

# THE ASYMPTOTIC DISTRIBUTION OF ELKIES PRIMES FOR REDUCTIONS OF ABELIAN VARIETIES IS GAUSSIAN

ALEXANDRE BENOIST AND JEAN KIEFFER

**ABSTRACT.** We generalize the notion of Elkies primes for elliptic curves to the setting of abelian varieties, possibly equipped with real multiplication (RM), and prove the following. Let  $A$  be such an abelian variety over a number field whose Galois representation has large image with respect to the chosen RM. Then the distribution of the number of Elkies primes (in a suitable range) for reductions of  $A$  modulo primes converges weakly to a Gaussian distribution around its expected value. This refines and generalizes results obtained by Shparlinski and Sutherland in the case of non-CM elliptic curves, and has implications for the complexity of the SEA point counting algorithm for abelian surfaces over finite fields.

## 1. INTRODUCTION

**1.1. Setup.** Let  $E$  be an elliptic curve over a finite field  $\mathbb{F}_q$ . We say that a prime number  $\ell$  is *Elkies* for  $E$  if there exists an  $\ell$ -isogeny with domain  $E$  defined over  $\mathbb{F}_q$ . This terminology stems from the Schoof–Elkies–Atkin (SEA) algorithm for determining  $\#E(\mathbb{F}_q)$  [15]; this algorithm is faster if  $E$  has many small Elkies primes  $\ell$ , as Elkies’s method can then be applied to determine  $\#E(\mathbb{F}_q) \bmod \ell$ . In order to assess the overall complexity of the SEA algorithm, Shparlinski and Sutherland proved that there are enough Elkies primes on average, either when considering all elliptic curves over a fixed  $\mathbb{F}_q$  [20] or when considering reductions of a fixed, non-CM elliptic curve over  $\mathbb{Q}$  modulo primes in a large interval [21]. For further results in a non-average setting, see [19].

We may also consider Elkies primes for abelian varieties of higher dimensions. Let  $A$  be a polarized abelian variety of dimension  $g$  over  $\mathbb{F}_q$ . We say that a prime  $\ell$ , coprime to  $q$  and the degree of the polarization, is *Elkies* for  $A$  if there exists an  $\mathbb{F}_q$ -rational subgroup  $G \subset A[\ell]$  which is maximal isotropic for the Weil pairing; in that case, the quotient  $A/G$  is also equipped with a polarization of the same degree. More generally, if  $A$  has real multiplication (RM) by an order  $\mathcal{O}$  in a totally real number field  $K$  of degree  $d$ , i.e. if  $A$  is equipped with a primitive embedding  $\mathcal{O} \hookrightarrow \text{End}_{\mathbb{F}_q}(A)$  such that every  $x \in \mathcal{O}$  is invariant under the Rosati involution, we say that a prime ideal  $\mathfrak{l}$  of  $\mathcal{O}$  is *Elkies* for  $A$  if  $A[\mathfrak{l}]$  admits a maximal isotropic subgroup  $G$  defined over  $\mathbb{F}_q$  and stable under  $\mathcal{O}$ , or in other words, if there exists an  $\mathbb{F}_q$ -rational  $\mathfrak{l}$ -isogeny from  $A$ , as defined in [5]. This notion of Elkies primes

---

*Date:* July 10, 2025.

*2020 Mathematics Subject Classification.* 14K02, 11G05, 11G10.

*Key words and phrases.* Abelian varieties, Isogenies, Real multiplication, Elkies primes.

is a suitable analogue of the classical definition in the context of the SEA algorithm on principally polarized abelian surfaces with or without RM [9].

**1.2. Main results.** In this paper, we show that the number of Elkies primes in certain ranges for reductions of a fixed abelian variety  $A$  with RM over a number field asymptotically follows a Gaussian distribution, provided that the Galois representation attached to  $A$  has a large enough adelic image.

To formulate this last condition precisely, we introduce the following notation. Let  $F$  be the field of definition of  $A$  and let  $G_F$  be its absolute Galois group. If  $\ell$  is a large enough prime, the  $\ell$ -adic Tate module  $T_\ell(A)$  of  $A$  is a free  $\mathcal{O} \otimes \mathbb{Z}_\ell$ -module of rank  $2h$  where  $h = g/d$ , endowed with a nondegenerate alternating form with values in  $\mathcal{O} \otimes \mathbb{Z}_\ell$ , as we review in Section 2. If  $n$  is a sufficiently large integer, we can therefore consider the global Galois representation

$$\hat{\rho}_n : G_F \rightarrow \mathrm{GSp}_{2h}(\mathcal{O} \otimes \hat{\mathbb{Z}}_{\geq n}), \quad \text{where } \hat{\mathbb{Z}}_{\geq n} := \prod_{\ell \text{ prime}, \ell \geq n} \mathbb{Z}_\ell.$$

We say that  $A$  has *large Galois image* if  $\hat{\rho}_n(G_F)$  contains  $\mathrm{Sp}_{2h}(\mathcal{O} \otimes \hat{\mathbb{Z}}_{\geq n})$  for large enough  $n$ . Assuming that  $\mathcal{O}$  is the whole endomorphism ring of  $A$  over  $\mathbb{Q}$  (a necessary condition), one can sometimes guarantee that  $A$  has large Galois image, as in Serre's open image theorem in the case  $d = 1$  [17]: we review this theorem and its RM analogues in Section 2.

Our main result on the distribution of Elkies primes is then the following.

**Theorem 1.1.** *Assume the generalized Riemann hypothesis (GRH). Let  $\mathcal{O}$  be an order in a totally real number field  $K$  of degree  $d$ , and let  $A$  be a polarized abelian variety of dimension  $g \geq 1$  defined over a number field  $F$  with RM by  $\mathcal{O}$  with large Galois image.*

*For a real number  $L$ , denote by  $\mathcal{P}_K(L, 2L)$  the set of prime ideals  $\mathfrak{l}$  of  $K$  such that  $N_{K/\mathbb{Q}}(\mathfrak{l}) \in [L, 2L]$ , and define  $\mathcal{P}_F(P, 2P)$  similarly. For a prime  $\mathfrak{p}$  of  $F$  of good reduction for  $A$  and  $L \geq 1$ , let  $N_e(\mathfrak{p}, L)$  be the number of Elkies primes  $\mathfrak{l} \in \mathcal{P}_K(L, 2L)$  for  $A_{\mathfrak{p}}$ . Further define  $\alpha_h \in (0, 1)$  by the formula*

$$\alpha_h = \sum_{(d_1, \dots, d_r) \in \Sigma_h} \frac{1}{2^r} \cdot \prod_{i=1}^r \frac{1}{d_i} \cdot \prod_{k=1}^h \frac{1}{\#\{j : d_j = k\}!}$$

where  $\Sigma_h$  denotes the set of unordered partitions of the integer  $h = g/d$ .

Then, as  $L, P \rightarrow \infty$  with  $P \gg L^n$  for every positive integer  $n$ , the function

$$\begin{aligned} X_{P,L} : \mathcal{P}_F(P, 2P) &\longrightarrow \mathbb{R} \\ \mathfrak{p} &\longmapsto \frac{N_e(\mathfrak{p}, L) - \alpha_h \#\mathcal{P}_K(L, 2L)}{\sqrt{\alpha_h(1 - \alpha_h) \#\mathcal{P}_K(L, 2L)}} \end{aligned}$$

converges weakly to the standard Gaussian distribution with mean value 0 and variance 1.

Intuitively,  $\alpha_h$  is the probability that  $\mathfrak{l}$  will be Elkies for  $A_{\mathfrak{p}}$  for random  $\mathfrak{l}$  and  $\mathfrak{p}$ ; weak convergence to the Gaussian distribution of Theorem 1.1 is what we would obtain from the central limit theorem in the naive probabilistic model where the events “ $\mathfrak{l}$  is Elkies for  $A_{\mathfrak{p}}$ ” are all independent. We list the first few values of  $\alpha_h$  in Table 1.

$h$	1	2	3	4	5	6	7	8
$\alpha_h$ (exact value)	$\frac{1}{2}$	$\frac{3}{8}$	$\frac{5}{16}$	$\frac{35}{128}$	$\frac{63}{256}$	$\frac{231}{1024}$	$\frac{429}{2048}$	$\frac{6435}{32768}$
$\alpha_h$ (approximate value)	0.5	0.375	0.3125	0.2734	0.2461	0.2256	0.2095	0.1964

TABLE 1. Values of  $\alpha_h$ 

We prove Theorem 1.1 by analyzing the moments of  $X_{P,L}$  at all orders  $k \geq 0$ , which we somewhat abusively denote by

$$\mathbb{E}(X_{P,L}^k) := \frac{1}{\#\mathcal{P}_F(P, 2P)} \sum_{\mathfrak{p} \in \mathcal{P}_F(P, 2P)} X_{P,L}(\mathfrak{p})^k.$$

In fact, Theorem 1.1 follows directly from the following result: see [2, Theorem 30.2].

**Theorem 1.2.** *Assume GRH, and keep notation from Theorem 1.1. Let  $k \geq 0$  be any integer, and let  $M_k$  be the moment of order  $k$  of the standard Gaussian distribution (thus  $M_k = 0$  for odd  $k$ ). Then  $\mathbb{E}(X_{P,L}^k)$  converges to  $M_k$  as  $P, L \rightarrow \infty$  with  $P \gg L^n$  for every positive integer  $n$ . More precisely, we have*

$$\mathbb{E}(X_{P,L}^k) = M_k + O_{A,k} \left( \frac{1}{L^{1/2} \log(L)^{1/2}} + \frac{L^{k(2h^2+h+3/2)} \log(P)^2}{\log(L)^{k/2} P^{1/2}} \right).$$

Here the notation  $O_{A,k}$  means that the implicit constants in Landau's notation are allowed to depend on  $A$  (hence on  $F$ ,  $\mathcal{O}$ , and  $h$ ) and  $k$ .

In the case of elliptic curves, Theorem 1.2 refines [21] as we consider moments of all orders and provide an asymptotic equivalent of the even moments rather than an upper bound. To the best of our knowledge, Theorem 1.2 is also the first quantitative result on the distribution of Elkies primes in higher dimensions. In particular, a consequence of this theorem is that there are enough Elkies primes to run the SEA algorithm in dimension 2 on average over reductions of a fixed abelian variety: see [9, Def. 3.7].

The proof of Theorem 1.2 is inspired from [21]: we apply an explicit version of the Čebotarev density theorem (which relies on GRH) to number field extensions of  $F$  cut out by torsion subgroups of  $A$ , and count how many elements in their Galois groups correspond to  $\mathfrak{l}$  being Elkies for  $A_{\mathfrak{p}}$ . The result then follows from rearranging the summations and from a combinatorial argument to determine the leading term in the moments of  $X_{P,L}$ .

We also provide numerical experiments on the distribution of Elkies primes in large ranges in the case of elliptic curves: it was actually the very smooth aspect of the data which prompted us to try and prove Theorem 1.1.

One might wonder if this convergence result to a Gaussian distribution also holds when considering all elliptic curves (or more generally abelian varieties) over a fixed  $\mathbb{F}_q$  as in [20]. To answer this, it seems that one would need careful control on the class numbers appearing in the distribution of traces of Frobenius for elliptic curves over  $\mathbb{F}_q$ .

**1.3. Organization.** In Section 2, we review the properties of Galois representations attached to abelian varieties with RM, characterize Elkies primes both in terms of Frobenius elements in the Galois representation and in terms of the existence of isogenies, and recall results from the literature on large Galois images. In Section 3, we count matrices in  $\mathrm{GSp}_{2h}(\mathcal{O}/I\mathcal{O})$  (and related groups) corresponding to Elkies primes, a key input to the Čebotarev density theorem. We prove Theorem 1.2 in Section 4, and report on our numerical experiments in Section 5.

**1.4. Acknowledgments.** The first author was supported by the Agence Nationale de la Recherche/France 2030 grant CRYPTANALYSE (reference 22-PECY-0010.) This research was funded in whole, or in part, by the Luxembourg National Research Fund (FNR), grant reference PRIDE23/18685085. For the purpose of open access, and in fulfilment of the obligations arising from the grant agreement, the authors have applied a Creative Commons Attribution 4.0 International (CC BY 4.0) license to any Author Accepted Manuscript version arising from this submission.

**1.5. Statement on competing interests.** The authors declare no competing interests.

**1.6. Data availability statement.** The code used to generate the figures in Section 5 is available as one of the paper’s source files at <https://arxiv.org/abs/2411.18171>.

## 2. GALOIS REPRESENTATIONS AND ELKIES PRIMES

In this section, we review basic facts on the structure of torsion subgroups of abelian varieties with RM over any field (§2.1). Then we characterize Elkies primes for such abelian varieties in terms of the existence of isogenies (§2.2) and, in the case of finite fields or reductions of abelian varieties over number fields, in terms of the action of Frobenius on torsion subgroups (§2.3). Finally, we review deeper results on large Galois images (§2.4).

**2.1. Torsion subgroups of abelian varieties with RM.** Throughout, we use the notation listed in Table 2. For the reader’s convenience, the table also includes symbols defined later in this section. For now,  $F$  is any field, and  $A$  is a polarized abelian variety over  $F$  with real multiplication by an order  $\mathcal{O}$  as in the introduction. We write  $d_A$  for the degree of the polarization of  $A$  and  $c_{\mathcal{O}}$  for the conductor of  $\mathcal{O}$ .

Recall that whenever  $n \geq 1$  is prime to  $p$ , the  $n$ -torsion subgroup  $A[n]$  of  $A$ , seen as group scheme, is étale. Throughout, we abuse notation and identify these group schemes (as well as their subgroups) with their groups of points over a separable closure  $F^{sep}$  of  $F$ , endowed with an action of the absolute Galois group  $G_F$  of  $F$ . For all such  $n$ , there is a canonical nondegenerate pairing  $e_n$  on  $A[n] \times A^{\vee}[n]$ , called the Weil pairing, whose values are  $n$ -th roots of unity in  $F^{sep}$ . Now if  $\ell \neq p$  is a prime number, by making compatible choices of  $\ell$ -power roots of unity in  $F^{sep}$  and by composing with the polarization of  $A$  on the second argument, we obtain a new pairing

$$e_{\ell} : T_{\ell}(A) \times T_{\ell}(A) \rightarrow \mathbb{Z}_{\ell}$$

on the  $\ell$ -adic Tate module  $T_{\ell}(A)$ . We will work with this version of the Weil pairing in the rest of the paper. The Tate module  $T_{\ell}(A)$  is then a free  $\mathbb{Z}_{\ell}$ -module of rank  $2g$  on which  $e_{\ell}$

$K$	a totally real number field
$d$	the degree of $K$ over $\mathbb{Q}$
$\mathcal{O}$	an order of $K$
$\mathcal{O}_K$	the ring of integers in $K$
$c_{\mathcal{O}}$	the conductor of $\mathcal{O}$ , an ideal supported at primes dividing $[\mathcal{O}_K : \mathcal{O}]$
$N_{K/\mathbb{Q}}$	the norm map for ideals or elements of $K/\mathbb{Q}$
$\mathrm{Tr}_{K/\mathbb{Q}}$	the trace map for elements of $K/\mathbb{Q}$
$\ell$	a prime number in $\mathbb{Z}_{\geq 1}$
$\mathfrak{l}$	a prime ideal of $\mathcal{O}$ above $\ell$
$F$	a field
$p$	the characteristic exponent of $F$ (a prime number, or 1 if $\mathrm{char}(F) = 0$ )
$G_F$	the absolute Galois group of $F$
$\chi_{\ell}$	the cyclotomic character $G_F \rightarrow \mathbb{Z}_{\ell}^{\times}$
$A$	a polarized abelian variety over $F$ with RM by $\mathcal{O}$ , i.e. endowed with a primitive embedding $\mathcal{O} \hookrightarrow \mathrm{End}_F(A)$ , with $1 \mapsto \mathrm{id}_A$ , whose image consists of elements that are invariant under the Rosati involution
$g$	the dimension of $A$ ; in particular $d g$
$h$	the integer $g/d$
$d_A$	the degree of the polarization of $A$
$\pi_A$	the Frobenius endomorphism of $A$ (if $F$ is finite)
$T_{\ell}(A)$	the $\ell$ -adic Tate module of $A$
$e_{\ell}$	the Weil pairing on $T_{\ell}(A)$ , with values in $\mathbb{Z}_{\ell}$
$A[\ell]$	the $\ell$ -torsion subgroup of $A$
$\psi_{\ell}$	the $\mathcal{O}$ -linear alternating form on $A[\ell]$ defined in Lemma 2.1
$A[\mathfrak{l}]$	the $\mathfrak{l}$ -torsion subgroup of $A$ , as defined in (1) below
$\rho_{\ell}$	the $\ell$ -adic Galois representation with target $\mathrm{GSp}_{2h}(\mathcal{O} \otimes \mathbb{Z}_{\ell})$ , cf. (2) below
$\bar{\rho}_{\ell}, \bar{\rho}_{\mathfrak{l}}$	the Galois representations modulo $\ell$ and $\mathfrak{l}$ as in (3), (4) below
$\lambda$	the multiplier character $\mathrm{GSp}_{2h} \rightarrow \mathbb{G}_m$ , as in Definition 2.3
$\mathrm{GSp}_{2h}(R; U)$	the subset of $\mathrm{GSp}_{2h}(R)$ given by $\lambda^{-1}(U)$ , as in Definition 2.3
$\mathcal{S}_{2h, \mathbb{F}_q}(\lambda_0)$	the split matrices in $\mathrm{GSp}_{2h}(\mathbb{F}_q)$ with multiplier $\lambda_0$ , as in Definition 2.8.

TABLE 2. List of notations

is nondegenerate. If further  $\ell$  is prime to  $d_A$ , then  $e_{\ell}$  also gives a nondegenerate alternating form on  $A[\ell]$  with values in  $\mathbb{F}_{\ell} = \mathbb{Z}/\ell\mathbb{Z}$ . We may also view  $T_{\ell}(A)$  as an  $\mathcal{O} \otimes \mathbb{Z}_{\ell}$ -module, using the action of  $\mathcal{O}$  as endomorphisms of  $A$ .

**Lemma 2.1.** *Assume that  $\ell$  is coprime to  $p$ ,  $d_A$  and  $c_{\mathcal{O}}$ , so that  $\mathcal{O} \otimes \mathbb{Z}_{\ell} = \mathcal{O}_K \otimes \mathbb{Z}_{\ell}$ .*

(1)  *$T_{\ell}(A)$  is a free  $\mathcal{O} \otimes \mathbb{Z}_{\ell}$ -module of rank  $2h$ .*

- (2) *There exists a unique  $\mathcal{O} \otimes \mathbb{Z}_\ell$ -bilinear alternating form  $\psi_\ell : T_\ell(A) \times T_\ell(A) \rightarrow \mathcal{O} \otimes \mathbb{Z}_\ell$  with the following property: for every  $x, y \in T_\ell(A)$ ,  $e_\ell(x, y) = \text{Tr}_{K/\mathbb{Q}}(\psi_\ell(x, y))$ .*

*Proof.* (1) This is [14, Prop. 2.1.1].

- (2) The existence and uniqueness of  $\psi_\ell$  after tensoring with  $\mathbb{Q}_\ell$  is [7, Lemma 1.2.1]. In fact,  $\psi_\ell$  exists at the level of  $\mathcal{O} \otimes \mathbb{Z}_\ell$ -modules by [1, Lemma 3.1].  $\square$

Under the assumptions of Lemma 2.1, we also consider the decomposition of  $\mathcal{O}/\ell\mathcal{O}$  as a product of fields:

$$\mathcal{O}/\ell\mathcal{O} = \prod_{\mathfrak{l}|\ell} \mathcal{O}/\mathfrak{l}\mathcal{O}.$$

Then for each  $\mathfrak{l}|\ell$ , we define the  $\mathfrak{l}$ -torsion subgroup  $A[\mathfrak{l}] \subset A[\ell]$  as

$$(1) \quad A[\mathfrak{l}] = \bigcap_{f \in \mathfrak{l}} \ker(f) = \{x \in A[\ell] : f(x) = 0 \text{ for every } f \in \mathfrak{l}\}.$$

**Lemma 2.2.** *Assume that  $\ell$  is coprime to  $p$ ,  $d_A$  and  $c_{\mathcal{O}}$ . Then we have a direct sum decomposition*

$$A[\ell] = \bigoplus_{\mathfrak{l}|\ell} A[\mathfrak{l}]$$

where for each  $\mathfrak{l}|\ell$ , the summand  $A[\mathfrak{l}]$  is an  $(\mathcal{O}/\mathfrak{l}\mathcal{O})$ -vector space of dimension  $2h$ . This direct sum is orthogonal with respect to  $\psi_\ell$ , and the restriction of  $\psi_\ell$  to each  $A[\mathfrak{l}]$  is nondegenerate.

*Proof.* The decomposition of  $A[\ell]$  as a direct sum is a consequence of Lemma 2.1(1). Let us check that this decomposition is orthogonal with respect to  $\psi_\ell$ . Let  $\mathfrak{l} \neq \mathfrak{l}'$  be prime ideals above  $\ell$ , and fix an element  $f \in \mathfrak{l}$  which is invertible modulo  $\mathfrak{l}'$ . If  $x \in A[\mathfrak{l}]$  and  $y \in A[\mathfrak{l}']$ , then there exists  $y' \in A[\mathfrak{l}']$  such that  $y = f(y')$ . By  $\mathcal{O}$ -linearity of  $\psi_\ell$ , we get

$$\psi_\ell(x, y) = \psi_\ell(x, f(y')) = \psi_\ell(f(x), y') = \psi_\ell(0, y') = 0.$$

Finally, each piece is nondegenerate by [1, Lemma 3.2].  $\square$

We now include the action of the Galois group  $G_F$  in the picture. Let  $\ell$  be coprime to  $p$ ,  $d_A$  and  $c_{\mathcal{O}}$ . By equivariance of the Weil pairing (see for instance [1, Lemma 4.7]), we have for all  $\sigma \in G_F$  and  $x, y \in T_\ell(A)$ :

$$e_\ell(\sigma(x), \sigma(y)) = \chi_\ell(\sigma) e_\ell(x, y).$$

The action of  $\sigma$  on  $A[\ell]$  is also  $\mathcal{O}$ -linear because the elements of  $\mathcal{O}$ , seen as endomorphisms, are defined over  $F$  by assumption. By nondegeneracy of  $\text{Tr}_{K/\mathbb{Q}}$ , we have for all  $x, y \in T_\ell(A)$ :

$$\psi_\ell(\sigma(x), \sigma(y)) = \chi_\ell(\sigma) \psi_\ell(x, y).$$

In other words,  $\sigma$  preserves  $\psi_\ell$  up to multiplication by the scalar  $\chi_\ell(\sigma) \in \mathbb{Z}_\ell^\times$ .

In order to identify the action of  $\sigma$  on  $A[\ell]$  as an element in a standard symplectic group, we choose once and for all a symplectic basis  $(v_1, \dots, v_{2h})$  of  $T_\ell(A)$  as an  $\mathcal{O} \otimes \mathbb{Z}_\ell$ -module. This means that the alternating form  $\psi_\ell$  in this basis takes the standard form

$$J_{2h} = \begin{pmatrix} 0 & I_h \\ -I_h & 0 \end{pmatrix},$$

where  $I_h$  denotes the  $h \times h$  identity matrix. We summarize our notation for the attached symplectic group in the following definition.

**Definition 2.3.** We denote by  $\mathrm{GSp}_{2h}$  the general symplectic group with respect to the standard form  $J_{2h}$ : for any commutative ring  $R$ , we have

$$\mathrm{GSp}_{2h}(R) = \{m \in \mathrm{GL}_{2h}(R) : m^\top J_{2h} m = \lambda(m) J_{2h} \text{ for some } \lambda(m) \in R^\times\}.$$

We call the character  $\lambda : \mathrm{GSp} \rightarrow \mathbb{G}_m$  appearing in this equation the *multiplier*. The kernel of  $\lambda$  is  $\mathrm{Sp}_{2h}$ , the usual symplectic group. If  $U$  is a subset of  $R^\times$ , we also write

$$\mathrm{GSp}_{2h}(R; U) = \{m \in \mathrm{GSp}_{2h}(R) : \lambda(m) \in U\}.$$

Assuming that  $\ell$  is coprime to  $d_A$  and  $c_{\mathcal{O}}$ , the same vectors  $v_1, \dots, v_{2h}$  also form a symplectic basis of  $A[\ell]$  as an  $\mathcal{O}/\ell\mathcal{O}$ -module, and for every prime  $\mathfrak{l}|\ell$  of  $\mathcal{O}$ , a symplectic basis of  $A[\mathfrak{l}]$  as an  $(\mathcal{O}/\mathfrak{l}\mathcal{O})$ -vector space.

Summarizing, we identify the action of  $\sigma \in G_F$  on  $T_\ell(A)$  with an element of the general symplectic group,

$$(2) \quad \rho_\ell(\sigma) \in \mathrm{GSp}_{2h}(\mathcal{O} \otimes \mathbb{Z}_\ell; \mathbb{Z}_\ell^\times) \subset \mathrm{GSp}_{2h}(\mathcal{O} \otimes \mathbb{Z}_\ell)$$

such that

$$\lambda(\rho_\ell(\sigma)) = \chi_\ell(\sigma) \in \mathbb{Z}_\ell^\times \subset (\mathcal{O} \otimes \mathbb{Z}_\ell)^\times.$$

We identify the action of  $\sigma$  on the  $\ell$ -torsion subgroup  $A[\ell]$  with the image of  $\sigma$  under the reduced representation

$$(3) \quad \bar{\rho}_\ell(\sigma) \in \mathrm{GSp}_{2h}(\mathcal{O}/\ell\mathcal{O}; \mathbb{F}_\ell^\times).$$

For each prime  $\mathfrak{l}$  of  $\mathcal{O}$ , we also identify the action of  $\sigma$  on  $A[\mathfrak{l}]$  with an element

$$(4) \quad \bar{\rho}_\mathfrak{l}(\sigma) \in \mathrm{GSp}_{2h}(\mathcal{O}/\mathfrak{l}\mathcal{O}).$$

with the same multiplier  $\chi_\ell(\sigma)$ . We call  $\rho_\ell$  the  $\ell$ -adic Galois representation, and  $\bar{\rho}_\ell$  (resp.  $\bar{\rho}_\mathfrak{l}$ ) the Galois representation modulo  $\ell$  (resp  $\mathfrak{l}$ ), attached to  $A$ . By Lemma 2.1(1) and Lemma 2.2, the decompositions

$$A[\ell] = \bigoplus_{\mathfrak{l}|\ell} A[\mathfrak{l}] \quad \text{and} \quad \mathrm{GSp}_{2h}(\mathcal{O}/\ell\mathcal{O}) = \prod_{\mathfrak{l}|\ell} \mathrm{GSp}_{2h}(\mathcal{O}/\mathfrak{l}\mathcal{O})$$

are compatible in the sense that the following diagram commutes:

$$\begin{array}{ccc} G_F & \xrightarrow{\bar{\rho}_\ell} & \mathrm{GSp}_{2h}(\mathcal{O}/\ell\mathcal{O}; \mathbb{F}_\ell^\times) \longrightarrow \mathrm{GSp}_{2h}(\mathcal{O}/\mathfrak{l}\mathcal{O}). \\ & \searrow & \uparrow \bar{\rho}_\mathfrak{l} \end{array}$$

In particular, if  $\ell$  splits completely in  $\mathcal{O}$ , then  $\bar{\rho}_\ell(G_F)$  is a subgroup of  $\mathrm{GSp}_{2h}(\mathbb{F}_\ell)^d$  consisting of tuples of matrices  $(m_1, \dots, m_d)$  such that  $\lambda(m_1) = \dots = \lambda(m_d)$ . At the other extreme, if  $\ell$  is inert in  $\mathcal{O}$ , then  $\bar{\rho}_\ell(G_F)$  is a subgroup of  $\mathrm{GSp}_{2h}(\mathbb{F}_{\ell^d}; \mathbb{F}_\ell^\times)$ .

The representation  $\bar{\rho}_\mathfrak{l}$  can be seen as the restriction modulo  $\mathfrak{l}$  of the  $\mathfrak{l}$ -adic representation considered in [7, §1.1].



**2.2. Elkies primes for abelian varieties with RM.** Let us restate the definition of Elkies primes given in the introduction. We are mainly interested in finite fields, but for now, our discussion remains valid over any field  $F$ . We keep notation from Table 2, and assume throughout that the prime ideals  $\mathfrak{l}$  we consider are coprime with  $p$ ,  $d_A$ , and  $c_{\mathcal{O}}$ .

**Definition 2.4.** We say that  $\mathfrak{l}$  is *Elkies* for  $A$  if there exists an  $F$ -rational subgroup of  $A[\mathfrak{l}]$  that is maximal isotropic for the Weil pairing  $e_{\ell}$  and stable under  $\mathcal{O}$ . Note that this last condition is automatic when  $N_{F/\mathbb{Q}}(\mathfrak{l}) = \ell$ , as  $\mathcal{O}/\mathfrak{l}\mathcal{O}$  only consists of scalars.

We can equivalently phrase this definition in terms of isotropic subspaces for  $\psi_{\ell}$ .

**Lemma 2.5.** *The prime  $\mathfrak{l}$  is Elkies for  $A$  if and only if there exists a maximal isotropic sub- $(\mathcal{O}/\mathfrak{l}\mathcal{O})$ -vector space of  $A[\mathfrak{l}]$  that is maximal isotropic for  $\psi_{\ell}$  and  $F$ -rational.*

*Proof.* Suppose  $\mathfrak{l}$  is Elkies for  $A$ , i.e. there exists an  $F$ -rational  $\mathbb{F}_{\ell}$ -vector space  $G \subset A[\mathfrak{l}]$  which is maximal isotropic for the Weil pairing and stable under  $\mathcal{O}$ . We may also view  $G \subset A[\mathfrak{l}]$  as an  $F$ -rational sub- $\mathcal{O}/\ell\mathcal{O}$ -vector space of dimension  $h$ . By Lemma 2.1(2), the trace of  $\psi_{\ell}$  vanishes on  $G \times G$ , so  $\psi_{\ell}$  vanishes on  $G \times G$  as well as the trace is nondegenerate.

Conversely, if  $G \subset A[\mathfrak{l}]$  be a maximal isotropic subspace for  $\psi_{\ell}$  in  $A[\mathfrak{l}]$ . Seen as an  $\mathbb{F}_{\ell}$ -vector space,  $G$  is isotropic for the Weil pairing by Lemma 2.1(2), and is maximal for dimension reasons. Therefore,  $\mathfrak{l}$  is Elkies for  $A$ .  $\square$

Definition 2.4 is a suitable generalization of the notion of Elkies primes for elliptic curves [20], abelian surfaces without RM [9, §3.2], and abelian surfaces with RM in the case of split primes [9, §4.1]. Moreover, there is still a close link between Elkies primes and the existence of  $F$ -rational isogenies compatible with the RM structure and the polarization of  $A$ . Let us specify this link in more detail, for motivation only, as it will not be used in the rest of the paper.

First we introduce the following notation. The Néron–Severi group  $\mathrm{NS}(A)$  of  $A$  (the group of line bundles on  $A$  up to algebraic equivalence) is related to the endomorphisms of  $A$ , as follows. The  $\mathbb{Q}$ -algebra  $\mathrm{End}^0(A) = \mathrm{End}_{\overline{F}}(A) \otimes \mathbb{Q}$  is endowed with the Rosati involution  $\dagger$  coming from our choice of polarization on  $A$ . Let  $\mathrm{End}^0(A)^{\dagger}$  denote the sub-vector space of elements invariant under  $\dagger$ , and  $\mathrm{End}(A)^{\dagger} = \mathrm{End}^0(A)^{\dagger} \cap \mathrm{End}(A)$ . There is an isomorphism  $\mathrm{NS}(A) \otimes \mathbb{Q} \simeq \mathrm{End}^0(A)^{\dagger}$ , which depends on the chosen polarization of  $A$  [13, (3) p.190]. Given  $\alpha \in \mathrm{End}(A)^{\dagger}$  and two polarized abelian varieties  $A, B$  with RM by  $\mathcal{O}$ , we say that an isogeny  $\phi : A \rightarrow B$  is an  $\alpha$ -isogeny if the RM structures of  $A$  and  $B$  are compatible via  $\phi$ , and if the pullback of the polarization of  $B$  via  $\phi$  (seen as an element of  $\mathrm{NS}(A)$ ) corresponds to  $\alpha$  via the previous isomorphism. The element  $\alpha$  is then necessarily totally positive [13, (IV) p.209]. Equivalently, we ask that the diagram

$$\begin{array}{ccccc} A & \xrightarrow{\alpha} & A & \longrightarrow & A^{\vee} \\ \downarrow \phi & & & & \uparrow \phi^{\vee} \\ B & \longrightarrow & & & B^{\vee} \end{array}$$

commutes, where  $\vee$  denotes duals and the unlabeled arrows are the polarizations. This implies that  $\ker(\phi)$  is maximal isotropic in  $A[\alpha]$  for its canonical nondegenerate pairing;



conversely, if  $G \subset A[\alpha]$  is a maximal isotropic subspace, then  $A/G$  carries a unique polarization of degree  $d_A$  such that the quotient isogeny  $A \rightarrow A/G$  is an  $\alpha$ -isogeny [13, Cor. p. 231]. Recall that our Elkies primes are prime to  $p$ ,  $d_A$  and  $c_{\mathcal{O}}$ .

**Proposition 2.6.** (1) *The prime  $\mathfrak{l}$  is Elkies if and only if there exists an abelian variety  $B$  over  $F$  with RM by  $\mathcal{O}$  and an  $F$ -rational  $\mathfrak{l}$ -isogeny  $\phi : A \rightarrow B$  in the sense of [5, Def. 4.1].*  
 (2) *Let  $\mathfrak{l}_1, \dots, \mathfrak{l}_r$  be distinct Elkies primes for  $A$ , and let  $k_1, \dots, k_r \geq 0$  be integers such that  $\mathfrak{l}_1^{k_1} \dots \mathfrak{l}_r^{k_r}$  is trivial in the narrow class group of  $\mathcal{O}$ . Let  $\alpha \in \mathcal{O}$  be a totally positive generator of this product. Then there exists an abelian variety  $B$  over  $F$  with RM by  $\mathcal{O}$  and endowed with a polarization of degree  $d_A$ , and an  $F$ -rational  $\alpha$ -isogeny  $\phi : A \rightarrow B$ .*

*Proof of Proposition 2.6.* (1) directly comes from the definition of  $\mathfrak{l}$ -isogenies.

We now prove (2). For  $1 \leq i \leq r$ , let  $K_i \subset A[\mathfrak{l}_i]$  be  $F$ -rational, maximal isotropic, and  $\mathcal{O}$ -stable subgroups as in Definition 2.4. Define now  $K'_i = A[\mathfrak{l}_i^{m_i}]$  if  $k_i = 2m_i$  is even, and  $K'_i = A[\mathfrak{l}_i^{m_i+1}] \cap \eta^{-1}(K_i)$ , where  $\eta \in \mathcal{O}$  is any element whose  $\mathfrak{l}_i$ -adic valuation is exactly  $m_i$ , when  $k_i = 2m_i + 1$  is odd. We can check that  $K'_i$  is independent of the choice of  $\eta$ , and that it is an  $F$ -rational,  $\mathcal{O}$ -stable, maximal isotropic subspace in  $A[\mathfrak{l}_i^{k_i}]$ . By Lemma 2.1 and the Chinese remainder theorem, we have

$$A[\alpha] = \bigoplus_{i=1}^r A[\mathfrak{l}_i^{k_i}].$$

Moreover, the restriction of the pairing on  $A[\alpha]$  to each subgroup  $A[\mathfrak{l}_i^{k_i}]$  is precisely the Weil pairing  $e_{\ell_i} \pmod{\ell_i^{k_i}}$ , where  $\ell_i \in \mathbb{Z}$  denotes the prime below  $\mathfrak{l}_i$ , and the direct sum is orthogonal, as can be seen from the functorial properties of those pairings [13, p. 228]. Therefore  $K = K'_1 \oplus \dots \oplus K'_r$  is maximal isotropic in  $A[\alpha]$ , and is the kernel of the isogeny  $\phi$  we are looking for.  $\square$

**2.3. Elkies primes and the action of Frobenius.** We keep the notation of Table 2, and assume first that  $F = \mathbb{F}_q$  is a finite field. Let  $\pi_A$  denote the Frobenius endomorphism of  $A$ . We continue to assume that  $\mathfrak{l}$  is prime to  $p$ ,  $d_A$  and  $c_{\mathcal{O}}$ . We can also view the Frobenius map as an element  $\pi \in G_F$ .

**Lemma 2.7.** *Let  $A$  be an abelian variety over  $F = \mathbb{F}_q$  with RM by  $\mathcal{O}$ . The prime  $\mathfrak{l}$  is Elkies for  $A$  if and only if  $A[\mathfrak{l}]$  admits a maximal isotropic  $\mathcal{O}$ -stable subspace stable under  $\pi_A$ , if and only if  $\bar{\rho}_{\mathfrak{l}}(\pi) \in \mathrm{GSp}_{2h}(\mathcal{O}/\mathfrak{l}\mathcal{O})$  stabilizes a maximal isotropic stable subspace in  $(\mathcal{O}/\mathfrak{l}\mathcal{O})^{2h}$ .*

*Proof.* This is a restatement of Lemma 2.5, using the fact that a subspace of  $A[\mathfrak{l}]$  is  $\mathbb{F}_q$ -rational if and only if it is stable under  $\pi_A$ .  $\square$

Lemma 2.7 prompts us to make the following definition.

**Definition 2.8.** Let  $k$  be a finite field. We say that a matrix  $m \in \mathrm{GSp}_{2h}(k)$  is *split* if it leaves some maximal isotropic subspace of  $k^{2h}$  stable. We denote by  $\mathcal{S}_{2h,k} \subset \mathrm{GSp}_{2h}(k)$  the

subset of split matrices, and for  $\lambda_0 \in k^\times$ , we write

$$\mathcal{S}_{2h,k}(\lambda_0) := \{m \in \mathcal{S}_{2h,k} : \lambda(m) = \lambda_0\}.$$

We note that  $\mathcal{S}_{2h,k}(\lambda_0)$  is a conjugacy-invariant subset of  $\mathrm{GSp}_{2h}(k)$ .

Since  $\chi_\ell(\pi) = q$ , another restatement of Lemma 2.5 is the following.

**Lemma 2.9.** *The prime  $\mathfrak{l}$  is Elkies for  $A$  if and only if  $\bar{\rho}_\ell(\pi) \in \mathcal{S}_{2h,\mathcal{O}/\mathfrak{l}\mathcal{O}}(q)$ .*

We now switch gears and assume that  $F$  is a number field. We fix a polarized abelian variety  $A$  over  $F$  with RM by  $\mathcal{O}$ . For every prime  $\mathfrak{p}$  of  $F$  with residue field  $F_{\mathfrak{p}}$  of good reduction for  $A$ , the reduction  $A_{\mathfrak{p}}$  of  $A$  modulo  $\mathfrak{p}$  is a polarized abelian variety of dimension  $g$  over  $F_{\mathfrak{p}}$  with RM by  $\mathcal{O}$ . Indeed, the listed properties can all be formulated in terms of isogenies between abelian varieties and their duals, and such isogenies extend uniquely to Néron models at  $\mathfrak{p}$  by [3, §1.4, Prop. 4]. We can characterize Elkies primes for  $A_{\mathfrak{p}}$  in terms of the Galois representations  $\bar{\rho}_\ell$  evaluated at Frobenius elements in  $G_F$ .

**Proposition 2.10.** *Let  $\mathfrak{p}$  be a prime of good reduction for  $A$  above  $p \in \mathbb{Z}$ , and let  $\mathfrak{l}$  be a prime of  $\mathcal{O}$  that is coprime to  $p, d_A$  and  $c_{\mathcal{O}}$ . Then  $\mathfrak{l}$  is Elkies for the reduction  $A_{\mathfrak{p}}$  if and only if  $\bar{\rho}_\ell(\sigma_{\mathfrak{p}}) \in \mathcal{S}_{2h,\mathcal{O}/\mathfrak{l}\mathcal{O}}(N_{F/\mathbb{Q}}(\mathfrak{p}))$ , where  $\sigma_{\mathfrak{p}} \in G_F$  is any Frobenius element at  $\mathfrak{p}$  (unique up to conjugation in  $G_F$ ).*

*Proof.* Denote by  $F'$  the field of definition of  $A[\mathfrak{l}]$ , i.e. the smallest number field such that the representation  $\bar{\rho}_\ell : G_F \rightarrow \mathrm{GSp}_{2h}(\mathcal{O}/\mathfrak{l}\mathcal{O})$  factors through  $\mathrm{Gal}(F'/F)$ . Let  $\mathfrak{P}$  be a prime of  $F'$  above  $\mathfrak{p}$ , and let  $\sigma_{\mathfrak{p}} \in G_F$  be a Frobenius element stabilizing  $\mathfrak{P}$ ; we can consider  $\sigma_{\mathfrak{p}}$  as a (uniquely specified) element of  $\mathrm{Gal}(F'/F)$ . Reduction modulo  $\mathfrak{P}$  defines a bijection  $A[\mathfrak{l}] \rightarrow A_{\mathfrak{p}}[\mathfrak{l}]$  by [18, §1, Lemma 2], so our choice of fixed symplectic basis of  $T_\ell(A)$  also fixes a symplectic basis of  $A_{\mathfrak{p}}[\mathfrak{l}]$  as an  $(\mathcal{O}/\mathfrak{l}\mathcal{O})$ -vector space. By definition,  $\sigma_{\mathfrak{p}}$  induces the Frobenius map of the extension of residue fields  $F'_{\mathfrak{P}}/F_{\mathfrak{p}}$ . Therefore,  $\bar{\rho}_\ell(\sigma_{\mathfrak{p}})$  is precisely the matrix of the Frobenius endomorphism  $\pi_{A_{\mathfrak{p}}}$  in the symplectic basis of  $A_{\mathfrak{p}}[\mathfrak{l}]$  specified above. We now apply Lemma 2.9, using the fact that  $\chi_\ell(\sigma_{\mathfrak{p}}) \equiv N_{F/\mathbb{Q}}(\mathfrak{p}) \pmod{\ell}$ .  $\square$

Proposition 2.10 indicates that the Čebotarev density theorem in  $F'/F$  will provide information on how often a fixed prime  $\mathfrak{l}$  is Elkies for the reduced abelian varieties  $A_{\mathfrak{p}}$  as  $\mathfrak{p}$  grows. In order to apply this theorem, we need to know what the Galois group  $\mathrm{Gal}(F'/F)$  is: this is the purpose of the “large Galois image” hypothesis in Theorem 1.1.

**2.4. Large Galois images.** We keep notation from Table 2; here,  $F$  is a number field. To formalize the definition of large Galois images used in the introduction, we introduce the following notation. If  $n$  is an integer, we write

$$\widehat{\mathbb{Z}}_{\geq n} = \prod_{\ell \text{ prime}, \ell \geq n} \mathbb{Z}_\ell.$$

The  $\ell$ -adic Galois representations  $\rho_\ell : G_F \rightarrow \mathrm{GSp}_{2h}(\mathcal{O} \otimes \mathbb{Z}_\ell)$  can be combined into a global representation

$$\widehat{\rho}_n : G_F \rightarrow \mathrm{GSp}_{2h}(\mathcal{O} \otimes \widehat{\mathbb{Z}}_{\geq n})$$

**Definition 2.11.** We say that  $A$  has *large Galois image* if for some integer  $n \geq 1$ , the image of  $\hat{\rho}_n$  contains  $\mathrm{Sp}_{2h}(\mathcal{O} \otimes \hat{\mathbb{Z}}_{\geq n})$ . Because the cyclotomic character  $\chi_\ell$  is surjective for large enough  $\ell$ , an equivalent condition is that for some large enough  $n$ ,

$$\hat{\rho}_n(G_F) = \mathrm{GSp}_{2h}(\mathcal{O} \otimes \hat{\mathbb{Z}}_{\geq n}; (\hat{\mathbb{Z}}_{\geq n})^\times).$$

In the main results of this paper, Theorems 1.1 and 1.2, we only consider abelian varieties with RM that have large Galois images. In this subsection, we gather some necessary and sufficient conditions for this to happen.

**Proposition 2.12.** *If  $A$  has large Galois image, then  $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathcal{O}$ . In particular  $A$  is simple of type I in Albert's classification.*

*Proof.* Since we assumed the RM embedding  $\mathcal{O} \hookrightarrow \mathrm{End}(A)$  to be primitive, it is sufficient to prove that  $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q} = K$ . Let  $F'$  be a number field over which all endomorphisms of  $A$  are defined. Since  $G_{F'}$  is an open subgroup of finite index in  $G_F$ , there exists a prime  $\ell$  such that  $\rho_\ell(G_{F'})$  still contains  $\mathrm{Sp}_{2h}(\mathcal{O} \otimes \mathbb{Z}_\ell)$ . By Faltings [8],  $\mathrm{End}_{F'}(A) \otimes \mathbb{Q}_\ell$  is the commutant of  $\rho_\ell(G_{F'})$  in  $\mathrm{End}(T_\ell(A) \otimes \mathbb{Q}_\ell)$ .

We claim that the commutant of  $\mathrm{Sp}_{2h}(\mathcal{O} \otimes \mathbb{Z}_\ell)$  in  $\mathrm{End}(T_\ell(A) \otimes \mathbb{Q}_\ell)$  is precisely given by the action of elements of  $\mathcal{O} \otimes \mathbb{Q}_\ell$  on  $T_\ell(A)$ . This would prove that  $\mathrm{End}_{F'}(A) \otimes \mathbb{Q}_\ell$  is contained in  $\mathcal{O} \otimes \mathbb{Q}_\ell$ , hence  $\mathrm{End}_{\overline{\mathbb{Q}}}(A) \otimes \mathbb{Q} = K$  as required.

To show that the claim holds, choose an element  $\gamma \in \mathrm{End}(T_\ell(A) \otimes \mathbb{Q}_\ell)$  commuting with  $\mathrm{Sp}_{2h}(\mathcal{O} \otimes \mathbb{Z}_\ell)$ . In particular, considering scalar matrices in  $\mathrm{Sp}_{2h}$ , we see that  $\gamma$  acts  $\mathcal{O}$ -linearly: we can therefore consider  $\gamma$  as a  $2h \times 2h$  matrix with coefficients in  $\mathcal{O} \otimes \mathbb{Q}_\ell$ . Since  $\mathcal{O} \otimes \mathbb{Q}_\ell$  is a product of fields, it is now sufficient to show that for any field  $k$ , the commutant of  $\mathrm{Sp}_{2h}(k)$  consists of scalar matrices only.

This last fact is well-known (the Lie algebra representation of  $\mathfrak{sp}_{2h}$  on  $\mathfrak{sl}_{2h}$  is irreducible), but for completeness, we include a short proof when  $k$  is infinite. Let  $\gamma$  be a  $2h \times 2h$  matrix over  $k$  commuting with  $\mathrm{Sp}_{2h}(k)$ . Consider any symplectic basis  $(v_1, \dots, v_{2h})$  of  $k^{2h}$ , and let  $x_1, \dots, x_h \in k^\times$  be such that  $x_1, \dots, x_h, x_1^{-1}, \dots, x_h^{-1}$  are distinct. The endomorphism whose matrix in the basis  $(v_1, \dots, v_{2h})$  is  $\mathrm{Diag}(x_1, \dots, x_h, x_1^{-1}, \dots, x_h^{-1})$  is symplectic, so  $v_1, \dots, v_{2h}$  are eigenvectors of  $\gamma$ . As each nonzero element of  $k^{2h}$  is part of some symplectic basis, we deduce that each nonzero vector is an eigenvector for  $\gamma$ , hence  $\gamma$  is a scalar.  $\square$

Conversely, we have the following theorem, after results of Serre [17], Ribet [14], Chi [7] and Banaszak–Gajda–Krasoń [1].

**Theorem 2.13.** *Assume that  $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathcal{O}$  and either:*

- $d = 1$  and  $g \in \{2, 6\}$ , or
- $h = g/d$  is odd.

*Then  $A$  has large Galois image.*

*Proof.* After making a finite extension of  $F$ , which only shrinks the image of the Galois representation, we may assume that the Zariski closure  $\mathcal{G}_\ell$  of  $\rho_\ell(G_F)$  inside  $\mathrm{GSp}_{2h}(\mathbb{Q}_\ell)$  is connected for all  $\ell$  [17, §2.5]. After taking another finite extension of  $F$ , we may also assume that the  $\ell$ -adic Galois representations of  $A$  are all independent in the sense of [17, §2.1].

The goal is then to prove that  $\rho_\ell(G_F)$  contains  $\mathrm{Sp}_{2h}(\mathcal{O} \otimes \mathbb{Z}_\ell)$  for large enough  $\ell$ . The case  $d = 1$  is Serre's open image theorem [17, Thm. 3], while [1, Thm. 6.16] covers the cases where  $h$  is odd (and can be applied as  $\mathcal{G}_\ell$  is connected.)  $\square$

In particular, if  $\mathrm{End}_{\overline{\mathbb{Q}}}(A) = \mathcal{O}$  and  $A$  is either an abelian surface or has odd dimension, then  $A$  has large Galois image.

### 3. COUNTING SPLIT MATRICES IN $\mathrm{GSp}_{2h}(\mathbb{F}_q)$

Our goal here is to provide estimates for the cardinality of  $\mathcal{S}_{2h, \mathbb{F}_q}(\lambda_0)$  for  $\lambda_0 \in \mathbb{F}_q^\times$ . In Section 4, we will use them with  $\mathbb{F}_q = \mathcal{O}/\mathfrak{l}\mathcal{O}$  when applying the Čebotarev density theorem.

Since  $\mathcal{S}_{2h, \mathbb{F}_q}(\lambda_0)$  is conjugacy-invariant, it is a union of conjugacy classes of  $\mathrm{GSp}_{2h}(\mathbb{F}_q)$ , and those have been classified: see for instance [23, Section 6.2]. One key element of the classification is the characteristic polynomial, so we start by studying its link with Elkies primes in §3.1. We use this to count elements in  $\mathcal{S}_{2h, \mathbb{F}_q}(\lambda_0)$ , up to negligible terms, in §3.2.

#### 3.1. Characteristic polynomials and Elkies primes.

**Lemma 3.1.** *Let  $m \in \mathrm{GSp}_{2h}(\mathbb{F}_q)$ . Then  $m$  leaves a maximal isotropic subspace of  $\mathbb{F}_q^{2h}$  stable if and only if  $m$  is conjugate in  $\mathrm{GSp}_{2h}(\mathbb{F}_q)$  to a matrix of the form*

$$\begin{pmatrix} w & \star \\ 0 & \lambda(m)w^{-\top} \end{pmatrix}$$

for some  $w \in \mathrm{GL}_h(\mathbb{F}_q)$ , where  $w^{-\top}$  denotes the inverse transpose of  $w$ .

*Proof.* Assume that  $m$  stabilizes a maximal isotropic subspace  $V \subset \mathbb{F}_q^{2h}$ . Then we can find a symplectic basis of  $\mathbb{F}_q^{2h}$  whose first  $h$  vectors generate  $V$ , i.e. we can find  $Q \in \mathrm{Sp}_{2h}(\mathbb{F}_q)$  such that

$$QmQ^{-1} = \begin{pmatrix} w & \star \\ 0 & w' \end{pmatrix}$$

where  $w, w' \in \mathrm{GL}_h(\mathbb{F}_q)$ . Because  $QmQ^{-1}$  belongs to  $\mathrm{GSp}_{2h}(\mathbb{F}_q)$  and  $\lambda(QmQ^{-1}) = \lambda(m)$ , we must have  $w' = \lambda(m)w^{-\top}$ .

Conversely, assume that  $QmQ^{-1}$  has the specified form for some  $Q \in \mathrm{GSp}_{2h}(\mathbb{F}_q)$ . Let  $V$  be the span of the first  $h$  vectors of the canonical basis of  $\mathbb{F}_q^{2h}$ . Then  $Q(V)$  is a maximal isotropic subspace of  $\mathbb{F}_q^{2h}$  that is stable under  $m$ .  $\square$

**Definition 3.2.** For a monic polynomial  $P \in \mathbb{F}_q[X]$  of degree  $r$  with constant coefficient  $a_0 \in \mathbb{F}_q^\times$  and  $\lambda_0 \in \mathbb{F}_q^\times$ , we define the  $\lambda_0$ -reciprocal polynomial of  $P$  to be the monic polynomial

$$\tilde{P}^{\lambda_0}(X) = \frac{1}{a_0} X^r P\left(\frac{\lambda_0}{X}\right).$$

**Proposition 3.3.** *Let  $m \in \mathrm{GSp}_{2h}(\mathbb{F}_q)$ , let  $\lambda_0 = \lambda(m)$ , and let  $\chi_m$  be the characteristic polynomial of  $m$ . If  $m$  is split, then there exists  $P \in \mathbb{F}_q[X]$  such that  $\chi_m = P\tilde{P}^{\lambda_0}$ .*

*Proof.* We may assume  $m$  is block-triangular as in Lemma 3.1. Let  $P$  denote the characteristic polynomial of  $w$ . Then the characteristic polynomial of  $\lambda(m)w^{-\top}$  is  $\tilde{P}^{\lambda_0}$ .  $\square$

Our next aim is to prove a partial converse to Proposition 3.3 when  $\chi_m$  is squarefree. For a monic polynomial  $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$  of  $\mathbb{F}_q[X]$  of degree  $n$ , we denote by  $c_P$  its companion matrix:

$$c_P = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & \ddots & & \vdots & -a_1 \\ 0 & 1 & \ddots & \vdots & \vdots \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}.$$

**Proposition 3.4.** *Let  $\chi \in \mathbb{F}_q[X]$  be a monic squarefree polynomial of degree  $2h$  of the form  $\chi(X) = P\tilde{P}^{\lambda_0}$  with  $P \in \mathbb{F}_q[X]$  and  $\lambda_0 \in \mathbb{F}_q^\times$ . Factor  $P = P_1 \dots P_r \in \mathbb{F}_q[X]$  into irreducible polynomials in  $\mathbb{F}_q[X]$ . Then all the elements of  $\mathrm{GSp}_{2h}(\mathbb{F}_q)$  whose characteristic polynomial is  $\chi$  and multiplier is  $\lambda_0$  are conjugate to the matrix*

$$\mathrm{Diag} \left( c_{P_1}, \dots, c_{P_r}, \lambda_0 c_{P_1}^{-\top}, \dots, \lambda_0 c_{P_r}^{-\top} \right) = \begin{pmatrix} c_{P_1} & & & & \\ & \ddots & & & \\ & & c_{P_r} & & \\ & & & \lambda_0 c_{P_1}^{-\top} & \\ & & & & \ddots \\ & & & & & \lambda_0 c_{P_r}^{-\top} \end{pmatrix}.$$

In particular, they form a single conjugacy class in  $\mathrm{GSp}_{2h}(\mathbb{F}_q)$ .

*Proof.* Let  $m$  be an element of  $\mathrm{GSp}_{2h}(\mathbb{F}_q)$  whose characteristic polynomial is  $\chi$  and multiplier is  $\lambda_0$ . Assume that  $m$  is the matrix of an endomorphism  $u$  in a symplectic basis  $(e_i)_{1 \leq i \leq 2h}$  of  $\mathbb{F}_q^{2h}$ . For every  $i$ , we write  $V_i = \ker(P_i(u))$  and  $\tilde{V}_i = \ker(\tilde{P}_i^{\lambda_0}(u))$ , noting that  $P_i \neq \tilde{P}_i^{\lambda_0}$  because  $\chi$  is squarefree. By adapting directly Lemma 3.1 of [12] in the case where  $t \in \mathrm{GSp}_{2h}(\mathbb{F}_q)$ , we see that the subspaces  $V_i$  and  $\tilde{V}_i$  are totally isotropic, and that there is an orthogonal decomposition

$$\bigoplus_{i=1}^r (V_i \oplus \tilde{V}_i).$$

For every  $i$ , let  $(\alpha_i, \beta_i)$  be a symplectic basis of  $V_i \oplus \tilde{V}_i$ ; both  $\alpha_i$  and  $\beta_i$  have length  $\deg(P_i)$ . The concatenation  $(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r)$  is a symplectic basis of  $\mathbb{F}_q^{2h}$ . Calling  $Q \in \mathrm{Sp}_{2h}(\mathbb{F}_q)$  the base change matrix from  $(e_i)$  to  $(\alpha_1, \dots, \alpha_r, \beta_1, \dots, \beta_r)$ , we have

$$m = Q \cdot \mathrm{Diag}(m_1, \dots, m_r, m'_1, \dots, m'_r) \cdot Q^{-1}$$

where  $m_i, m'_i \in \mathrm{GL}_{\deg(P_i)}(\mathbb{F}_q)$  for all  $i$ . For every  $i$ , the characteristic polynomial of  $m_i$  is  $P_i$ , so  $m_i$  is conjugate to  $c_{P_i}$  in  $\mathrm{GL}_{\deg(P_i)}(\mathbb{F}_q)$ : there is  $R_i \in \mathrm{GL}_{\deg(P_i)}(\mathbb{F}_q)$  such that

$m_i = R_i c_{P_i} R_i^{-1}$ . We define

$$R = \text{Diag} \left( R_1, \dots, R_r, R_1^{-\top}, \dots, R_r^{-\top} \right) \in \text{Sp}_{2h}(\mathbb{F}_q)$$

and we have

$$m = QR \cdot \text{Diag} \left( c_{P_1}, \dots, c_{P_r}, R_1^{\top} m'_1 R_1^{-\top}, \dots, R_r^{\top} m_r R_r^{-\top} \right) \cdot R^{-1} Q^{-1}.$$

Because

$$\text{Diag} \left( c_{P_1}, \dots, c_{P_r}, R_1^{\top} m'_1 R_1^{-\top}, \dots, R_r^{\top} m_r R_r^{-\top} \right)$$

is in  $\text{GSp}_{2h}(\mathbb{F}_q)$  with multiplier  $\lambda_0$ , we have  $R_i^{\top} m'_i R_i^{-\top} = \lambda_0 c_{P_i}^{-\top}$  for every  $i$ , so  $m$  is conjugate to the block-diagonal matrix specified in the lemma.  $\square$

A direct consequence of Proposition 3.4, noting that the block-diagonal matrix specified there is of the form required by Lemma 3.1, is that the converse to Proposition 3.3 holds when  $\chi_m$  is squarefree.

In fact, following a referee's kind suggestions, we are able to prove the stronger result that the converse to Proposition 3.3 holds in general. This result will not be used in the rest of the paper, so the reader could directly proceed to §3.2, where our counting arguments rely on Proposition 3.4 instead (which does not hold in the non-squarefree case).

**Proposition 3.5.** *Let  $m \in \text{GSp}_{2h}(\mathbb{F}_q)$ , and let  $\lambda_0 = \lambda(m)$ . Then  $m \in \mathcal{S}_{2h, \mathbb{F}_q}(\lambda_0)$  if and only if its characteristic polynomial  $\chi_m$  factors as  $\chi_m = P \tilde{P}^{\lambda_0}$  for some  $P \in \mathbb{F}_q[X]$ .*

We start with a lemma.

**Lemma 3.6.** *Let  $m \in \text{GSp}_{2h}(\mathbb{F}_q)$ , let  $\lambda_0 = \lambda(m)$ , and assume that  $\chi_m$  is of the form  $R^h$  where  $R$  is monic, irreducible of degree 2 and satisfies  $\tilde{R}^{\lambda_0} = R$ . Assume that  $h \geq 2$ . Then there exists a 2-dimensional isotropic subspace  $V \subset \mathbb{F}_q^{2h}$  stable under  $m$ .*

*Proof.* We prove this lemma by induction on  $h$ . In any case, considering the Jordan decomposition of  $m$ , there always exist a 2-dimensional subspace  $V \subset \mathbb{F}_q^{2h}$  that is stable under  $m$ , and on which the characteristic polynomial of  $m$  is  $R$ . Because  $m \in \text{GSp}_{2h}(\mathbb{F}_q)$ , it is easy to see that  $m$  also stabilizes the orthogonal complement  $V^{\perp}$  of  $V$ . We may assume that  $V$  is not isotropic, in other words  $V \cap V^{\perp} = \{0\}$ . Since the symplectic form is nondegenerate, we have  $\dim V + \dim V^{\perp} = 2h$ , which implies that we have an orthogonal decomposition

$$\mathbb{F}_q^{2h} = V \oplus V^{\perp}.$$

If  $h > 2$ , then by induction there exists a 2-dimensional isotropic subspace  $W \subset V^{\perp}$ , so we are done. Assume now  $h = 2$ , and write  $R = (X - \mu)(X - \lambda_0/\mu)$  for some  $\mu \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$ . Extending scalars to  $\mathbb{F}_{q^2}$ , we have a direct sum decomposition

$$V = V_1 \oplus W_1 \quad \text{and} \quad V^{\perp} = V_2 \oplus W_2$$

where the  $V_i$  (resp.  $W_i$ ) for  $i = 1, 2$  are generated by eigenvectors of  $m$  for the eigenvalue  $\mu$  (resp.  $\lambda_0/\mu$ ). Let  $v_1, v_2$  be generators of  $V_1$  and  $V_2$  respectively, and let  $w_1, w_2$  be their

Galois conjugates, which generate  $W_1$  and  $W_2$  respectively. Denoting the alternating form by  $\langle \cdot, \cdot \rangle$  and the generator of  $\text{Gal}(\mathbb{F}_{q^2}/\mathbb{F}_q)$  by  $\sigma$ , we have

$$\sigma(\langle v_1, w_1 \rangle) = \langle w_1, v_1 \rangle = -\langle v_1, w_1 \rangle,$$

and similarly for  $v_2, w_2$ . Hence

$$-\frac{\langle v_1, w_1 \rangle}{\langle v_2, w_2 \rangle} \in \mathbb{F}_q^\times.$$

Let  $\alpha \in \mathbb{F}_{q^2}^\times$  be an element with this specific norm, and define  $W$  as the  $\mathbb{F}_{q^2}$ -span of the vectors  $v_1 + \alpha v_2$  and  $w_1 + \bar{\alpha} w_2$ , where the bar denotes conjugation. Then we directly check that  $W$  is isotropic and descends to  $\mathbb{F}_q$ .  $\square$

For an alternative proof of Lemma 3.6 in the case  $h = 2$  (at least when  $q$  is an odd prime), we can use the classification of conjugacy classes in  $\text{GSp}_4(\mathbb{F}_q)$  from [23, Section 6.2]. In particular, each class whose characteristic polynomial splits as  $P\tilde{P}^{\lambda_0}$  admits a representative of the form

$$m = \begin{pmatrix} w & \star \\ 0 & \lambda(m)w^{-\top} \end{pmatrix}.$$

*Proof of Proposition 3.5.* By assumption,  $\chi_m$  factors over  $\mathbb{F}_q[X]$  as

$$\chi_m = \prod_{i=1}^{n_1} (P_i \tilde{P}_i^{\lambda_0})^{a_i} \cdot \prod_{j=1}^{n_2} Q_j^{2b_j}$$

where the polynomials  $P_i$ ,  $\tilde{P}_i^{\lambda_0}$  and  $Q_j$  are coprime, the exponents  $a_i$  and  $b_j$  are integers, and  $\tilde{Q}_j^{\lambda_0} = Q_j$  for each  $1 \leq j \leq n_2$ . We make the following reductions.

- (1) *We can assume  $n_1 = 0$  and  $n_2 = 1$ .* To see this, define  $V_i$  (resp.  $V'_i$ ) as the primary subspace for  $m$  relative to  $P_i$  (resp.  $\tilde{P}_i^{\lambda_0}$ ) for each  $1 \leq i \leq n_1$ , and define  $W_j$  as the primary subspace for  $m$  relative to  $Q_j$  for each  $1 \leq j \leq n_2$ . As in [12, Lemma 3.1], we have

$$\mathbb{F}_q^{2h} = \bigoplus_{i=1}^{n_1} (V_i \oplus V'_i) \oplus \bigoplus_{j=1}^{n_2} W_j$$

where the two big direct sums are also orthogonal. Moreover, the spaces  $V_i$  and  $V'_i$  are isotropic. If the result holds when  $n_1 = 0$  and  $n_2 = 1$ , then one can construct a maximal isotropic subspace  $W'_j \subset W_j$  stable under  $m$  for each  $j$ . Then, the direct sum

$$\bigoplus_{i=1}^{n_1} V_i \oplus \bigoplus_{j=1}^{n_2} W'_j$$

is maximal isotropic in  $\mathbb{F}_q^{2h}$  and stable under  $m$ .

From now on, we assume  $\chi_m = Q^{2b}$  where  $Q \in \mathbb{F}_q[X]$  is irreducible and satisfies  $\tilde{Q}^{\lambda_0} = Q$ . The map  $\mu \mapsto \lambda_0/\mu$  is an involution of the roots of  $Q$  in an algebraic closure of  $\mathbb{F}_q$ .



- (2) *We can assume that this involution has no fixed points.* Otherwise, since  $Q$  is irreducible, we actually have  $Q = X \pm \mu_0$  where  $\mu_0 \in \mathbb{F}_q^\times$  is a square root of  $\lambda_0$ . Considering the Jordan decomposition of  $m$ , we only need to prove that any unipotent element in  $\mathrm{GSp}_{2h}(\mathbb{F}_q)$  stabilizes a maximal isotropic subspace. This is a well-known fact that is easy to prove by induction on the dimension.

From now on, we assume that the involution  $\mu \mapsto \lambda_0/\mu$  has no fixed points among the roots of  $Q$ . This implies that  $Q$  has even degree  $2r$ , and that there exists an irreducible polynomial  $R \in \mathbb{F}_q[X]$  of degree  $r$  that is the minimal polynomial of  $\mu + \lambda_0/\mu$  over  $\mathbb{F}_q$  for each root  $\mu$  of  $Q$ .

- (3) *We can assume that  $Q$  has degree 2.* Indeed, working over  $\mathbb{F}_{q^r}$  (seen as the splitting field of  $R$ ), we can factor  $Q$  as

$$Q = \prod_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)} \sigma(Q'),$$

where  $Q' = X^2 - (\mu + \lambda_0/\mu)X + \lambda_0 \in \mathbb{F}_{q^r}[X]$  is irreducible of degree 2. Because the polynomials  $\sigma(Q')$  for  $\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$  are coprime, another application of [12, Lemma 3.1] yields an orthogonal decomposition

$$\mathbb{F}_{q^r}^{2h} = \bigoplus_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)} \ker(\sigma(Q')^{2b}(m)).$$

If we are able to construct a maximal isotropic subspace  $V' \subset \ker(\sigma(Q')^{2b}(m))$  defined over  $\mathbb{F}_{q^r}$  and stable under  $m$ , then the subspace

$$V = \bigoplus_{\sigma \in \mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)} \sigma(V')$$

descends to  $\mathbb{F}_q$  and yields a maximal isotropic subspace of  $\mathbb{F}_q^{2h}$  stable under  $m$ .

After these reductions, we can assume that  $h = 2b$  is even, and that  $\chi_m = Q^{2b}$  where  $Q \in \mathbb{F}_q[X]$  is irreducible of degree 2 and satisfies  $\tilde{Q}^{\lambda_0} = Q$ . We construct a maximal isotropic subspace  $V \subset \mathbb{F}_q^{2h}$  stable under  $m$  by induction. By Lemma 3.6, we can construct a 2-dimensional isotropic subspace  $W \subset \mathbb{F}_q^{2h}$  stable under  $m$ . If  $h = 2$ , we are done with  $V = W$ . Otherwise, the quotient space  $W^\perp/W$  carries an induced alternating form which is nondegenerate, and  $m$  induces an endomorphism of that space. By the induction hypothesis on  $h - 2$ , there exists a maximal isotropic subspace  $V' \subset W^\perp/W$  stable under (the endomorphism induced by)  $m$ . We let  $V$  be the preimage of  $V'$  under the quotient map  $W^\perp \rightarrow W^\perp/W$ , which is maximal isotropic for dimension reasons.  $\square$

**3.2. Estimating the size of  $\mathcal{S}_{2h, \mathbb{F}_q}(\lambda_0)$ .** We recall that

$$\# \mathrm{GSp}_{2h}(\mathbb{F}_q) = (q-1) \cdot \# \mathrm{Sp}_{2h}(\mathbb{F}_q) = (q-1) \cdot q^{h^2} \cdot \prod_{i=1}^h (q^{2i} - 1) = q^{2h^2+h+1} + O(q^{2h^2+h}).$$

In the following, we will write  $f(h) = 2h^2 + h + 1$ . As in Theorem 1.1, we set

$$\alpha_h = \sum_{(d_1, \dots, d_r) \in \Sigma_h} \frac{1}{2^r} \cdot \prod_{i=1}^r \frac{1}{d_i} \cdot \prod_{k=1}^h \frac{1}{\#\{j : d_j = k\}!}.$$

The main result in this subsection is the following. Recall that the notation  $O_h$  means that the implied constants are allowed to depend on  $h$ , but not on  $\lambda_0$ .

**Proposition 3.7.** *We have  $\#\mathcal{S}_{2h, \mathbb{F}_q}(\lambda_0) = \alpha_h q^{f(h)-1} + O_h(q^{f(h)-2})$ .*

Let  $\mathcal{S}_{2h, \mathbb{F}_q}^{\text{sqf}}(\lambda_0)$  (resp.  $\mathcal{S}_{2h, \mathbb{F}_q}^{\text{nsqf}}(\lambda_0)$ ) be the set of elements  $m \in \mathcal{S}_{2h, \mathbb{F}_q}(\lambda_0)$  such that  $\chi_m$  is squarefree (resp. not squarefree). We obviously have

$$\mathcal{S}_{2h, \mathbb{F}_q}(\lambda_0) = \mathcal{S}_{2h, \mathbb{F}_q}^{\text{sqf}}(\lambda_0) \sqcup \mathcal{S}_{2h, \mathbb{F}_q}^{\text{nsqf}}(\lambda_0),$$

and we will count elements in each subset separately.

**Lemma 3.8.** *We have  $\#\mathcal{S}_{2h, \mathbb{F}_q}^{\text{nsqf}}(\lambda_0) = O_h(q^{f(h)-2})$ .*

*Proof.* Define  $\text{GSp}_{2h}^{\text{nsqf}}(\mathbb{F}_q; \{\lambda_0\})$  as the set of elements of  $\text{GSp}_{2h}(\mathbb{F}_q)$  of multiplier  $\lambda_0$  and whose characteristic polynomial is not squarefree. We will in fact prove the stronger claim

$$\#\text{GSp}_{2h}^{\text{nsqf}}(\mathbb{F}_q; \{\lambda_0\}) = O_h(q^{f(h)-2}).$$

To this end, we wish to view  $\text{GSp}_{2h}^{\text{nsqf}}(\mathbb{F}_q; \{\lambda_0\})$  as the set of  $\mathbb{F}_q$ -points of a certain variety. Let  $\Delta : \text{GSp}_{2h} \rightarrow \mathbb{A}^1$  be the morphism which maps  $m$  to the discriminant of its characteristic polynomial. The points  $m \in \text{GSp}_{2h}$  for which  $\Delta(m) = 0$  are precisely the elements whose characteristic polynomial is not squarefree. Moreover, the restriction of the morphism  $\lambda : \text{GSp}_{2h} \rightarrow \mathbb{G}_m$  to elements  $m$  for which  $\Delta(m) = 0$  is surjective on geometric points (hence as a map of schemes): indeed, if  $\lambda_1$  is a point of  $\mathbb{G}_m$ , then  $\lambda(\sqrt{\lambda_1} \text{id}_{2h}) = \lambda_1$ . Thus, the set of points of  $\text{GSp}_{2h}$  of multiplier  $\lambda_0$  and whose characteristic polynomial is not squarefree is a subvariety of  $\text{GSp}_{2h}$  of dimension  $\dim(\text{GSp}_{2h}) - 2 = f(h) - 2$ , defined by polynomial equations whose degrees are independent of  $\lambda_0$ .

In [11], Lang and Weil prove that the number of points defined over  $\mathbb{F}_q$  of a variety of dimension  $r$  is  $O(q^r)$ , where the implicit constant only depends on the dimension and the degree of the variety. We conclude that  $\#\text{GSp}_{2h}^{\text{nsqf}}(\mathbb{F}_q; \lambda_0) = O_h(q^{f(h)-2})$ .  $\square$

We now estimate the size of  $\mathcal{S}_{2h, \mathbb{F}_q}^{\text{sqf}}(\lambda_0)$ . For a partition  $(d_1, \dots, d_r)$  of the integer  $h$  such that  $d_1 \leq \dots \leq d_r$ , we denote by  $D_{(d_1, \dots, d_r)}(\lambda_0)$  the set of conjugacy classes contained in  $\text{GSp}_{2h}(\mathbb{F}_q)(\lambda_0)$  whose characteristic polynomial is squarefree and factors as

$$P_1 \dots P_r \cdot \tilde{P}_1^{\lambda_0} \dots \tilde{P}_r^{\lambda_0}$$

where  $P_i \in \mathbb{F}_q[X]$  is irreducible of degree  $d_i$  for every  $i \in \{1, \dots, r\}$ . By Proposition 3.4, the set  $D_{(d_1, \dots, d_r)}(\lambda_0)$  is in one-to-one correspondence with those characteristic polynomials. Moreover,  $\mathcal{S}_{2h, \mathbb{F}_p}^{\text{sqf}}(\lambda_0)$  is the union of all elements of  $D_{(d_1, \dots, d_r)}(\lambda_0)$  as  $(d_1, \dots, d_r)$  runs through partitions of  $h$ .

We first show that the conjugacy classes of  $D_{(d_1, \dots, d_r)}(\lambda_0)$  all have the same size. Recall that for a element  $m \in \mathrm{GSp}_{2h}(\mathbb{F}_q)$ , the number of elements conjugate to  $m$  is

$$\# \mathrm{GSp}_{2h}(\mathbb{F}_q) / \# C(m)$$

where  $C(m)$  is the centralizer of  $m$ .

**Lemma 3.9.** *Let  $P(X) = X^n + a_{n-1}X^{n-1} + \dots + a_0$  be a monic irreducible polynomial of  $\mathbb{F}_q[X]$  of degree  $n$ . The number of elements  $m \in \mathrm{GL}_n(\mathbb{F}_q)$  which commute with the companion matrix  $c_P$  is equal to  $q^n - 1$ .*

*Proof.* Let  $u$  be the endomorphism of  $\mathbb{F}_q^n$  associated to the matrix  $c_P$ . Then, for every nonzero  $x \in \mathbb{F}_q^n$ , the family  $(x, u(x), \dots, u^{n-1}(x))$  is a basis of  $\mathbb{F}_q^n$  because  $P$  is irreducible. An element  $v$  in  $C(u)$  is determined by  $v(x)$  since for every  $i \in \{0, \dots, n-1\}$ , we have  $v(u^i(x)) = u^i(v(x))$ . If  $v(x) \neq 0$ , then  $v$  maps the basis  $(x, u(x), \dots, u^{n-1}(x))$  to the basis  $(v(x), u(v(x)), \dots, u^{n-1}(u(x)))$ , so  $v$  is invertible. Therefore, the elements  $m \in \mathrm{GL}_n(\mathbb{F}_q)$  commuting with  $c_P$  are in one-to-one correspondence with the nonzero elements of  $\mathbb{F}_q^n$ .  $\square$

**Lemma 3.10.** *With the above notation, the cardinality of each element of  $D_{(d_1, \dots, d_r)}(\lambda_0)$  is*

$$\frac{\# \mathrm{GSp}_{2h}(\mathbb{F}_q)}{(q-1) \prod_{i=1}^r (q^{d_i} - 1)}.$$

*Proof.* By Proposition 3.4, a representative of the class is the block-diagonal matrix

$$m = \mathrm{Diag} \left( c_{P_1}, \dots, c_{P_r}, \lambda_0 c_{P_1}^{-\top}, \dots, \lambda_0 c_{P_r}^{-\top} \right).$$

Matrices in  $C(m)$  preserve the invariant subspaces of  $m$ , so they are also block-diagonal of the form

$$\mathrm{Diag} \left( N_1, \dots, N_r, \lambda'_1 N_1^{-\top}, \dots, \lambda'_r N_r^{-\top} \right)$$

where  $N_i$  commutes with  $c_{P_i}$  for every  $i$ . By Lemma 3.9, the number of elements  $N_i$  in  $\mathrm{GL}_{d_i}(\mathbb{F}_q)$  which commute with  $c_{P_i}$  is  $q^{d_i} - 1$ . Hence,

$$\# C(m) = (q-1) \prod_{i=1}^r (q^{d_i} - 1),$$

where the first factor  $(q-1)$  corresponds to the choice of the multiplier  $\lambda'$ .  $\square$

Second, we estimate the size of  $D_{(d_1, \dots, d_r)}(\lambda_0)$ . We denote by  $I_{(d_1, \dots, d_r)}(\lambda_0)$  the set of tuples of irreducible polynomials  $(P_1, \dots, P_r) \in \mathbb{F}_q[X]^r$  such that  $P_i$  is irreducible of degree  $d_i$  for all  $i$  and the product  $P_1 \cdots P_r \cdot \tilde{P}_1^{\lambda_0} \cdots \tilde{P}_r^{\lambda_0}$  is squarefree. In the next lemma, we identify  $D_{(d_1, \dots, d_r)}(\lambda_0)$  with a set of characteristic polynomials.

**Lemma 3.11.** *Consider the map*

$$H : \begin{cases} I_{(d_1, \dots, d_r)}(\lambda_0) & \rightarrow D_{(d_1, \dots, d_r)}(\lambda_0) \\ (P_1, \dots, P_r) & \mapsto P_1 \cdots P_r \cdot \tilde{P}_1^{\lambda_0} \cdots \tilde{P}_r^{\lambda_0}. \end{cases}$$

Then, for every  $\chi \in D_{(d_1, \dots, d_r)}(\lambda_0)$ , we have

$$\#H^{-1}(\chi) = 2^r \cdot \prod_{k=1}^h \#\{j : d_j = k\}!.$$

*Proof.* Fix an element  $(P_1, \dots, P_r) \in H^{-1}(\chi)$ . Then, because  $\chi$  is squarefree, choosing another element of  $H^{-1}(\chi)$  consists in choosing one element of the pair  $\{P_i, \tilde{P}_i^{\lambda_0}\}$  for every  $i \in \{1, \dots, r\}$ , as well as a permutation of the tuple  $(P_{i_{k,1}}, \dots, P_{i_{k,s}})$  where  $P_{i_{k,1}}, \dots, P_{i_{k,s}}$  are the polynomials of degree  $k$ , for every  $k \in \{1, \dots, h\}$ .  $\square$

*Proof of Proposition 3.7.* By Lemma 3.10, the number of elements in  $\mathcal{S}_{2h, \mathbb{F}_q}^{\text{sqf}}(\lambda_0)$  is

$$\#\mathcal{S}_{2h, \mathbb{F}_q}^{\text{sqf}}(\lambda_0) = \sum_{(d_1, \dots, d_r) \in \Sigma_h} \#D_{(d_1, \dots, d_r)}(\lambda_0) \cdot \frac{\#\text{GSp}_{2h}(\mathbb{F}_q)}{(q-1) \prod_{i=1}^r (q^{d_i} - 1)}.$$

For a partition  $(d_1, \dots, d_r)$  of  $h$  with  $d_1 \leq \dots \leq d_r$ , we estimate the size of  $D_{(d_1, \dots, d_r)}(\lambda_0)$  by determining the size of  $I_{(d_1, \dots, d_r)}(\lambda_0)$  and using Lemma 3.11.

The last coefficients of a monic polynomial  $P$  of degree  $d$  such that  $P = \tilde{P}^{\lambda_0}$  are determined by the first coefficients, so the number of irreducible polynomials  $P$  such that  $P = \tilde{P}^{\lambda_0}$  is  $O(q^{d-1})$ . For every  $i$ , one has to choose  $P_i$  such that  $P_i \neq \tilde{P}_i^{\lambda_0}$  and  $P_i \neq P_j, \tilde{P}_j^{\lambda_0}$  for indices  $j < i$ . Then, according to a formula from Gauss for the number of irreducible polynomials of  $\mathbb{F}_q[X]$  of given degree (see [6] for a proof), the number of choices for  $P_i$  is  $\frac{1}{d_i} q^{d_i} + O(q^{d_i-1})$ . Hence

$$\#I_{(d_1, \dots, d_r)}(\lambda_0) = \left( \prod_{i=1}^r \frac{1}{d_i} \right) q^h + O_h(q^{h-1}).$$

Therefore,

$$\#D_{(d_1, \dots, d_r)}(\lambda_0) = \left( \frac{1}{2^r} \cdot \prod_{i=1}^r \frac{1}{d_i} \cdot \prod_{k=1}^h \frac{1}{\#\{j : d_j = k\}!} \right) q^h + O_h(q^{h-1})$$

and consequently

$$\#\mathcal{S}_{2h, \mathbb{F}_q}^{\text{sqf}}(\lambda_0) = \alpha_h q^{f(h)-1} + O(q^{f(h)-2}).$$

Combining this with Lemma 3.8 ends the proof.  $\square$

Even using Proposition 3.5, we note that giving an exact count of  $\mathcal{S}_{2h, \mathbb{F}_q}^{\text{nsqf}}(\lambda_0)$  would be more difficult than in the squarefree case, because a given characteristic polynomial may correspond to several conjugacy classes, contrary to Proposition 3.4. For our purposes, the asymptotic upper bound of Lemma 3.8 is sufficient.

As a final remark, when  $h = 2$  and  $q = \ell$  is an odd prime, we are able to determine the exact cardinality of  $\mathcal{S}_{2h, \mathbb{F}_\ell}$ , through the classification of the conjugacy classes of  $\text{GSp}_4(\mathbb{F}_\ell)$  and the computation of the cardinality of the classes in [4].

**Proposition 3.12.** *We have*

$$\#\mathcal{S}_{4,\mathbb{F}_\ell} = \frac{(3\ell^3 + 7\ell^2 + 7\ell + 11)(\ell + 1)(\ell - 1)^3\ell^4}{8}.$$

*Proof.* Conjugacy classes of  $\mathrm{GSp}_4(\mathbb{F}_\ell)$  have been sorted in different types [23, Section 6.2] according to the factorization of the characteristic polynomial, and the number of classes of each type is known. The order of each center has been computed in [4, Table 1] (beware that the antisymmetric matrix used to define  $\mathrm{GSp}_{2h}$  there is not  $J_{2h}$ , so notation differs from [23]). Thus we can deduce the size of each conjugacy class; we omit the detailed calculation.  $\square$

#### 4. THE DISTRIBUTION OF ELKIES PRIMES

In this section, we prove Theorem 1.2. We introduce the character sum  $U_k$ , similar to the sum  $U$  in [21, eq. (4)], in §4.1. We control the small terms in this sum in §4.2 and we estimate the dominant term in §4.3. Finally, we conclude the proof in §4.4.

**4.1. Setup.** We keep the notation from Theorem 1.1. We may assume that  $P$  and  $L$  are sufficiently large, so that  $A_{\mathfrak{p}}$  is well-defined for every  $\mathfrak{p} \in \mathcal{P}_F(P, 2P)$ , and if  $\mathcal{L} = \mathfrak{l}_1 \cdots \mathfrak{l}_r$  is the product of  $r$  distinct primes of  $\mathcal{P}_K(L, 2L)$ , then

$$G_{\mathcal{L}} := \mathrm{Gal}(F(A[\mathcal{L}])/F)$$

contains  $\mathrm{Sp}_{2h}(\mathcal{O}/\mathcal{LO})$ . (Recall that we always have  $G_{\mathcal{L}} \subset \mathrm{GSp}_{2h}(\mathcal{O}/\mathcal{LO})$ .) This assumption is harmless since we want to establish an asymptotic result.

The Landau prime ideal theorem [10] for the fields  $K$  and  $F$  asserts that

$$\#\mathcal{P}_K(L, 2L) \sim \frac{L}{\log(L)} \quad \text{and} \quad \#\mathcal{P}_F(P, 2P) \sim \frac{P}{\log(P)}.$$

Let

$$\delta_{\mathfrak{p}, \mathfrak{l}} = \begin{cases} (1 - \alpha_h) & \text{if } \mathfrak{l} \text{ is Elkies for } A_{\mathfrak{p}}, \\ -\alpha_h & \text{otherwise} \end{cases}$$

For a product  $\mathfrak{l}_1 \cdots \mathfrak{l}_r$ , we define

$$\delta_{\mathfrak{p}, \mathfrak{l}_1 \cdots \mathfrak{l}_r} = \delta_{\mathfrak{p}, \mathfrak{l}_1} \cdots \delta_{\mathfrak{p}, \mathfrak{l}_r}.$$

We further set

$$\mu = \alpha_h \#\mathcal{P}_K(L, 2L) \quad \text{and} \quad \sigma = \sqrt{\alpha_h(1 - \alpha_h) \#\mathcal{P}_K(L, 2L)}.$$

By definition,

$$\begin{aligned} N_e(\mathfrak{p}, L) - \mu &= (1 - \alpha_h)N_e(\mathfrak{p}, L) - \alpha_h(\#\mathcal{P}_K(L, 2L) - N_e(\mathfrak{p}, L)) \\ &= \sum_{\mathfrak{l} \in \mathcal{P}_K(L, 2L)} \delta_{\mathfrak{p}, \mathfrak{l}}. \end{aligned}$$

For any integer  $k \geq 1$ , the  $k$ -th moment of  $X_{P,L}$  is

$$\begin{aligned} \mathbb{E}(X_{P,L}^k) &= \frac{1}{\#\mathcal{P}_F(P, 2P)} \sum_{\mathfrak{p} \in \mathcal{P}_F(P, 2P)} \left( \frac{N_e(\mathfrak{p}, L) - \mu}{\sigma} \right)^k \\ &= \frac{1}{\#\mathcal{P}_F(P, 2P) \cdot \sigma^k} \sum_{\mathfrak{p} \in \mathcal{P}_F(P, 2P)} \left( \sum_{\mathfrak{l} \in \mathcal{P}_K(L, 2L)} \delta_{\mathfrak{p}, \mathfrak{l}} \right)^k \\ &= \frac{1}{\#\mathcal{P}_F(P, 2P) \cdot \sigma^k} \sum_{\mathfrak{p} \in \mathcal{P}_F(P, 2P)} \sum_{\substack{\mathfrak{l}_1, \dots, \mathfrak{l}_k \\ \in \mathcal{P}_K(L, 2L)}} \delta_{\mathfrak{p}, \mathfrak{l}_1 \cdots \mathfrak{l}_k}. \end{aligned}$$

Hence, we are led to considering the sums

$$U_k := \sum_{\mathfrak{p} \in \mathcal{P}_F(P, 2P)} \sum_{\substack{\mathfrak{l}_1, \dots, \mathfrak{l}_k \\ \in \mathcal{P}_K(L, 2L)}} \delta_{\mathfrak{p}, \mathfrak{l}_1 \cdots \mathfrak{l}_k}.$$

We expect compensations in the sum  $U_k$  when some primes among  $\mathfrak{l}_1, \dots, \mathfrak{l}_k$  appear an odd number of times, and we will sort terms according to the number of distinct primes. In the spirit of the proof of [21, Theorem 1], for  $0 \leq j \leq k$ , let  $\mathcal{Q}_{k,j}$  be the set of tuples  $(\mathfrak{l}_1, \dots, \mathfrak{l}_k)$  of primes in  $\mathcal{P}_K(L, 2L)$  such that  $\mathfrak{l}_1 \cdots \mathfrak{l}_k = \mathfrak{a}^2 \mathfrak{b}$  where  $\mathfrak{b}$  is a squarefree product of  $j$  prime ideals and  $\mathfrak{a}$  is the product of  $\frac{k-j}{2}$  prime ideals ( $\mathcal{Q}_{k,j}$  is empty if  $k-j$  is odd). If  $k = 2\nu$  is even, we also define  $\mathcal{Q}'_{k,0} \subset \mathcal{Q}_{k,0}$  to be the set of tuples  $(\mathfrak{l}_1, \dots, \mathfrak{l}_k)$  such that  $\mathfrak{l}_1 \cdots \mathfrak{l}_k = \mathfrak{a}^2$  where  $\mathfrak{a}$  is a product of  $\nu$  *distinct* prime ideals. We will see that the dominant term comes from the contribution of the terms of  $\mathcal{Q}'_{k,0}$ . We begin by estimating the other terms.

**4.2. Small terms.** We want to prove the following result, which generalizes Lemmas 5 and 6 in [21]. As in Theorem 1.1, the dependency on  $A$  in Landau's notation includes the dependency on  $F$ ,  $\mathcal{O}$  and  $h$ .

**Proposition 4.1.** *Assume GRH. For  $P > 2L$  and a product  $\mathcal{L} = \mathfrak{l}_1 \cdots \mathfrak{l}_r$  of  $r$  distinct primes of  $\mathcal{P}_K(L, 2L)$ , we have*

$$\sum_{\mathfrak{p} \in \mathcal{P}_F(P, 2P)} \delta_{\mathfrak{p}, \mathcal{L}} = O_{A,r} \left( \frac{P}{\log(P)L^r} + L^{f(h)r} P^{1/2} \log(P) \right).$$

The proof of this proposition is based on the Čebotarev density theorem in the Galois group  $G_{\mathcal{L}}$ , which is a subgroup of

$$\mathrm{GSp}_{2h} \left( \prod_{i=1}^r \mathcal{O}/\mathfrak{l}_i \mathcal{O} \right) \cong \prod_{i=1}^r \mathrm{GSp}_{2h}(\mathcal{O}/\mathfrak{l}_i \mathcal{O}).$$

Thus, an element  $m \in G_{\mathcal{L}}$  can be identified with an element

$$(m_1, \dots, m_r) \in \prod_{i=1}^r \mathrm{GSp}_{2h}(\mathcal{O}/\mathfrak{l}_i \mathcal{O})$$

and its multiplier  $\lambda(m)$  with an element

$$(\lambda_1, \dots, \lambda_r) \in \prod_{i=1}^r (\mathcal{O}/\mathfrak{l}_i \mathcal{O})^\times.$$

For  $(\lambda_1, \dots, \lambda_r) \in \lambda(G_{\mathcal{L}})$ , we define

$$G_{\mathcal{L}}(\lambda_1, \dots, \lambda_r) := \{m \in G_{\mathcal{L}} : \lambda(m) = (\lambda_1, \dots, \lambda_r)\}$$

which can be identified with

$$\prod_{i=1}^r \mathrm{GSp}_{2h}(\mathcal{O}/\mathfrak{l}_i \mathcal{O}, \{\lambda_i\}).$$

In particular, by the large Galois image assumption,

$$\#G_{\mathcal{L}}(\lambda_1, \dots, \lambda_r) = \prod_{i=1}^r \#\mathrm{Sp}_{2h}(\mathcal{O}/\mathfrak{l}_i \mathcal{O}) \quad \text{and} \quad \#G_{\mathcal{L}} = \#\lambda(G_{\mathcal{L}}) \cdot \prod_{i=1}^r \#\mathrm{Sp}_{2h}(\mathcal{O}/\mathfrak{l}_i \mathcal{O}).$$

Let us now construct the conjugacy-invariant subsets of  $G_{\mathcal{L}}$  we are interested in. Given a tuple  $\varepsilon = (\varepsilon_1, \dots, \varepsilon_r) \in \{\pm 1\}^r$ , we denote by

$$\mathcal{C}_{\mathfrak{l}_1, \dots, \mathfrak{l}_r}(\varepsilon_1, \dots, \varepsilon_r) \subset G_{\mathcal{L}}$$

the set of elements  $m = (m_1, \dots, m_r)$  of  $G_{\mathcal{L}}$  such that  $m_i \in \mathcal{S}_{2h, \mathcal{O}/\mathfrak{l}_i \mathcal{O}}$  if  $\varepsilon_i = 1$  and  $m_i \notin \mathcal{S}_{2h, \mathcal{O}/\mathfrak{l}_i \mathcal{O}}$  if  $\varepsilon_i = -1$ . These sets  $\mathcal{C}_{\mathfrak{l}_1, \dots, \mathfrak{l}_r}(\varepsilon_1, \dots, \varepsilon_r)$  are indeed stable by conjugation in  $G_{\mathcal{L}}$ , and form a partition of  $G_{\mathcal{L}}$  as  $\varepsilon$  varies.

We also need to determine the size of these sets. For  $\lambda_i \in (\mathcal{O}/\mathfrak{l}_i \mathcal{O})^\times$ , we define

$$\begin{cases} C_{\mathfrak{l}_i}^1(\lambda_i) &= \#\mathcal{S}_{2h, \mathcal{O}/\mathfrak{l}_i \mathcal{O}}(\lambda_i), \\ C_{\mathfrak{l}_i}^{-1}(\lambda_i) &= \#(\mathrm{GSp}_{2h}(\mathcal{O}/\mathfrak{l}_i \mathcal{O}; \{\lambda_i\}) - \mathcal{S}_{2h, \mathcal{O}/\mathfrak{l}_i \mathcal{O}}(\lambda_i)). \end{cases}$$

Considering the preimage of each multiplier  $(\lambda_1, \dots, \lambda_r) \in \lambda(G_{\mathcal{L}})$  separately, we immediately obtain

$$\#\mathcal{C}_{\mathfrak{l}_1, \dots, \mathfrak{l}_r}(\varepsilon_1, \dots, \varepsilon_r) = \sum_{(\lambda_1, \dots, \lambda_r) \in \lambda(G_{\mathcal{L}})} \prod_{i=1}^r C_{\mathfrak{l}_i}^{\varepsilon_i}(\lambda_i).$$

For a given prime  $\mathfrak{p}$  of good reduction for  $A$ , if we set

$$\varepsilon_{\mathfrak{p}, \mathfrak{l}_i} = \begin{cases} 1 & \text{if } \mathfrak{l}_i \text{ is Elkies for } A_{\mathfrak{p}}, \\ -1 & \text{otherwise.} \end{cases}$$

then by Proposition 2.10, the Frobenius element  $\sigma_{\mathfrak{p}}$  at  $\mathfrak{p}$  in  $G_{\mathcal{L}}$  satisfies

$$(\bar{\rho}_{\mathfrak{l}_1}(\sigma_{\mathfrak{p}}), \dots, \bar{\rho}_{\mathfrak{l}_r}(\sigma_{\mathfrak{p}})) \in \mathcal{C}_{\mathfrak{l}_1, \dots, \mathfrak{l}_r}(\varepsilon_{p, \mathfrak{l}_1}, \dots, \varepsilon_{p, \mathfrak{l}_r}).$$



**Lemma 4.2.** *Let  $\mathcal{L} = \mathfrak{l}_1 \cdots \mathfrak{l}_r$  be a product of distinct primes of  $\mathcal{P}_K(L, 2L)$  and  $(\varepsilon_1, \dots, \varepsilon_r)$  be an element of  $\{\pm 1\}^r$ . Then, for  $x > 2L$ , we have*

$$\begin{aligned} \#\{\mathfrak{p} : N(\mathfrak{p}) \leq x \text{ and } \varepsilon_{\mathfrak{p}, \mathfrak{l}_i} = \varepsilon_i \text{ for all } i\} &= \frac{\sum_{(\lambda_1, \dots, \lambda_r) \in \lambda(G_{\mathcal{L}})} \prod_{i=1}^r C_{\mathfrak{l}_i}^{\varepsilon_i}(\lambda_i)}{\#G_{\mathcal{L}}} \frac{x}{\log(x)} \\ &\quad + O_{A,r} \left( N(\mathfrak{l}_1)^{f(h)} \cdots N(\mathfrak{l}_r)^{f(h)} x^{1/2} \log(x) \right). \end{aligned}$$

*Proof.* This follows from an effective version of the Čebotarev density theorem in  $G_{\mathcal{L}}$  [16, §2, Equation (20<sub>R</sub>)] for the set  $\mathcal{C}_{\mathfrak{l}_1, \dots, \mathfrak{l}_r}(\varepsilon_1, \dots, \varepsilon_r)$ . In the left-hand side of (20<sub>R</sub>), an upper bound on  $\#\mathcal{C}_{\mathfrak{l}_1, \dots, \mathfrak{l}_r}(\varepsilon_1, \dots, \varepsilon_r)$  is the order of  $G_{\mathcal{L}}$ , which is  $O_r(N(\mathfrak{l}_1)^{f(h)} \cdots N(\mathfrak{l}_r)^{f(h)})$ . The degree  $n$  of the extension  $F(A[\mathcal{L}])/F$  is equal to the order of  $G_{\mathcal{L}}$ . Since  $x > 2L$ , we have  $\log(n) = O_{r,h}(\log(x))$ . For every  $i \in \{1, \dots, r\}$ , let  $\ell_i$  be the prime number below  $\mathfrak{l}_i$ . The ramified primes in the extension  $F(A[\mathcal{L}])/F$  lie among the divisors of  $\ell_1, \dots, \ell_r$  and the primes of bad reduction of  $A$  (this follows from the Néron-Ogg-Shafarevich criterion), so

$$\log \left( \prod_{i=1}^r \ell_i \right) = O_r(\log(x))$$

under the assumption  $x > 2L$ . □

*Proof of Proposition 4.1.* We have

$$\sum_{\mathfrak{p} \in \mathcal{P}_F(P, 2P)} \delta_{\mathfrak{p}, \mathcal{L}} = \sum_{\substack{(\gamma_1, \dots, \gamma_r) \\ \in \{1 - \alpha_h, -\alpha_h\}^r}} \gamma_1 \cdots \gamma_r \cdot \#\{\mathfrak{p} : N(\mathfrak{p}) \leq x \text{ and } \varepsilon_{\mathfrak{p}, \mathfrak{l}_i} = \varepsilon_i \text{ for all } i\}$$

where  $\varepsilon_i = 1$  if  $\gamma_i = 1 - \alpha_h$  and  $\varepsilon_i = -1$  if  $\gamma_i = -\alpha_h$ . Write

$$S_{(\lambda_1, \dots, \lambda_r)}(\mathfrak{l}_1, \dots, \mathfrak{l}_r) = \sum_{\substack{(\gamma_1, \dots, \gamma_r) \\ \in \{1 - \alpha_h, -\alpha_h\}^r}} \gamma_1 \cdots \gamma_r \cdot \prod_{i=1}^r C_{\mathfrak{l}_i}^{\varepsilon_i}(\lambda_i).$$

By the previous lemma,

$$\begin{aligned} (5) \quad \sum_{\mathfrak{p} \in \mathcal{P}_F(P, 2P)} \delta_{\mathfrak{p}, \mathcal{L}} &= \frac{\sum_{(\lambda_1, \dots, \lambda_r) \in \lambda(G_{\mathcal{L}})} S_{(\lambda_1, \dots, \lambda_r)}(\mathfrak{l}_1, \dots, \mathfrak{l}_r)}{\#G_{\mathcal{L}}} \cdot \frac{P}{\log(P)} \\ &\quad + O_{A,r} \left( N(\mathfrak{l}_1)^{f(h)} \cdots N(\mathfrak{l}_r)^{f(h)} P^{1/2} \log(P) \right). \end{aligned}$$

Fix  $(\lambda_1, \dots, \lambda_r) \in \lambda(G_{\mathcal{L}})$ . Then,

$$S_{(\lambda_1, \dots, \lambda_r)}(\mathfrak{l}_1, \dots, \mathfrak{l}_r) = \prod_{i=1}^r S_{\lambda_i}(\mathfrak{l}_i)$$

where  $S_{\lambda_i}(\mathfrak{l}_i) := (1 - \alpha_h)C_{\mathfrak{l}_i}^1(\lambda_i) - \alpha_h C_{\mathfrak{l}_i}^{-1}(\lambda_i)$ . We have  $S_{\lambda_i}(\mathfrak{l}_i) = O_h(N(\mathfrak{l}_i)^{f(h)-2})$  according to Proposition 3.7. Thus,

$$S_{(\lambda_1, \dots, \lambda_r)}(\mathfrak{l}_1, \dots, \mathfrak{l}_r) = O_{A,r} \left( N(\mathfrak{l}_1)^{f(h)-2} \dots N(\mathfrak{l}_r)^{f(h)-2} \right).$$

In this equation, the implicit constant is independent of  $(\lambda_1, \dots, \lambda_r)$ . Therefore,

$$\sum_{(\lambda_1, \dots, \lambda_r) \in \lambda(G_{\mathcal{L}})} S_{(\lambda_1, \dots, \lambda_r)}(\mathfrak{l}_1, \dots, \mathfrak{l}_r) = O_{A,r} \left( \#\lambda(G_{\mathcal{L}}) \cdot N(\mathfrak{l}_1)^{f(h)-2} \dots N(\mathfrak{l}_r)^{f(h)-2} \right).$$

Consequently,

$$\frac{\sum_{(\lambda_1, \dots, \lambda_r) \in \lambda(G_{\mathcal{L}})} S_{(\lambda_1, \dots, \lambda_r)}(\mathfrak{l}_1, \dots, \mathfrak{l}_r)}{\#G_{\mathcal{L}}} = O_{A,r} \left( \frac{1}{L^r} \right).$$

Inserting this upper bound and writing  $N(\mathfrak{l}_i) \leq 2L$  in (5) ends the proof.  $\square$

**4.3. The dominant term.** When  $k$  is even, the dominant term of  $U_k$  corresponds to the contribution of elements of  $\mathcal{Q}'_{k,0}$ . We begin by estimating the size of this set. For a positive integer  $\nu$ , we recall that  $M_{2\nu}$  is the moment of order  $2\nu$  of the standard Gaussian distribution. Its value is

$$M_{2\nu} = (2\nu - 1) \cdot (2\nu - 3) \dots 3 \cdot 1.$$

**Lemma 4.3.** *Let  $\nu$  be a positive integer. Then,*

$$\begin{aligned} \#\mathcal{Q}'_{2\nu,0} &= M_{2\nu} \frac{L^\nu}{\log(L)^\nu} + O_\nu \left( \frac{L^{\nu-1}}{\log(L)^{\nu-1}} \right), \quad \text{and} \\ \#(\mathcal{Q}_{2\nu,0} - \mathcal{Q}'_{2\nu,0}) &= O_\nu \left( \frac{L^{\nu-1}}{\log(L)^{\nu-1}} \right). \end{aligned}$$

*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:

- for every  $i \in \{1, \dots, n\}$ ,  $A_i \neq \emptyset$ ,
- for every  $i \in \{1, \dots, n\}$ ,  $\#A_i$  is even,
- $\bigsqcup_{i=1}^n A_i = \{1, \dots, 2\nu\}$ .

We equip  $\mathcal{P}_K(L, 2L)$  with an arbitrary total order  $<$ . We also define  $\mathcal{B}_L^n$  to be the set of ordered  $n$ -tuples of distinct prime ideals of  $\mathcal{P}_K(L, 2L)$ . Let  $s = (\mathfrak{l}_1, \dots, \mathfrak{l}_{2\nu})$  be an element of  $\mathcal{Q}_{2\nu,0}$  such that  $\text{lcm}(\mathfrak{l}_1, \dots, \mathfrak{l}_{2\nu})$  has  $n$  distinct prime factors, and  $\mathfrak{l}'_1 < \dots < \mathfrak{l}'_n$  be the primes such that

$$\{\mathfrak{l}_1, \dots, \mathfrak{l}_{2\nu}\} = \{\mathfrak{l}'_1, \dots, \mathfrak{l}'_n\}.$$

Then, we define  $b_s = (\mathfrak{l}'_1, \dots, \mathfrak{l}'_n)$ . For  $j \in \{1, \dots, n\}$ , we set

$$A_j^s = \{i \in \{1, \dots, 2\nu\} : \mathfrak{l}_i = \mathfrak{l}'_j\}$$

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

With this notation, the set  $\mathcal{Q}_{2\nu,0}$  is in one-to-one correspondence with

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

via  $s \mapsto (a_s, b_s)$ , and  $\mathcal{Q}'_{2\nu,0}$  is in one-to-one correspondence with  $\mathcal{A}_\nu \times \mathcal{B}_L^\nu$ .

If  $n$  is fixed, we have

$$\#\mathcal{B}_L^n = \binom{\#\mathcal{P}_K(L, 2L)}{n} \sim \frac{L^n}{n! \log(L)^n}$$

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  $\#(\mathcal{A}_\nu \times \mathcal{B}_L^\nu) \sim M_{2\nu} \frac{L^\nu}{\log(L)^\nu}$ . On the other hand, for  $n \leq \nu - 1$ , we have

$$\#\mathcal{B}_L^n = O\left(\frac{L^{\nu-1}}{\log(L)^{\nu-1}}\right).$$

Since  $\#\mathcal{A}_n$  is a constant independent of  $L$ , we obtain

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

We are able to prove a more precise statement than Proposition 4.1 for elements of  $\mathcal{Q}'_{2\nu,0}$ .

**Proposition 4.4.** *Let  $(l_1, \dots, l_{2\nu}) \in \mathcal{Q}'_{2\nu,0}$ . Then,*

$$\sum_{\mathfrak{p} \in \mathcal{P}_F(P, 2P)} \delta_{\mathfrak{p}, l_1 \dots l_{2\nu}} = (\alpha_h(1 - \alpha_h))^\nu \frac{P}{\log(P)} + O_{A,\nu} \left( \frac{P}{\log(P)L} + L^{f(h)\nu} P^{1/2} \log(P) \right).$$

*Proof.* Assume that  $\{l_1, \dots, l_{2\nu}\} = \{l'_1, \dots, l'_\nu\}$  where  $l'_1 < \dots < l'_\nu$ . Given  $(\gamma_1, \dots, \gamma_\nu)$  in  $\{1 - \alpha_h, -\alpha_h\}^\nu$ , denote by  $\mathcal{D}_{l'_1, \dots, l'_\nu}(\gamma_1, \dots, \gamma_\nu)$  the set of primes  $\mathfrak{p} \in \mathcal{P}_F(P, 2P)$  such that for every  $i$ , the prime  $l'_i$  is Elkies for  $A_{\mathfrak{p}}$  if  $\gamma_i = 1 - \alpha_h$ , and  $l'_i$  is not Elkies for  $A_{\mathfrak{p}}$  if  $\gamma_i = -\alpha_h$ . As in Lemma 4.2, the Čebotarev density theorem yields:

$$\begin{aligned} \#\mathcal{D}_{l'_1, \dots, l'_\nu}(\gamma_1, \dots, \gamma_\nu) &= \frac{\sum_{(\lambda_1, \dots, \lambda_\nu) \in \lambda(G_{l'_1 \dots l'_\nu})} \prod_{i=1}^{\nu} C_{l'_i}^{\varepsilon_i}(\lambda_i)}{\#G_{l'_1 \dots l'_\nu}} \frac{P}{\log(P)} + O_{A,\nu} \left( L^{\nu f(h)} P^{1/2} \log(P) \right) \\ &= (\alpha_h)^{k_1} (1 - \alpha_h)^{\nu - k_1} \frac{P}{\log(P)} + O_{A,\nu} \left( \frac{P}{\log(P)L} + L^{\nu f(h)} P^{1/2} \log(P) \right) \end{aligned}$$

where  $k_1$  is the number of entries  $\gamma_i$  equal to  $1 - \alpha_h$ . Then,

$$\begin{aligned}
\sum_{\mathbf{p} \in \mathcal{P}_F(P, 2P)} \delta_{\mathbf{p}, \mathbf{l}_1 \dots \mathbf{l}_{2\nu}} &= \sum_{\substack{(\gamma_1, \dots, \gamma_\nu) \\ \in \{1 - \alpha_h, -\alpha_h\}^\nu}} (1 - \alpha_h)^{2k_1} (\alpha_h)^{2(\nu - k_1)} \cdot \#D_{\mathbf{l}'_1, \dots, \mathbf{l}'_\nu}(\gamma_1, \dots, \gamma_\nu) \\
&= \sum_{k_1=0}^{\nu} \binom{\nu}{k_1} (1 - \alpha_h)^{2k_1} (\alpha_h)^{2(\nu - k_1)} (\alpha_h)^{k_1} (1 - \alpha_h)^{\nu - k_1} \frac{P}{\log(P)} \\
&\quad + O_{A, \nu} \left( \frac{P}{\log(P) \cdot L} + L^{f(h)\nu} P^{1/2} \log(P) \right) \\
&= (\alpha_h(1 - \alpha_h))^\nu \frac{P}{\log(P)} + O_{A, \nu} \left( \frac{P}{\log(P) \cdot L} + L^{f(h)\nu} P^{1/2} \log(P) \right). \quad \square
\end{aligned}$$

**4.4. Conclusion of the proof.** We go back to estimating the moments of  $X_{P, L}$ . First, assume that  $k$  is odd, and write  $k = 2\nu + 1$ . Then

$$U_k = \sum_{j=0}^{\nu} \sum_{\substack{(\mathbf{l}_1, \dots, \mathbf{l}_{2\nu+1}) \\ \in \mathcal{Q}_{2\nu+1, 2j+1}}} \sum_{\mathbf{p} \in \mathcal{P}_F(P, 2P)} \delta_{\mathbf{p}, \mathbf{l}_1 \dots \mathbf{l}_{2\nu+1}}.$$

For  $j \in \{0, \dots, \nu\}$ , we have

$$\#\mathcal{Q}_{2\nu+1, 2j+1} = O_\nu \left( \frac{L^{\nu+j+1}}{\log(L)^{\nu+j+1}} \right),$$

so by Proposition 4.1,

$$\begin{aligned}
&\sum_{\substack{(\mathbf{l}_1, \dots, \mathbf{l}_{2\nu+1}) \\ \in \mathcal{Q}_{2\nu+1, 2j+1}}} \sum_{\mathbf{p} \in \mathcal{P}_F(P, 2P)} \delta_{\mathbf{p}, \mathbf{l}_1 \dots \mathbf{l}_{2\nu+1}} \\
&= O_{A, \nu} \left( \frac{L^{\nu+j+1}}{\log(L)^{\nu+j+1}} \left( \frac{P}{L^{2j+1} \log(P)} + L^{f(h)(2j+1)} P^{1/2} \log(P) \right) \right).
\end{aligned}$$

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

$$U_k = O_{A, k} \left( \frac{L^\nu P}{\log(L)^{\nu+1} \log(P)} + \frac{L^{(2\nu+1)(f(h)+1)} P^{1/2} \log(P)}{\log(L)^{2\nu+1}} \right).$$

We finally plug this upper bound into the expression for  $\mathbb{E}(X_{P, L}^k)$  in §4.1. We have

$$\sigma^k \cdot \#\mathcal{P}_F(P, 2P) \underset{P, L \rightarrow +\infty}{\sim} (\alpha_h(1 - \alpha_h))^{\nu+1/2} \frac{P}{\log(P)} \cdot \frac{L^{\nu+1/2}}{\log(L)^{\nu+1/2}}.$$

Hence,

$$\begin{aligned}\mathbb{E}(X_{P,L}^k) &= \frac{U_k}{\#\mathcal{P}_F(P, 2P)\sigma^k} \\ &= O_{A,k} \left( \frac{1}{L^{1/2} \log(L)^{1/2}} + \frac{L^{(2\nu+1)(f(h)+1)-\nu-1/2} \log(P)^2}{\log(L)^{\nu+1/2} P^{1/2}} \right),\end{aligned}$$

proving Theorem 1.2 for odd  $k$ .

Second, assume that  $k = 2\nu$  is even. We also write

$$U_{2\nu} = \sum_{j=0}^{\nu} \sum_{(l_1, \dots, l_{2\nu}) \in \mathcal{Q}_{2\nu, 2j}} \sum_{\mathbf{p} \in \mathcal{P}_F(P, 2P)} \delta_{\mathbf{p}, l_1 \dots l_{2\nu}}.$$

For  $j \in \{1, \dots, \nu\}$ , we obtain as above

$$\sum_{(l_1, \dots, l_{2\nu}) \in \mathcal{Q}_{2\nu, 2j}} \sum_{\mathbf{p} \in \mathcal{P}_F(P, 2P)} \delta_{\mathbf{p}, l_1 \dots l_{2\nu}} = O_{A,\nu} \left( \frac{L^{\nu+j}}{\log(L)^{\nu+j}} \left( \frac{P}{L^{2j} \log(P)} + L^{2f(h)j} P^{1/2} \log(P) \right) \right).$$

Now assume that  $j = 0$ . By Lemma 4.3 and Proposition 4.4, the contribution of elements of  $\mathcal{Q}'_{2\nu, 0}$  to  $U_k$  is

$$\begin{aligned}M_{2\nu} \frac{L^\nu}{\log(L)^\nu} (\alpha_h \cdot (1 - \alpha_h))^\nu \frac{P}{\log(P)} \\ + O_{A,\nu} \left( \frac{P}{\log(P)L} + \frac{PL^{\nu-1}}{\log(P) \log(L)^{\nu-1}} + \frac{L^{(f(h)+1)\nu} P^{1/2} \log(P)}{\log(L)^\nu} \right)\end{aligned}$$

while the contribution of elements from  $\mathcal{Q}_{2\nu, 0} - \mathcal{Q}'_{2\nu, 0}$  is

$$O_\nu \left( \frac{P \log(L)^{\nu-1}}{\log(P) \log(L)^{\nu-1}} \right).$$

The dominant terms in the above upper bounds occur for  $j = 0$  and  $j = \nu$ , and we have

$$\begin{aligned}U_{2\nu} &= M_{2\nu} \frac{L^\nu}{\log(L)^\nu} (\alpha_h \cdot (1 - \alpha_h))^\nu \frac{P}{\log(P)} \\ &\quad + O_{A,\nu} \left( \frac{P}{\log(P)} \frac{L^{\nu-1}}{\log(L)^{\nu-1}} + \frac{L^{(2f(h)+2)\nu} P^{1/2} \log(P)}{\log(L)^{2\nu}} \right).\end{aligned}$$

Therefore,

$$\mathbb{E}(X_{P,L}^k) = M_k + O_{A,k} \left( \frac{\log(L)}{L} + \frac{L^{(2f(h)+1)\nu} \log(P)^2}{\log(L)^\nu P^{1/2}} \right).$$

This concludes the proof of Theorem 1.2; Theorem 1.1 is a consequence of this theorem and [2, Theorem 30.2].

## 5. NUMERICAL EXPERIMENTS

At the beginning of this project, we performed numerical experiments with *SageMath* [22] in order to confirm experimentally the estimate of [21, Theorem 1]. All the experiments presented in this section were made with the non-CM elliptic curve  $E$  given by the Weierstrass equation  $y^2 + y = x^3 - x^2$  defined over  $\mathbb{Q}$  (Cremona label 11a3). We began by computing some values of the left-hand side of [21, Theorem 1] for  $\nu = 1$ , namely

$$\frac{1}{\pi(2P) - \pi(P)} \sum_{p \in \mathcal{P}_{\mathbb{Q}}(P, 2P)} \left( N_e(p, L) - \frac{\pi(2L) - \pi(L)}{2} \right)^2,$$

by fixing one of the variable  $L$  or  $P$  and by letting the other one vary. Fig. 1 shows the evolution of the left-hand side for three values of  $L$  (namely 25, 100 and 250) and  $P$  varying between  $10^3$  and  $5 \cdot 10^6$ .

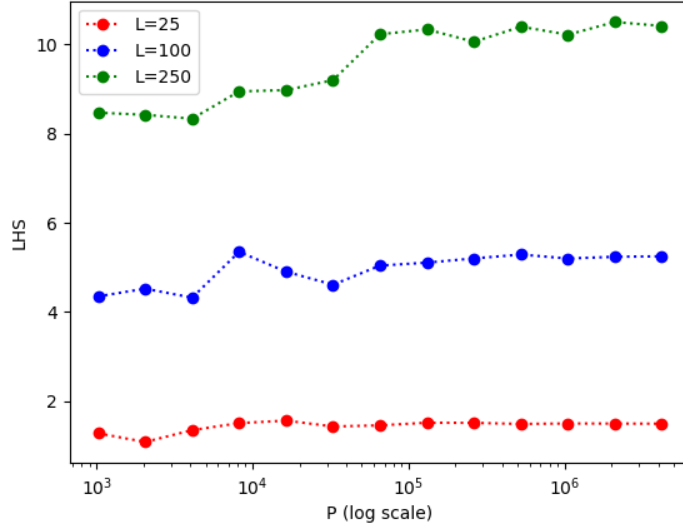


FIGURE 1. Moment of order 2 for  $P \in [10^3, 5 \cdot 10^6]$

This graph suggests that the left-hand side has a finite limit (which depends on  $L$ ) as  $P$  goes to infinity. To go further, we analyzed the distribution of  $N_e(p, L)$ , i.e. the number of primes  $p \in \mathcal{P}_{\mathbb{Q}}(P, 2P)$  such that  $N_e(p, L) = n$  as  $n$  varies between 0 and  $\pi(2L) - \pi(L) + 1$ . We observed that this distribution has a Gaussian shape when  $P$  is much larger than  $L$  as in Fig. 2.

We then tried to predict the mean value and the standard deviation as a function of  $L$  through a naive probabilistic model, relying on the standard hypothesis that roughly 50% of prime numbers are Elkies. (Indeed, for a given elliptic curve  $E$  defined  $\mathbb{F}_q$  of trace of Frobenius  $t$ , the prime  $\ell$  is Elkies if and only if  $t^2 - 4q$  is a square modulo  $\ell$ , and half

of the elements of  $\mathbb{F}_\ell^\times$  are squares; we neglect the probability that  $t^2 - 4q$  is 0 modulo  $\ell$ .) In other words, for every  $p \in \mathcal{P}_\mathbb{Q}(P, 2P)$ , a prime  $\ell \in [L, 2L]$  has a probability  $1/2$  to be Elkies for the reduced curve  $E_p$ , and those events are independent. Then, the number of Elkies primes for  $E_p$  in  $[L, 2L]$  follows a binomial distribution  $\mathcal{B}(\pi(2L) - \pi(L), 1/2)$ , whose expected value  $\mu$  and deviation  $\sigma$  are

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

Therefore, when  $P$  is much larger than  $L$ , we expect the actual distribution of Elkies primes to look like a Gaussian function with those parameters. In Fig. 2, we plot the distribution for  $L = 250$  and  $P = 10^7$  in blue and the associated Gaussian red; we see that the naive model fits very well with the reality.

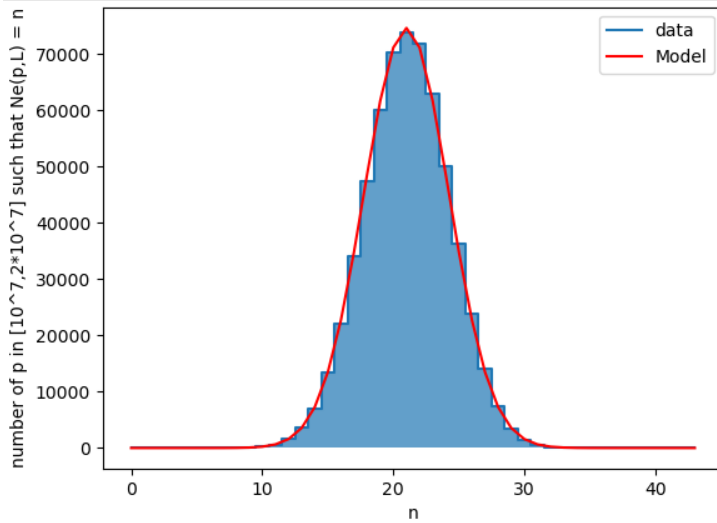


FIGURE 2. Distribution with  $L = 250$  and  $P = 10^7$

The predicted value of the left-hand side of [21, Theorem 1] for  $\nu = 1$  is the moment of order 2 of the binomial distribution  $\mathcal{B}(\pi(2L) - \pi(L), 1/2)$ , which is  $(\pi(2L) - \pi(L))/4$ . In Fig. 3, we fix  $P = 10^5$  and we let  $L$  vary in  $[20, 500]$ . We plot the evolution of the left-hand side for in blue and the predicted value in red. We see that the model is accurate for small values of  $L$ , but when  $L$  is larger than  $\sqrt{P}$ , a gap between the model and the reality starts appearing.

All in all, these numerical experiments gave us the idea that the distribution of Elkies primes converges to a Gaussian function when  $P$  and  $L$  go to infinity with  $P$  growing quickly compared with  $L$ . The naive model allowed us to predict the parameters of this Gaussian function in the setting of elliptic curves, setting us on the path towards Theorem 1.1.



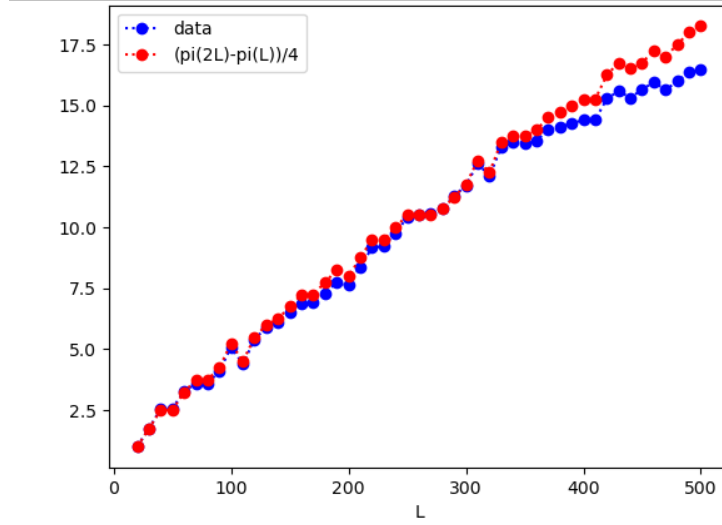


FIGURE 3. Evolution of the moment of order 2, with  $P = 10^5$  and  $L \in [20, 500]$

#### REFERENCES

- [1] G. Banaszak, W. Gajda, and P. Krasoń. “On the image of  $\ell$ -adic Galois representations for abelian varieties of type I and II”. In: *A Collection of manuscripts written in honour of John H. Coates on the occasion of his sixtieth birthday*. Doc. Math. EMS Press, 2006, pp. 35–75.
- [2] P. Billingsley. “Probability and Measure.” Third edition. John Wiley & Sons, 1995.
- [3] S. Bosch, W. Lütkebohmert, and M. Raynaud. “Néron Models”. Springer, 1990.
- [4] J. Breeding II. “Irreducible characters of  $\mathrm{GSp}(4, q)$  and dimensions of spaces of fixed vectors”. *Ramanujan J.* 36 (2011).
- [5] E. H. Brooks, D. Jetchev, and B. Wesolowski. “Isogeny graphs of ordinary abelian varieties”. *Res. Number Theory* 3 (2017), p. 28.
- [6] S. K. Chebolu and J. Miná. “Counting irreducible polynomials over finite fields using the inclusion-exclusion principle”. *Math. Mag.* 84.5 (2011), pp. 369–371.
- [7] W. Chi. “ $\ell$ -adic and  $\lambda$ -adic representations associated to abelian varieties defined over number fields”. *Amer. J. Math.* 114.2 (1992), pp. 315–353.
- [8] G. Faltings. “Endlichkeitssätze für abelsche Varietäten über Zahlkörpern”. *Invent. Math.* 73.3 (1983), pp. 349–366.
- [9] J. Kieffer. “Counting points on abelian surfaces over finite fields with Elkies’s method”. 2022.
- [10] E. Landau. “Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes.” *Math. Ann.* 56 (1903), pp. 645–670.
- [11] S. Lang and A. Weil. “Number of points of varieties in finite fields.” *Amer. J. of Math.* 76.4 (1954), pp. 819–827.
- [12] J. Milnor. “On isometries of inner product spaces”. *Invent. Math.* 8 (1969), pp. 83–97.
- [13] D. Mumford. “Abelian varieties.” Published for the Tata Institute of Fundamental Research, Bombay, by Oxford University Press, 1970.

- [14] K. A. Ribet. “Galois action on division points of abelian varieties with real multiplication”. *Amer. J. Math.* 98.3 (1976), pp. 751–804.
- [15] R. Schoof. “Counting points on elliptic curves over finite fields”. *J. Théor. Nombres Bordeaux* 7.1 (1995), pp. 219–254.
- [16] J.-P. Serre. “Quelques applications du théorème de densité de Chebotarev”. *Pub. Math. –IHES* 54 (1981), pp. 123–201.
- [17] J.-P. Serre. “Résumé des cours au Collège de France.” *Annuaire du Collège de France* (1985–1986), pp. 95–100.
- [18] J.-P. Serre and J. Tate. “Good reduction of abelian varieties”. *Ann. Math.* 88.3 (1968), pp. 492–517.
- [19] I. E. Shparlinski. “On the product of small Elkies primes”. *Proc. Amer. Math. Soc.* 143.4 (2015), pp. 1441–1448.
- [20] I. E. Shparlinski and A. V. Sutherland. “On the distribution of Atkin and Elkies primes”. *Found. Comput. Math.* 14 (2014), pp. 285–297.
- [21] I. E. Shparlinski and A. V. Sutherland. “On the distribution of Atkin and Elkies primes for reductions of elliptic curves on average”. *LMS J. Comput. Math.* 18.1 (2015), pp. 308–322.
- [22] The Sage Developers. *SageMath, the Sage Mathematics Software System*. Version 10.3. 2024.
- [23] C. L. Williams. “Conjugacy classes of matrix groups over local rings and an application to the enumeration of abelian varieties.” PhD thesis. Colorado State University, 2012.

(Alexandre Benoist) UNIVERSITY OF LUXEMBOURG, DEPARTMENT OF MATHEMATICS.  
 ORCID: 0009-0002-3942-0961  
*Email address:* alexandre.benoist@uni.lu

(Jean Kieffer) UNIVERSITÉ DE LORRAINE, CNRS, INRIA, LORIA  
 ORCID: 0000-0002-9953-0137  
*Email address:* jean.kieffer@loria.fr