of a 1-dimensional eigenspace of $\phi_q \in \mathrm{GL}(E[\ell])$. This is equivalent to the existence of a root of the characteristic polynomial over $\mathbb{F}_\ell$. A root exists if and only if the discriminant of the polynomial is a square in $\mathbb{F}_\ell$. □

A subgroup $C \subseteq E[\ell]$ of order ℓ defined over $\mathbb{F}_q$ is described by a polynomial $h(x)$ of degree $\frac{\ell-1}{2}$ which is a factor of $\psi_\ell(x)$.If such a C exists, we can replace the ring R_ℓ in Schoof's algorithm by

$$\frac{\mathbb{F}_q[x, y]}{(y^2 - x^3 - ax - b, h(x))},$$

in which it is faster to compute x^q, y^q, x^{q^2} and y^{q^2}.

Definition 2.27. Let E be an elliptic curve defined over a finite field $\mathbb{F}_q$ and $t_E^2 - 4q$ its Frobenius discriminant. An odd prime $\ell \nmid q$ is said to be an Elkies prime for E if $t_E^2 - 4q$ is a quadratic residue modulo ℓ, otherwise ℓ is said to be an Atkin prime.

There are some other modifications due to Atkin to compute a set of possible values of $t_E \bmod \ell$ if ℓ is an Atkin prime.

In the SEA algorithm, one computes $t_E \bmod \ell$ using Elkies' method for small Elkies primes $\ell \leq \ell_{max}$ such that $\prod_{\ell \leq \ell_{max}} \ell > 4\sqrt{q}$ (here, ℓ_{max} is not the same as in Schoof's algorithm). Therefore one needs that lots of primes are Elkies to make significant improvements compared to Schoof's algorithm. Given an odd prime ℓ, there are $\frac{\ell+1}{2}$ quadratic residues modulo ℓ. Hence, the heuristic is that 50% of the primes are Elkies primes for E. In that case, the complexity of the algorithm is $\widetilde{O}(\log(q)^4)$ using exponentiation by squaring.

3 Distribution of Elkies and Atkin primes

Our goal is to introduce the proofs of two theorems about the distribution of Atkin and Elkies primes, established by Shparlinski and Sutherland [SS14, SS15]. Both are results on average over a class of elliptic curves. In the first one, we fix a finite field $\mathbb{F}_q$ and we consider all the elliptic curves defined over $\mathbb{F}_q$. In the second one, we consider the set of the reductions of an elliptic curve E defined over $\mathbb{Q}$ modulo primes of good reduction.

3.1 Statements of the main theorems

We fix a finite field $\mathbb{F}_q$. As in Proposition 2.11, we denote by $\mathcal{E}_q$ a set of representatives of all isomorphism class of elliptic curves defined over $\mathbb{F}_q$. For an elliptic curve E defined over $\mathbb{F}_q$ and a real number $L \geq 3$, we denote by $N_e(E, L)$ (resp. $N_a(E, L)$) the number of Elkies (resp. Atkin) primes for E in the interval $[L, 2L]$. In the statement of the theorem, $N_*(E, L)$ is either $N_e(E, L)$ or $N_a(E, L)$.

Theorem 3.1. *Let $\nu \geq 1$ be an integer. Then we have*

$$\begin{aligned}&\frac{1}{|\mathcal{E}_q|}\sum_{E\in\mathcal{E}_q}\left|N_*(E,L)-\tfrac{1}{2}(\pi(2L)-\pi(L))\right|^{2\nu}\\ &=O\left(\frac{L^\nu}{\log(L)^\nu}\log(q)\log(\log(q))+\frac{L^{2\nu}}{\log(L)^{2\nu}}q^{-1/2}L^\nu\log(L)\right)\end{aligned}$$

where the big-O constant just depends on ν.

The notation O (or $\ll$) for two variables (L and q) indicates that there is a constant C such that for every values of q and $L \geq 3$, we have

$$\begin{aligned}&\frac{1}{|\mathcal{E}_q|}\sum_{E\in\mathcal{E}_q}\left|N_*(E,L)-\tfrac{1}{2}(\pi(2L)-\pi(L))\right|^{2\nu}\\ &\leq C\left(\frac{L^\nu}{\log(L)^\nu}\log(q)\log(\log(q))+\frac{L^{2\nu}}{\log(L)^{2\nu}}q^{-1/2}L^\nu\log(L)\right).\end{aligned}$$

We now fix an elliptic curve E_0 defined over $\mathbb{Q}$ without complex multiplication. For a prime p of good reduction and a real number $L \geq 1$, we denote by $R_e(p, L)$ (resp. $R_a(p, L)$) the number of Elkies (resp. Atkin) primes for the reduction E_p of E_0 modulo p. We denote by $\mathcal{C}_P$ the set of primes of good reduction in $[P, 2P]$:

$$\mathcal{C}_P = \{p \in [P, 2P] \ : \ p \nmid N_{E_0}\}.$$

We have

$$|\mathcal{C}_P| = \pi(2P) - \pi(P) + O(1).$$

Again, $R_*(p, L)$ is either $R_a(p, L)$ or $R_e(p, L)$.

Theorem 3.2. *Let ν be equal to 1 or 2. Under the generalised Riemann hypothesis (GRH) we have*

$$\frac{1}{|\mathcal{C}_P|}\sum_{p\in\mathcal{C}_P}\left|R_*(p,L)-\frac{\pi(2L)-\pi(L)}{2}\right|^{2\nu}=O\left(\frac{L^\nu}{\log(L)^\nu}+\frac{L^{8\nu}\log(P)^2}{P^{1/2}\log(L)^{2\nu}}\right)$$

where the big-O constant depends on ν and E_0.

Given an elliptic curve E defined over a finite field, one expects that 50% of primes are Elkies, so there would be roughly $\frac{\pi(2L)-\pi(L)}{2}$ Elkies primes in $[L,2L]$. The left-hand sides in these two theorems quantify the difference between this expectation and the reality, on average over a family of elliptic curves. In statistical terms, they are analogous to a variance for $\nu=1$. Before proving the results, we also make a few comments on the bounds in the right-hand sides.

For Theorem 3.1, we have $0\leq N_*(E,L)\leq\pi(2L)-\pi(L)+1$ for every $E\in\mathcal{E}_q$, so a trivial bound for the left-hand side is $O(\frac{L^{2\nu}}{\log(L)^{2\nu}})$ (we recall that $\pi(L)\sim\frac{L}{\log(L)}$ by the prime number theorem). Hence, the bound of the theorem is not trivial if $q^{-1/2}L^\nu\log(L)=o(1)$ and $\log(q)\log(\log(q))=o(\frac{L^\nu}{\log(L)^\nu})$ when q becomes large. For $\nu=1$, these conditions hold if

$$(\log(q))^{1+\varepsilon}\leq L\leq q^{1/2}(\log(q))^{-3/2-\varepsilon}$$

where $\varepsilon>0$.

For Theorem 3.2, we have $0\leq R_*(p,L)\leq\pi(2L)-\pi(L)+1$ for every prime p of good reduction, so a trivial bound for the left-hand side is $O(\frac{L^{2\nu}}{\log(L)^{2\nu}})$. Hence, the bound of the theorem is not trivial when $\frac{L^{8\nu}\log(P)^2}{P^{1/2}\log(L)^{2\nu}}=o(\frac{L^{2\nu}}{\log(L)^{2\nu}})$. For $\nu=1$, this condition is satisfied as soon as

$$\Psi(P)\leq L\leq P^{1/12}\log(P)^{-1/3}\Psi(P)^{-1}$$

where Ψ is a function such that $\Psi(P)\xrightarrow[P\to+\infty]{}+\infty$.

The proofs of Shparlinski and Sutherland rely on technical lemmas on character sums. We provide this material in the next two subsections.

3.2 Technical lemmas for Theorem 3.1

The proofs of Theorems 3.1 and 3.2 will involve character sums and lemmas from analytic number theory. In this subsection, we supply the technical material that

will be used later.

The two first lemmas enable to evaluate a complete sum of Jacobi symbols.

Lemma 3.3. *Let a be an integer and let ℓ be an odd prime such that* $\gcd(a,\ell)=1$. *Then,* $\sum_{t=0}^{\ell-1}\left(\frac{t^2-a}{\ell}\right)=-1$.

Proof. We write

$$S=\sum_{t=0}^{\ell-1}\left(\frac{t^2-a}{\ell}\right)=\sum_{t=0}^{\ell-1}\left(\frac{4t^2-4a}{\ell}\right)=\sum_{t=0}^{\ell-1}\left(\frac{(2t)^2-4a}{\ell}\right)=\sum_{t=0}^{\ell-1}\left(\frac{t^2-4a}{\ell}\right).$$

Indeed, since ℓ is odd, $t\mapsto 2t$ is a bijection of $\mathbb{Z}/\ell\mathbb{Z}$ onto itself. By Euler's criterion, writing $k=\frac{\ell-1}{2}$,

$$\begin{aligned}
S &\equiv \sum_{t=0}^{\ell-1}(t^2-4a)^k \\
&\equiv \sum_{t=1}^{\ell}(t^2-4a)^k \\
&\equiv \sum_{t=1}^{\ell}\sum_{r=0}^{k}\binom{k}{r}(-4a)^{k-r}t^{2r} \\
&\equiv \sum_{r=0}^{k}\left(\binom{k}{r}(-4a)^{k-r}\sum_{t=1}^{\ell}t^{2r}\right) \bmod \ell.
\end{aligned}$$

If $n=0$, then $\sum_{t=1}^{\ell}t^n\equiv\sum_{t=1}^{\ell}1\equiv 0 \bmod \ell$. If $n\geq 1$, we know that

$$\sum_{t=1}^{\ell}t^n\equiv\begin{cases}-1 & \text{if } (\ell-1)|n,\\ 0 & \text{otherwise.}\end{cases}$$

Indeed, if $\ell-1$ divides n, then for every $t\in\{1,\dots,\ell-1\}$, $t^n\equiv 1 \bmod \ell$ by Fermat's little theorem and $\ell^n\equiv 0 \bmod \ell$. If $\ell-1$ doesn't divide n, we know that the multiplicative group $(\mathbb{Z}/\ell\mathbb{Z})^*$ is cyclic, so if g is a primitive root, then

$$\sum_{t=1}^{\ell}t^n=\sum_{m=1}^{\ell}g^{mn}\equiv\frac{g^{\ell n}-g^n}{g^n-1}\equiv\frac{g^n-g^n}{g^n-1}\equiv 0 \bmod \ell$$

($g^n \neq 1$ because $\ell - 1$ doesn't divide n). Hence, $\sum_{t=1}^{\ell} t^{2r} \equiv -1 \bmod \ell$ if and only if $r = k$, otherwise this sum is equal to 0 mod ℓ. We deduce that $S \equiv -1 \bmod \ell$. But $-\ell \leq S \leq \ell$, so $S = -1$ or $S = \ell - 1$. For $t \in \{1, \ldots, \ell - 1\}$, we have $t^2 \equiv (\ell - t)^2 \bmod \ell$, so $S = \left(\frac{-a}{\ell}\right) + 2\sum_{t=1}^{k} \left(\frac{t^2-a}{\ell}\right)$, so S is odd because $\left(\frac{-a}{\ell}\right) = \pm 1$ (remember that ℓ doesn't divide a), and $S = -1$. □

Lemma 3.4. *Let a be an integer and $m = \ell_1 \ldots \ell_s$ a product of s distinct odd primes such that $\gcd(a, m) = 1$. Then, $\left|\sum_{t=0}^{m-1} \left(\frac{t^2-a}{m}\right)\right| = 1$.*

Proof. This is a consequence of the Chinese Remainder Theorem and the previous lemma:

$$\sum_{t=0}^{m-1} \left(\frac{t^2-a}{m}\right) = \sum_{t=0}^{m-1} \left(\prod_{i=1}^{s} \left(\frac{t^2-a}{\ell_i}\right)\right) = \prod_{i=1}^{s} \left(\sum_{t=0}^{\ell_i - 1} \left(\frac{t^2-a}{\ell_i}\right)\right) = (-1)^s.$$

□

Now we consider incomplete sums.

Lemma 3.5. *Let a and $T \geq 1$ be two integers, and $m = \ell_1 \ldots \ell_s$ a product of s distinct odd primes such that $\gcd(a, m) = 1$. We have:*

$$\sum_{|t| \leq T} \left(\frac{t^2-a}{m}\right) \ll T/m + C^s m^{1/2} \log(m)$$

where C is an absolute constant.

Proof. In the case $s = 0$, we have $\sum_{|t| \leq T} \left(\frac{t^2-a}{m}\right) \leq 2T$. We now take $s \geq 1$ and we write

$$\sum_{|t| \leq T} \left(\frac{t^2-a}{m}\right) = 2 \sum_{0 \leq t \leq T} \left(\frac{t^2-a}{m}\right) - \left(\frac{-a}{m}\right).$$

We write $T = \lfloor T/m \rfloor m + L$ and we set $K + 1 = \lfloor T/m \rfloor m$. We decompose the sum $\sum_{\substack{t \leq T \\ t \geq 0}} \left(\frac{t^2-a}{m}\right)$ into $\lfloor \frac{T}{m} \rfloor$ complete sums and one partial sum as follows:

$$\sum_{\substack{t \leq T \\ t \geq 0}} \left(\frac{t^2-a}{m}\right) = \left[\sum_{t=0}^{m-1} \left(\frac{t^2-a}{m}\right) + \ldots + \sum_{t=(\lfloor T/m \rfloor - 1)m}^{K} \left(\frac{t^2-a}{m}\right)\right] + \sum_{t=K+1}^{K+L} \left(\frac{t^2-a}{m}\right).$$

According to Lemma 3.4, each of the complete sums is bounded by 1 in absolute value. We have $\lfloor \frac{T}{m} \rfloor$ such sums, so this gives the term T/m in the upper bound. It remains to estimate the partial sum $\sum_{t=K+1}^{K+L} \left(\frac{t^2-a}{m}\right)$.

We first look at the complete sum $\sum_{t=1}^{m} \left(\frac{t^2-a}{m}\right) \exp(2i\pi\frac{\lambda t}{m})$ for $\lambda \in \mathbb{Z}$. For i in $\{1, \dots, s\}$, the Weil bound applied to mixed sums of characters gives

$$\sum_{t=1}^{\ell_i} \left(\frac{t^2-a}{\ell_i}\right) \exp\left(\frac{2i\pi\lambda t}{\ell_i}\right) \ll C\ell_i^{1/2}$$

where C is an absolute constant (see [CZ02, Section 7]). Applying the multiplicativity of complete character sums gives

$$\sum_{t=1}^{m} \left(\frac{t^2-a}{m}\right) \exp\left(2i\pi\frac{\lambda t}{m}\right) \ll C^s m^{1/2}.$$

To estimate the incomplete sum $\sum_{t=K+1}^{K+L} \left(\frac{t^2-a}{m}\right) \exp(2i\pi\frac{\lambda t}{m})$, we apply a method consisting in reducing to complete sums as in [IK04, Chapter 12].

For $\lambda \in \mathbb{Z}$, we call $S_\lambda(K, L)$ the incomplete sum $\sum_{t=K+1}^{K+L} \left(\frac{t^2-a}{m}\right) \exp(2i\pi\frac{\lambda t}{m})$ and we write $F_\lambda(t) = \left(\frac{t^2-a}{m}\right) \exp(2i\pi\frac{\lambda t}{m})$. Finally, we define the complete sum

$$S_\lambda(b) = \sum_{x=0}^{m-1} F_\lambda(x) \exp\left(-2i\pi\frac{bx}{m}\right) = \sum_{x=0}^{m-1} F_{\lambda-b}(x).$$

Our partial sum $S_\lambda(K, L)$ can be expressed in terms of complete sums $S_\lambda(b)$ as

follows: $S_\lambda(K,L) = \frac{1}{m}\sum_{b=0}^{m-1} g(b)S_\lambda(b)$ where $g(b) = \sum_{t=K+1}^{K+L} \exp(2i\pi\frac{bt}{m})$. Indeed,

$$\begin{aligned}
\sum_{b=0}^{m-1} g(b)S_\lambda(b) &= \sum_{b=0}^{m-1}\sum_{t=K+1}^{K+L} \exp\left(2i\pi\frac{bt}{m}\right)\sum_{x=0}^{m-1} F_\lambda(x)\exp\left(-2i\pi\frac{bx}{m}\right)\\
&= \sum_{t=K+1}^{K+L}\sum_{x=0}^{m-1}\sum_{b=0}^{m-1} F_\lambda(x)\exp\left(\frac{2i\pi}{m}b(t-x)\right)\\
&= \sum_{t=K+1}^{K+L}\sum_{x=0}^{m-1} F_\lambda(x)\sum_{b=0}^{m-1}\exp\left(\frac{2i\pi}{m}b(t-x)\right)\\
&= m\sum_{t=K+1}^{K+L} F_\lambda(t).
\end{aligned}$$

To pass from the third line to the last one, we have used the orthogonality relations of characters :

$$\sum_{b=0}^{m-1}\exp\left(\frac{2i\pi}{m}b(t-x)\right) = \begin{cases} 0 & \text{if } x\neq t,\\ m & \text{if } x=t.\end{cases}$$

We get that

$$S_\lambda(K,L) - \frac{S_\lambda(0)}{m} = \sum_{b=1}^{m-1} g(b)S_\lambda(b).$$

Since $g(m-b) = \overline{g(b)}$ and $S_\lambda(m-b) = S_{-\lambda}(b)$,

$$\left|S_\lambda(K,L) - \frac{S_\lambda(0)}{m}\right| \leq \sum_{1\leq b\leq\frac{m}{2}} \frac{|g(b)|}{m}(|S_\lambda(b)+S_{-\lambda}(b)|).$$

For $1\leq\frac{m}{2}$, we have

$$|g(b)| = \left|\frac{1-\exp(\frac{2i\pi bL}{m})}{1-\exp(\frac{2i\pi b}{m})}\right| \leq \frac{2}{|1-\exp(\frac{2i\pi b}{m})|} \leq \frac{m}{b},$$

so

$$\left|S_\lambda(K,L) - \frac{S_\lambda(0)}{m}\right| \leq \sum_{1\leq b\leq\frac{m}{2}} \frac{1}{b}(|S_\lambda(b)+S_{-\lambda}(b)|).$$

By the estimation of complete sums, we have

$$|S_\lambda(b)+S_{-\lambda}(b)| \ll C^s m^{1/2}.$$

Moreover, $\sum_{1\leq b\leq \frac{m}{2}} \frac{1}{b} \ll \log(m)$, so

$$S_0(K,L) \ll C^s m^{1/2}\log(m).$$

□

For a positive integer n and a real number $L>0$, we denote by $\omega_L(n)$ the number of prime divisors of n which lie in the interval $[L,2L]$. In particular,

$$\left|\left\{\ell\in[L,2L]\ :\ \left(\frac{t^2-4q}{\ell}\right)=0\right\}\right|,$$

which will appear in the proof of the main theorem, is $\omega_L(t^2-4q)$.

Lemma 3.6. *Let $\nu\geq 1$ be an integer and $T\geq 1$. For $L\geq 3$, we have*

$$\sum_{|t|<T}\omega_L^{\nu}(t^2-a) \ll \frac{T}{\log(L)}+\frac{L^{\nu}}{(\log L)^{\nu}},$$

where the implied constant depends on ν.

Proof. We have

$$\sum_{|t|<T}\omega_L^{\nu}(t^2-a)=\sum_{|t|<T}\left(\sum_{\substack{L\leq \ell\leq 2L\\ \ell\mid t^2-a}}1\right)^{\nu}=\sum_{L\leq \ell_1,\dots,\ell_\nu\leq 2L}\ \sum_{\substack{|t|\leq T\\ \mathrm{lcm}(\ell_1,\dots,\ell_\nu)\mid t^2-a}}1.$$

Let $m=r_1\dots r_j$ be a squarefree integer. We show that

$$\sum_{\substack{|t|<T\\ m\mid t^2-a}}1 \ll 2^j(T/m+1).$$

Let t be an integer such that m divides t^2-a. Then t is a solution of the system

$$\begin{cases} t^2\equiv a \bmod r_1\\ \vdots\\ t^2\equiv a \bmod r_j. \end{cases}$$

For each i between 1 and j, let a_i be a square root of a modulo r_i if it exists (otherwise there is no solution to the previous system). Then, t is a solution of

$$\begin{cases} t \equiv \pm a_1 \bmod r_1 \\ \vdots \\ t \equiv \pm a_j \bmod r_j. \end{cases}$$

Choosing the signs gives 2^j different congruence systems, each of them having only one solution modulo m by the Chinese Remainder Theorem. We divide the interval of integers $\{0, \dots, T\}$ in $\lfloor T/m \rfloor$ intervals of m consecutive integers

$$\{0, \dots, m-1\}, \dots, \{(\lfloor T/m \rfloor - 1)m, \dots, \lfloor T/m \rfloor m - 1\}$$

and one final interval $\{\lfloor T/m \rfloor m, \dots, T\}$. In every interval, there are at most 2^j integers which divide $t^2 - a$. This also applies to negative values of t, so the number of integers t such that $|t| < T$ and $m | t^2 - a$ is at most $2 \cdot 2^j \cdot (T/m + 1)$.

Finally, for every $j \in \{1, \dots, \nu\}$, we gather the terms of the sum

$$\sum_{L \le \ell_1, \dots, \ell_\nu \le 2L} \sum_{\substack{|t| \le T \\ \operatorname{lcm}(\ell_1, \dots, \ell_\nu) | t^2 - a}} 1$$

such that among the primes $\ell_1, \dots, \ell_\nu$, only j are distinct. Thus,

$$\begin{aligned} \sum_{|t|<T} \omega_L^\nu(t^2 - a) &\ll \sum_{j=1}^{\nu} \sum_{L \le \ell_1, \dots, \ell_j \le 2L} \left(\frac{T}{\ell_1 \dots \ell_j} + 1 \right) \\ &\ll \sum_{j=1}^{\nu} \left(T \left(\sum_{L \le \ell_1, \dots, \ell_j \le 2L} \frac{1}{\ell_1 \dots \ell_j} \right) + \sum_{L \le \ell_1, \dots, \ell_j \le 2L} 1 \right) \\ &\ll \sum_{j=1}^{\nu} \left(T \left(\sum_{L \le \ell \le 2L} \frac{1}{\ell} \right)^j + \pi(2L)^j \right). \end{aligned}$$

In the first inequality, the implied constant depends on ν: given a tuple $(\ell_1, \dots, \ell_j)$ of j distinct primes of $[L, 2L]$, the number of tuples $(\ell'_1, \dots, \ell'_\nu)$ of primes of $[L, 2L]$ such that

$$\{\ell_i \ : \ i \in \{1, \dots, j\}\} = \{\ell'_i \ : \ i \in \{1, \dots, \nu\}\}$$

can be expressed as a function of ν (not depending on the other parameters). By the prime number theorem, $\sum_{j=1}^{\nu} \pi(2L)^j \sim \frac{2^\nu L^\nu}{\log(L)^\nu}$. Moreover,

$$\left(\sum_{L\leq \ell \leq 2L} \frac{1}{\ell}\right)^j \ll \left(\frac{1}{\log(L)}\right)^j \ll \frac{1}{\log(L)},$$

so $\sum_{j=1}^{\nu} \left(\sum_{L\leq \ell \leq 2L} \frac{1}{\ell}\right)^j \ll \frac{1}{\log(L)}$. Hence we get the result claimed. □

3.3 Lemmas for Theorem 3.2

In this subsection, we state and prove lemmas about character sums which rely on the Chebotarev density theorem. We fix a non-CM elliptic curve E defined over $\mathbb{Q}$. For a prime p of good reduction for E, we denote by E_p the reduction of E modulo p and by $D_p = t_{E_p}^2 - 4p$ the Frobenius discriminant of E_p.

3.3.1 Effective versions of the Chebotarev density theorem

Let K be a finite Galois extension of $\mathbb{Q}$, and $G = \mathrm{Gal}(K/\mathbb{Q})$. We denote by n_K the degree of this extension and by d_K its discriminant. Let C be a subset of G stable by conjugation. For a prime p which is not in the set $\mathcal{P}(K)$ of ramified primes in K, we denote by σ_p the Frobenius element at p in $K/\mathbb{Q}$ defined up to conjugation in G. We define

$$\pi_C(x, K) := |\{p \text{ prime } :\ p \leq x, p \notin \mathcal{P}(K), \sigma_p \in C\}|.$$

The Chebotarev density theorem asserts that $\pi_C(x, K) \sim \frac{|C|}{|G|}\mathrm{li}(x)$, where li is the logarithmic integral function: $\mathrm{li}(x) = \int_0^x \frac{dt}{\log(t)}$ (we recall that $\mathrm{li}(x) \underset{x\to+\infty}{\sim} \frac{x}{\log(x)}$). We will need effective versions of this theorem, which are given below. The first one is due to Lagarias and Odlyzko (see [LO77]).

Theorem 3.7. *Under GRH, there is an absolute constant $c > 0$ such that for every $x \geq 2$:*

$$\left|\pi_C(x, K) - \frac{|C|}{|G|}\mathrm{li}(x)\right| \leq c\frac{|C|}{|G|}x^{1/2}(\log(d_K) + n_K \log(x))$$

for some absolute constant $c > 0$.

In our applications, we will often replace $\log(d_K)$ by the upper bound of the next lemma.

Lemma 3.8. *We have* $\log(d_K) \leq (n_K - 1) \sum_{p \in \mathcal{P}(K)} \log(p) + n_K |\mathcal{P}(K)| \log(n_K)$.

Proof. The first idea of the proof is to write the discriminant as the norm of the different ideal $\mathcal{D}_{K/\mathbb{Q}}$. For a non-archimedean place v of K, we denote by $\mathfrak{p}_v$ the prime ideal associated to v. A result of Hensel makes it possible to bound the exponent $v(\mathcal{D}_{K/\mathbb{Q}})$ of the ideal $\mathfrak{p}_v$ in the factorisation of $\mathcal{D}_{K/\mathbb{Q}}$. Then, the result follows from a sequence of inequalities. We refer the reader to [Ser81, § 1] for the details. □

Lemma 3.8 directly implies the following version of Theorem 3.7 that we will use to prove the lemmas of the following subsection.

Theorem 3.9. *Under GRH, there is an absolute constant* $c > 0$ *such that for every* $x \geq 2$*:*

$$\left| \pi_C(x, K) - \frac{|C|}{|G|} \mathrm{li}(x) \right| \leq c|C| x^{1/2} \log \left(n_K x \prod_{p \in \mathcal{P}(K)} p \right).$$

3.3.2 Conjugacy classes in GL_2 and PGL_2

With a view towards applying the Chebotarev density theorem in number fields with Galois groups of the form $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ or $\mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})$ (with m an odd square-free integer), we study conjugacy classes in those groups.

Let N_E be the conductor of E and $A(E)$ Serre's constant which was introduced in subsection 2.3.3. Recall that the primes of good reduction for E are the primes which don't divide N_E. From now on, the notation p will be only used for primes of good reduction. In particular, if a sum is indexed by $p \in [P, 2P]$, it means that p ranges all the primes of good reduction between P and $2P$. For an integer $r \geq 2$, $t \in \mathbb{Z}/r\mathbb{Z}$ and $d \in (\mathbb{Z}/r\mathbb{Z})^*$, we define

$$C_r(t, d) := \{ g \in \mathrm{GL}_2(\mathbb{Z}/r\mathbb{Z}) \ : \ \det(g) = d, \mathrm{tr}(g) = t \}.$$

Lemma 3.10. *Let* $r = \ell_1 \dots \ell_s$ *be an odd square-free integer,* t *in* $\mathbb{Z}/r\mathbb{Z}$ *and* d *in* $(\mathbb{Z}/r\mathbb{Z})^*$*. Then,*

$$|C_r(t, d)| = \prod_{i=1}^{s} \ell_i \left(\ell_i + \left(\frac{t^2 - 4d}{\ell_i} \right) \right).$$

Proof. We only consider the case where $r = \ell_1$ is an odd prime, because the general case can be obtained from this case by applying the Chinese Remainder Theorem. Let $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ be an element of $\mathrm{GL}(\mathbb{Z}/\ell_1\mathbb{Z})$. Then, the element g satisfies $\det(g) = d$ and $\mathrm{tr}(g) = t$ if and only if $\alpha\delta - \beta\gamma = d$ and $\alpha + \delta = t$. The last condition on $\mathrm{tr}(g)$ shows that δ is determined by α. If β and γ are fixed, the number of elements g with $\mathrm{tr}(g) = t$ and $\det(g) = d$ is the number of solutions of the following equation in α:

$$\alpha^2 - \alpha t + \beta\gamma + d = 0.$$

The discriminant is $\Delta = t^2 - 4(\beta\gamma + d)$, so the number of solutions is $1 + \left(\frac{t^2-4(\beta\gamma+d)}{\ell_1}\right)$. Summing over all the values of β and γ, we find that

$$\begin{aligned} |C_{\ell_1}(t,d)| &= \sum_{\beta\in\mathbb{Z}/\ell_1\mathbb{Z}} \sum_{\gamma\in\mathbb{Z}/\ell_1\mathbb{Z}} \left(1 + \left(\frac{t^2 - 4(\beta\gamma + d)}{\ell_1}\right)\right) \\ &= \ell_1^2 + \sum_{\gamma\in\mathbb{Z}/\ell_1\mathbb{Z}} \left(\frac{t^2 - 4d}{\ell_1}\right) + \sum_{\beta\in(\mathbb{Z}/\ell_1\mathbb{Z})^*} \sum_{\gamma\in(\mathbb{Z}/\ell_1\mathbb{Z})} \left(\frac{t^2 - 4(\beta\gamma + d)}{\ell_1}\right) \\ &= \ell_1^2 + \ell_1 \left(\frac{t^2 - 4d}{\ell_1}\right). \end{aligned}$$

Indeed, if $\beta \in (\mathbb{Z}/\ell_1\mathbb{Z})^*$, then $\gamma \mapsto t^2 - 4(\beta\gamma + d)$ is a bijection of $\mathbb{Z}/\ell_1\mathbb{Z}$ onto itself, so the sum $\sum_{\gamma\in(\mathbb{Z}/\ell_1\mathbb{Z})} \left(\frac{t^2-4(\beta\gamma+d)}{\ell_1}\right)$ is equal to 0. □

Summing over t and d, one checks that

$$|\mathrm{GL}_2(\mathbb{Z}/r\mathbb{Z})| = r^4 \prod_{i=1}^{s} \left(1 - \frac{1}{\ell_i}\right)\left(1 - \frac{1}{\ell_i^2}\right)$$

and so

$$|\mathrm{PGL}_2(\mathbb{Z}/r\mathbb{Z})| = \frac{r^4 \prod_{i=1}^{s} \left(1 - \frac{1}{\ell_i}\right)\left(1 - \frac{1}{\ell_i^2}\right)}{\varphi(r)}.$$

Lemma 3.11. *Let ℓ be an odd prime. Define*

$$C_\ell(1) := \left\{ g \in \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) \ : \ \left(\frac{\mathrm{tr}(g)^2 - 4\det(g)}{\ell}\right) = 1 \right\}$$

and

$$C_\ell(-1) := \left\{ g \in \mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z}) \ : \ \left(\frac{\mathrm{tr}(g)^2 - 4\det(g)}{\ell}\right) = -1 \right\}.$$

Then, $|C_\ell(1)| = \frac{\ell^3-\ell^2}{2} - \ell$ *and* $|C_\ell(-1)| = \frac{\ell^3-\ell^2}{2}$.

Proof. We first notice that these sets are well-defined in $\mathrm{PGL}_2(\mathbb{Z}/\ell\mathbb{Z})$. For $C_\ell(1)$, we count the matrices $g \in \mathrm{GL}_2(\mathbb{Z}/\ell Z)$ satisfying $\left(\frac{\mathrm{tr}(g)^2-4\det(g)}{\ell}\right) = 1$ and divide by $\ell - 1$ to obtain the cardinality of $C_\ell(1)$. There are $\frac{\ell-1}{2}$ nonzero squares in $\mathbb{Z}/\ell\mathbb{Z}$. Fixing $\mathrm{tr}(g)^2 - \det(g)$ and $\mathrm{tr}(g)$ also fixes $\det(g)$. For each square, there are $\ell - 2$ possible values for $\mathrm{tr}(g)$ because $\det(g)$ must be nonzero. Moreover, there are $\ell(\ell+1)$ elements g of $\mathrm{GL}_2(\mathbb{Z}/\ell\mathbb{Z})$ having a given trace and determinant if $\left(\frac{\mathrm{tr}(g)^2-4\det(g)}{\ell}\right) = 1$ by Lemma 3.10. Thus, $|C_\ell(1)| = \frac{\ell(\ell+1)\frac{\ell-1}{2}(\ell-2)}{\ell-1} = \frac{\ell^3-\ell^2}{2} - \ell$. Replacing the factor $\ell+1$ by $\ell - 1$ gives the result for $|C_\ell(-1)|$. □

Now we fix two distinct primes ℓ_1 and ℓ_2. By the Chinese Remainder Theorem,

$$\mathrm{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z}) \cong \mathrm{PGL}_2(\mathbb{Z}/\ell_1\mathbb{Z}) \times \mathrm{PGL}_2(\mathbb{Z}/\ell_2\mathbb{Z}).$$

For $(\gamma_1, \gamma_2) \in \{1, -1\}^2$, we define C_{γ_1,γ_2} to be the set of elements

$$(g_1, g_2) \in \mathrm{PGL}_2(\mathbb{Z}/\ell_1\mathbb{Z}) \times \mathrm{PGL}_2(\mathbb{Z}/\ell_2\mathbb{Z})$$

such that

$$\left(\left(\frac{\mathrm{tr}(g_1)^2 - 4\det(g_1)}{\ell_1}\right), \left(\frac{\mathrm{tr}(g_2)^2 - 4\det(g_2)}{\ell_2}\right)\right) = (\gamma_1, \gamma_2).$$

Lemma 3.12. *We have*

$$\begin{cases} |C_{1,1} \cup C_{-1,-1}| & = O(\ell_1^3\ell_2^3), \\ |C_{1,-1} \cup C_{-1,1}| & = O(\ell_1^3\ell_2^3), \\ |C_{1,1} \cup C_{-1,-1}| - |C_{1,-1} \cup C_{-1,1}| & = \ell_1\ell_2 \end{cases}$$

Proof. These identities are straightforward consequences of the last lemma, using that

$$\begin{cases} |C_{1,1} \cup C_{-1,-1}| & = |C_{\ell_1}(1)| \cdot |C_{\ell_2}(1)| + |C_{\ell_1}(-1)| \cdot |C_{\ell_2}(-1)|, \\ |C_{1,-1} \cup C_{-1,1}| & = |C_{\ell_1}(1)| \cdot |C_{\ell_2}(-1)| + |C_{\ell_1}(-1)| \cdot |C_{\ell_2}(1)|. \end{cases}$$

□

We finally consider the case of four distinct primes $\ell_1, \ell_2, \ell_3, \ell_4$. For $(\gamma_1, \gamma_2, \gamma_3, \gamma_4)$ in $\{1, -1\}^4$, we define $C_{\gamma_1,\gamma_2,\gamma_3,\gamma_4}$ analogously as C_{γ_1,γ_2}. Its cardinality is

$$C_{\ell_1}(\gamma_1)C_{\ell_2}(\gamma_2)C_{\ell_3}(\gamma_3)C_{\ell_4}(\gamma_4).$$

We define

$$\begin{cases} A_1(m) & = \displaystyle\sum_{\substack{(\gamma_1,\gamma_2,\gamma_3,\gamma_4)\in\{-1,1\}^4 \\ \gamma_1\gamma_2\gamma_3\gamma_4=1}} C_{\ell_1}(\gamma_1)C_{\ell_2}(\gamma_2)C_{\ell_3}(\gamma_3)C_{\ell_4}(\gamma_4) \\ A_{-1}(m) & = \displaystyle\sum_{\substack{(\gamma_1,\gamma_2,\gamma_3,\gamma_4)\in\{-1,1\}^4 \\ \gamma_1\gamma_2\gamma_3\gamma_4=-1}} C_{\ell_1}(\gamma_1)C_{\ell_2}(\gamma_2)C_{\ell_3}(\gamma_3)C_{\ell_4}(\gamma_4). \end{cases}$$

Lemma 3.13. *We have*

$$A_1(\ell_1\ell_2\ell_3\ell_4) - A_{-1}(\ell_1\ell_2\ell_3\ell_4) = \ell_1\ell_2\ell_3\ell_4.$$

Proof. It is an easy but quite long computation using Lemma 3.11. □

3.3.3 Applying the Chebotarev density theorem

We now state and prove the lemmas for Theorem 3.2 relying on the Chebotarev density theorem. In everything what follows, the implied constants just depend on ν.

Lemma 3.14. *Let ν be a positive integer and $s \leq \nu$. For s distinct odd primes $\ell_1, \dots, \ell_s$ coprime with $A(E)$. Under GRH, for $P \geq \ell_1, \dots, \ell_s$ we have*

$$|\{p \in \mathcal{C}_P \ : \ D_p \equiv 0 \bmod r\}| \ll \frac{P}{\varphi(r)\log(P)} + r^3 P^{1/2}\log(P).$$

Proof. We will apply Theorem 3.9 with $K = \mathbb{Q}(E[r])$. We denote $\mathrm{Gal}(\mathbb{Q}(E[r])/\mathbb{Q})$ by G_r. Since $\ell_1, \dots, \ell_s$ are coprime with $A(E)$, the Galois representation

$$\rho_r : G_r \to \mathrm{GL}_2(\mathbb{Z}/r\mathbb{Z})$$

is bijective, where we keep the notations of subsection 2.3.3. Then $G_r = \mathrm{GL}_2(\mathbb{Z}/r\mathbb{Z})$. We will take

$$C(r) := \{g \in \mathrm{GL}_2(\mathbb{Z}/r\mathbb{Z}) \ : \ 4\det(g) = \mathrm{tr}(g)^2\}$$

for the set stable by conjugation. If p is unramified in $\mathbb{Q}(E[r])$ (recall that the ramified primes are the prime divisors of rN_E), Proposition 2.24 asserts that the Frobenius element σ_p is in $C(r)$ if and only if $D_p \equiv 0 \bmod r$. Thus, we have

$$|\{p \in \mathcal{C}_P \ : \ D_p \equiv 0 \bmod r\}| = \pi_{C(r)}(2P, \mathbb{Q}(E[r])) - \pi_{C(r)}(P, \mathbb{Q}(E[r])) + O(1).$$

In $C(r)$, choosing the value of the trace determines the value of the determinant. By Lemma 3.10, we get that $|C(r)| \leq r \prod_{i=1}^{s} \ell_i(\ell_i+1)$ (in particular, $|C(r)| \ll r^3$ because the number of factors is bounded from above by ν). Hence,

$$\begin{aligned}\frac{|C(r)|}{|G_r|} &\leq \frac{r^2 \prod_{i=1}^{s}(\ell_i+1)}{r^4 \prod_{i=1}^{s}\left(1-\frac{1}{\ell_i}\right)\left(1-\frac{1}{\ell_i^2}\right)} \\ &\leq \prod_{i=1}^{s} \frac{\ell_i+1}{(\ell_i-1)\left(\ell_i-\frac{1}{\ell_i}\right)} \\ &\leq 2^s \prod_{i=1}^{s} \frac{1}{\ell_i-1} \\ &\leq 2^s \frac{1}{\varphi(r)}.\end{aligned}$$

Moreover, using Proposition 2.23, $\prod_{p \in \mathcal{P}(\mathbb{Q}(E[r]))} p \leq rN_E$, so Theorem 3.9 gives

$$\pi_{C(r)}(2P, \mathbb{Q}(E[r])) \ll \frac{P}{\varphi(r)\log(P)} + r^3 P^{1/2}\log(r^4 P \cdot rN_E).$$

Because the primes ℓ_i are smaller than P, we have $\log(r^5 N_E P) \ll \log(P)$ and

$$\pi_{C(r)}(2P, \mathbb{Q}(E[r])) \ll \frac{P}{\varphi(r)\log(P)} + r^3 P^{1/2}\log(P).$$

□

Lemma 3.15. *Let ν be a positive integer. Under GRH, for $P > 2L$ we have*

$$\sum_{p \in \mathcal{C}_P} \omega_L(D_p)^\nu \ll \frac{P}{\log(L)\log(P)} + \frac{L^{4\nu} P^{1/2}\log(P)}{\log(L)^\nu}.$$

Proof. We write our sum as

$$\sum_{p \in \mathcal{C}_P} \omega_L(D_p)^\nu = \sum_{\ell_1,\ldots,\ell_\nu \in [L,2L]} \sum_{\substack{p \in \mathcal{C}_P \\ \operatorname{lcm}(\ell_1,\ldots,\ell_\nu) | D_p}} 1.$$

We sort the terms by the number of distinct primes among $\ell_1, \dots, \ell_\nu$. Let j be an element of $\{1, \dots, \nu\}$. There are $O\left(\frac{L^j}{\log(L)^j}\right)$ tuples $(\ell_1, \dots, \ell_\nu)$ of primes of $[L, 2L]$ such that $r := \mathrm{lcm}(\ell_1, \dots, \ell_\nu)$ is the product of j distinct primes. For such a tuple, the last lemma gives

$$\begin{aligned}\sum_{\substack{p \in \mathcal{C}_P \\ r | D_p}} 1 &\ll \frac{P}{\varphi(r)\log(P)} + r^3 P^{1/2}\log(P) \\ &\ll \frac{P}{L^j \log(P)} + L^{3j} P^{1/2}\log(P)\end{aligned}$$

because the prime divisors of r lie in $[L, 2L]$. Therefore, we get

$$\begin{aligned}\sum_{p \in \mathcal{C}_P} \omega_L(D_p)^\nu &\ll \sum_{j=1}^{\nu} \frac{L^j}{\log(L)^j}\left(\frac{P}{L^j\log(P)} + L^{3j}P^{1/2}\log(P)\right) \\ &\ll \frac{P}{\log(L)\log(P)} + \frac{L^{4\nu}P^{1/2}\log(P)}{\log(L)^\nu}\end{aligned}$$

by keeping only the dominant terms. □

Lemma 3.16. *Under GRH, for distinct primes ℓ_1, ℓ_2 coprime with $A(E)$ and $P \geq \ell_1, \ell_2$, we have*

$$\sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1\ell_2}\right) = \kappa_{\ell_1\ell_2}(\pi(2P) - \pi(P)) + O(\ell_1^3\ell_2^3 P^{1/2}\log(P)),$$

with $\kappa_{\ell_1\ell_2} = \frac{1}{(\ell_1^2-1)(\ell_2^2-1)}$.

Proof. As in subsection 2.3.3, we consider the representation

$$\overline{\rho_{\ell_1\ell_2}} : \mathrm{Gal}(L_{\ell_1\ell_2,E}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})$$

where $L_{\ell_1\ell_2,E}$ is the subextension of $\mathbb{Q}(E[\ell_1\ell_2])$ such that the last representation is bijective. We consider the sum $S(x) := \sum_{\substack{p \leq x \\ p \nmid \ell_1\ell_2 N_E}} \left(\frac{D_p}{\ell_1\ell_2}\right)$. Notice that $S(2P) - S(P)$ and $\sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1\ell_2}\right)$ only differ by at most 1 term. We have

$$S(x) = \sum_{\substack{p \leq x, \\ p \nmid \ell_1\ell_2 N_E, \\ \left(\frac{D_p}{\ell_1}\right)\left(\frac{D_p}{\ell_2}\right)=1}} 1 - \sum_{\substack{p \leq x \\ p \nmid \ell_1\ell_2 N_E \\ \left(\frac{D_p}{\ell_1}\right)\left(\frac{D_p}{\ell_2}\right)=-1}} 1 = \pi_{C_{1,1}\cup C_{-1,-1}}(x, L_{\ell_1\ell_2,E}) - \pi_{C_{1,-1}\cup C_{-1,1}}(x, L_{\ell_1\ell_2,E}).$$

By Lemma 3.12, $|C_{1,1} \cup C_{-1,-1}|$ and $|C_{1,-1} \cup C_{-1,1}|$ can be bounded from above by $O(\ell_1^3\ell_2^3)$ and

$$\frac{|C_{1,1} \cup C_{-1,-1}| - |C_{1,-1} \cup C_{-1,1}|}{|\mathrm{PGL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})|} = \frac{1}{(\ell_1^2-1)(\ell_2^2-1)}.$$

Finally, we have $\mathcal{P}(L_{\ell_1\ell_2,E}) \subseteq \mathcal{P}(\mathbb{Q}(E[\ell_1\ell_2]))$ because $L_{\ell_1\ell_2,E}$ is a subextension of $\mathbb{Q}(E[\ell_1\ell_2])$. Hence, $\prod_{p\in\mathcal{P}(L_{\ell_1\ell_2,E})} p \leq \ell_1\ell_2 N_E$. Theorem 3.9 implies that

$$S(x) = \frac{1}{(\ell_1^2-1)(\ell_2^2-1)}\pi(x) + O(\ell_1^3\ell_2^3 x^{1/2}\log(\ell_1^4\ell_2^4 N_E x)).$$

Because ℓ_1 and ℓ_2 are smaller than P, one can replace the error term by $O(\ell_1^3\ell_2^3 P^{1/2}\log(P))$ in $S(P)$ and $S(2P)$.

□

Remark 3.17. Considering the representation $\rho_{\ell_1\ell_2} : G_{\ell_1\ell_2} \to \mathrm{GL}_2(\mathbb{Z}/\ell_1\ell_2\mathbb{Z})$ instead of $\overline{\rho_{\ell_1\ell_2}}$ gives the error term $O(\ell_1^4\ell_2^4 P^{1/2}\log(P))$ (see [CFRM05]).

This lemma can be generalised to products of four primes.

Lemma 3.18. *Under GRH, for distinct primes $\ell_1, \ell_2, \ell_3, \ell_4$ coprime with $A(E)$ and $P \geq \ell_1, \ell_2, \ell_3, \ell_4$, we have*

$$\sum_{p\in\mathcal{C}_P} \left(\frac{D_p}{\ell_1\ell_2\ell_3\ell_4}\right) = \kappa_{\ell_1\ell_2\ell_3\ell_4}(\pi(2P) - \pi(P)) + O(\ell_1^3\ell_2^3\ell_3^3\ell_4^3 P^{1/2}\log(P)),$$

with $\kappa_{\ell_1\ell_2\ell_3\ell_4} = \prod_{i=1}^{4} \frac{1}{\ell_i^2-1}$.

Proof. Let $m = \ell_1\ell_2\ell_3\ell_4$ and $\widetilde{S}(x) := \sum_{\substack{p\leq x \\ p\nmid \ell_1\ell_2\ell_3\ell_4 N_E}} \left(\frac{D_p}{\ell_1\ell_2\ell_3\ell_4}\right)$. We have

$$\widetilde{S}(x) = \sum_{\substack{(\gamma_1,\gamma_2,\gamma_3,\gamma_4)\in\{-1,1\}^4 \\ \gamma_1\gamma_2\gamma_3\gamma_4=1}} \pi_{C_{\gamma_1,\gamma_2,\gamma_3,\gamma_4}}(x, L_{m,E}) - \sum_{\substack{(\gamma_1,\gamma_2,\gamma_3,\gamma_4)\in\{-1,1\}^4 \\ \gamma_1\gamma_2\gamma_3\gamma_4=-1}} \pi_{C_{\gamma_1,\gamma_2,\gamma_3,\gamma_4}}(x, L_{m,E}).$$

Applying the Chebotarev density theorem, we get that

$$\widetilde{S}(x) = \frac{A_1(m) - A_{-1}(m)}{|\mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})|}\pi(x) + O(\ell_1^3\ell_2^3\ell_3^3\ell_4^3 x^{1/2}\log(\ell_1^4\ell_2^4\ell_3^4\ell_4^4 N_E x)).$$

Lemma 3.13 tells us that $\frac{A_1(m)-A_{-1}(m)}{|\mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})|} = \prod_{i=1}^{4} \frac{1}{\ell_i^2-1}$. □

3.4 Proofs of the two main theorems

We will prove the two theorems in parallel, as the proofs involve very similar ideas.

Proof. Let E be an element of $\mathcal{E}_q$. If L is a prime number, there are $\pi(2L)-\pi(L)+1$ primes in $[L, 2L]$, otherwise there are $\pi(2L) - \pi(L)$ primes in this interval. Hence we have

$$N_e(E, L) + N_a(E, L) = \pi(2L) - \pi(L) + \varepsilon_L$$

where $\varepsilon_L = 1$ if L is a prime number and $\varepsilon_L = 0$ otherwise. Moreover, by the definition of Elkies and Atkin primes,

$$N_e(E, L) - N_a(E, L) = \sum_{L\leq \ell\leq 2L} \left(\frac{t_E^2 - 4q}{\ell}\right) + \omega_L(t_E^2 - 4q).$$

Hence we get

$$N_*(E, L) - \frac{1}{2}(\pi(2L) - \pi(L)) = \frac{1}{2}\left(\sum_{L\leq \ell\leq 2L} \left(\frac{t_E^2 - 4q}{\ell}\right) + \omega_L(t_E^2 - 4q) + O(1)\right).$$

Therefore,

$$\left|N_*(E, L) - \frac{1}{2}(\pi(2L) - \pi(L))\right|^{2\nu} \ll \left|\sum_{L\leq \ell\leq 2L} \left(\frac{t_E^2 - 4q}{\ell}\right)\right|^{2\nu} + \omega_L(t_E^2 - 4q)^{2\nu} + 1.$$

By averaging over $\mathcal{E}_q$,

$$\frac{1}{|\mathcal{E}_q|}\sum_{E\in\mathcal{E}_q} \left|N_*(E, L) - \frac{1}{2}(\pi(2L) - \pi(L))\right|^{2\nu} \ll \frac{1}{|\mathcal{E}_q|}U_{2\nu} + \frac{1}{|\mathcal{E}_q|}V_{2\nu} + 1 \tag{3.1}$$

where we set

$$\begin{cases} U_{2\nu} &= \displaystyle\sum_{E\in\mathcal{E}_q} \left|\sum_{L\leq \ell\leq 2L} \left(\frac{t_E^2-4q}{\ell}\right)\right|^{2\nu} \\ V_{2\nu} &= \displaystyle\sum_{E\in\mathcal{E}_q} \omega_L(t_E^2 - 4q)^{2\nu}. \end{cases}$$

We have an analogous relation for $R_*(p, L)$:

$$\begin{aligned} &\tfrac{1}{|\mathcal{C}_P|}\sum_{p\in\mathcal{C}_P} \left|R_*(p, L) - \tfrac{1}{2}(\pi(2L) - \pi(L))\right|^{2\nu} \\ &\qquad \ll \tfrac{1}{|\mathcal{C}_P|}\widetilde{U}_{2\nu} + \tfrac{1}{|\mathcal{C}_P|}\widetilde{V}_{2\nu} + 1 \end{aligned} \tag{3.2}$$

this time with

$$\begin{cases} \widetilde{U}_{2\nu} &= \sum_{p\in\mathcal{C}_P} \left| \sum_{L\le\ell\le 2L} \left(\frac{D_p}{\ell}\right)\right|^{2\nu} \\ \widetilde{V}_{2\nu} &= \sum_{p\in\mathcal{C}_P} \omega_L(D_p)^{2\nu}. \end{cases}$$

The rest of the proof consists in estimating the sums $U_{2\nu}$, $V_{2\nu}$, $\widetilde{U}_{2\nu}$ and $\widetilde{V}_{2\nu}$ with the lemmas of subsections 3.2 and 3.3. We start with the upper bounds on $U_{2\nu}$ and $V_{2\nu}$ for Theorem 3.1.

Bounding $U_{2\nu}$:
Sorting the elements of $\mathcal{E}_q$ by their trace of Frobenius, we get

$$\begin{aligned} U_{2\nu} &= \sum_{|t|\le 2q^{1/2}} f_q(t) \left| \sum_{L\le\ell\le 2L} \left(\frac{t^2-4q}{\ell}\right)\right|^{2\nu} \\ &\ll q^{1/2}\log(q)\log(\log(q)) \sum_{|t|\le 2q^{1/2}} \left| \sum_{L\le\ell\le 2L} \left(\frac{t^2-4q}{\ell}\right)\right|^{2\nu} \end{aligned}$$

by using the estimate of Proposition 2.13. By interverting the summations,

$$U_{2\nu} \ll q^{1/2}\log(q)\log(\log(q)) \sum_{L\le\ell_1,\dots,\ell_{2\nu}\le 2L} \sum_{|t|\le 2q^{1/2}} \left(\frac{t^2-4q}{\ell_1\dots\ell_{2\nu}}\right).$$

For every $j\in\{0,\dots,\nu\}$, we define $\mathcal{Q}_{2\nu,2j}$ as the set of tuples $(\ell_1,\dots,\ell_{2\nu})$ such that $L\le\ell_1,\dots,\ell_{2\nu}\le 2L$ and $\ell_1\dots\ell_{2\nu}=n^2m$ with m a squarefree product of $2j$ primes and n a product of $\nu-j$ primes. Choosing an element of $\mathcal{Q}_{2\nu,2j}$ involves choosing $\nu+j$ primes in $[L,2L]$ (we choose a subset of $2j$ primes for the factor m, then a subset of $\nu-j$ for n disjoint from the first). Thus

$$|\mathcal{Q}_{2\nu,2j}| \ll (\pi(2L)-\pi(L))^{\nu+j} \ll \frac{L^{\nu+j}}{\log(L)^{\nu+j}}.$$

We have

$$\begin{aligned} \sum_{L\le\ell_1,\dots,\ell_\nu\le 2L} \sum_{|t|\le 2q^{1/2}} \left(\frac{t^2-4q}{\ell_1\dots\ell_{2\nu}}\right) &= \sum_{j=0}^{\nu} \sum_{(\ell_1,\dots,\ell_{2\nu})\in\mathcal{Q}_{2\nu,2j}} \sum_{|t|\le 2q^{1/2}} \left(\frac{t^2-4q}{n^2m}\right) \\ &\le \sum_{j=0}^{\nu} \sum_{(\ell_1,\dots,\ell_{2\nu})\in\mathcal{Q}_{2\nu,2j}} \sum_{|t|\le 2q^{1/2}} \left(\frac{t^2-4q}{m}\right). \end{aligned}$$

Lemma 3.5 provides us with the estimate

$$\sum_{|t|\leq 2q^{1/2}} \left(\frac{t^2-4q}{m}\right) \ll \frac{2q^{1/2}}{m} + C^s m^{1/2}\log(m).$$

Since $L^{2j} \leq m \leq (2L)^{2j}$, we have

$$\sum_{|t|\leq 2q^{1/2}} \left(\frac{t^2-4q}{m}\right) \ll \frac{2q^{1/2}}{L^{2j}} + L^j\log(L).$$

Hence,

$$\begin{aligned}\sum_{L\leq \ell_1,\dots,\ell_\nu \leq 2L} \sum_{|t|\leq 2q^{1/2}} \left(\frac{t^2-4q}{\ell_1\dots\ell_{2\nu}}\right) &\ll \sum_{j=0}^{\nu} |\mathcal{Q}_{2\nu,2j}| \left(\frac{q^{1/2}}{L^{2j}} + L^j\log(L)\right) \\ &\ll \sum_{j=0}^{\nu} \left(\frac{q^{1/2}L^{\nu-j}}{\log(L)^{\nu+j}} + \frac{L^{\nu+2j}}{\log(L)^{\nu+j-1}}\right) \\ &\ll \frac{q^{1/2}L^\nu}{\log(L)^\nu} + \frac{L^{3\nu}}{\log(L)^{2\nu-1}}.\end{aligned}$$

Finally, we get

$$U_{2\nu} \ll q^{1/2}\log(q)\log(\log(q))\left(q^{1/2}\frac{L^\nu}{\log(L)^\nu} + \frac{L^{3\nu}}{\log(L)^{2\nu-1}}\right).$$

Bounding $V_{2\nu}$:
We also sort the terms in the sum defining $V_{2\nu}$ by the trace of Frobenius:

$$\begin{aligned}V_{2\nu} &= \sum_{|t|\leq 2q^{1/2}} f_q(t)\omega_L(t^2-4q)^{2\nu} \\ &\ll q^{1/2}\log(q)\log(\log(q)) \sum_{|t|\leq 2q^{1/2}} \omega_L(t^2-4q)^{2\nu} \\ &\ll q^{1/2}\log(q)\log(\log(q))\left(\frac{q^{1/2}}{\log(L)} + \frac{L^{2\nu}}{\log(L)^{2\nu}}\right)\end{aligned}$$

where the last inequality results from Lemma 3.6.

Injecting our upper bounds for $U_{2\nu}$ and $V_{2\nu}$ in equation (3.1) and getting rid of non-dominant terms yields Theorem 3.1. We now consider the case of $\widetilde{U}_{2\nu}$ and $\widetilde{V}_{2\nu}$

for $\nu = 1, 2$. In order to apply the lemmas of subsection 3.3, we will assume without loss of generality that $2L \leq P$ (otherwise the bound in Theorem 3.2 is trivial). We also assume that L is greater than Serre's constant $A(E_0)$.

Bounding $\widetilde{U}_4$:

We have $\widetilde{U}_4 = \sum_{L \leq \ell_1, \ell_2, \ell_3, \ell_4 \leq 2L} \sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1 \ell_2 \ell_3 \ell_4} \right)$. For the sum over $\ell_1, \ell_2, \ell_3, \ell_4$, we will sort the terms according to the three following cases:

- $\ell_1 \ell_2 \ell_3 \ell_4$ is a perfect square. There are $O(\frac{L^2}{\log(L)^2})$ such terms, because choosing $(\ell_1, \ell_2, \ell_3, \ell_4)$ such that $\ell_1 \ell_2 \ell_3 \ell_4$ is a perfect square involves choosing only two primes in $[L, 2L]$. In this case,

$$\sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1 \ell_2 \ell_3 \ell_4} \right) \leq \sum_{p \in \mathcal{C}_P} 1 = O\left(\frac{P}{\log(P)} \right)$$

  so the total contribution of these terms in $\widetilde{U}_4$ is

$$O\left(\frac{L^2 P}{\log(L)^2 \log(P)} \right).$$

- $\ell_1 \ell_2 \ell_3 \ell_4$ is not a perfect square but is divisible by a non-trivial square. There are $O(\frac{L^3}{\log(L)^3})$ such terms. Without loss of generality, if $\ell_1 \neq \ell_2$ and $\ell_3 = \ell_4$, Lemma 3.16 gives

$$\begin{aligned} \sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1 \ell_2 \ell_3 \ell_4} \right) &\leq \sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1 \ell_2} \right) \\ &\leq \kappa_{\ell_1 \ell_2} (\pi(2P) - \pi(P)) + O(\ell_1^3 \ell_2^3 P^{1/2} \log(P)) \end{aligned}$$

  with $\kappa_{\ell_1 \ell_2} = O\left(\frac{1}{L^4}\right)$ since $L \leq \ell_1, \ell_2 \leq 2L$. Hence, we get the upper bound

$$\sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1 \ell_2 \ell_3 \ell_4} \right) = O\left(\frac{P}{L^4 \log(P)} + L^6 P^{1/2} \log(P) \right).$$

  The total contribution of these terms in $\widetilde{U}_4$ is

$$O\left(\frac{L^3}{\log(L)^3} \left(\frac{P}{L^4 \log(P)} + L^6 P^{1/2} \log(P) \right) \right).$$

- $\ell_1\ell_2\ell_3\ell_4$ is squarefree. There are $O(\frac{L^4}{\log(L)^4})$ such terms. Lemma 3.18 gives

$$\sum_{p\in\mathcal{C}_P}\left(\frac{D_p}{\ell_1\ell_2\ell_3\ell_4}\right) \leq \kappa_{\ell_1\ell_2\ell_3\ell_4}(\pi(2P)-\pi(P)) + O(\ell_1^3\ell_2^3\ell_3^3\ell_4^3 P^{1/2}\log(P))$$

with $\kappa_{\ell_1\ell_2\ell_3\ell_4} = O\left(\frac{1}{L^8}\right)$, so

$$\sum_{p\in\mathcal{C}_P}\left(\frac{D_p}{\ell_1\ell_2\ell_3\ell_4}\right) = O\left(\frac{P}{L^8\log(P)} + L^{12}P^{1/2}\log(P)\right).$$

The total contribution of these terms in $\widetilde{U}_4$ is

$$O\left(\frac{L^4}{\log(L)^4}\left(\frac{P}{L^8\log(P)} + L^{12}P^{1/2}\log(P)\right)\right)$$

By getting rid of non-dominant terms, we find that

$$\widetilde{U}_4 = O\left(\frac{L^2P}{\log(L)^2\log(P)} + \frac{L^{16}P^{1/2}\log(P)}{\log(L)^4}\right).$$

Bounding $\widetilde{U}_2$:

To bound $\widetilde{U}_2 = \sum_{L\leq\ell_1,\ell_2\leq 2L]}\sum_{p\in\mathcal{C}_P}\left(\frac{D_p}{\ell_1\ell_2}\right)$, we sort the terms according to these two cases:

- $\ell_1 = \ell_2$. There are $O\left(\frac{L}{\log(L)}\right)$ such terms. In that case,

$$\sum_{p\in\mathcal{C}_P}\left(\frac{D_p}{\ell_1\ell_2}\right) \leq \sum_{p\in\mathcal{C}_P} 1 = O\left(\frac{P}{\log(P)}\right).$$

- $\ell_1 \neq \ell_2$. There are $O\left(\frac{L^2}{\log(L)^2}\right)$ such terms. Lemma 3.16 gives

$$\sum_{p\in\mathcal{C}_P}\left(\frac{D_p}{\ell_1\ell_2}\right) = O\left(\frac{P}{\log(P)}\frac{1}{L^4} + L^6P^{1/2}\log(P)\right).$$

Hence, $\widetilde{U}_2 = O\left(\frac{LP}{\log(L)\log(P)} + \frac{L^8P^{1/2}\log(P)}{\log(L)^2}\right)$.

Bounding $\widetilde{V}_{2\nu}$:

Lemma 3.15 gives

$$\widetilde{V}_4 = O\left(\frac{P}{\log(L)\log(P)} + \frac{L^{16}P^{1/2}\log(P)}{\log(L)^4}\right)$$

and

$$\widetilde{V}_2 = O\left(\frac{P}{\log(L)\log(P)} + \frac{L^{8}P^{1/2}\log(P)}{\log(L)^2}\right).$$

We find the statement of Theorem 3.2 by injecting our upper bounds for $\widetilde{U}_{2\nu}$ and $\widetilde{V}_{2\nu}$ in (3.2).

□

4 Numerical experiments

We performed numerical experiments with *SageMath* in order to confirm experimentally the estimates of the theorems 3.1 and 3.2 and to assess how accurate they are. In this section, we introduce our methodology and our results.

4.1 Experiments about Theorem 3.1

4.1.1 Methodology

For a finite field $\mathbb{F}_q$, we are interested in computing the left-hand side of Theorem 3.1

$$LHS(q, L, \nu) := \frac{1}{|\mathcal{E}_q|} \sum_{E \in \mathcal{E}_q} \left| N_e(E, L) - \frac{1}{2}(\pi(2L) - \pi(L)) \right|^{2\nu}.$$

We consider Elkies primes here, but everything that follows would also work with Atkin primes instead. We first discuss the relevant values of L and q for our study.

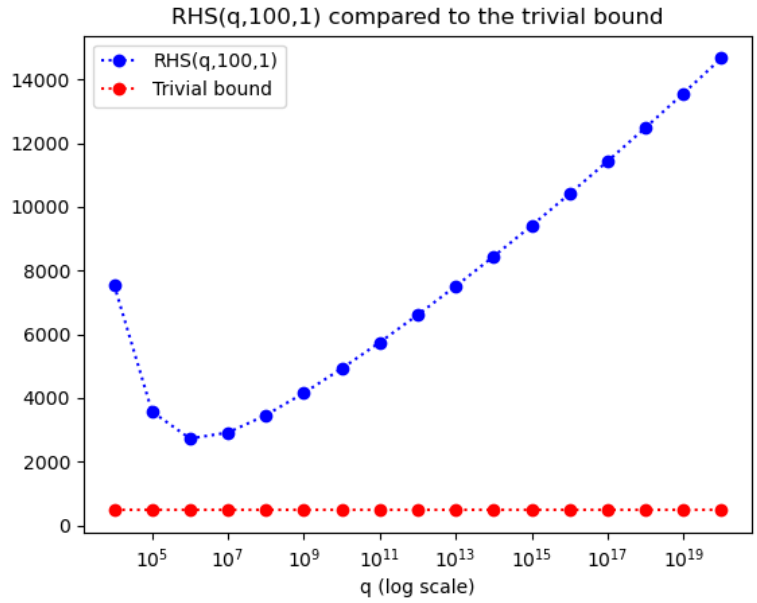
Theorem 3.1 provides nontrivial information when the right-hand side

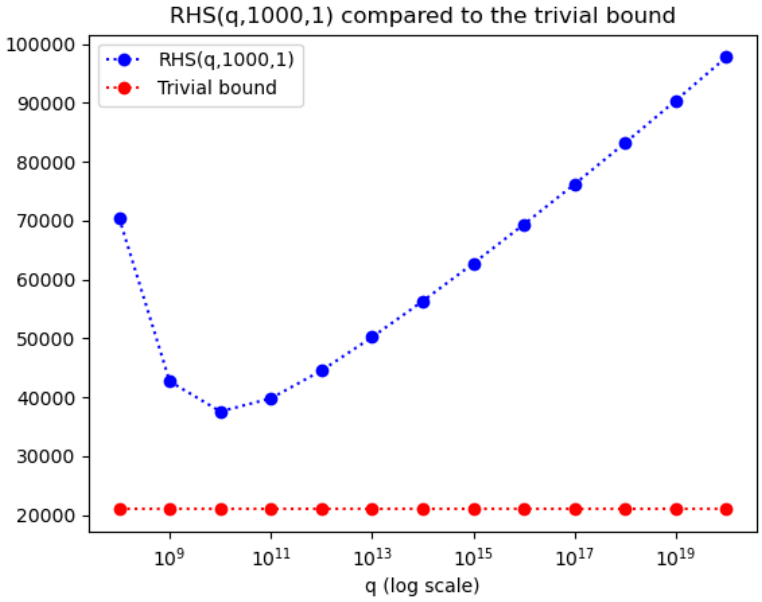
$$O\left(\frac{L^\nu}{\log(L)^\nu} \log(q) \log(\log(q)) + \frac{L^{2\nu}}{\log(L)^{2\nu}} q^{-1/2} L^\nu \log(L) \right)$$

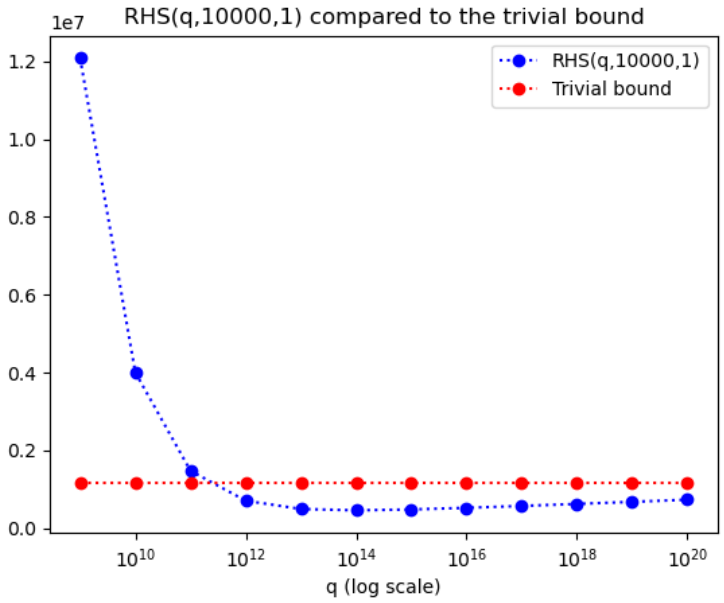
is smaller than the trivial bound $O\left(\frac{L^{2\nu}}{\log(L)^{2\nu}}\right)$. The difficulty is that the implicit big-O constant is not known. In order to have an idea of the approximate size of L and q, we will take it equal to 1 and we define

$$RHS(L, q, \nu) = \frac{L^\nu}{\log(L)^\nu} \log(q) \log(\log(q)) + \frac{L^{2\nu}}{\log(L)^{2\nu}} q^{-1/2} L^\nu \log(L).$$

The next graphs shows $RHS(q, L, 1)$ as a function of q and $\frac{L^2}{\log(L)^2}$ with $L = 100, 1000$ and 10000.


RHS(q,100,1) compared to the trivial bound
RHS(q,100,1)
Trivial bound
14000
12000
10000
8000
6000
4000
2000
0
10^5
10^7
10^9
10^{11}
10^{13}
10^{15}
10^{17}
10^{19}
q (log scale)


RHS(q,1000,1) compared to the trivial bound
RHS(q,1000,1)
Trivial bound
100000
90000
80000
70000
60000
50000
40000
30000
20000
10^9
10^{11}
10^{13}
10^{15}
10^{17}
10^{19}
q (log scale)



The last figure shows that the bound of Theorem 3.1 is minimal for $q \approx 10^{12}$ when $L = 10000$. Therefore, we aim at being able to compute $C_{L,q}$ for values of q around 10^{12}.

A naive approach described in Algorithm 2 consists in enumerating all the elliptic curves defined over $\mathbb{F}_q$ by the coefficients of the Weierstrass equations (since an elliptic curve E can arise from different Weierstrass equations, we have to normalise by the number of Weierstrass equations which define an elliptic curve in the isomorphism class of E, which is $\frac{q-1}{|\mathrm{Aut}(E)|}$).

However, there are $q^2 - q$ nonsingular Weierstrass equations. Determining the trace of Frobenius of an elliptic curve E can be done in polynomial time in $\log(q)$. Hence the total complexity is $\widetilde{O}(q^2)$, so this method can't be used in practice for large values of q. It is possible to enumerate the j-invariants instead of enumerating the Weierstrass equations to get a complexity $\widetilde{O}(q)$. For a given j-invariant different from 0 or 1728, there are two isomorphism classes of elliptic curves whose traces of Frobenius are opposite, these classes are called quadratic twists of each other. It takes more than one hour on a standard laptop with *SageMath* for $q \approx 10^7$, so it can't be used in practice for $q \approx 10^{10}$.

Another approach is to enumerate the traces of Frobenius, rather than the curves themselves. Writing $N_e(t, L)$ the number of primes $\ell \in [L, 2L]$ such that $\left(\frac{t^2-4q}{\ell}\right) \neq -1$,

Algorithm 2: Computation of $LHS(q, L, \nu)$

Data: q, L, ν
Result: The quantity $LHS(q, L, \nu)$
$LHS \leftarrow 0$
$N \leftarrow$ number of isomorphism classes of elliptic curves over $\mathbb{F}_q$
for $A \in \mathbb{F}_q$ **do**
  for $B \in \mathbb{F}_q$ **do**
    if $4A^3 + 27B^2 \neq 0$ **then**
      $t \leftarrow$ trace of Frobenius of the elliptic curve $E : y^2 = x^3 + Ax + B$
      $a \leftarrow$ number of automorphisms of E
      $u \leftarrow \frac{q-1}{a}$
      $n \leftarrow 0$
      for ℓ *prime in* $[L, 2L]$ **do**
        if $\left(\frac{t^2-4q}{\ell}\right) \neq -1$ **then**
          $n \leftarrow n + 1$
        end
      end
      $LHS \leftarrow LHS + \frac{1}{uN}\left|n - \frac{\pi(2L)-\pi(L)}{2}\right|^{2\nu}$
    end
  end
end
return LHS

we have

$$LHS(q, L, \nu) = \frac{1}{|\mathcal{E}_q|} \sum_{|t| \leq \sqrt{q}} f_q(t) \left| N_e(t, L) - \frac{\pi(2L) - \pi(L)}{2} \right|^{2\nu}$$

where the numbers $f_q(t)$ were introduced in the subsection 2.2. They are computed with the formula of Proposition 2.12 for the ordinary case:

$$f_q(t) = H(t^2 - 4q) = \sum_{\mathcal{O}(t^2-4q) \subseteq \mathcal{O}'} h(\mathcal{O}').$$

The traces of Frobenius belong to the Hasse interval, whose size is $4\sqrt{q}$, so we have at most $4\sqrt{q}$ values of the function H to compute. According to Cohen, computing the values of $h(\Delta_K)$ is very fast where Δ_K is a fundamental discriminant, and it is easy to compute $h(\Delta)$ from $h(\Delta_K)$ if $\Delta = u^2\Delta_K$ (see Algorithm 5.3.5 and the following remark in [Coh93]). In *SageMath*, we use the can compute the function `quadratic_order_class_number` from the module `sage.rings.number_field.order` to compute the values of h, which we use to compute the values of H.

With this approach, we only consider ordinary curves for our experiments. It doesn't really matter, because supersingular curves are rare (Porposition 2.12 shows that there are $\widetilde{O}(\sqrt{q})$ supersingular curves defined over $\mathbb{F}_q$, so their contribution to $LHS(q, L, \nu)$ is asymptotically insignificant compared with the contribution of ordinary elliptic curves).

Beyond the LHS, we may also be interested in the distribution of the values of $N_e(E, L)$, namely determine the number of $E \in \mathcal{E}_q$ such that $N_e(E, L) = n$ for every $n \leq \pi(2L) - \pi(L) + 1$. In fact, it is possible to compute $LHS(q, L, \nu)$ from this distribution. Writing $F_{q,L}(n)$ for the number of $E \in \mathcal{E}_q$ such that $N_e(E, L) = n$, we have

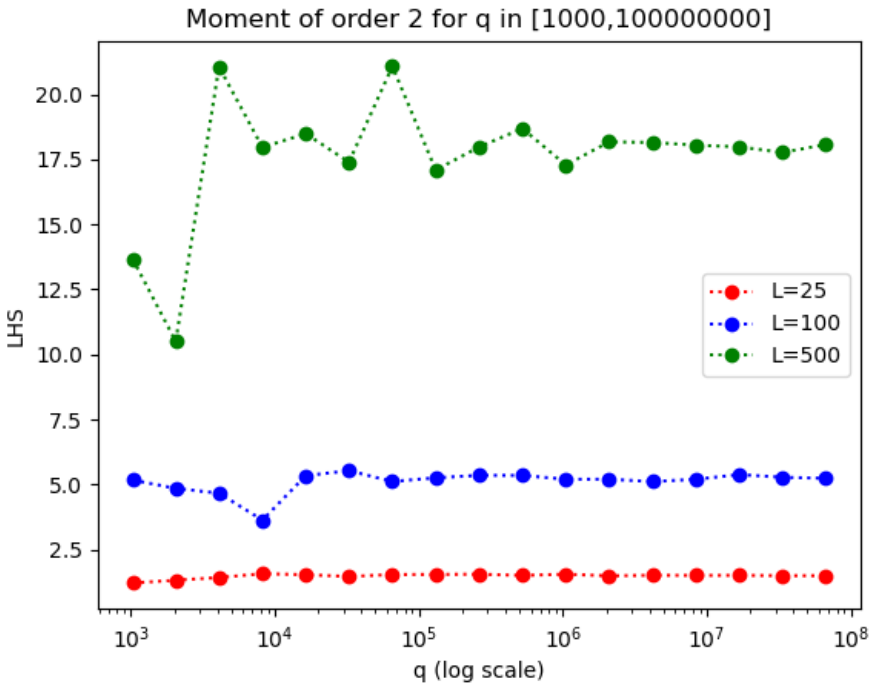
$$LHS(q, L, \nu) = \frac{1}{|\mathcal{E}_q|} \sum_{n=0}^{\pi(2L)-\pi(L)+1} F_{q,L}(n) \left| n - \frac{\pi(2L) - \pi(L)}{2} \right|^{2\nu}.$$

Moreover, the distribution gives an idea of how many curves have approximately the same number of Elkies and Atkin primes in $[L, 2L]$ (the LHS is a numerical measurement to quantify the difference with the expected value, but plotting the distribution is more visual).

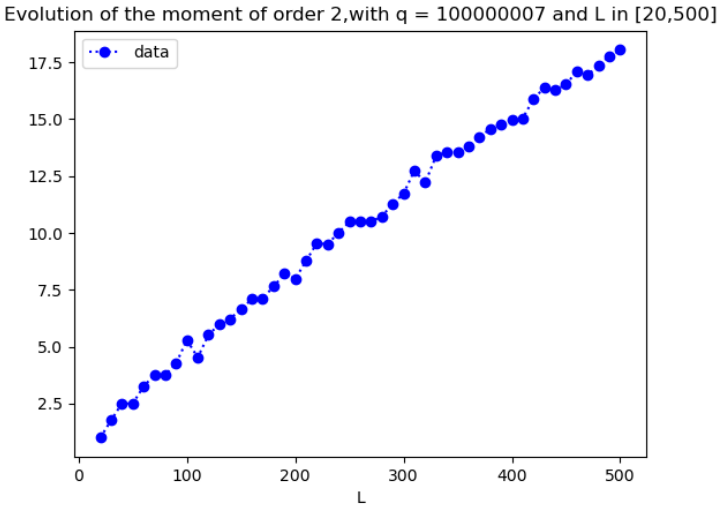
For repeated experiments with a given finite field $\mathbb{F}_q$, it is possible to construct a dictionary whose keys are the integers $t \in [-2\sqrt{q}, 2\sqrt{q}]$ and values are the numbers $f_q(t)$. It can be stored in a text file, so the computation of the numbers $f_q(t)$ is done once for all. Creating this dictionary takes less than two minutes for $q \approx 10^{10}$ and less than one hour for $q \approx 10^{12}$ on a standard laptop.

4.1.2 First observations

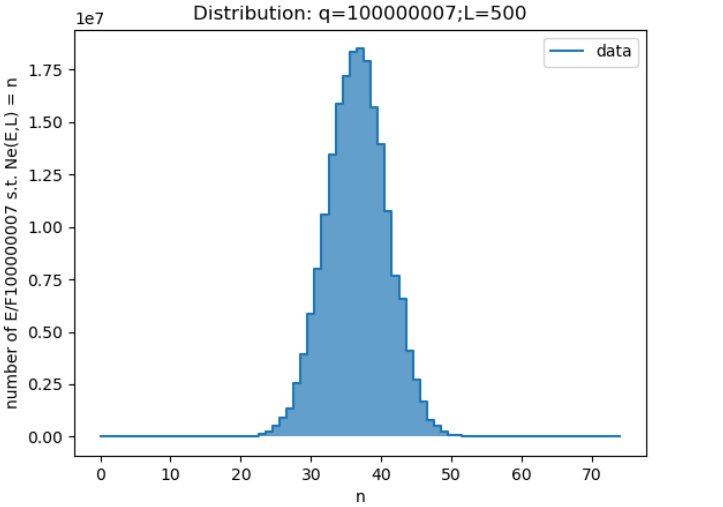
We first fix the parameter L and let q vary. The next graph shows the evolution of $LHS(q, L, 1)$ for $L = 25, 100, 500$ and $10^3 \leq q \leq 10^{10}$ (in order to gain time, $LHS(q, L, 1)$ was just computed for the prime values of q consecutive to powers of 2).



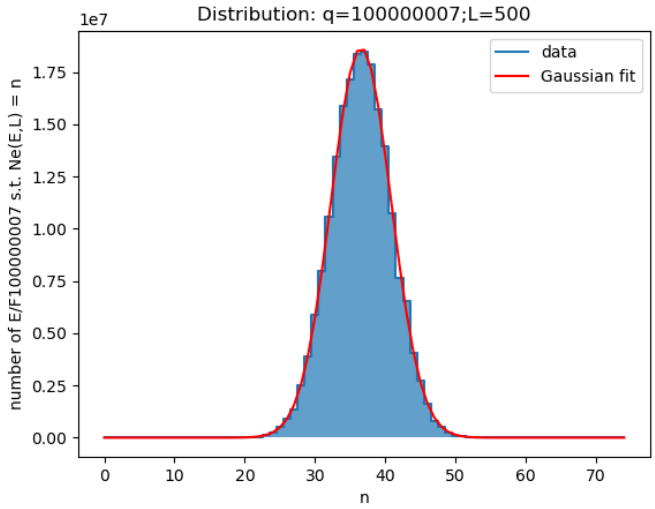
This graph suggests that $LHS(q, L, 1)$ tends to a finite limit when $q \to +\infty$. We fixed $q \approx 10^8$ and we plotted the evolution of $LHS(q, L, 1)$ for $L \in [20, 500]$ to have an idea of the value of the limit as a function of L.



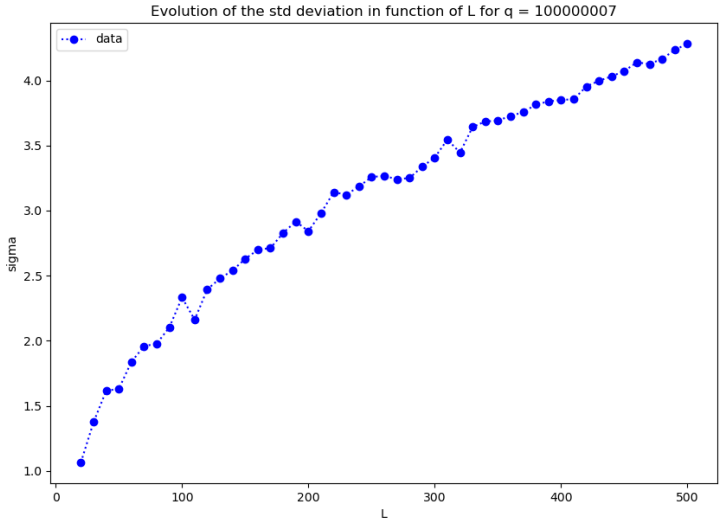
We notice that the evolution seems to be roughly linear and we next focus on the distribution. For q large compared with L, the distribution seems to be a Gaussian function (on the next graph, $q = 10^8 + 7$ and $L = 500$).



With the function `curve_fit` of the Python module `scipy.optimize`, it is possible to find a Gaussian function that fits with the curve of the distribution (notice that we have to give a guess of the parameters of the Gaussian, even very approximate, as an optional argument in `curve_fit`, otherwise `curve_fit` can return an almost constant Gaussian function with extra large standard deviation).



The next graph shows the evolution of the standard deviation of the Gaussian fit as a function of L (with $q \approx 10^8$).



4.1.3 Comparison with a simple probabilistic model

We would like to predict the expressions of the limit of $LHS(q, L, 1)$ and the parameters of the Gaussian fit of the distribution as a function of L through a

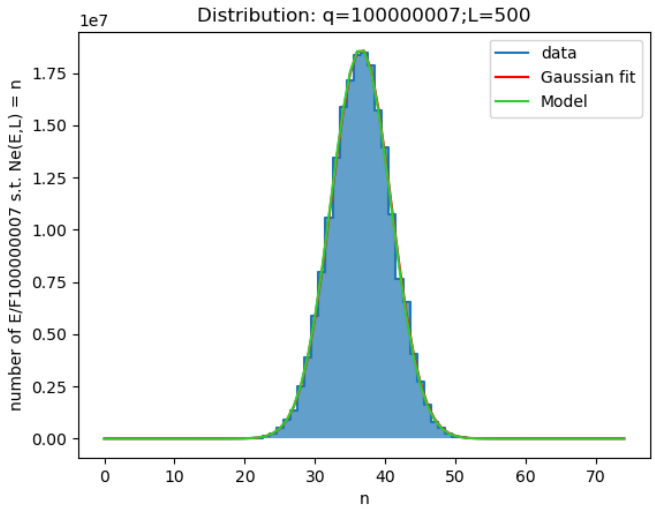
simple probabilistic model. Let us fix q. For an integer t with $|t| \leq 2\sqrt{q}$, we assume that the hypothesis that roughly 50% of prime numbers are Elkies is correct. So for a prime ℓ, the probability of the Legendre symbol $\left(\frac{t^2-4q}{\ell}\right)$ to be equal to 0 or 1 is roughly 1/2. Thus, we model $\left(\frac{t^2-4q}{\ell}\right)$ by a random variable $X_{t,\ell}$ following a Bernoulli distribution $B(1/2)$. We further assume that all the variables $X_{t,\ell}$ are independent. For $L > 0$, the random variable

$$X_t := \sum_{\ell \in [L,2L]} X_{t,\ell}$$

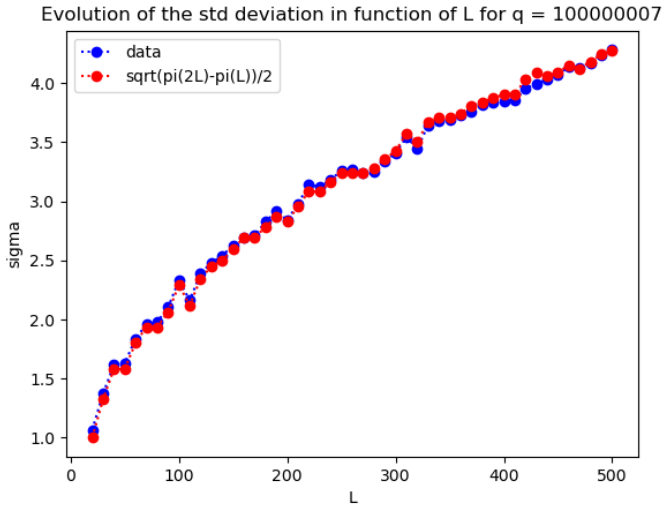
models the number of Elkies primes of a curve of trace of Frobenius t in $[L, 2L]$ and it follows a binomial distribution $B(\pi(2L) - \pi(L), 1/2)$. We have

$$E(X_t) = \frac{\pi(2L) - \pi(L)}{4} \quad \text{and} \quad \sigma(X_t) = \frac{\sqrt{\pi(2L) - \pi(L)}}{2}.$$

The next graph is the distribution of the last paragraph ($q = 10^8 + 7$ and $L = 500$), with the curve of the Gaussian of mean value $E(X_t)$ and standard deviation $\frac{\sqrt{\pi(2L)-\pi(L)}}{2}$ in green. The model seems to be very accurate.



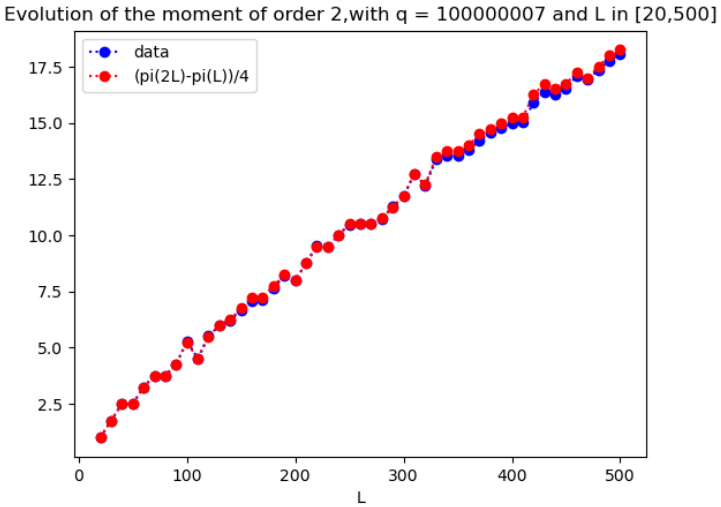
The next graph shows the evolution of the standard deviation of the Gaussian fit (in blue) and the value given by the model: $\frac{\pi(2L)-\pi(L)}{2}$ (in red on the next graph).



Moreover,

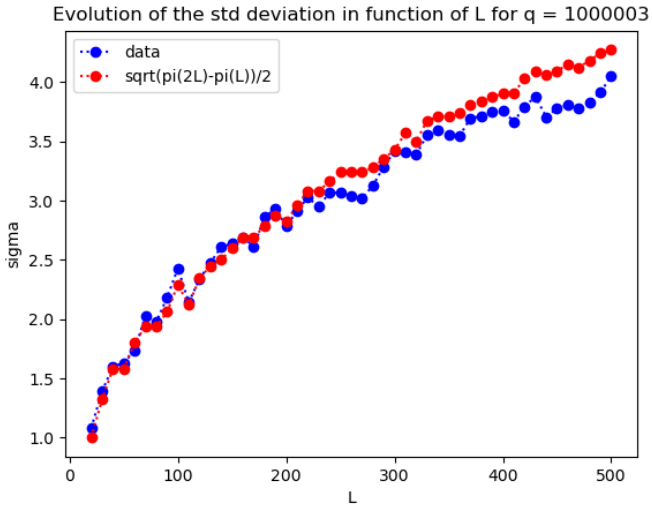
$$\mathbb{E}\left(\frac{1}{|\mathcal{E}_q|}\sum_{|t|\leq 2\sqrt{q}} f_q(t)\left|X_t - \frac{\pi(2L)-\pi(L)}{2}\right|^2\right) = \mathbb{E}\left(\left|X_t - \frac{\pi(2L)-\pi(L)}{2}\right|^2\right)$$
$$= \frac{\pi(2L)-\pi(L)}{4}.$$

The evolution of $LHS(q, L, 1)$ as a function of L also fits well with this value.



Therefore, the bound of Theorem 3.1 seems non-optimal.

When q is not large enough, side effects occur: the curve of the standard deviation as a function of L deviates from the model for $L \geq 400$, with $q = 10^6 + 7$. This suggests that the model is satisfactory only if q is very large compared with L.



Finally, we try to summarise our observations as an open question. We write $m = \frac{\pi(2L)-\pi(L)}{2}$ and $\sigma = \frac{\sqrt{\pi(2L)-\pi(L)}}{2}$.

Question 4.1. *For $x \in \mathbb{R}$, we define*

$$f_{q,L}(x) = \frac{|\{E \in \mathcal{E}_q \ : \ \frac{N_e(E,L)-m}{\sigma} \leq x\}|}{|\mathcal{E}_q|}.$$

Does $f_{q,L}$ converges pointwise to the cumulative distribution function of the standard normal distribution as q and L goes to infinity with $q \gg L^n$ for every $n \in \mathbb{N}$?

4.2 Experiments about Theorem 3.2

Let E be an elliptic curve defined over $\mathbb{Q}$ and

$$LHS(P, L, \nu) := \frac{1}{|\mathcal{C}_P|} \sum_{p \in \mathcal{C}_P} \left| R_e(p, L) - \frac{\pi(2L) - \pi(L)}{2} \right|^{2\nu}.$$

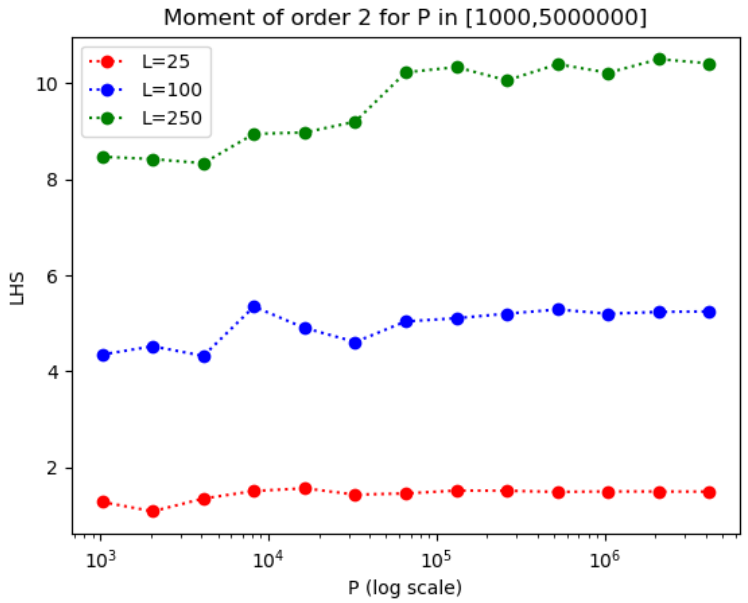
We slightly adapt our probabilistic model. For a prime $p \nmid N_E$ and $\ell \neq p$, let $X_{p,\ell}$ be a random variable following a Bernoulli distribution $B(1/2)$. It models

whether D_p is a square modulo ℓ or not (we recall the notation D_p for the Frobenius discriminant of the reduction modulo p of E). We also assume that the variables $X_{p,\ell}$ are independent, so the random variable

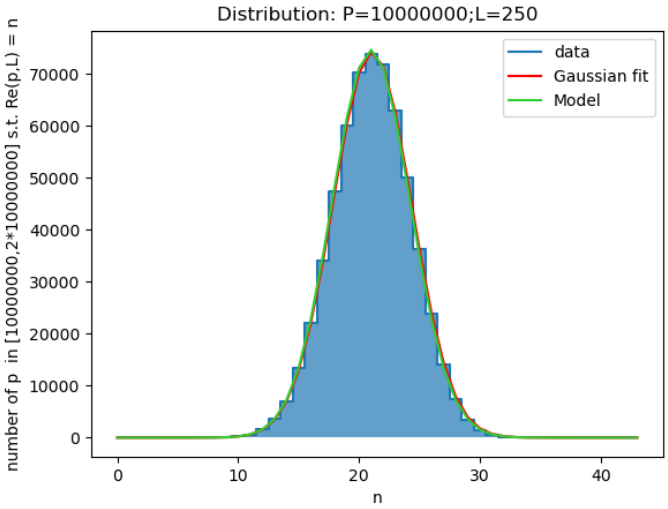
$$X_p = \sum_{\ell \in [L,2L]} X_{p,\ell}$$

follows a binomial distribution $B(\pi(2L) - \pi(L), 1/2)$. This last variable models the number of Elkies primes in $[L, 2L]$ for the reduction of E modulo p. Since it follows the same law as the variable X_t of the last paragraph, we expect similar observations. The numerical experiments were made with the elliptic curve E of conductor 11 (small conductor) given by the Weierstrass equation $y^2 + y = x^3 - x^2$. Using the straightforward approach of computing t_{E_p} for each p independently, we were only able to reach values of P up to 10^7, but this is sufficient to see that it fits with the model. Should we want to increase this value, we can use an algorithm developed by Sutherland to investigate the Sato-Tate conjecture which computes efficiently t_{E_p} for several p simultaneously. We directly give the graphs with the expectations of the model.

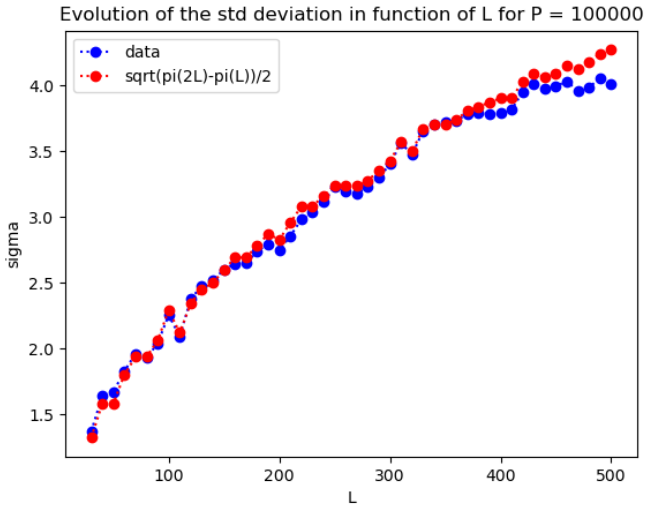
When L is fixed, $LHS(P, L, 1)$ also seems to tend to a finite limit when $P \to +\infty$.

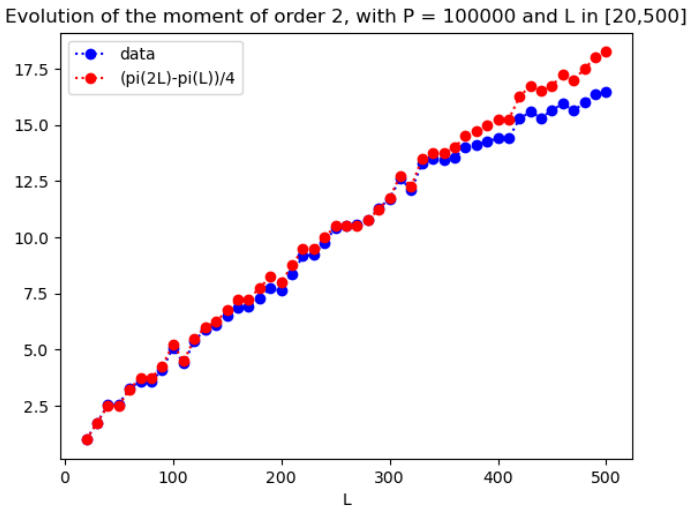


The distribution also seems to tend to a Gaussian of mean value $\frac{\pi(2L)-\pi(L)}{2}$ and standard deviation $\frac{\sqrt{\pi(2L)-\pi(L)}}{2}$.



For the evolution of the standard deviation and $LHS(P, L, 1)$, we notice some significant difference with the model for values of L between 400 and 500. Thus, the expectations of the model seem to be valid only for large values of P in comparison with L.





One might formulate a similar question as Question 4.1. However, in this context, we are actually able to prove a statement of convergence in distribution. This will be the topic of the next section.

5 Convergence of the distribution of Elkies primes for reductions of an elliptic curve over $\mathbb{Q}$

5.1 Formalisation of the context

Let E be an elliptic curve defined over $\mathbb{Q}$. The numerical experiments of the last section suggest that the distribution of the quantities $R_e(p, L)$ converges to a Gaussian distribution when P and L tend to infinity. The goal of this section is to state and prove a theorem which justifies our observation.

For $P > 0$, we equip the set of primes in $[P, 2P]$ of good reduction $\mathcal{C}_P$ with a uniform probability measure $\mathbb{P}_P$. For $p \in \mathcal{C}_P$, we define $X_{P,L}(p) = R_e(p, L)$ and

$$F_{P,L}(n) := |\{p \in C_P \ : \ X_{P,L}(p) = n\}|.$$

Then,

$$\mathbb{P}_P(X_{P,L} = n) = \frac{F_{P,L}(n)}{|\mathcal{C}_P|}$$

and

$$\frac{1}{|\mathcal{C}_P|} \sum_{p \in \mathcal{C}_P} \left| R_e(p, L) - \frac{\pi(2L) - \pi(L)}{2} \right|^{2\nu} = \mathbb{E}\left(\left(X_{P,L} - \frac{\pi(2L) - \pi(L)}{2} \right)^{2\nu} \right).$$

In other words, the left-hand side of Theorem 3.2 is the moment of order 2ν of $X_{P,L} - \frac{\pi(2L)-\pi(L)}{2}$. We define

$$m = \frac{\pi(2L) - \pi(L)}{2}, \quad \sigma = \frac{\sqrt{\pi(2L) - \pi(L)}}{2}, \quad Y_{P,L} = \frac{X_{P,L} - m}{\sigma}.$$

According to the previous section, we expect that the distribution of $X_{P,L}$ converges in some sense to a Gaussian distribution of mean value m and standard deviation σ. This is the content of the next theorem, that we will prove in this section. We will use the random variable $Y_{P,L}$, which is a normalisation of $X_{P,L}$ by the expected mean and standard deviation. Let $\psi : \mathbb{R}_+ \to \mathbb{R}$ be a function such that $\frac{\psi(x)}{x^n} \xrightarrow[x \to +\infty]{} +\infty$ for every $n \in \mathbb{N}$. For $L \geq 3$ the cumulative distribution function of $Y_{\psi(L),L}$ is the function

$$G_L : \left\{ \begin{array}{ll} \mathbb{R} & \to [0, 1] \\ x & \mapsto \mathbb{P}_{\psi(L)}(Y_{\psi(L),L} \leq x). \end{array} \right.$$

Denote by G the cumulative distribution function of a standard normal random variable Z. We say that $(Y_{\psi(L),L})$ converges in distribution to Z if the sequence of functions (G_L) converges pointwise to G when L goes to infinity. The theorem that we will prove in this section is the following:

Theorem 5.1. *Under GRH, the sequence of random variables $(Y_{\psi(L),L})$ converges in distribution to a standard normal random variable Z when L goes to infinity.*

5.2 The moments of the standard normal distribution

Let Z be a standard normal random variable. The moments of Z are the quantities

$$m_k = \mathbb{E}(Z^k)$$

for $k \in \mathbb{N}$. We have $m_{2k+1} = 0$ and an integration by parts shows that

$$m_{2k} = (2k-1) \cdot (2k-3) \cdots 3 \cdot 1.$$

The standard normal distribution is characterised by its moments: if X is a random variable such that $\mathbb{E}(X^k) = m_k$ for every k, then X is a standard normal random variable. To prove Theorem 5.1, we will use the following result (see [Bil95, Theorem 30.2]).

Theorem 5.2. *Let $(X_n)_n$ be a sequence of random variables such that for every $k \in \mathbb{N}$,*

$$\mathbb{E}(X_n^k) \xrightarrow[n \to +\infty]{} m_k.$$

Then $(X_n)_n$ converges in distribution to a standard normal random variable Z.

To prove Theorem 5.1, we will show that the moments of $Y_{\psi(L),L}$ converge to the moments m_k when L goes to infinity.

We generalise Lemmas 3.16 and 3.18 to an arbitrary number of distinct odd primes.

Lemma 5.3. *Under GRH, for $m = \ell_1 \dots \ell_s$ a product of s distinct primes coprime with $A(E)$, we have for $P \geq \ell_1, \dots, \ell_s$*

$$\sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{m} \right) = \kappa_m (\pi(2P) - \pi(P)) + O(m^3 P^{1/2} \log(P))$$

where $\kappa_m = (-1)^s \prod_{i=1}^{s} \frac{1}{\ell_i^2 - 1}$.

Proof. The proof mimics that of Lemmas 3.16 and 3.18. We consider the bijective Galois representation

$$\overline{\rho_m} : \mathrm{Gal}(L_{m,E}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})$$

and $S(x) := \sum_{\substack{p\leq x,\\ p\nmid mN_E}} \left(\frac{D_p}{m}\right)$ (as in the case $s=2$, the sums $S(2P)-S(P)$ and $\sum_{p\in\mathcal{C}_P}\left(\frac{D_p}{m}\right)$ differ by at most one term). We have

$$S(x) = \sum_{\substack{(\gamma_1,\dots,\gamma_s)\in\{-1,1\}^s\\ \gamma_1\cdots\gamma_s=1}} \pi_{C_{\gamma_1,\dots,\gamma_s}}(x, L_{m,E}) - \sum_{\substack{(\gamma_1,\dots,\gamma_s)\in\{-1,1\}^s\\ \gamma_1\dots\gamma_s=-1}} \pi_{C_{\gamma_1,\dots,\gamma_s}}(x, L_{m,E})$$

where the sets $C_{\gamma_1,\dots,\gamma_s}$ are defined as in the paragraph 3.3.2. Theorem 3.9 implies that

$$S(x) = \frac{A_1(m) - A_{-1}(m)}{|\mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})|}\pi(x) + O(m^3x^{1/2}\log(m^3x\cdot mN_E))$$

where for $\varepsilon\in\{1,-1\}$, we write

$$\sum_{\substack{(\gamma_1,\dots,\gamma_s)\in\{-1,1\}^s\\ \gamma_1\cdots\gamma_s=\varepsilon}} C_{\ell_1}(\gamma_1)\cdots C_{\ell_s}(\gamma_s).$$

We show by induction on s that $A_1(m)-A_{-1}(m) = (-1)^s\prod_{i=1}^{s}\ell_i$. Lemma 3.11 directly gives the result for $s=1$. Assume that $A_1(m)-A_{-1}(m)$ and let ℓ_{s+1} be a prime such that $\gcd(m,\ell_{s+1})=1$. Then,

$$\begin{aligned}
A_1(m\ell_{s+1}) - A_{-1}(m\ell_{s+1}) &= A_1(m)A_1(\ell_{s+1}) + A_{-1}(m)A_{-1}(\ell_{s+1})\\
&\quad - A_1(m)A_{-1}(\ell_{s+1}) - A_{-1}(m)A_1(\ell_{s+1})\\
&= A_1(m)(A_1(\ell_{s+1}) - A_{-1}(\ell_{s+1})) - A_{-1}(m)(A_1(\ell_{s+1}) - A_{-1}(\ell_{s+1}))\\
&= -(A_1(m) - A_{-1}(m))\ell_{s+1}\\
&= (-1)^{s+1}\prod_{i=1}^{s+1}\ell_i.
\end{aligned}$$

Therefore, $S(x) = (-1)^s\prod_{i=1}^{s}\frac{1}{\ell_i^2-1}\pi(x) + O(m^3x^{1/2}\log(m^4N_Ex))$. Because $\ell_1,\dots,\ell_s$ are all smaller than P, one can replace the error term by $O(m^3P^{1/2}\log(P))$ in $S(P)$ and $S(2P)$. □

As in the proof of Theorem 3.1, for a positive integer k and $0\leq j\leq k$, let $\mathcal{Q}_{k,j}$ be the set of tuples $(\ell_1,\dots,\ell_k)$ of primes in $[L,2L]$ such that $\ell_1\dots\ell_k = n^2m$ where m is a squarefree product of j primes and n is the product of $\frac{k-j}{2}$ primes ($\mathcal{Q}_{k,j}$ is empty if $k-j$ is odd). We will need the following lemma.

Lemma 5.4. *Let ν be a positive integer. Then,*

$$|\mathcal{Q}_{2\nu,0}| = m_{2\nu}\frac{L^\nu}{\log(L)^\nu} + O\left(\frac{L^{\nu-1}}{\log(L)^{\nu-1}}\right).$$

Proof. For $n \in \{1,\dots,\nu\}$, let $\mathcal{A}_n$ be the set of tuples $(A_1,\dots,A_n)$ of disjoint subsets of $\{1,\dots,2\nu\}$ such that:

- $\forall i \in \{1,\dots,n\}$, $A_i \neq \emptyset$,
- $\forall (i,j) \in \{1,\dots,n\}^2$, $A_i \cap A_j = \emptyset$,
- $\forall i \in \{1,\dots,n\}$, $|A_i|$ is even,
- $\bigsqcup_{i=1}^{n} A_i = \{1,\dots,2\nu\}$.

We also define $\mathcal{B}_L^n$ to be the set of ordered n-tuples of distinct primes in $[L,2L]$. Let $s = (\ell_1,\dots,\ell_{2\nu})$ be an element of $\mathcal{Q}_{2\nu,0}$ such that $\mathrm{lcm}(\ell_1\cdots\ell_{2\nu})$ has n distinct prime factors, and $\ell_1' < \ldots < \ell_n'$ primes such that

$$\{\ell_1,\ldots\ell_{2\nu}\} = \{\ell_1',\dots,\ell_n'\}.$$

Then, we define $b_s = (\ell_1',\dots,\ell_n')$. For $j \in \{1,\dots,n\}$, we set

$$A_j^s = \{i \in \{1,\dots,2\nu\} \ : \ \ell_i = \ell_j'\}$$

and $a_s = (A_1^s,\dots,A_n^s)$.

The set $\mathcal{Q}_{2\nu,0}$ is in one-to-one correspondence with

$$\bigsqcup_{1\le n\le \nu} \mathcal{A}_n \times \mathcal{B}_L^n$$

via $s \mapsto (a_s, b_s)$.

If n is fixed, we have $\mathcal{B}_L^n = \binom{\pi(2L)-\pi(L)+O(1)}{n} \sim \frac{L^n}{n!\log(L)^n}$ as L goes to infinity. For $n = \nu$, we have

$$|\mathcal{A}_\nu| = \binom{2\nu}{2}\cdot\binom{2\nu-2}{2}\cdots\binom{2}{2} = \nu!\cdot m_{2\nu},$$

so

$$|\mathcal{A}_\nu \times \mathcal{B}_L^\nu| \sim m_{2\nu}\frac{L^\nu}{\log(L)^\nu}.$$

Moreover,

$$\sum_{n=1}^{\nu-1} |\mathcal{A}_n| \cdot |\mathcal{B}_L^n| = \sum_{n=1}^{\nu-1} |\mathcal{A}_n| \cdot O\left(\frac{L^{\nu-1}}{\log(L)^{\nu-1}}\right).$$

The sum

$$\sum_{n=1}^{\nu-1} |\mathcal{A}_n|$$

just depends on ν and not on L, and it can be absorbed in the big-O constant. $\square$

5.3 Proof of Theorem 5.1

As in the proof of Theorem 3.2, for a prime $p \in \mathcal{C}_P$, we write

$$\begin{cases} R_e(p,L) + R_a(p,L) &= \pi(2L) - \pi(L) + \varepsilon_L \\ R_e(p,L) - R_a(p,L) &= \sum\limits_{\ell \in [L,2L]} \left(\frac{D_p}{\ell}\right) + \omega_L(D_p). \end{cases}$$

Let us fix $k \in \mathbb{N}^*$. Then, by the multinomial theorem

$$\begin{aligned} \mathbb{E}(Y_{P,L}^k) &= \frac{1}{\sigma^k |\mathcal{C}_P|} \sum_{p \in \mathcal{C}_P} \left(R_e(p,L) - \frac{\pi(2L) - \pi(L)}{2} \right)^k \\ &= \frac{1}{\sigma^k |\mathcal{C}_P|} \sum_{p \in \mathcal{C}_P} \left(\frac{\sum\limits_{\ell \in [L,2L]} \left(\frac{D_p}{\ell}\right) + \omega_L(D_p) + \varepsilon_L}{2} \right)^k \\ &= \frac{\sum\limits_{k_1+k_2+k_3=k} \binom{n}{k_1,k_2,k_3} \widetilde{U}_{k_1} \widetilde{V}_{k_2} \varepsilon_L^{k_3}}{\sigma^k 2^k} \end{aligned}$$

where $\binom{n}{k_1,k_2,k_3} = \frac{n!}{k_1!k_2!k_3!}$ and

$$\begin{cases} \widetilde{U}_{k_1} &= \sum\limits_{p \in \mathcal{C}_P} \left(\sum\limits_{\ell \in [L,2L]} \left(\frac{D_p}{\ell}\right) \right)^{k_1} = \sum\limits_{\ell_1,\ldots,\ell_{k_1} \in [L,2L]} \sum\limits_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1 \ldots \ell_{k_1}}\right) \\ \widetilde{V}_{k_2} &= \sum\limits_{p \in \mathcal{C}_P} \omega_L(D_p)^{k_2}. \end{cases}$$

For every $k_2 \in \{0, \ldots, k\}$, Lemma 3.15 already gives us

$$\widetilde{V}_{k_2} = O\left(\frac{P}{\log(L)\log(P)} + \frac{L^{4k_2} P^{1/2} \log(P)}{\log(L)^{k_2}} \right).$$

We will now estimate the sums $\widetilde{U}_{k_1}$ for every $k_1 \in \{0, \dots, k\}$.

First, assume that k_1 is odd: $k_1 = 2\nu + 1$ where $\nu \in \mathbb{N}$. Then,

$$\widetilde{U}_{2\nu+1} = \sum_{j=0}^{\nu} \sum_{\substack{(\ell_1,\dots,\ell_{2\nu+1}) \\ \in \mathcal{Q}_{2\nu+1,2j+1}}} \sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1 \dots \ell_{2\nu+1}} \right).$$

For $j \in \{0, \dots, \nu\}$, we have $|\mathcal{Q}_{2\nu+1,2j+1}| = O\left(\frac{L^{\nu+j+1}}{\log(L)^{\nu+j+1}} \right)$, so by Lemma 5.3, we have

$$\sum_{\substack{(\ell_1,\dots,\ell_{2\nu+1}) \\ \in \mathcal{Q}_{2\nu+1,2j+1}}} \sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1 \dots \ell_{2\nu+1}} \right) = O\left(\frac{L^{\nu+j+1}}{\log(L)^{\nu+j+1}} \left(\frac{P}{L^{4j+2}\log(P)} + L^{6j+3} P^{1/2} \log(P) \right) \right).$$

The dominant terms occur for $j = 0$ and $j = \nu$. By getting rid of the non-dominant terms, we obtain

$$\widetilde{U}_{2\nu+1} = O\left(\frac{L^{\nu-1} P}{\log(L)^{\nu+1}\log(P)} + \frac{L^{8\nu+4} P^{1/2} \log(P)}{\log(L)^{2\nu+1}} \right).$$

Now, we assume that k_1 is even: $k_1 = 2\nu$. We also write

$$\widetilde{U}_{2\nu} = \sum_{j=0}^{\nu} \sum_{(\ell_1,\dots,\ell_{2\nu}) \in \mathcal{Q}_{2\nu,2j}} \sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1 \dots \ell_{2\nu}} \right).$$

Take $j \in \{1, \dots, \nu\}$. Then, $|\mathcal{Q}_{2\nu,2j}| = O\left(\frac{L^{\nu+j}}{\log(L)^{\nu+j}} \right)$, so by Lemma 5.3, we have

$$\sum_{(\ell_1,\dots,\ell_{2\nu}) \in \mathcal{Q}_{2\nu,2j}} \sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1 \dots \ell_{2\nu}} \right) = O\left(\frac{L^{\nu+j}}{\log(L)^{\nu+j}} \left(\frac{P}{L^{4j}\log(P)} + L^{6j} P^{1/2} \log(P) \right) \right).$$

Now assume that $j = 0$. Then, for $(\ell_1, \dots, \ell_{2\nu}) \in \mathcal{Q}_{2\nu,0}$ and $p \in \mathcal{C}_P$, we have $\left(\frac{D_p}{\ell_1 \dots \ell_{2\nu}} \right) = 1$ except if some ℓ_i divides D_p. By Lemma 3.14, we have

$$\begin{aligned} |\{p \in \mathcal{C}_P \ : \ D_p \equiv 0 \bmod \ell_1 \dots \ell_{2\nu}\}| &\leq |\{p \in \mathcal{C}_P \ : \ D_p \equiv 0 \bmod \min_{1 \leq i \leq 2\nu} \ell_i\}| \\ &= O\left(\frac{P}{L\log(P)} + L^3 P^{1/2} \log(P) \right). \end{aligned}$$

Then, if $(\ell_1, \dots, \ell_\nu) \in \mathcal{Q}_{2\nu,0}$,

$$\sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1 \dots \ell_{2\nu}} \right) = |\mathcal{C}_P| + O\left(\frac{P}{L \log(P)} + L^3 P^{1/2} \log(P) \right).$$

We use Lemma 5.4 to get

$$\sum_{(\ell_1,\dots,\ell_{2\nu}) \in \mathcal{Q}_{2\nu,0}} \sum_{p \in \mathcal{C}_P} \left(\frac{D_p}{\ell_1 \dots \ell_{2\nu}} \right) = m_{2\nu} |\mathcal{C}_P| \frac{L^\nu}{\log(L)^\nu} + m_{2\nu} |\mathcal{C}_P| O\left(\frac{L^{\nu-1}}{\log(L)^{\nu-1}} \right) + O\left(\frac{L^{\nu-1} P}{\log(L)^\nu \log(P)} + \frac{L^{3+\nu} P^{1/2} \log(P)}{\log(L)^\nu} \right).$$

The dominant terms occur for $j = 0$ and $j = \nu$, and we have

$$\widetilde{U}_{2\nu} = m_{2\nu} |\mathcal{C}_P| \frac{L^\nu}{\log(L)^\nu} + O\left(m_{2\nu} |\mathcal{C}_P| \frac{L^{\nu-1}}{\log(L)^{\nu-1}} + \frac{L^{\nu-1} P}{\log(L)^\nu \log(P)} + \frac{L^{8\nu} P^{1/2} \log(P)}{\log(L)^{2\nu}} \right).$$

Assume that k is odd. Then, $\frac{\widetilde{U}_{k_1}}{\sigma^k |\mathcal{C}_P|}$ and $\frac{\widetilde{V}_{k_2}}{\sigma^k |\mathcal{C}_P|}$ converge to 0 for every k_1 and k_2 smaller than or equal to k if $P = \psi(L)$ and L goes to infinity. So $\mathbb{E}(Y^k_{\psi(L),L}) \xrightarrow[L \to +\infty]{} 0$.

Assume that k is even and $P = \psi(L)$. Then, $\frac{U_k}{\sigma^k |\mathcal{C}_P|}$ converge to m_k as L goes to infinity, whereas $\frac{U_{k_1}}{\sigma^k |\mathcal{C}_P|}$ tend to 0 for $k_1 < k$ and $\frac{V_{k_2}}{\sigma^k |\mathcal{C}_P|}$ tend to 0 for $k_2 \leq k$. Therefore, $\mathbb{E}(Y^k_{\psi(L),L}) \xrightarrow[L \to +\infty]{} m_k$.

Remark 5.5. Since we have shown that

$$\widetilde{U}_{2\nu} = m_{2\nu} |\mathcal{C}_P| \frac{L^\nu}{\log(L)^\nu} + O\left(\frac{L^{8\nu} P^{1/2} \log(P)}{\log(L)^{2\nu}} \right),$$

we also proved Theorem 3.2 for every ν in passing.

We were not able to prove the equivalent of Theorem 5.1 for the distribution of Elkies primes for the family of elliptic curves defined over a finite field. In the proof of Theorem 3.2, the upper bound on $\widetilde{U}_{2\nu}$ after dividing by $|\mathcal{C}_P|$ involves the two terms

$$O\left(\frac{L^\nu}{\log(L)^\nu} \right) \quad \text{and} \quad O\left(\frac{L^{8\nu} \log(P)^2}{P^{1/2} \log(L)^{2\nu}} \right).$$

The second term tends to 0 if $P = \psi(L)$ and $L \to \infty$. Our analysis in the proof of the previous theorem shows that the implied constant for the first term is $m_{2\nu}$, and after

normalising by $\sigma^{2\nu}$, the first term tends to $m_{2\nu}$. The bound on $U_{2\nu}$ in Theorem 3.1 also involves two terms (after dividing by $|\mathcal{E}_q|$):

$$O\left(\frac{L^\nu}{\log(L)^\nu} q^{1/2}\log(q)\log(\log(q))\right) \quad \text{and} \quad O\left(\frac{L^{2\nu}}{\log(L)^\nu} q^{-1/2} L^\nu \log(L)\right).$$

The second one tends to 0 if q and L tend to infinity and $q \gg L^n$ for every $n \in \mathbb{N}$. However, the first term normalised by $\sigma^{2\nu}$ doesn't tend to a finite limit because of the factor $q^{1/2}\log(q)\log(\log(q))$. In fact, in the estimation of $U_{2\nu}$, the numbers $f_q(t)$ are uniformly bounded (in t) by this factor, so we get a character sum indexed by t:

$$\sum_{|t|\leq 2q^{1/2}} \left| \sum_{L\leq \ell \leq 2L} \left(\frac{t^2-4q}{\ell}\right)\right|^{2\nu}.$$

This estimation is not sharp enough. A better understanding of the distribution of the distribution of elliptic curves according to their trace of Frobenius seems to be required to estimate $U_{2\nu}$ more precisely and to prove an analogue of Theorem 5.1 in this context.

References

[Bil95] P. Billingsley. *Probability and Measure*. John Wiley & Sons, third edition, 1995.

[CD08] A. C. Cojocaru and C. David. Frobenius fields for elliptic curves. *American Journal of Mathematics*, 130(6):1535–1560, 2008.

[CFRM05] A. C. Cojocaru, E. Fouvry, and M. Ram Murty. The square sieve and the Lang-Trotter conjecture. *Canadian Journal of Mathematics*, 57(6):1155–1177, 2005.

[Che18] G. Chenevier. Théorie algébrique des nombres, Lecture notes of a Master 1 course delivered at École polytechnique. `http://gaetan.chenevier.perso.math.cnrs.fr/TAN_chenevier.pdf`, 2017-2018.

[Coh93] H. Cohen. *A Course in Computational Algebraic Number Theory*. Springer, Graduate Texts in Mathematics, 1993.

[Coj05] A. C. Cojocaru. On the surjectivity of the Galois representations associated to non-CM elliptic curves. *Canadian Mathematical Bulletin*, 48(1):16–31, 2005.

[Cox13] D. A. Cox. *Primes of the form $x^2 + ny^2$. Fermat, Class Field Theory and Complex Multiplication*. Wiley, 2nd edition, 2013.

[CZ02] T. Cochrane and Z. Y. Zheng. A survey on pure and mixed exponential sums modulo prime powers. In *Proceedings of Illinois Millennial Conference on Number Theory*, volume 1, pages 271–300. A.K. Peters, Natick, MA, 2002.

[Dat19] J.-F. Dat. Introduction à l'arithmétique des courbes elliptiques, Lecture notes of a Master 2 course delivered at Sorbonne Université. `https://webusers.imj-prg.fr/~jean-francois.dat/enseignement/CourbesEll/CE.pdf`, 2018-2019.

[Dav80] H. Davenport. *Multiplicative Number Theory*. Springer, 2nd edition, 1980.

[DW12a] C. David and J. Wu. Almost prime values of the order of elliptic curves over finite fields. *Forum Mathematicum*, 24(1):99–119, 2012.

[DW12b] C. David and J. Wu. Pseudoprime reductions of elliptic curves. *Canadian Journal of Mathematics*, 64(1):81–101, 2012.

[HMV04] D. Hankerson, A. Menezes, and S. Vanstone. *Guide to Elliptic Curve Cryptography*. Springer, 2004.

[IK04] H. Iwaniec and E. Kowalski. *Analytic Number Theory*. American Mathematical Society, Colloquium Publications, vol. 53, 2004.

[Izq23] D. Izquierdo. Introduction à la géométrie algébrique et aux courbes elliptiques, Lecture notes of a Master 2 course delivered at École polytechnique, 2022-2023.

[Jeo09] E. Jeong. Isomorphism classes of elliptic curves over finite fields with characteristic 3. *Journal of the Chungcheong Mathematical Society*, 22(3), 2009.

[LJ87] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Annals of Mathematics*, 126(3):649–673, 1987.

[LO77] J. C. Lagarias and A. M. Odlyzko. Effective versions of the Chebotarev density theorem. In *Algebraic Number Fields (A. Fröhlich edit.)*, pages 409–464, 1977.

[Lou92] S. Louboutin. l-functions and class numbers of imaginary quadratic fields and of quadratic extensions of an imaginary quadratic field. *Mathematics of Computation*, 59:213–230, 1992.

[McK99] J. McKee. Subtleties in the distribution of the numbers of points on elliptic curves over a finite prime field. *Journal of the Mathematical London Society*, 59(2):448–460, 1999.

[PP18] R. K. Pandey and A. Parashar. On certain sums with quadratic expressions involving the Legendre symbol. *Journal of Integer Sequences*, 21, article 18.4.7, 2018.

[Sch85] R. Schoof. Elliptic curves over finite fields and the computation of square roots mod p. *Mathematics of computation*, 44(170):483–494, 1985.

[Sch87] R. Schoof. Nonsingular plane cubic curves over finite fields. *Journal of Combinatorial Theory*, 46(2):183–208, 1987.

[Sch95] R. Schoof. Counting points on elliptic curves over finite fields. *Journal de Théorie des Nombres de Bordeaux*, 7(1):219–254, 1995.

[Ser81] J.-P. Serre. Quelques applications du théorème de densité de Chebotarev. *Publications mathématiques de l'I.H.É.S, tome 54*, pages 123–201, 1981.

[Ser97] J.-P. Serre. *Corps Locaux*. Hermann, 4th edition, 1997.

[Sil94] J. H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*. Springer, Graduate Texts in Mathematics, 1994.

[Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Springer, Graduate Texts in Mathematics, 2nd edition, 2009.

[SS14] I. E. Shparlinski and A. V. Sutherland. On the distribution of Atkin and Elkies primes. *Foundations of Computational Mathematics*, 14:285–297, 2014.

[SS15] I. E. Shparlinski and A. V. Sutherland. On the distribution of Atkin and Elkies primes for reductions of elliptic curves on average. *LMS Journal of Computation and Mathematics*, 18(1):308–322, 2015.

[Sut22] A. V. Sutherland. Lecture notes on elliptic curves. `https://math.mit.edu/classes/18.783/2022/`, 2022.

[Was08] L. C. Washington. *Elliptic Curves: Number Theory and Cryptography*. Chapman and Hall/CRC, second edition, 2008.

[Wat69] W. C. Waterhouse. Abelian varieties over finite fields. *Annales scientifiques de l'E.N.S, 4e série, tome 2, numéro 4*, pages 521–560, 1969.

[Wei48] A. Weil. On some exponential sums. In *Proceedings of the National Academy of Sciences of the United States of America*, volume 34, pages 204–207, 1948.

[Wie08] G. Wiese. Galois representations. `https://math.uni.lu/~wiese/notes/GalRep.pdf`, 2008.