ETH Zürich

Bachelor Thesis

The Probability that the Number of Rational Points on an Elliptic Curve or a Genus 2 Jacobian is Prime

By
Ole Ossen

Supervised by
Prof. Richard Pink

September, 2017

Contents

Introduction

In public key cryptography, one considers the following situation: Two parties A and B wish to privately exchange information, but can only use a channel monitored by an adversary for communication. Here is one possible solution to A and B's problem: They agree on a group G and an element $g \in G$ of finite order. This information is publicly known. Next, A randomly chooses an integer a and B randomly chooses an integer b; then they compute g^a respectively g^b. Now A sends g^a to B and B sends g^b to A. Then both A and B have access to the *shared secret* $(g^b)^a = (g^a)^b$.

The adversary monitoring the channel can find out this secret if she can solve the following problem:

The discrete logarithm problem. *Let G be a group and let $g \in G$ be an element of finite order n. Given a power h of g, the* discrete logarithm problem *is to find an exponent $x \in \mathbb{Z}/(n)$ with $g^x = h$.*

For this reason, one is interested in groups for which no efficient way of solving the discrete logarithm problem is known. One such class of groups is the groups of rational points on elliptic curves over finite fields and, more generally, the groups of rational points on the Jacobian varieties of hyperelliptic curves over finite fields.

By the *Pohlig-Hellman Algorithm* ([HPS08, Theorem 2.32]), solving the discrete logarithm problem for an element g of order n is not significantly more difficult than solving it for an element of order the largest power of a prime number dividing n. Therefore, one is interested in knowing when groups suitable for public key cryptography have elements of large prime order.

In their paper [GM00], Galbraith and McKee derive a conjecture ([GM00, Conjecture A]) on the probability that the number of rational points on an elliptic curve over a finite field is prime. Castryck, Folsom, Hubrechts, and Sutherland rederive this conjecture ([CFHS12, Conjecture 1]), which appears as Conjecture 2.5 below. They then go on to generalize it to Jacobian varieties of hyperelliptic curves of genus 2 ([CFHS12, Conjectures 2 and 3], the first of which appears below as Conjecture 3.10) and study several related questions.

This thesis is intended as an accessible discussion of the methods employed by the authors of [CFHS12] to arrive at these conjectures. In Section 2, we treat the case of elliptic curves in detail; in Section 3, we consider the case of genus 2 hyperelliptic curves.

Prerequisite for reading this thesis is a basic understanding of algebraic geometry. Further necessary theory is summarized in Section 1. The most important results here are Propositions 1.2 and 1.4 and Theorems 1.5 (for Section 2) and 1.6 (for Section 3). To make reading Section 2 on its own easier, separate references are given for the special case of elliptic curves when possible.

I would like to thank my supervisor Professor Pink, whose comments on earlier versions of this thesis have been invaluable.

Notations and Conventions

Throughout, we will let p denote a prime number greater than 3.

For any prime number ℓ, we denote the field with ℓ elements by $\mathbb{F}_\ell$, its algebraic closure by $\overline{\mathbb{F}_\ell}$, and the Galois group of the field extension $\overline{\mathbb{F}_\ell}/\mathbb{F}_\ell$ by $\mathrm{Gal}(\overline{\mathbb{F}_\ell}/\mathbb{F}_\ell)$. We write μ_ℓ for the group of ℓ-th roots of unity of $\overline{\mathbb{F}_\ell}$.

We denote affine n-space over a field K by $\mathbb{A}^n_K$ and projective n-space over K by $\mathbb{P}^n_K$. We write $V(f_1, \ldots, f_k)$ for the — not necessarily irreducible — affine algebraic variety defined by polynomials $f_1, \ldots, f_k \in K[X_1, \ldots, X_n]$, and likewise write $V(f_1, \ldots, f_k)$ for the projective variety defined by homogenous polynomials $f_1, \ldots, f_k \in K[X_0, \ldots, X_n]$. In the case $n = 2$, we denote the indeterminates by X, Y, Z instead of X_0, X_1, X_2.

If $V \subset \mathbb{P}^n_K$ is an algebraic variety, we denote its base change with respect to the algebraic closure $\overline{K}$ by $\overline{V}$. We denote the K-valued points of V by $V(K)$ and the $\overline{K}$-valued points of $\overline{V}$ by $\overline{V}(\overline{K})$.

Given a curve $C \subset \mathbb{P}^n_K$, we denote its function field by $K(C)$ and its local ring at a point C by $K[C]_P$.

We write $R^\times$ for the group of units of a ring R.

The boldface letter $\mathbf{P}$ denotes probabilities.

1 Preliminaries

1.1 Curves and their Jacobian Varieties

Let p be a prime number greater than 3. For an integer $k \geqslant 3$, let $\mathcal{H}_k^p$ denote the set of squarefree degree k polynomials with coefficients in $\mathbb{F}_p$.

Consider a polynomial $f = \sum_{i=0}^{3} a_i X^i$ in $\mathcal{H}_3^p$. The projective closure E of the affine variety $V(Y^2 - f) \subset \mathbb{A}^2_{\mathbb{F}_p}$ is called an *elliptic curve* over $\mathbb{F}_p$: Homogenize f to obtain a homogenous polynomial

$$f' = a_3X^3 + a_2X^2Z + a_1XZ^2 + a_0Z^3$$

and set $E := V(Y^2Z - f') \subset \mathbb{P}^2_{\mathbb{F}_p}$. The projective variety E is a one-dimensional irreducible projective variety. That f is squarefree implies that E is smooth. In Section 2, we will study the number $\#E(\mathbb{F}_p)$ of *rational points* on E or $\mathbb{F}_p$*-valued points* of E, that is the number of morphisms $\operatorname{Spec} \mathbb{F}_p \to E$. The original equation $Y^2 = f$ is called a *Weierstrass equation* for E.

Let $g \geqslant 2$ be an integer. For a polynomial f in $\mathcal{H}_{2g+1}^p$ or $\mathcal{H}_{2g+2}^p$, the projective closure of $V(Y^2 - f) \subset \mathbb{A}^2_{\mathbb{F}_p}$ is no longer smooth. However, it is possible to find a smooth projective curve containing the affine part $V(Y^2 - f)$ — see for example [Har77, Section I.6]. Such a projective curve H is called a *hyperelliptic curve* over $\mathbb{F}_p$. Like for elliptic curves, the original equation $Y^2 = f$ is called a *Weierstrass equation for* H.

We now introduce the notion of *divisor*, following Silverman's book [Sil09]. Let $C \subset \mathbb{P}^n_{\mathbb{F}_p}$ be a smooth curve and consider the base change $\overline{C}$ with respect to the algebraic closure $\overline{\mathbb{F}_p}$; for example, C might be a hyperelliptic curve over $\mathbb{F}_p$. A *divisor* on $\overline{C}$ is an element of the *divisor group* $\operatorname{Div}(\overline{C})$ of $\overline{C}$, which is the free abelian group generated by the closed points P of $\overline{C}$. That is, divisors are finite linear combinations

$$\sum_P n_P(P), \qquad n_P \in \mathbb{Z}.$$

The *degree* of a divisor $D = \sum_P n_P(P)$ is

$$\deg(D) = \sum_P n_P \in \mathbb{Z}.$$

Denote the subgroup of $\operatorname{Div}(\overline{C})$ consisting of all degree zero divisors by $\operatorname{Div}^0(\overline{C})$.

Note that for every closed point P of $\overline{C}$, the local ring $\overline{\mathbb{F}_p}[\overline{C}]_P$ is a regular local noetherian integral domain, and therefore is a discrete valuation ring (for example by [AM69, Proposition 9.2]). Let $\operatorname{ord}_P : \overline{\mathbb{F}_p}(\overline{C}) \to \mathbb{Z} \cup \{\infty\}$ be the corresponding normalized valuation. If a function $f \in \overline{\mathbb{F}_p}(\overline{C})^\times$ satisfies $\operatorname{ord}_P(f) > 0$, it is said to have a *zero* of order $\operatorname{ord}_P(f)$ at P. If f satisfies $\operatorname{ord}_P(f) < 0$, it is said to have a *pole* of order $-\operatorname{ord}_P(f)$ at P.

It turns out that every rational function f in $\overline{\mathbb{F}_p}(\overline{C})^\times$ only has finitely many zeros and only finitely many poles; see for example [Har77, Lemma I.6.5] for a proof of this. Thus, we can associate to f a divisor

$$\operatorname{div}(f) = \sum_P \operatorname{ord}_P(f)(P).$$

The divisors of this form are the *principal divisors*. By [Har77, Corollary II.6.10], every principal divisor has degree zero. We can therefore take the quotient

$$\operatorname{Pic}^0(\overline{C}) = \operatorname{Div}^0(\overline{C}) \Big/ \{\operatorname{div}(f) \mid f \in \overline{\mathbb{F}_p}(\overline{C})^\times\},$$

which is called the *Picard group* of $\overline{C}$.

Consider the group action of $\operatorname{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ on $\operatorname{Div}^0(\overline{C})$ given by

$$\gamma\left(\sum_P n_p(P)\right) = \sum_P n_P(\gamma(P)) \qquad \text{for } \gamma \in \operatorname{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p).$$

Since this action maps principal divisors to principal divisors, it induces an action of $\operatorname{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ on $\operatorname{Pic}^0(\overline{C})$. Denote by $\operatorname{Pic}^0_{\mathbb{F}_p}(\overline{C})$ the subgroup of $\operatorname{Pic}^0(C)$ that is fixed by this action. It is the order of this group that we will study in Section 3.

To view $\operatorname{Pic}^0_{\mathbb{F}_p}(\overline{C})$ from a different angle, we will need the notion of *abelian variety* — see Chapter 4 of [CFA$^+$06] for a more thorough discussion tailored to the case of elliptic and hyperelliptic curves. The following definition is taken from [Sta17, Tag 0BF9]:

An *abelian variety* over a field K is a geometrically integral proper variety A over K together with three morphisms: A *multiplication* $m : A \times_K A \to A$, an *inversion* $i : A \to A$, and a morphism $e : \operatorname{Spec} K \to A$ such that the K-valued points $A(K)$ form an abelian group with composition given by m, inversion given by i, and the neutral element given by e.

All elliptic curves over $\mathbb{F}_p$ are abelian varieties over $\mathbb{F}_p$ (see [Sil09, Section III.2] for an introduction).

For any abelian variety A over $\mathbb{F}_p$, the base change $\overline{A}$ with respect to the algebraic closure $\overline{\mathbb{F}_p}$ is an abelian variety over $\overline{\mathbb{F}_p}$.

Theorem 1.1. *Let H be a hyperelliptic curve of genus g over $\mathbb{F}_p$. Then there exists an abelian variety J of dimension g such that there are isomorphisms of groups*

$$J(\mathbb{F}_p) \cong \operatorname{Pic}^0_{\mathbb{F}_p}(\overline{H}) \qquad \textit{and} \qquad \overline{J}(\overline{\mathbb{F}_p}) \cong \operatorname{Pic}^0(\overline{H}).$$

Proof. See [CFA$^+$06, Section 4.4.4]. ■

This abelian variety J is called the *Jacobian variety* of H.

1.2 Isogenies

We will only consider the following special case, following [CFA+06, Section 4.3.4]: Let A be an elliptic curve over $\mathbb{F}_p$ or the Jacobian variety of a hyperelliptic curve over $\mathbb{F}_p$, and consider the base change $\overline{A}$ of A with respect to the algebraic closure $\overline{\mathbb{F}_p}$. Then an *isogeny* from $\overline{A}$ to $\overline{A}$ is a surjective morphism $\varphi : \overline{A} \to \overline{A}$ that is a group homomorphism.

For any integer $N \geqslant 0$, there is an isogeny

$$[N] : \overline{A} \to \overline{A}, \qquad P \mapsto P + \ldots + P \ (N \text{ times}).$$

Its kernel, denoted $\overline{A}[N]$, is called the *N-torsion subgroup* of $\overline{A}$. Similarly, we can consider the N-torsion subgroup $\overline{A}(\overline{\mathbb{F}_p})[N]$ of the $\overline{\mathbb{F}_p}$-valued points of $\overline{A}$.

Proposition 1.2. *For any prime number ℓ different from p,*

$$\overline{A}(\overline{\mathbb{F}_p})[\ell] \cong (\mathbb{Z}/(\ell))^{2\dim(A)}.$$

Furthermore,

$$\overline{A}(\overline{\mathbb{F}_p})[p] \cong (\mathbb{Z}/(p))^k$$

for some $0 \leqslant k \leqslant \dim(A)$.

Proof. For the case that A is an elliptic curve, see [Sil09, Corollary III.6.4]. For the case that A is the Jacobian variety of a hyperelliptic curve, see [Mum70, Section II.6]. ■

If A is an elliptic curve, then $\overline{A}(\overline{\mathbb{F}_p})[\ell] \cong (\mathbb{Z}/(\ell))^2$; if A is the Jacobian variety of a genus g hyperelliptic curve, then $\overline{A}(\overline{\mathbb{F}_p})[\ell] \cong (\mathbb{Z}/(\ell))^{2g}$.

Another important isogeny is the *Frobenius endomorphism* $\mathrm{Frob} : \overline{A} \to \overline{A}$. On an affine open subscheme

$$\operatorname{Spec} \overline{\mathbb{F}_p}[X_1, \ldots, X_n]/(f_1, \ldots, f_k)$$

of $\overline{A}$, it is given by the ring homomorphism with

$$X_1 \mapsto X_1^p, \ \ldots \ , X_k \mapsto X_k^p$$

that is the identity on $\overline{\mathbb{F}_p}$.

For any isogeny $\varphi : \overline{A} \to \overline{A}$, there is a corresponding injection of function fields

$$\varphi^* : \overline{\mathbb{F}_p}(\overline{A}) \to \overline{\mathbb{F}_p}(\overline{A}).$$

This field extension consists of two finitely generated field extensions of $\overline{\mathbb{F}_p}$ of the same transcendence degree $\dim(A)$. It is therefore a finite field extension whose degree is called the *degree of* φ and denoted by $\deg(\varphi)$.

The degrees of the two isogenies $[N]$ and Frob discussed above are $N^{2\dim(A)}$ and $p^{\dim(A)}$, respectively. We will only use this in the case that A is an elliptic curve, and thus $\dim(A) = 1$.

In this case, proofs can be found in [Sil09, Theorem III.6.2] respectively [Sil09, Proposition II.2.11].

Let $\varphi : \overline{A} \to \overline{A}$ be an isogeny. A key tool used throughout this thesis is to consider the linear transformation φ_ℓ induced by φ on the ℓ-torsion subgroup $\overline{A}(\overline{\mathbb{F}_p})[\ell]$ for prime numbers ℓ different from p. Among its invariants are the trace $\operatorname{tr}(\varphi_\ell) \in \mathbb{F}_\ell$, the determinant $\det(\varphi_\ell) \in \mathbb{F}_\ell$, and the characteristic polynomial $\operatorname{char}_{\varphi_\ell} \in \mathbb{F}_\ell[X]$. The next propositions describe connections between properties of these invariants and properties of φ and A we are interested in.

Proposition 1.3. *We have*

$$\det(\varphi_\ell) = (\deg(\varphi) \bmod \ell).$$

Proof. For the case of elliptic curves, see [Sil09, Proposition III.8.6]. For the general case, see [Mum70, Section 19, Theorem 4]. ■

Proposition 1.4. *Let ℓ be a prime number. Then ℓ divides the number of rational points on A if and only if* 1 *is an eigenvalue of* Frob_ℓ.

Proof. The key fact here is that the rational points on A are in 1-to-1-correspondence with the $\overline{\mathbb{F}_p}$-valued points of $\overline{A}$ fixed by the Frobenius endomorphism.

Now suppose that 1 is an eigenvalue of Frob_ℓ. Then there exists a nontrivial element of $\overline{A}(\overline{\mathbb{F}_p})[\ell]$ fixed by Frob, and by Proposition 1.2, the number of such elements is divisible by ℓ. By the fact above, so is the order of $A(\mathbb{F}_p)[\ell]$.

Conversely, if ℓ divides the number of rational points on A, then in particular there exists a nontrivial element of $\overline{A}(\overline{\mathbb{F}_p})[\ell]$ fixed by Frob and 1 is an eigenvalue of Frob_ℓ. ■

If E is an elliptic curve, then the linear transformation Frob_ℓ induced by $\operatorname{Frob} : \overline{E} \to \overline{E}$ satisfies

$$\operatorname{char}_{\operatorname{Frob}_\ell}(1) = (X^2 - \operatorname{tr}(\operatorname{Frob}_\ell)X + \det(\operatorname{Frob}_\ell))(1) = 1 - \operatorname{tr}(\operatorname{Frob}_\ell) + p.$$

That is, ℓ divides the number of rational points on E if and only if $\operatorname{tr}(\operatorname{Frob}_\ell)$ is congruent to $(p + 1)$ modulo ℓ. For any (2×2)-matrix M, we have

$$\operatorname{tr}(M) = 1 + \det(M) - \det(I_2 - M).$$

Therefore, by Proposition 1.3, there exists an integer whose reduction modulo ℓ is $\operatorname{tr}(\operatorname{Frob}_\ell)$ for all ℓ. It is called the *trace of Frobenius* of E.

We conclude this section with two results on bounds on the number of rational points:

Theorem 1.5 (Hasse). *Let E be an elliptic curve over $\mathbb{F}_p$. Then its number of rational points is contained in the interval*

$$[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}] = [(\sqrt{p} - 1)^2, (\sqrt{p} + 1)^2].$$

Proof. See [Sil09, Theorem V.1.1]. ■

This interval is called the *Hasse interval*.

Theorem 1.6. *Let J be the Jacobian variety of a hyperelliptic curve over $\mathbb{F}_p$ of genus g. Then its number of rational points is contained in the interval*

$$[(\sqrt{p}-1)^{2g}, (\sqrt{p}+1)^{2g}].$$

Proof. See [CFA+06, Corollary 5.79]. ■

This interval is called the *Hasse-Weil interval*.

2 The Case of Elliptic Curves

In this section, we consider an elliptic curve E associated to a squarefree degree 3 polynomial in $\mathcal{H}_3^p$. We deduce a result by Lenstra ([Len87, Proposition 1.14]) that lets us estimate the probability that the group of rational points on E has ℓ-torsion for any prime number ℓ different from p. We use this to elaborate Galbraith and McKee's derivation in [GM00, Section 4] of their Conjecture 2.5 on the probability that E has a prime number of rational points.

Let ℓ be a prime number different from p and consider the linear transformation of $\overline{E}(\overline{\mathbb{F}_p})[\ell] \cong \mathbb{F}_\ell^2$ induced by the Frobenius endomorphism $\mathrm{Frob} : \overline{E} \to \overline{E}$. The matrix of this transformation with respect to any ordered basis lies in

$$\mathrm{GL}_2^{(p)}(\mathbb{F}_\ell) := \{F \in \mathrm{GL}_2(\mathbb{F}_\ell) \mid \det(F) = p\}$$

by Proposition 1.3 and is called a *matrix of Frobenius* associated to E.

The group $\mathrm{GL}_2(\mathbb{F}_\ell)$ acts on $\mathrm{GL}_2^{(p)}(\mathbb{F}_\ell)$ by conjugation. Let $\mathcal{F}_E$ denote the orbit of our matrix of Frobenius. Thus the set $\mathcal{F}_E$ consists of the matrices of Frobenius associated to E with respect to all possible ordered bases of $\overline{E}(\overline{\mathbb{F}_p})[\ell]$.

Now suppose that the polynomial defining E is chosen uniformly at random from $\mathcal{H}_3^p$. Let $\mathbf{P}(\mathcal{F}_E \subset \mathcal{C})$ denote the probability that $\mathcal{F}_E$ is contained in a subset $\mathcal{C}$ of $\mathrm{GL}_2^{(p)}(\mathbb{F}_\ell)$.

A crucial tool will be the following statement — called "Principle" in [CFHS12] for lack of a published proof. See [CFHS12, Section 4.1] for a discussion of its validity.

Principle 2.1. *There exist constants $C \in \mathbb{R}_{>0}$ and $c \in \mathbb{Z}_{>0}$ such that for all prime numbers $p > 3$ and $\ell \neq p$ and for any union $\mathcal{C}$ of orbits of the action of $\mathrm{GL}_2(\mathbb{F}_\ell)$ on $\mathrm{GL}_2^{(p)}(\mathbb{F}_\ell)$, we have*

$$\left| \mathbf{P}(\mathcal{F}_E \subset \mathcal{C}) - \frac{\#\mathcal{C}}{\#\mathrm{GL}_2^{(p)}(\mathbb{F}_\ell)} \right| \leqslant \frac{C\ell^c}{\sqrt{p}}. \tag{1}$$

That is, as p goes to infinity, the probability that a matrix of Frobenius of E belongs to a certain conjugacy class of $\mathrm{GL}_2^{(p)}(\mathbb{F}_\ell)$ approaches the proportion of matrices belonging to this conjugacy class.

In [GM00], Galbraith and McKee use a slightly different notion of randomness for choosing an elliptic curve E, and in [CFHS12, Section 4.1], the same is true: Instead of taking a polynomial f uniformly at random from $\mathcal{H}_3^p$, they obtain E from a polynomial $f = X^3 + AX + B$, where the pair (A, B) is chosen uniformly at random from the set

$$\{(A, B) \in \mathbb{F}_p^2 \mid 4A^3 + 27B^2 \neq 0\}.$$

The quantity $D = 4A^3 + 27B^2$ is the discriminant of the polynomial f; thus f is squarefree if and only if $D \neq 0$. Let $\mathcal{H}_{3,m}^p$ denote the set of squarefree monic degree 3 polynomials with coefficients in $\mathbb{F}_p$ and let $\mathcal{H}^p_{AB}$ denote the set of squarefree monic degree 3 polynomials with coefficients in $\mathbb{F}_p$ whose degree 2 term vanishes. Define a map

$$\mathcal{H}^p_3 \to \mathcal{H}^p_{3,m}, \qquad f \mapsto \alpha^2 f(X/\alpha), \qquad \text{where } \alpha \text{ is the leading coefficient of } f,$$

and a "completing-the-cube" map

$$\mathcal{H}^p_{3,m} \to \mathcal{H}^p_{AB}, \qquad (X^3+a_2X^2+a_1X+a_0) \mapsto \left(X-\frac{a_2}{3}\right)^3+a_2\left(X-\frac{a_2}{3}\right)^2+a_1\left(X-\frac{a_2}{3}\right)+a_0.$$

In this way, we can associate to each polynomial $f \in \mathcal{H}^p_3$ a polynomial in $\mathcal{H}^p_{AB}$. This does not change the number of rational points on the associated curve E. Therefore, the following lemma shows that the probability that E has a prime number of rational points is not affected by whether we choose the defining polynomial from $\mathcal{H}^p_3$ or from $\mathcal{H}^p_{AB}$.

Lemma 2.2. *The map $\mathcal{H}^p_3 \to \mathcal{H}^p_{AB}$ is surjective and all preimages under it have the same size.*

Proof. The map $\mathcal{H}^p_3 \to \mathcal{H}^p_{3,m}$ is given by

$$a_3X^3+a_2X^2+a_1X+a_0 \mapsto X^3+a_2X^2+a_3a_1X+a_3^2a_0.$$

The preimage of a polynomial $X^3+b_2X^2+b_1X+b_0$ consists of the $p-1$ polynomials

$$a_3X^3+b_2X^2+\frac{b_1}{a_3}X+\frac{b_0}{a_3^2}, \qquad a_3 \in \mathbb{F}_p^\times.$$

The map $\mathcal{H}^p_{3,m} \to \mathcal{H}^p_{AB}$ is given by

$$X^3+b_2X^2+b_1X+b_0 \mapsto X^3+\left(b_1-\frac{b_2^2}{3}\right)X+b_0+\frac{2b_2^3}{27}-\frac{b_2b_1}{3}.$$

Consider any polynomial $f = X^3+AX+B \in \mathcal{H}^p_{AB}$. A polynomial $X^3+b_2X^2+b_1+b_0 \in \mathcal{H}^p_{3,m}$ lies in the preimage of f if and only if

$$b_1-\frac{b_2^2}{3}=A \qquad \text{and} \qquad b_0+\frac{2b_2^3}{27}-\frac{b_2b_1}{3}=B.$$

For any choice of b_2, there exists exactly one b_1 satisfying the first equation. Having chosen b_2 and b_1, there exists exactly one b_0 satisfying the second equation. Therefore, there are p polynomials in the preimage of f.

We conclude that the composition $\mathcal{H}^p_3 \to \mathcal{H}^p_{AB}$ is surjective and that all its preimages have size $(p-1)p$. ■

Recall that ℓ denotes a prime number different from p. Let $\mathbf{P}(p,\ell)$ denote the probability that for a polynomial chosen uniformly at random from $\mathcal{H}^p_3$, the number of rational points on the associated elliptic curve E is divisible by ℓ. Using Principle 2.1 and the remark following Proposition 1.4 we can approximate this probability by counting the number of matrices in $\mathrm{GL}_2^{(p)}(\mathbb{F}_\ell)$ with trace $p+1$. The following lemma does this, in a slightly more general form for use in Section 3 as well:

Lemma 2.3. *For any $q \in \mathbb{F}_\ell^\times$, there are precisely $\ell^3 - \ell$ matrices in $\mathrm{GL}_2^{(q)}(\mathbb{F}_\ell)$. Among those, the number of matrices with trace $q+1$ is*

$$\begin{cases} \ell^2 & \textit{if} \quad \ell | q-1, \\ \ell^2 + \ell & \textit{if} \quad \ell \not| \, q-1. \end{cases}$$

Proof. By Lemma 3.6, there are precisely $(\ell^2-1)(\ell^2-\ell)$ matrices in $\mathrm{GL}_2(\mathbb{F}_\ell)$. Since $\det : \mathrm{GL}_2(\mathbb{F}_\ell) \to \mathbb{F}_\ell^\times$ is a surjective group homomorphism, the set $\mathrm{GL}_2^{(q)}(\mathbb{F}_\ell)$ consists of

$$\frac{(\ell^2-1)(\ell^2-\ell)}{\ell-1} = \ell^3 - \ell$$

matrices. Writing

$$F = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

we will count the number of matrices $F \in \mathrm{GL}_2^{(q)}(\mathbb{F}_\ell)$ with trace $q+1$, that is, the number of matrices satisfying

$$\mathrm{tr}(F) = a + d = q + 1 \qquad \text{and} \qquad \det(F) = ad - bc = q.$$

We do this by first considering the number of such matrices for which $ad = q$, that is, the number of matrices satisfying $a + d = q + 1$ and $ad = q$. The solutions to these two equations are $a = q$, $d = 1$ and $a = 1$, $d = q$.

If $\ell \not| \, q-1$, we therefore have two choices of a and d such that $a + d = q + 1$ and $ad = q$. Then one of b and c must be zero and the other can be chosen freely. For the $\ell - 2$ choices of a and d with $ad = q$, but $a + d \neq q + 1$, there are exactly $\ell - 1$ ways to choose b and c. In total, we get

$$2 \cdot (1 + 2(\ell-1)) + (\ell-2) \cdot (\ell-1) = \ell^2 + \ell$$

matrices in $\mathrm{GL}_2^{(q)}(\mathbb{F}_\ell)$ with trace $q+1$.

If, on the other hand, we have $\ell | q-1$, there is only one choice of a and d such that $a + d = q + 1$ and $ad = q$. In total, we get

$$1 \cdot (1 + 2(\ell-1)) + (\ell-1) \cdot (\ell-1) = \ell^2$$

matrices in $\mathrm{GL}_2^{(q)}(\mathbb{F}_\ell)$ with trace $q+1$. ■

Applying this lemma with $q = p$, we obtain the following result, proved (with better error bounds) by Lenstra in [Len87, Proposition 1.14]:

Theorem 2.4 (Lenstra). *There exist constants $C \in \mathbb{R}_{>0}$ and $c \in \mathbb{Z}_{>0}$ such that for all prime numbers $p > 3$ and $\ell \neq p$,*

$$\left| \mathbf{P}(p, \ell) - \frac{\ell}{\ell^2 - 1} \right| \leqslant C \frac{\ell^c}{\sqrt{p}} \quad \textit{if} \quad \ell | p - 1,$$

$$\left|\mathbf{P}(p,\ell)-\frac{1}{\ell-1}\right| \leqslant C\frac{\ell^c}{\sqrt{p}} \quad \textit{if} \quad \ell \nmid p-1.$$

Proof. Let $\mathcal{C}$ denote the union of all conjugacy classes of $\mathrm{GL}_2^{(p)}(\mathbb{F}_\ell)$ of matrices with trace $p+1$. Then the result immediately follows from inserting the formulas of Lemma 2.3 into the inequality (1) of Principle 2.1. ■

Lenstra's result is a proven theorem. However, we will now use it heuristically to derive the Conjecture 2.5 of Galbraith and McKee. A similar kind of reasoning is used for the case of hyperelliptic curves in Section 3. Indeed, the derivations of all the conjectures in [CFHS12] are of a similar nature.

Let $\mathbf{P}_1(p)$ denote the probability that an integer n chosen uniformly at random from the Hasse interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ is prime. Approximate this probability by

$$\prod_{\ell\leqslant\sqrt{p}+1} \mathbf{P}(\ell \nmid n) \approx \prod_{\ell\leqslant\sqrt{p}+1}\left(1-\frac{1}{\ell}\right), \tag{2}$$

where the products range over all prime numbers $\ell \leqslant \sqrt{p}+1$ (the square root of the upper endpoint of the Hasse interval). The symbol $\approx$ means equality in the limit as p tends to infinity.

This approximation is not precise even asymptotically as p tends to infinity. Indeed, Mertens's third theorem ((15.) in [Mer74]) and the prime number theorem imply

$$\prod_{\ell\leqslant\sqrt{p}+1}\left(1-\frac{1}{\ell}\right) \approx \frac{e^{-\gamma}}{\log(\sqrt{p})} \approx 2e^{-\gamma}\mathbf{P}_1(p),$$

where $\gamma = 0.577...$ is the Euler-Mascheroni constant.

The idea now is to similarly approximate the probability $\mathbf{P}_2(p)$ that the number of rational points on an elliptic curve E, whose associated polynomial is chosen uniformly at random from $\mathcal{H}_3^p$, is prime. Following Lenstra's theorem, this approximation is

$$\prod_{\substack{\ell\nmid p-1\\ \ell\leqslant\sqrt{p}+1}}\left(1-\frac{1}{\ell-1}\right)\prod_{\substack{\ell\mid p-1\\ \ell\leqslant\sqrt{p}+1}}\left(1-\frac{\ell}{\ell^2-1}\right). \tag{3}$$

We hope that in analogy to $\mathbf{P}_1(p)$, this product will approach $2e^{-\gamma}\mathbf{P}_2(p)$ as p tends to infinity, allowing us to approximate the quotient $\mathbf{P}_2(p)/\mathbf{P}_1(p)$ by the quotient of (3) and (2). That this assumption is reasonable is supported both by empirical evidence in favor of the following conjecture ([GM00, Section 2], [CFHS12, Section 11]) and by the fact that Galbraith and McKee give a second and independent derivation of it in [GM00, Section 3].

Conjecture 2.5 (Galbraith-McKee)**.** *Define*

$$c_p := \frac{2}{3} \cdot \prod_{\ell > 2} \left(1 - \frac{1}{(\ell-1)^2}\right) \prod_{\substack{\ell \mid p-1 \\ \ell > 2}} \left(1 + \frac{1}{(\ell+1)(\ell-2)}\right), \tag{4}$$

where the products range over all prime numbers ℓ satisfying the stated conditions. Then with $\mathbf{P}_1(p)$ and $\mathbf{P}_2(p)$ as above, we have

$$\lim_{p \to \infty} \left((\mathbf{P}_2(p)/\mathbf{P}_1(p)) \Big/ c_p \right) = 1.$$

Derivation. As explained above, we start with approximating $\mathbf{P}_2(p)/\mathbf{P}_1(p)$ by the quotient of (3) and (2), that is,

$$\frac{\prod_{\substack{\ell \nmid p-1 \\ \ell \leqslant \sqrt{p}+1}} \left(1 - \frac{1}{\ell-1}\right) \prod_{\substack{\ell \mid p-1 \\ \ell \leqslant \sqrt{p}+1}} \left(1 - \frac{\ell}{\ell^2-1}\right)}{\prod_{\ell \leqslant \sqrt{p}+1} \left(1 - \frac{1}{\ell}\right)} = \frac{\prod_{\substack{\ell \nmid p-1 \\ \ell \leqslant \sqrt{p}+1}} \left(\frac{\ell-2}{\ell-1}\right) \prod_{\substack{\ell \mid p-1 \\ \ell \leqslant \sqrt{p}+1}} \left(\frac{\ell^2-\ell-1}{\ell^2-1}\right)}{\prod_{\ell \leqslant \sqrt{p}+1} \left(\frac{\ell-1}{\ell}\right)}.$$

The rest is algebraic manipulations: Pulling the factor corresponding to $\ell = 2$ out of the second product, we obtain

$$\frac{2}{3} \cdot \prod_{\substack{\ell \nmid p-1 \\ 2 < \ell \leqslant \sqrt{p}+1}} \left(\frac{\ell^2 - 2\ell}{(\ell-1)^2}\right) \prod_{\substack{\ell \mid p-1 \\ 2 < \ell \leqslant \sqrt{p}+1}} \left(\frac{\ell^3 - \ell^2 - \ell}{(\ell+1)(\ell-1)^2}\right).$$

We eliminate the first product's condition that $\ell \nmid p-1$ by multiplying the second product with $(\ell-1)^2/(\ell^2-2\ell)$, obtaining

$$\frac{2}{3} \cdot \prod_{2 < \ell \leqslant \sqrt{p}+1} \left(1 - \frac{1}{(\ell-1)^2}\right) \prod_{\substack{\ell \mid p-1 \\ 2 < \ell \leqslant \sqrt{p}+1}} \left(1 + \frac{1}{(\ell+1)(\ell-2)}\right).$$

Finally, taking the limit as p goes to infinity completes the derivation. ■

We can approximate the number c_p from (4) as follows: Since all factors of the first infinite product are smaller than 1 and all factors of the second infinite product are greater than 1, a lower bound is given by 2/3 times the first product. An upper bound is obtained by discarding the condition $\ell | p-1$ for the second product.

Numerically evaluating these products shows that c_p is contained in the interval $[0.44010, 0.61514]$. This indicates a bias against a randomly chosen elliptic curve having a prime number of rational points.

3 Generalization to Genus 2 Curves

In this section, we consider a hyperelliptic curve H associated to a squarefree degree 6 polynomial in $\mathcal{H}_6^p$. Let J denote the Jacobian variety of H. We deduce a result similar to Lenstra's Theorem 2.4 that will let us estimate the probability that the number of rational points on J has ℓ-torsion for any prime number ℓ different from p. We then use this to derive an analog to Conjecture 2.5, namely Conjecture 3.10 ([CFHS12, Conjecture 2]).

3.1 The Weil Pairing and Symplectic Matrices

For a prime number ℓ different from p, consider the group μ_ℓ of ℓ-th roots of unity of $\overline{\mathbb{F}_\ell}$. There exists a pairing

$$e_\ell : \overline{J}(\overline{\mathbb{F}_p})[\ell] \times \overline{J}(\overline{\mathbb{F}_p})[\ell] \to \mu_\ell$$

on the ℓ-torsion-subgroup of $\overline{J}(\overline{\mathbb{F}_p})$, called the *Weil pairing*, with the following properties:

(i) Bilinearity: For all $P, P_1, P_2, Q, Q_1, Q_2 \in \overline{J}(\overline{\mathbb{F}_p})[\ell]$, we have

$$e_\ell(P_1 + P_2, Q) = e_\ell(P_1, Q)e_\ell(P_2, Q) \qquad \text{and}$$
$$e_\ell(P, Q_1 + Q_2) = e_\ell(P, Q_1)e_\ell(P, Q_2).$$

(ii) It is alternating: For all $P \in \overline{J}(\overline{\mathbb{F}_p})[\ell]$, we have $e_\ell(P, P) = 1$.

(iii) Nondegenerateness: For every $0 \neq P \in \overline{J}(\overline{\mathbb{F}_p})[\ell]$, there exists some $Q \in \overline{J}(\overline{\mathbb{F}_p})[\ell]$ with $e_\ell(P, Q) \neq 1$.

(iv) Galois invariance: For all $\gamma \in \mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ and all $P, Q \in \overline{J}(\overline{\mathbb{F}_p})[\ell]$, we have

$$e_\ell(\gamma(P), \gamma(Q)) = \gamma(e_\ell(P, Q)).$$

See [Mum70, Section 20]. A Weil pairing $\overline{E}(\overline{\mathbb{F}_p})[\ell] \times \overline{E}(\overline{\mathbb{F}_p})[\ell] \to \mu_\ell$ also exists for elliptic curves E; for a discussion of this, see [Sil09, Section III.8].

We now review the notion of *symplectic matrices*.

Consider the matrix

$$\Omega = \begin{pmatrix} 0_2 & I_2 \\ -I_2 & 0_2 \end{pmatrix} \in \mathrm{Mat}_{4\times4}(\mathbb{F}_\ell).$$

For $d \in \mathbb{F}_\ell^\times$, the matrices

$$\mathrm{GSp}_4^{(d)}(\mathbb{F}_\ell) := \{M \in \mathrm{GL}_4(\mathbb{F}_\ell) \mid M^T\Omega M = d\Omega\}$$

are called *d-symplectic matrices*. The 1-symplectic matrices $\mathrm{Sp}_4(\mathbb{F}_\ell) := \mathrm{GSp}_4^{(1)}(\mathbb{F}_\ell)$ form a group under matrix multiplication and are just called *symplectic matrices*. The union $\mathrm{GSp}_4(\mathbb{F}_\ell)$ of all $\mathrm{GSp}_4^{(d)}(\mathbb{F}_\ell)$ also forms a group, called the group of *symplectic similitudes*.

Lemma 3.1. *The group* $\mathrm{GSp}_4(\mathbb{F}_\ell)$ *is generated by* $\mathrm{Sp}_4(\mathbb{F}_\ell)$ *and the matrices*

$$\Delta_d = \begin{pmatrix} I_2 & 0_2 \\ 0_2 & dI_2 \end{pmatrix} \in \mathrm{Mat}_{4\times 4}(\mathbb{F}_\ell), \qquad d \in \mathbb{F}_\ell^\times.$$

Proof. The matrices Δ_d are contained in $\mathrm{GSp}_4^{(d)}(\mathbb{F}_\ell)$ by an easy direct calculation. Now take any symplectic similitude, say $M \in \mathrm{GL}_4^{(d)}(\mathbb{F}_\ell)$. Then

$$(M\Delta_{1/d})^T\Omega(M\Delta_{1/d}) = \Delta_{1/d}^T(M^T\Omega M)\Omega_{1/d} = d(\Delta_{1/d}^T\Omega\Delta_{1/d}) = \Omega,$$

so $M = (M\Delta_{1/d})\Delta_d$ is a product of a symplectic matrix $M\Delta_{1/d}$ and a matrix Δ_d. ■

A consequence of this lemma is that $\mathrm{GSp}_4(\mathbb{F}_\ell)$ acts on any set of similitudes $\mathrm{GSp}_4^{(d)}(\mathbb{F}_\ell)$ by conjugation.

We return to the situation of the Jacobian variety J of a hyperelliptic curve H associated to a polynomial in $\mathcal{H}_6^p$.

For a prime number ℓ different from p, consider the Weil pairing

$$e_\ell : \overline{J}(\overline{\mathbb{F}_p})[\ell] \times \overline{J}(\overline{\mathbb{F}_p})[\ell] \to \mu_\ell.$$

For any primitive root of unity $\zeta \in \mu_\ell$, there is a group isomorphism

$$\mathbb{Z}/(\ell) \to \mu_\ell, \qquad d \mapsto \zeta^d.$$

Composing its inverse with the Weil pairing gives a bilinear, alternating, and nondegenerate pairing

$$\omega_\zeta : \overline{J}(\overline{\mathbb{F}_p})[\ell] \times \overline{J}(\overline{\mathbb{F}_p})[\ell] \to \mathbb{F}_\ell.$$

Since this pairing depends on the choice of primitive root of unity ζ, we include ζ in the notation. A pair (V, ω), where V is a $\mathbb{F}_\ell$-vector space and ω is a bilinear, alternating, and nondegenerate pairing $V \times V \to \mathbb{F}_\ell$, is called a *symplectic* $\mathbb{F}_\ell$*-vector space.*

As in Section 2, we will consider the linear transformation $\overline{J}(\overline{\mathbb{F}_p})[\ell] \to \overline{J}(\overline{\mathbb{F}_p})[\ell]$ induced by the Frobenius endomorphism $\mathrm{Frob} : \overline{J} \to \overline{J}$. However, as opposed to considering the matrices of Frobenius with respect to all possible ordered bases, we will restrict ourselves to considering matrices of Frobenius with respect to so-called *Darboux* or *symplectic bases* of $\overline{J}(\overline{\mathbb{F}_p})[\ell] \cong \mathbb{F}_\ell^4$. An ordered basis is called *Darboux* or *symplectic basis* with respect to ω_ζ if the matrix of ω_ζ is Ω with respect to this basis.

Lemma 3.2. *An ordered basis* (P_1, P_2, Q_1, Q_2) *of* $\overline{J}(\overline{\mathbb{F}_p})[\ell]$ *is a Darboux basis with respect to* ω_ζ *if and only if*

$$e_\ell(P_1, P_2) = e_\ell(Q_1, Q_2) = e_\ell(P_1, Q_2) = e_\ell(P_2, Q_1) = 1 \qquad \textit{and}$$

$$e_\ell(P_1, Q_1) = e_\ell(P_2, Q_2) = \zeta.$$

Proof. Since the pairing ω_ζ is alternating, its matrix with respect to any ordered basis has zeros on the main diagonal. Furthermore, we have $e_\ell(P,Q) = e_\ell(Q,P)^{-1}$, so $\omega_\zeta(P,Q) = -\omega_\zeta(Q,P)$ for all $P, Q \in \overline{J}(\overline{\mathbb{F}_p})[\ell]$. Thus, an ordered basis is a Darboux basis if and only if the matrix of ω_ζ with respect to it coincides with Ω in the six entries above the main diagonal. But this corresponds exactly to the six conditions given in the lemma. ∎

Given a d-dimensional linear subspace U of a symplectic $\mathbb{F}_p$-vector space (V, ω) with ordered basis $(P_1, \dots, P_d)$, consider the linear subspace

$$U^\omega := \{P \in V \mid \text{ for all } Q \in U : \omega(P,Q) = 0\}. \tag{5}$$

Since U^ω is the kernel of the full rank linear map

$$V \to \mathbb{F}_p^d, \qquad P \mapsto (\omega(P, P_1), \dots, \omega(P, P_d)), \tag{6}$$

it is $(\dim(V) - d)$-dimensional. We clearly have $(U^\omega)^\omega \subset U$, and by dimensional reasoning conclude that $(U^\omega)^\omega = U$. In the special case that $U \cap U^\omega = \{0\}$, we call U a *symplectic subspace*. In this case, V is a direct sum of U and U^ω. Equivalently, ω restricted to U is still nondegenerate.

In the following lemma, we will apply the concept of symplectic subspaces to the case of the 4-dimensional symplectic vector space $(\overline{J}(\overline{\mathbb{F}_p})[\ell], \omega_\zeta)$.

Lemma 3.3. *There exists a Darboux basis of $\overline{J}(\overline{\mathbb{F}_p})[\ell]$ with respect to ω_ζ.*

Proof. The proof is adapted from [Gos06, Section 1.2].

Pick an arbitrary point $0 \neq P_1 \in \overline{J}(\overline{\mathbb{F}_p})[\ell]$. Since ω_ζ is nondegenerate, we can pick another point $Q_1 \in \overline{J}(\overline{\mathbb{F}_p})[\ell]$ with $\omega_\zeta(P_1, Q_1) = 1$.

Let U be the subspace of $\overline{J}(\overline{\mathbb{F}_p})[\ell]$ spanned by P_1 and Q_1. Since $\omega_\zeta(P_1, Q_1) = 1$, we have $U \cap U^{\omega_\zeta} = \{0\}$, that is, U is a symplectic subspace of $\overline{J}(\overline{\mathbb{F}_p})[\ell]$. Thus $\overline{J}(\overline{\mathbb{F}_p})[\ell]$ is a direct sum of U and U^{ω_ζ}, so the restriction of ω_ζ to U^{ω_ζ} is again nondegenerate.

We can therefore choose P_2 and Q_2 in U^{ω_ζ} with $\omega_\zeta(P_2, Q_2) = 1$, and

$$\omega_\zeta(P_1, P_2) = \omega_\zeta(Q_1, Q_2) = \omega_\zeta(P_1, Q_2) = \omega_\zeta(P_2, Q_1) = 0.$$

Together with $\omega_\zeta(P_1, Q_1) = 1$, this implies that the matrix of ω_ζ with respect to the ordered basis (P_1, P_2, Q_1, Q_2) is Ω. ∎

With respect to a Darboux basis, the linear transformation of $\overline{J}(\overline{\mathbb{F}_p})[\ell]$ induced by the Frobenius endomorphism has a p-symplectic matrix $F \in \mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$: Using the Galois invariance of the Weil pairing, we have

$$e_\ell(\mathrm{Frob}(P), \mathrm{Frob}(Q)) = \mathrm{Frob}(e_\ell(P,Q)) = e_\ell(P,Q)^p$$

for all $P, Q \in \overline{J}(\overline{\mathbb{F}_p})[\ell]$. But that is to say

$$\omega_\zeta(\mathrm{Frob}(P), \mathrm{Frob}(Q)) = p\omega_\zeta(P,Q),$$

so F satisfies $F^T \Omega F = p\Omega$.

3.2 Generalization of the Random Matrix Principle

We have seen that we can associate to a hyperelliptic curve H with Jacobian variety J a p-symplectic matrix of Frobenius $F \in \mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$ with respect to a Darboux basis (using Lemma 3.3). We can further associate to H the orbit $\mathcal{F}_H$ of F in $\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$ under $\mathrm{GSp}_4(\mathbb{F}_\ell)$-conjugation. The following lemma shows that this orbit is independent of the choices we have made in constructing F.

Lemma 3.4. *The orbit $\mathcal{F}_H$ is independent of the choice of Darboux basis and of the choice of primitive root of unity $\zeta \in \mu_\ell$ used in the definition of the pairing ω_ζ.*

Proof. First, suppose that we choose a different Darboux basis with respect to the pairing ω_ζ. Then the matrices of ω_ζ with respect to these bases are related by conjugation by a symplectic matrix.

Next, suppose that we choose a different primitive root of unity ζ^d, where $d \in \mathbb{F}_p^\times$, instead of ζ. If (P_1, P_2, Q_1, Q_2) is a Darboux basis with respect to ω_ζ, then (P_1, P_2, dQ_1, dQ_2) is a Darboux basis with respect to ω_{ζ^d} by Lemma 3.2 and bilinearity of the Weil pairing. The matrix of base change from (P_1, P_2, dQ_1, dQ_2) to (P_1, P_2, Q_1, Q_2) is Δ_d. Therefore, a matrix of Frobenius with respect to a Darboux basis and the pairing ω_{ζ^d} is always related to a matrix of Frobenius with respect to a Darboux basis and the pairing ω_ζ by conjugation by Δ_d.

Since $\mathrm{Sp}_4(\mathbb{F}_\ell)$ and the matrices Δ_d are contained in $\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$, we are done. ■

Suppose that the polynomial defining the curve H is chosen uniformly at random from $\mathcal{H}_6^p$. Denote the probability that the orbit $\mathcal{F}_H$ is contained in a subset $\mathcal{C}$ of $\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$ by $\mathbf{P}(\mathcal{F}_H \subset \mathcal{C})$.

We will make use of the following analog of Principle 2.1. Again, see [CFHS12, Section 4.2] for a discussion of its validity.

Principle 3.5. *There exist constants $C \in \mathbb{R}_{>0}$ and $c \in \mathbb{Z}_{>0}$ such that for all prime numbers $p > 3$ and $\ell \neq p$ and for any union $\mathcal{C}$ of orbits of the action of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ on $\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$, we have*

$$\left| \mathbf{P}(\mathcal{F}_H \subset \mathcal{C}) - \frac{\#\mathcal{C}}{\#\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)} \right| \leqslant \frac{C\ell^c}{\sqrt{p}}. \tag{7}$$

In Section 2, we estimated the probability that the group of rational points on an elliptic curve has ℓ-torsion by counting the number of matrices of Frobenius with trace $p+1$. Proposition 1.4 is also applicable to our current situation: The number of rational points on J is divisible by ℓ if and only if the characteristic polynomial of the linear transformation $\mathrm{Frob}_\ell : J(\overline{F_p})[\ell] \to J(\overline{\mathbb{F}}_p)[\ell]$ induced by the Frobenius endomorphism evaluated at 1 vanishes.

By Principle 3.5, we can therefore estimate the probability that J has ℓ-torsion by counting the proportion of matrices in $\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$ whose characteristic polynomial evaluated at 1 is zero, that is, the proportion of matrices in $\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$ that have 1 as an eigenvalue. In Proposition 3.9, we will determine this proportion using a recursive argument. To this end, let

$$\mathfrak{Q}(p, \ell, r)$$

denote the proportion of matrices in $\mathrm{GSp}_{2r}^{(p)}(\mathbb{F}_\ell)$ that have 1 as an eigenvalue, where $r \in \{1, 2\}$.

We will also need closed-form formulas for the numbers of invertible and symplectic matrices over $\mathbb{F}_\ell$:

Lemma 3.6. *We have*

$$\#\mathrm{GL}_g(\mathbb{F}_\ell) = \ell^{(g^2-g)/2} \prod_{j=1}^{g} (\ell^j - 1) \qquad \textit{and} \qquad \#\mathrm{Sp}_{2g}(\mathbb{F}_\ell) = \ell^{g^2} \prod_{j=1}^{g} (\ell^{2j} - 1).$$

Proof. The number of matrices in $\mathrm{GL}_g(\mathbb{F}_\ell)$ is the same as the number of ordered bases of $\mathbb{F}_\ell^g$. There are $\ell^g - 1$ ways to choose the first vector of such a basis. Having chosen the first vector, there are $(\ell^g - \ell)$ ways to choose the second vector of such a basis and so on. In total, we get

$$\#\mathrm{GL}_g(\mathbb{F}_p) = \prod_{j=1}^{g} (\ell^g - \ell^{j-1}) = \prod_{j=1}^{g} \ell^{j-1} \prod_{j=1}^{g} (\ell^j - 1) = \ell^{(g^2-g)/2} \prod_{j=1}^{g} (\ell^j - 1).$$

Similarly, the number of matrices in $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ is the same as the number of ordered bases of $\mathbb{F}_\ell^g$ that are Darboux bases with respect to the form

$$\omega : \mathbb{F}_\ell^g \times \mathbb{F}_\ell^g \to \mathbb{F}_\ell, \qquad (P, Q) \mapsto P^T \Omega Q.$$

Write $(P_1, \dots, P_g, Q_1, \dots, Q_g)$ for such a basis. There are $\ell^{2g} - 1$ ways to choose P_1. Having chosen P_1, the vector Q_1 must satisfy $P_1^T \Omega Q_1 = 1$, which leaves ℓ^{2g-1} choices. If V is the subspace spanned by P_1 and Q_1, the remaining basis elements must lie in V^ω, which is $(2g - 2)$-dimensional. Continuing in this manner, we get

$$\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell) = \prod_{j=1}^{g} \ell^{2j-1} \prod_{j=1}^{g} (\ell^{2j} - 1) = \ell^{g^2} \prod_{j=1}^{g} (\ell^{2j} - 1).$$

■

A matrix $M \in \mathrm{Mat}_{r\times r}(\mathbb{F}_\ell)$ is called *unipotent* if $M - I_r$ is nilpotent. Since a matrix in $\mathrm{Mat}_{r\times r}(\mathbb{F}_\ell)$ is nilpotent if and only if its characteristic polynomial is X^r, a matrix $M \in \mathrm{Mat}_{r\times r}(\mathbb{F}_\ell)$ is unipotent if and only if $\mathrm{char}_M = (X - 1)^r$.

Lemma 3.7. *The number of unipotent matrices in* $\mathrm{Sp}_2(\mathbb{F}_\ell)$ *is* ℓ^2. *The number of unipotent matrices in* $\mathrm{Sp}_4(\mathbb{F}_\ell)$ *is* ℓ^8.

Proof. Since $\mathrm{Sp}_2(\mathbb{F}_\ell) = \mathrm{SL}_2(\mathbb{F}_\ell)$, the unipotent matrices in $\mathrm{Sp}_2(\mathbb{F}_\ell)$ are precisely the matrices similar to

$$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{or} \qquad U := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The centralizer of U with respect to the action of $\mathrm{GL}_2(\mathbb{F}_\ell)$ by conjugation is the matrices

$$\left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \,\middle|\, a \in \mathbb{F}_\ell^\times,\ b \in \mathbb{F}_\ell \right\}.$$

Thus, the number of matrices similar to U is

$$\frac{\#\mathrm{GL}_2(\mathbb{F}_\ell)}{\ell(\ell-1)} = \frac{\ell(\ell-1)(\ell^2-1)}{\ell-1} = \ell^2 - 1$$

and, adding I_2, the result follows.

We do not give a proof for the number of unipotent matrices in $\mathrm{Sp}_4(\mathbb{F}_\ell)$. Proofs can be found in [Ful00, Corollary 1] and [Hum95, Section 8.14]. ■

Proposition 3.8. *The proportion* $\mathfrak{Q}(p, \ell, 2)$ *of matrices in* $\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$ *that have* 1 *as an eigenvalue is*

$$\begin{cases} \dfrac{\ell(\ell^4 - \ell - 1)}{(\ell^4-1)(\ell^2-1)} & \textit{if} \quad \ell | p-1, \\ \dfrac{\ell^2 - 2}{(\ell^2-1)(\ell-1)} & \textit{if} \quad \ell \not| \, p-1. \end{cases}$$

Proof. The proof is adapted from Lemmas 3.1 and 3.2 of the paper [AH03] by Achter and Holden, who use ideas from Section 3 of Chavdarov's paper [Cha97]. Similar ideas are used in [CFHS12, Section 5]. We divide the proof into several steps.

Step 1: Suppose that $F \in \mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$. We have

$$\begin{aligned} \mathrm{char}_F = \det(F^T - XI_4) &= \det(F^T\Omega - \tfrac{X}{p} F^T \Omega F) / \det(\Omega) \\ &= \det(-\tfrac{1}{p} X F^T) \det(\Omega F - \tfrac{p}{X}\Omega) / \det(\Omega) \\ &= \det(-\tfrac{1}{p} X F^T) \mathrm{char}_F(\tfrac{p}{X}), \end{aligned}$$

so for any $a \in \mathbb{F}_\ell^\times$, the algebraic multiplicities of a and p/a are the same. In particular, the algebraic multiplicities of 1 and p are the same, and if p is congruent to 1 modulo ℓ, this algebraic multiplicity is an even number. In any case, we can write char_F as a product of $(X-1)^r(X-p)^r$ for some $r \in \{0, 1, 2\}$ and a polynomial that does not have 1 or p as a zero.

Step 2: For $r \in \{1,2\}$, consider the sets of matrices

$$S(r) := \{F \in \mathrm{GSp}_{2r}^{(p)}(\mathbb{F}_\ell) \mid \mathrm{char}_F = (X-1)^r(X-p)^r\}.$$

In [AH03, Lemma 3.1], formulas for $\#S(r)$ are given for arbitrary r. For reasons of self-containedness, we instead indicate an elementary way of arriving at formulas for the cases $r \in \{0,1\}$, following [CFHS12, Lemma 3] and [Cha97, Lemma 3.3].

Using the Jordan-Chevalley decomposition (see [Hum72, Section 4.2] for a reference that assumes — as we may — that char_F splits into linear factors), we can write any $F \in S(r)$ uniquely as a sum of a semisimple matrix $F_s \in \mathrm{GSp}_{2r}^{(p)}(\mathbb{F}_\ell)$ with $\mathrm{char}_{F_s} = \mathrm{char}_F$ and a nilpotent matrix F_n such that F_s and F_n commute. Hence we can write F uniquely as a commuting product of the semisimple matrix F_s and a unipotent matrix $F_u := I_{2r} + F_s^{-1}F_n$.

We claim that the action by conjugation of $\mathrm{Sp}_{2r}(\mathbb{F}_\ell)$ on these semisimple matrices F_s is transitive. To this end, consider the symplectic vector space $(\mathbb{F}_p^{2r}, \omega)$, where ω is given by

$$(P,Q) \mapsto P^T \begin{pmatrix} 0_r & I_r \\ -I_r & 0_r \end{pmatrix} Q.$$

As in Lemma 3.3, we can find a symplectic basis of $\mathbb{F}_p^{2r}$: Choose an eigenvector P_1 of F_s corresponding to the eigenvalue 1. Then choose another eigenvector Q_1 with $\omega(P_1, Q_1) = 1$; if λ is the eigenvalue corresponding to Q_1, then

$$p = \omega(F_sP_1, F_sQ_1) = \lambda\omega(P_1, Q_1) = \lambda.$$

If $r = 2$, do this procedure again to complete a basis of $\mathbb{F}_p^{2r}$. In any case, we have shown that F_s is related to the diagonal matrix

$$\Delta := \mathrm{diag}(\underbrace{1,\dots,1}_{r \text{ times}}, \underbrace{p,\dots,p}_{r \text{ times}}) \in S(r)$$

by conjugation by a symplectic matrix. In particular, the action of $\mathrm{Sp}_{2r}(\mathbb{F}_\ell)$ by conjugation on the F_s is transitive.

Step 3: We want to show that

$$\#S(1) = \begin{cases} \ell^2 & \text{if} \quad \ell | p-1, \\ \ell^2 + \ell & \text{if} \quad \ell \not| \, p-1, \end{cases}$$

$$\#S(2) = \begin{cases} \ell^8 & \text{if} \quad \ell | p-1, \\ \ell^8 + \ell^7 + \ell^6 + \ell^5 & \text{if} \quad \ell \not| \, p-1. \end{cases}$$

The formulas for $\ell | p-1$ follow immediately from Lemma 3.7, since the only semisimple matrix F_s with characteristic polynomial $(X-1)^{2r}$ is the identity.

For the case $\ell \not| \, p-1$, consider the transitive action of $\mathrm{Sp}_{2r}(\mathbb{F}_\ell)$ on the semisimple matrices F_s by conjugation. All the F_s lie in the orbit of the diagonal matrix Δ. Therefore, the total number of matrices F_s obtained from some $F \in S(r)$ is

$$\#\mathrm{Sp}_{2r}(\mathbb{F}_\ell)/\#C(\Delta),$$

where $C(\Delta)$ is the centralizer of Δ. The matrices in $\mathrm{GL}_{2r}(\mathbb{F}_\ell)$ commuting with Δ are the matrices

$$\left\{ \begin{pmatrix} M_1 & 0 \\ 0 & M_2 \end{pmatrix} \middle| \; M_1, M_2 \in \mathrm{GL}_r(\mathbb{F}_\ell) \right\}.$$

Considering only symplectic matrices among these, we find

$$C(\Delta) = \left\{ \begin{pmatrix} M & 0 \\ 0 & (M^{-1})^T \end{pmatrix} \middle| \; M \in \mathrm{GL}_r(\mathbb{F}_\ell) \right\}. \tag{8}$$

Next, we determine the number of possible unipotent matrices F_u for fixed F_s. This is the number of unipotent symplectic matrices commuting with a certain F_s, say with Δ for simplicity.

We are looking for the number of matrices as in (8) with characteristic polynomial $(X-1)^{2r}$, that is, the number of matrices in $\mathrm{GL}_r(\mathbb{F}_\ell)$ with characteristic polynomial $(X-1)^r$. If $r = 1$, there is only one such matrix; if $r = 2$, there are ℓ^2 such matrices by Lemma 3.7.

This yields the desired formulas

$$\#S(1) = \frac{\ell(\ell^2-1)}{\ell - 1} = \ell^2 + \ell,$$

$$\#S(2) = \frac{\ell^4(\ell^2-1)(\ell^4-1)}{\ell(\ell-1)(\ell^2-1)}\ell^2 = \ell^5(\ell^3+\ell^2+\ell+1) = \ell^8+\ell^7+\ell^6+\ell^5.$$

Step 4: Next, we count the number of matrices $F \in \mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$ that have 1 as an eigenvalue. We do this separately for the two possible algebraic multiplicities of 1 that can occur. Write char_F as a product of $(X-1)^r(X-p)^r$ and a polynomial that does not have 1 as a zero. First, we claim that for $r = 1$, there are

$$\frac{\#\mathrm{Sp}_4(\mathbb{F}_\ell)}{\#\mathrm{Sp}_2(\mathbb{F}_\ell)\#\mathrm{Sp}_2(\mathbb{F}_\ell)}\#S(1)\Big(\#\mathrm{Sp}_2(\mathbb{F}_\ell) - \mathfrak{Q}(p,\ell,1)\#\mathrm{Sp}_2(\mathbb{F}_\ell)\Big) \tag{9}$$

matrices in $\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$. To explain this, again consider the symplectic vector space $(\mathbb{F}_p^4, \omega)$. Given F, we can decompose $\mathbb{F}_p^4$ into two F-invariant 2-dimensional subspaces: The eigenspaces for eigenvalues 1 and p, whose direct sum we denote by U, and U^ω. Conversely, a decomposition of $\mathbb{F}_p^4$ into two 2-dimensional symplectic subspaces U and U^ω together with p-symplectic matrices acting on U and U^ω gives rise to a matrix F of the form we are considering.

We can now explain (9): The first factor in (9) is the number of ways of writing $\mathbb{F}_p^4$ as a direct sum of two 2-dimensional symplectic subspaces. The second factor counts by definition of $S(r)$ the number of ways F can act on U, and the third factor counts the number of ways F can act on U^ω. This concludes the case $r = 1$.

For $r = 2$, there are exactly $\#S(2)$ matrices in $\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$ by definition of $S(r)$.

Step 5: Dividing the sum of (9) and $\#S(2)$ by $\#\mathrm{Sp}_4(\mathbb{F}_\ell)$ we obtain

$$\begin{aligned}\mathfrak{Q}(p, \ell, 2) &= \frac{\#S(1)}{\#\mathrm{Sp}_2(\mathbb{F}_\ell)}(1 - \mathfrak{Q}(p, \ell, 1)) + \frac{\#S(2)}{\#\mathrm{Sp}_4(\mathbb{F}_\ell)} \\ &= \frac{\#S(1)}{\#\mathrm{Sp}_2(\mathbb{F}_\ell)}\left(1 - \frac{\#S(1)}{\#\mathrm{Sp}_2(\mathbb{F}_\ell)}\right) + \frac{\#S(2)}{\#\mathrm{Sp}_4(\mathbb{F}_\ell)}.\end{aligned}$$

Plugging in our formulas for $\#S(1)$ and $\#S(2)$ and the formula for the order of the symplectic group from Lemma 3.6 finishes the proof. ■

Proposition 3.8 and Principle 3.5 yield the generalization of Lenstra's Theorem 2.4 we want: Let $\mathbf{P}(p, \ell)$ denote the probability that for a polynomial chosen uniformly at random from $\mathcal{H}_6^p$, the number of rational points on the Jacobian variety J of the associated hyperelliptic curve is divisible by ℓ.

Proposition 3.9. *There exist constants $C \in \mathbb{R}_{>0}$ and $c \in \mathbb{Z}_{>0}$ such that for all prime numbers $p > 3$ and $\ell \neq p$,*

$$\left|\mathbf{P}(p, \ell) - \frac{\ell(\ell^4 - \ell - 1)}{(\ell^4 - 1)(\ell^2 - 1)}\right| \leqslant C\frac{\ell^c}{\sqrt{p}} \quad \text{if} \quad \ell | p - 1,$$

$$\left|\mathbf{P}(p, \ell) - \frac{\ell^2 - 2}{(\ell^2 - 1)(\ell - 1)}\right| \leqslant C\frac{\ell^c}{\sqrt{p}} \quad \text{if} \quad \ell \not| \, p - 1.$$

Proof. Let $\mathcal{C}$ denote the union of all conjugacy classes of $\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$ of matrices that have 1 as an eigenvalue. Then the result immediately follows from inserting the formulas of Proposition 3.8 into the inequality (7) of Principle 3.5. ■

We are now ready to derive the analog of the Galbraith-McKee conjecture for hyperelliptic curves defined by polynomials in $\mathcal{H}_6^p$. Let $\mathbf{P}_1(p)$ denote the probability that an integer n chosen uniformly at random from the Hasse-Weil interval $[(\sqrt{p} - 1)^4, (\sqrt{p} + 1)^4]$ is prime. Let $\mathbf{P}_2(p)$ denote the probability that the Jacobian variety of a hyperelliptic curve over $\mathbb{F}_p$, whose associated polynomial is chosen uniformly at random from $\mathcal{H}_6^p$, has a prime number of rational points.

Conjecture 3.10. *Define*

$$c_p := \frac{38}{45} \cdot \prod_{\ell > 2}\left(1 - \frac{\ell^2 - \ell - 1}{(\ell^2 - 1)(\ell - 1)^2}\right) \prod_{\substack{\ell | p-1 \\ \ell > 2}}\left(1 + \frac{\ell^4 - \ell^3 - \ell - 2}{(\ell^3 - 2\ell^2 - \ell + 3)(\ell^2 + 1)(\ell + 1)}\right), \quad (10)$$

where the products range over all prime numbers ℓ satisfying the stated conditions. Then with $\mathbf{P}_1(p)$ and $\mathbf{P}_2(p)$ as above, we have

$$\lim_{p\to\infty}\left(\left(\mathbf{P}_2(p)/\mathbf{P}_1(p)\right)\Big/c_p\right) = 1.$$

Derivation. This is similar to the derivation of Conjecture 2.5: Following Proposition 3.9, we approximate $\mathbf{P}_2(p)$ by

$$\prod_{\substack{\ell\nmid p-1\\ \ell\leqslant(\sqrt{p}+1)^2}}\left(1-\frac{\ell^2-2}{(\ell^2-1)(\ell-1)}\right)\prod_{\substack{\ell\mid p-1\\ \ell\leqslant(\sqrt{p}+1)^2}}\left(1-\frac{\ell(\ell^4-\ell-1)}{(\ell^4-1)(\ell^2-1)}\right) \tag{11}$$

and as before approximate $\mathbf{P}_1(p)$ by

$$\prod_{\ell\leqslant(\sqrt{p}+1)^2}\left(1-\frac{1}{\ell}\right). \tag{12}$$

Now, a calculation entirely analogous to the one found in the derivation of Conjecture 2.5 shows that the quotient of (11) and (12) satisfies

$$\prod_{\substack{\ell\nmid p-1\\ \ell\leqslant(\sqrt{p}+1)^2}}\left(1-\frac{\ell^2-2}{(\ell^2-1)(\ell-1)}\right)\prod_{\substack{\ell\mid p-1\\ \ell\leqslant(\sqrt{p}+1)^2}}\left(1-\frac{\ell(\ell^4-\ell-1)}{(\ell^4-1)(\ell^2-1)}\right)\prod_{\ell\leqslant(\sqrt{p}+1)^2}\left(1-\frac{1}{\ell}\right)^{-1}$$
$$=\frac{38}{45}\prod_{\substack{\ell<2\\ \leqslant(\sqrt{p}+1)^2}}\left(1-\frac{\ell^2-\ell-1}{(\ell^2-1)(\ell-1)^2}\right)\prod_{\substack{\ell\mid p-1\\ 2<\ell\leqslant(\sqrt{p}+1)^2}}\left(1+\frac{\ell^4-\ell^3-\ell-2}{(\ell^3-2\ell^2-\ell+3)(\ell^2+1)(\ell+1)}\right).$$

Taking the limit as p goes to infinity yields (10).

There is, however, one subtlety: Since $p<(\sqrt{p}+1)^2$, we need to consider the case $\ell=p$ as well now.

By Proposition 1.2, we have $\overline{J}(\overline{\mathbb{F}_p})[p]\cong(\mathbb{F}_p)^k$ for some $k\in\{0,1,2\}$. Choosing an ordered basis for $\overline{J}(\overline{\mathbb{F}_p})[p]$, we once again get a matrix of Frobenius in $\mathrm{GL}_k(\mathbb{F}_p)$, and, varying this basis, a conjugacy class $\mathcal{F}_H$ with respect to $\mathrm{GL}_k(\mathbb{F}_p)$-conjugation. Let $\mathbf{P}(\mathcal{F}_E\subset\mathcal{C})$ denote the probability that $k=2$ and that $\mathcal{F}_H$ is contained in a subset $\mathcal{C}$ of $\mathrm{GL}_2(\mathbb{F}_p)$. In analogy to Principles 2.1 and 3.5, we will make use of the following statement. See [CFHS12, Section 10] for a discussion of its validity.

Principle 3.11. *There exist constants $C\in\mathbb{R}_{>0}$ and $c\in\mathbb{Z}_{>0}$ such that for all prime numbers $p>3$ and any union $\mathcal{C}$ of orbits of the action of $\mathrm{GL}_2(\mathbb{F}_p)$ on itself,*

$$\left|\mathbf{P}(\mathcal{F}_H\subset\mathcal{C})-\frac{\#\mathcal{C}}{\#\mathrm{GL}_2(\mathbb{F}_p)}\right|\leqslant\frac{Cp^c}{\sqrt{p}}.$$

By Lemma 2.3, the proportion of matrices in $\mathrm{GL}_2(\mathbb{F}_p)$ that have 1 as an eigenvalue goes to zero as p goes to infinity. By Principle 3.11, we conclude that the probability that the number of rational points on J is no multiple of p approaches 1 as p goes to infinity, which justifies ignoring the influence of p-torsion. ■

As we did for Conjecture 2.5, we can give a numerical approximation for the number c_p from (10). It is contained in the interval $[0.63987, 0.79890]$ — the probability that the Jacobian variety of a randomly chosen hyperelliptic curve has a prime number of rational points is a bit higher than the probability that a randomly chosen elliptic curve has a prime number of rational points.

References

[AH03] J. Achter and J. Holden. Notes on an analogue of the fontaine-mazur conjecture. *Journal de Théorie des Nombres de Bordeaux*, 15:627–637, 2003.

[AM69] M. F. Atiyah and I. G. MacDonald. *Introduction to Commutative Algebra.* Addison-Wesley Series in Mathematics. Westview Press, Boulder (CO) and Oxford, 1969.

[CFA$^+$06] H. Cohen, G. Frey, R. Avanzi, C. Doche, T. Lange, K. Nguyen, and F. Vercauteren. *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* Discrete Mathematics and Its Applications. Chapman & Hall/CRC, Boca Raton, 2006.

[CFHS12] W. Castryck, A. Folsom, H. Hubrechts, and A. V. Sutherland. The probability that the number of points on the jacobian of a genus 2 curve is prime. *Proceedings of the London Mathematical Society*, 104, Issue 6:1235–1270, 2012.

[Cha97] N. Chavdarov. The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy. *Duke Mathematical Journal*, 87:151–180, 1997.

[Ful00] J. Fulman. A probabilistic approach to conjugacy classes in the finite symplectic and orthogonal groups. *Journal of Algebra*, 234:207–224, 2000.

[GM00] S. Galbraith and J. McKee. The probability that the number of points on an elliptic curve over a finite field is prime. *Journal of the London Mathematical Society*, 62:671–684, 2000.

[Gos06] M. De Gosson. *Symplectic Geometry and Quantum Mechanics*, volume 166 of *Operator Theory: Advances and Applications.* Birkhäuser Verlag, Basel, Boston, and Berlin, 2006.

[Har77] R. Hartshorne. *Algebraic Geometry*, volume 52 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1977.

[HPS08] J. Hoffstein, J. Pipher, and J. H. Silverman. *An Introduction to Mathematical Cryptography.* Undergraduate Texts in Mathematics. Springer-Verlag, New York, 2008.

[Hum72] J. E. Humphreys. *Introduction to Lie Algebras and Representation Theory*, volume 9 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1972.

[Hum95] J. E. Humphreys. *Conjugacy Classes in Semisimple Algebraic Groups*, volume 43 of *Mathematical Surveys and Monographs.* American Mathematical Society, Providence, 1995.

[Len87] H. Lenstra. Factoring integers with elliptic curves. *The Annals of Mathematics*, 126:649–673, 1987.

[Mer74] F. Mertens. Ein Beitrag zur analytischen Zahlentheorie. *Journal für die reine und angewandte Mathematik*, 78:46–62, 1874.

[Mum70] D. Mumford. *Abelian Varieties*, volume 5 of *Tata Institute of Fundamental Research Studies in Mathematics.* Oxford University Press, London, 1970.

[Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 2009.

[Sta17] The Stacks Project Authors. Stacks project. `http://stacks.math.columbia.edu`, 2017.