*Proc. London Math. Soc.* (3) 104 (2012) 1235–1270 
doi:10.1112/plms/pdr063

# The probability that the number of points on the Jacobian of a genus 2 curve is prime

Wouter Castryck, Amanda Folsom, Hendrik Hubrechts and Andrew V. Sutherland

Abstract

In 2000, Galbraith and McKee heuristically derived a formula that estimates the probability that a randomly chosen elliptic curve over a fixed finite prime field has a prime number of rational points. We show how their heuristics can be generalized to Jacobians of curves of higher genus. We then elaborate this in genus $g = 2$ and study various related issues, such as the probability of cyclicity and the probability of primality of the number of points on the curve itself. Finally, we discuss the asymptotic behavior for $g \to \infty$.

## 1. *Introduction and overview*

### 1.1. *The Galbraith–McKee conjecture: elliptic curves*

Galbraith and McKee [17] studied the probability that a randomly chosen elliptic curve over a finite prime field has a prime number of rational points. They conjectured the following. For a prime number $p > 3$, let $P_1(p)$ be the probability that a uniformly randomly chosen integer in the Hasse interval $[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$ is prime. Let $P_2(p)$ be the probability that the elliptic curve defined by $y^2 = x^3 + Ax + B$, for a uniformly randomly chosen pair $(A, B)$ in the set

$$\mathcal{H}_{AB} = \{(A, B) \in \mathbb{F}_p^2 | 4A^3 + 27B^2 \neq 0\},$$

has a prime number of rational points (including the point at infinity).

Conjecture 1 (Galbraith–McKee [17, Conjecture A]). Define

$$c_p = \frac{2}{3} \cdot \prod_{\ell > 2} \left(1 - \frac{1}{(\ell - 1)^2}\right) \cdot \prod_{\ell | p-1, \ell > 2} \left(1 + \frac{1}{(\ell + 1)(\ell - 2)}\right),$$

where the products are over all primes $\ell$ satisfying the stated conditions. Then

$$\lim_{p \to \infty} (P_2(p)/P_1(p) - c_p) = 0.$$

The constant $c_p$ lies between 0.44010 and 0.61514. In general, the conjecture predicts that elliptic curves are about half as likely to have prime orders as one might expect.

The study of the probability of primality is partly motivated by elliptic curve cryptography. For an elliptic curve over a finite field to be suitable as the underlying group for Diffie–Hellman key exchange, its number of rational points is preferably prime (although small cofactors are often tolerated). In practice, a 'good' elliptic curve is often found by repeatedly counting the number of rational points on randomly chosen elliptic curves, for example using the SEA

Received 22 January 2011; published online 6 February 2012.

2010 *Mathematics Subject Classification* 11N05, 11G10, 11G20.

The research of the first and the third author was financially supported by F.W.O.-Vlaanderen. The second author is grateful for the support of National Science Foundation grant DMS 1049553.

algorithm [31], until a prime number is hit. The above conjecture predicts that this process works slightly worse than one would naïvely assume.

Galbraith and McKee provided both experimental support and heuristic evidence in favor of Conjecture 1. Their main argument uses the Hurwitz–Kronecker class number formula, which counts bivariate quadratic forms up to equivalence. A second argument estimates the probability of primality by naïvely multiplying the expected probabilities of being coprime to $2, 3, 5, 7, 11, \ldots$ For elliptic curve orders, these expected probabilities were devised by Lenstra [25, Proposition 1.14]. When taking the quotient of the resulting estimates for $P_2(p)$ and $P_1(p)$, one exactly finds $c_p$. A reasoning of this kind had already been made by Koblitz [23, p. 160] in the dual setting where one fixes an elliptic curve over $\mathbb{Q}$ and reduces it modulo varying primes, a similar discussion on the case where one fixes a CM-curve of genus 2 over $\mathbb{Q}$ can be read in Weng's thesis [35, Section 5.2]. Galbraith and McKee called their second heuristics 'not very honest', however, due to subtleties reflected in Mertens' theorem. We will discuss these in Section 3.

### 1.2. *Genus 2 curves*

Nonetheless, and this may be thought of as an underlying meta-conjecture, these second heuristics work very well in practice, as is confirmed experimentally in Section 11. Moreover, they seem more flexible towards generalizing Conjecture 1 to Jacobians of curves of higher genus, which have also been proposed for use in cryptography. The required analogues of Lenstra's theorem are provided by a recursive formula due to Achter and Holden [3, Lemma 3.2], which we turn into a closed expression in Section 5.

In this article, we elaborate this for curves of genus 2, which is the most relevant case for cryptography. We derive the following conjecture. For a prime number $p > 2$, let $P_1(p)$ be the probability that a uniformly randomly chosen integer in the Hasse–Weil interval

$$[(\sqrt{p}-1)^4, (\sqrt{p}+1)^4]$$

is prime. Let $P_2(p)$ be the probability that the Jacobian of the genus 2 curve defined by $y^2 = f(x)$, for a randomly chosen polynomial $f(x)$ in the set

$$\mathcal{H}_6 = \{f(x) \in \mathbb{F}_p[x] | f(x) \text{ square-free of degree } 6\},$$

has a prime number of rational points.

Conjecture 2 (see Section 6). Define

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

where the products are over all primes $\ell$ satisfying the stated conditions. Then

$$\lim_{p\to\infty} (P_2(p)/P_1(p) - c_p) = 0.$$

We implicitly assume that $P_1(p) \neq 0$ for all $p$, which is an open problem in its own (see [8, Section 2.2] for a related discussion). The constant $c_p$ lies between 0.63987 and 0.79890. Summarizing, in genus 2, prime order Jacobians are also slightly disfavored, but to a lesser extent than in genus 1.

### 1.3. *Averaging over p*

By averaging $c_p$ over all primes $p$, it becomes meaningful to measure the prime-disfavoring behavior by a single constant. For elliptic curves, this gives the following lemma.

LEMMA 1 (see Section 3). *For each prime $p > 3$, let $c_p$ be as in Conjecture 1. Then*

$$\bar{c}_p = \lim_{n\to\infty} \frac{1}{\pi(n)} \sum_{3<p\leqslant n} c_p = \prod_{\ell} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell^2-1)(\ell-1)^2}\right) \approx 0.50517.$$

*Here, $\pi$ is the prime-counting function, and the product is over all primes $\ell$.*

This confirms a constant obtained by Koblitz [**23**, p. 160] and subsequently verified by Balog, Cojocaru and David [**5**, Theorem 1]. In genus 2, the average reads as follows.

LEMMA 2 (see Section 6). *For each prime $p > 2$, let $c_p$ be as in Conjecture 2. Then*

$$\bar{c}_p = \lim_{n\to\infty} \frac{1}{\pi(n)} \sum_{2<p\leqslant n} c_p = \prod_{\ell} \left(1 - \frac{\ell^6 - 2\ell^5 + 3\ell + 1}{(\ell^2-1)^2(\ell^2+1)(\ell-1)^2}\right) \approx 0.69464,$$

*where again the product is over all primes $\ell$.*

### 1.4. *Imposing a rational Weierstrass point*

Instead of using $\mathcal{H}_6$, we can choose $f(x)$ uniformly at random from the set

$$\mathcal{H}_5^{\mathrm{m}} = \{f(x) \in \mathbb{F}_p[x] | f(x) \text{ monic and square-free of degree } 5\}.$$

This situation matches better with common cryptographic practice. However, it alters the notion of taking a random genus 2 curve, since here one imposes the existence of a rational Weierstrass point. As before, for each prime $p > 2$, let $P_1(p)$ be the probability that a uniformly randomly chosen integer in the Hasse–Weil interval $[(\sqrt{p}-1)^4, (\sqrt{p}+1)^4]$ is prime, but now let $P_2(p)$ be the probability that a random genus 2 curve, in the above sense, has a Jacobian with a prime number of rational points.

CONJECTURE 3 (see Section 7). Let $c_p$ be as in Conjecture 2. Then

$$\lim_{p\to\infty} \left(P_2(p)/P_1(p) - \frac{9}{19} c_p\right) = 0.$$

The constant $\frac{9}{19}c_p$ lies between 0.30309 and 0.37843, so prime orders become dramatically less probable. This is entirely due to the fact that the probability of having rational 2-torsion increases from $\frac{26}{45}$ to $\frac{4}{5}$. In Section 7, we will illustrate why for odd $\ell$, the expected probability of having rational $\ell$-torsion is most likely unaffected.

Averaging $\frac{9}{19}c_p$ over all primes $p$ as in Section 1.3 gives approximately 0.32904 (that is, $\frac{9}{19}$ times the constant of Lemma 2).

### 1.5. *The number of points on the curve itself*

We can also estimate the probability that the number of rational points on the curve itself, rather than its Jacobian, is prime. For each prime $p > 2$ and with $f(x)$ chosen uniformly at random from $\mathcal{H}_6$, let $P_2(p)$ be the probability that the non-singular complete model of $y^2 = f(x)$ has a prime number of rational points. Let $P_1(p)$ be the probability that an integer, chosen uniformly at random from the Hasse–Weil interval

$$[p + 1 - 4\sqrt{p}, p + 1 + 4\sqrt{p}],$$

is prime. For $\ell \neq p$ prime, define

$$a_{\ell,p} := \#\{(x,y) \in \mathbb{F}_\ell^\times \times (\mathbb{F}_\ell^\times \backslash \{-p\}) \mid (x+y/x)(1+p/y) = p+1\},$$
$$\beta_{\ell,p} := (\ell-1)(\ell^5-\ell^3+2) - a_{\ell,p} - \begin{cases} (\ell^3-1) & \text{if } p \equiv -1 \bmod \ell, \\ 0 & \text{otherwise.} \end{cases}$$

Conjecture 4 (see Section 8). Define

$$c_p = \frac{38}{45} \prod_{\substack{\ell > 2 \\ \ell \neq p}} \frac{\ell \cdot \beta_{\ell,p}}{(\ell^4-1)(\ell^2-1)(\ell-1)},$$

where the product is over all primes satisfying the stated conditions. Then

$$\lim_{p\to\infty} (P_2(p)/P_1(p) - c_p) = 0.$$

The constant $c_p$ lies between 0.79605 and 0.86548, with an estimated average (in the sense of Section 1.3) of $\bar{c}_p \approx 0.83376$ . When switching to $\mathcal{H}_5^{\mathrm{m}}$ instead of $\mathcal{H}_6$, the leading factor $\frac{38}{45}$ should be replaced by $\frac{16}{15}$. The resulting constant $c_p$ lies between 1.00553 and 1.09323, with an estimated average of $\bar{c}_p \approx 1.05317$, so prime orders actually become slightly favoured.

### 1.6. *The probability of cyclicity*

Using similar heuristics, one can estimate for each prime $p > 2$ the probability $P(p,2)$ that the group of rational points on the Jacobian of the curve defined by $y^2 = f(x)$, with $f(x)$ chosen uniformly at random from $\mathcal{H}_6$, is cyclic. This is done by considering for each prime $\ell$ the corresponding probability for the $\ell$-torsion subgroup, and then taking the product.

For elliptic curves, one recovers a formula that was proven by Vlăduţ. Let $P(p,1)$ be the probability that the group of rational points on a randomly chosen elliptic curve over $\mathbb{F}_p$ (as in Section 1.1) is cyclic. Then we have the following theorem.

Theorem 1 (Vlăduţ [34, Theorem 6.1]). *For each prime $p$, define*

$$c_p = \prod_{\ell \mid p-1} \left(1 - \frac{1}{\ell(\ell^2-1)}\right),$$

*where the product is over all primes satisfying the stated condition. Then*

$$\lim_{p\to\infty} (P(p,1) - c_p) = 0.$$

The constant $c_p$ is contained in $[0.78816, 0.83334]$, with an average (in the sense of Section 1.3) of $\bar{c}_p \approx 0.81375$. In genus 2, the same reasoning gives the following conjecture.

Conjecture 5 (see Section 9). For each prime $p$, define

$$c_p = \frac{151}{180} \cdot \prod_{\ell > 2, \ell \nmid p-1} \left(1 - \frac{1}{\ell(\ell^2-1)(\ell-1)}\right) \cdot \prod_{\ell > 2, \ell \mid p-1} \frac{\ell^8 - \ell^6 - \ell^5 - \ell^4 + \ell^2 + \ell + 1}{\ell^2(\ell^4-1)(\ell^2-1)},$$

where the products are over all primes $\ell$ satisfying the stated conditions. Then

$$\lim_{p\to\infty} (P(p,2) - c_p) = 0.$$

The constant $c_p$ is contained in the interval $[0.79356, 0.81918]$, with an average value $\bar{c}_p \approx 0.80883$. If we replace $\mathcal{H}_6$ by $\mathcal{H}_5^{\mathrm{m}}$, then the leading factor should be replaced by $\frac{37}{60}$, in which case the constant $c_p$ is contained between 0.58335 and 0.60218, with an average value $\bar{c}_p \approx 0.59457$.

### 1.7. *Extension fields*

Fix a prime number $p$. Consider the alternative setup of finite fields $\mathbb{F}_{p^k}$ of growing extension degree $k$ over $\mathbb{F}_p$. For $g \in \{1, 2\}$, let $P_1(k, g)$ be the probability that a uniformly randomly chosen integer in the Hasse interval $[(\sqrt{p^k} - 1)^{2g}, (\sqrt{p^k} + 1)^{2g}]$ is prime. Let $P_2(k, g)$ be the probability that the Jacobian of the (hyper)elliptic curve defined by $y^2 + h(x)y = f(x)$, where the pair $(h, f)$ is chosen from

$$\mathcal{H}_{g+1,2g+2} = \{(f, h) \in \mathbb{F}_{p^k}[x] \times \mathbb{F}_{p^k}[x] | \deg h \leqslant g + 1, \deg f = 2g + 2, \\ y^2 + h(x)y = f(x) \text{ has geometric genus } g\}$$

uniformly at random, has a prime number of $\mathbb{F}_{p^k}$-rational points.

Then we have the following.

Conjecture 6 (see Section 10). Let

$$c_k = \mu_p \cdot \prod_{\ell>2} \left(1 - \frac{1}{(\ell - 1)^2}\right) \cdot \prod_{\ell | p^k - 1, \ell > 2} \left(1 + \frac{1}{(\ell + 1)(\ell - 2)}\right),$$

where the products are over all primes $\ell$ satisfying the stated conditions, and $\mu_p = 0$ if $p = 2$ versus $\mu_p = \frac{2}{3}$ if $p > 2$. Then

$$\lim_{k \to \infty} (P_2(k, 1)/P_1(k, 1) - c_k) = 0.$$

If $p > 2$, the formula for $c_k$ closely matches the formula from $c_p$ from Conjecture 1, with $p^k - 1$ in place of $p - 1$, and takes values between 0.44010 and 0.61514. For $p = 2$ we have $c_k = 0$. In genus 2, the estimate reads as follows.

Conjecture 7 (see Section 10). Let

$$c_k = \mu_p \cdot \prod_{\ell>2} \left(1 - \frac{\ell^2 - \ell - 1}{(\ell^2 - 1)(\ell - 1)^2}\right) \cdot \prod_{\ell | p^k - 1, \ell > 2} \left(1 + \frac{\ell^4 - \ell^3 - \ell - 2}{(\ell^3 - 2\ell^2 - \ell + 3)(\ell^2 + 1)(\ell + 1)}\right),$$

where the products are over all primes $\ell$ satisfying the stated conditions, and $\mu_p = \frac{2}{3}$ if $p = 2$ versus $\mu_p = \frac{38}{45}$ if $p > 2$. Then

$$\lim_{k \to \infty} (P_2(k, 2)/P_1(k, 2) - c_k) = 0.$$

Again for $p > 2$, the formula for $c_k$ matches the formula for $c_p$ in Conjecture 2 and takes values between 0.63987 and 0.79890. If $p = 2$, then $c_k$ lies between 0.50516 and 0.63071.

It is possible to average the above over $k$, where the result will depend on the multiplicative orders of $p$ modulo the various $\ell$. Also, one can adapt Conjectures 6 and 7, and in fact any of the conjectures stated above, to the mixed case of just considering finite fields $\mathbb{F}_q$ of growing cardinality.

### 1.8. *Asymptotics for growing genus*

Instead of elaborating similar, increasingly complicated formulas for higher genera $g$, we conclude with an analysis of the asymptotic behavior for $g \to \infty$. This may be of interest to people studying analogues of the Cohen–Lenstra heuristics [11, 24] in the case of function

fields, though we will not push this connection. Note that due to computational limitations, the conjectures below are no longer supported by experimental evidence and rely purely on the conjectured validity of our heuristic derivation.

For every prime number $p > 2$ and every integer $g \geqslant 1$, let $P_1(p, g)$ be the probability that a uniformly randomly chosen integer in the Hasse–Weil interval

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

is prime. Let $P_2(p, g)$ be the probability that the Jacobian of the genus $g$ curve defined by $y^2 = f(x)$, for a randomly chosen polynomial $f(x)$ in the set

$$\mathcal{H}_{2g+2} = \{f(x) \in \mathbb{F}_p[x] |\, f(x) \text{ square-free of degree } 2g + 2\},$$

has a prime number of rational points.

Then we have the following theorem.

THEOREM 2 (see Section 6). $\lim_{p,g\to\infty} P_2(p, g) = 0$.

Theorem 2 holds because the probability of having rational 2-torsion tends to 1 as $g \to \infty$. However, this is a hyperelliptic phenomenon. The limiting behavior becomes more interesting if instead one defines $P_2(p, g)$ as the probability that the Jacobian of a random genus $g$ curve over $\mathbb{F}_p$ (for example, chosen from the set

$$\mathcal{M}_g = \{\text{curves of genus } g \text{ over } \mathbb{F}_p\}/\cong_{\mathbb{F}_p}$$

uniformly at random, note that $\mathcal{M}_g$ is typically not well-understood) has a prime number of rational points. In this case, we expect the following conjecture.

CONJECTURE 8 (see Section 6). Define

$$c_p = \frac{1}{\prod_{j=2}^{\infty} \zeta(j)} \cdot \prod_{\ell | p-1} \prod_{j=1}^{\infty} \frac{\ell^{2j}}{\ell^{2j} - 1},$$

where $\zeta$ is Riemann's zeta function and the product is over all primes $\ell$ satisfying the stated condition. Then

$$\lim_{p,g\to\infty} (P_2(p, g)/P_1(p, g) - c_p) = 0.$$

Again, we implicitly assume that $P_1(p, g)$ is nowhere zero. The constant $c_p$ lies in the interval

$$\left[\frac{\prod_{j=1}^{\infty}(2^{2j}/(2^{2j} - 1))}{\prod_{j=2}^{\infty} \zeta(j)}, \frac{1}{\prod_{j=1}^{\infty} \zeta(2j + 1)}\right] \subset [0.63287, 0.79353].$$

In other words, the prime-disfavoring effect persists as the genus grows. It even becomes slightly more manifest than in genus 2. A more detailed analysis shows that the effect alternately strengthens and weakens as the genus becomes odd and even, respectively. As in Section 1.3, one can average $c_p$ over all primes $p > 2$, yielding a constant $\bar{c}_p \approx 0.68857$.

Similarly, for every prime number $p > 2$ and every integer $g \geqslant 1$, let $P(p, g)$ be the probability that the rational points of the Jacobian of the (hyper)elliptic curve $y^2 = f(x)$, with $f(x)$ picked from $\mathcal{H}_{2g+2}$ uniformly at random, constitute a cyclic group.

Then we have the following theorem.

THEOREM 3 (see Section 9). $\lim_{p,g\to\infty} P(p, g) = 0$.

Again, this is a hyperelliptic phenomenon due to 2-torsion issues. If instead we define $P(p,g)$ to be the probability that a curve chosen from $\mathcal{M}_g$ uniformly at random has a cyclic Jacobian, then we expect the following conjecture.

CONJECTURE 9 (see Section 9). Define

$$c_p = \frac{1}{\prod_{j=2}^{\infty}\zeta(j)} \cdot \prod_{\ell \mid p-1} \prod_{j=1}^{\infty} \frac{\ell^{2j}}{\ell^{2j}-1} \cdot \prod_{\ell \nmid p-1} \left(1+\frac{1}{\ell(\ell-1)}\right),$$

where $\zeta$ is Riemann's zeta function and the product is over all primes $\ell$ satisfying the stated conditions. Then

$$\lim_{p,g\to\infty} (P(p,g) - c_p) = 0.$$

Now the constant $c_p$ lies in the interval

$$\left[\frac{1}{\prod_{j=1}^{\infty}\zeta(2j+1)}, \frac{\prod_{j=1}^{\infty}(2^{2j}/(2^{2j}-1)\cdot\prod_{\ell>2}(1+1/\ell(\ell-1))}{\prod_{j=2}^{\infty}\zeta(j)}\right] \subset [0.79352, 0.82004],$$

with an average (in the sense of Section 1.3) of $\bar{c}_p \approx 0.80924$.

## 2. *Common notions of randomness*

By a randomly chosen (hyper)elliptic curve of genus $g \geqslant 1$ over a finite field $\mathbb{F}_q$ of odd characteristic, we will usually mean the non-singular complete model of a curve $y^2 = f(x)$, where $f$ is chosen from

$$\mathcal{H}_{2g+2} = \{f(x) \in \mathbb{F}_q[x] | f(x) \text{ is square-free and } \deg f = 2g+2\}$$

uniformly at random.

Alternatively, one could take the curve uniformly at random from

$$\mathcal{M}_g^{\mathrm{hyp}} = \{\text{(hyper)elliptic genus } g \text{ curves over } \mathbb{F}_q\}/\cong_{\mathbb{F}_q}.$$

This randomness notion may be preferred from a theoretical point of view. It is fundamentally different from our first, in the sense that the map

$$\mathcal{H}_{2g+2} \longrightarrow \mathcal{M}_g^{\mathrm{hyp}} : f \longmapsto [y^2 = f(x)]$$

is not uniform. For small $q$, it does not even need to be surjective. Therefore, the probability of having a certain geometric property may change when moving from one notion to the other. However, as $q$ gets bigger and bigger, the change becomes negligible. More precisely, for $q \to \infty$ ($g$ fixed), the proportion of elements of $\mathcal{M}_g^{\mathrm{hyp}}$ having $q(q^2-1)(q-1)/2$ pre-images in $\mathcal{H}_{2g+2}$ tends to 1. This can be elaborated following [**27**, Section 1]. Note that, despite the availability of a complete classification of (hyper)elliptic curves up to $\mathbb{F}_q$-isomorphism [**27**, Section 2], the set $\mathcal{M}_g^{\mathrm{hyp}}$ is quite cumbersome to work with.

Another setup, which is, for example, used in [**2**, Theorem 3.1], is to take $f$ uniformly at random from

$$\mathcal{H}_{2g+2}^{\mathrm{m}} = \{f(x) \in \mathbb{F}_q[x] |\ f(x) \text{ is monic, square-free and } \deg f = 2g+2\},$$

instead of $\mathcal{H}_{2g+2}$. Again, this is different from either of the above notions. For small $q$, there may exist curves having a model in $\mathcal{H}_{2g+2}$ that do not have a model in $\mathcal{H}_{2g+2}^{\mathrm{m}}$. But again, as $q \to \infty$ ($g$ fixed), the difference dissolves. Indeed, consider the set

$$\mathcal{S}_{2g+2} = \{(f,\alpha,\beta) \in \mathcal{H}_{2g+2} \times \mathbb{F}_q \times \mathbb{F}_q^{\times} | f(\alpha) = \beta^2\}.$$

Then we have a map

$$\mathcal{S}_{2g+2} \longrightarrow \mathcal{H}^{\mathrm{m}}_{2g+2} : (f, \alpha, \beta) \longmapsto \beta^{-2} x^{2g+2} f(1/x + \alpha),$$

which respects the isomorphism class of the corresponding curve, and which is onto and $q(q-1)$-to-1. Therefore, taking $f$ uniformly at random from $\mathcal{H}^{\mathrm{m}}_{2g+2}$ and using the $f$ of a uniformly randomly chosen $(f, \alpha, \beta) \in S_{2g+2}$ give rise to equivalent randomness notions. On the other hand, the map

$$\mathcal{S}_{2g+2} \longrightarrow \mathcal{H}_{2g+2} : (f, \alpha, \beta) \longmapsto f$$

is asymptotically uniform, since every $f \in \mathcal{H}_{2g+2}$ will have $q + O(\sqrt{q})$ pre-images by the Hasse–Weil bound. This proves the claim.

In Section 10, we will allow char $\mathbb{F}_q = 2$ and use curves of the form $y^2 + h(x)y = f(x)$ with $(f, h)$ chosen from

$$\mathcal{H}_{g+1,2g+2} = \{(f,h) \in \mathbb{F}_q[x] \times \mathbb{F}_q[x] | \deg h \leqslant g+1, \deg f = 2g+2, \\ y^2 + h(x)y = f(x) \text{ has geometric genus } g\}$$

uniformly at random. Again, it is easy to show that if $2 \nmid q$, the completing-the-square map $\mathcal{H}_{g+1,2g+2} \to \mathcal{H}_{2g+2}$ is essentially uniform.

In this article, we will always consider statistical behavior for $q \to \infty$. In particular, the validity of all statements below involving randomly chosen curves in the sense of $\mathcal{H}_{2g+2}$ is preserved when switching to either of the above alternatives, and vice versa. Some statements involve error terms, so in fact a more careful analysis is needed; we omit the details.

The picture does alter, however, when one takes $f$ uniformly at random from

$$\mathcal{H}_{2g+1} = \{f \in \mathbb{F}_q[x] | f(x) \text{ is square-free and } \deg f = 2g+1\}.$$

While this setting is often preferred in practice, this influences the story as soon as $g \geqslant 2$, since it induces the existence of a rational Weierstrass point. We will study this effect in detail for $g = 2$ in Section 7. On the other hand, writing

$$\mathcal{H}^{\mathrm{m}}_{2g+1} = \{f \in \mathbb{F}_q[x] | f(x) \text{ is monic, square-free and } \deg f = 2g+1\},$$

the geometry-preserving map

$$\mathcal{H}_{2g+1} \longrightarrow \mathcal{H}^{\mathrm{m}}_{2g+1} : f \longmapsto \alpha^{2g} f(x/\alpha) \quad (\text{where } \alpha = \mathrm{lc}(f))$$

is onto and $(q-1)$-to-1. Therefore, $\mathcal{H}_{2g+1}$ and $\mathcal{H}^{\mathrm{m}}_{2g+1}$ can be interchanged in any probability statement below. If $g = 1$ and moreover $3 \nmid q$, then this also accounts for

$$\mathcal{H}_{AB} = \{(A,B) \in \mathbb{F}_q^2 | 4A^3 + 27B^2 \neq 0\},$$

since the completing-the-cube map $\mathcal{H}_3 \to \mathcal{H}_{AB}$ is uniform.

Note that the sets $\mathcal{H}_{2g+2}, \mathcal{H}^{\mathrm{m}}_{2g+2}, \mathcal{H}_{g+1,2g+2}, \mathcal{H}_{2g+1}, \mathcal{H}^{\mathrm{m}}_{2g+1}, \mathcal{M}^{\mathrm{hyp}}_g$ and $\mathcal{H}_{AB}$ depend on $q$, while this is not included in the notation for the sake of readability. However, it will always be clear from the context which $q$ is used (it will typically be the prime number $p$ under consideration).

## 3. *Heuristic framework*

For prime numbers $p > 3$ and $\ell \neq p$, let $P(p, \ell)$ be the probability that the elliptic curve $E_{AB}$ defined by $y^2 = x^3 + Ax + B$, for a randomly chosen pair $(A, B)$ in the set $\mathcal{H}_{AB}$, has $\ell$ dividing its number of rational points (including the point at infinity).

THEOREM 4 (Lenstra). *There exist $C_1, C_2 \in \mathbb{R}_{>0}$, such that*

$$\left|P(p,\ell) - \frac{\ell}{\ell^2-1}\right| \leqslant C_1\ell/\sqrt{p} \quad \text{if } \ell \mid p-1 \quad \text{and}$$
$$\left|P(p,\ell) - \frac{1}{\ell-1}\right| \leqslant C_2\ell/\sqrt{p} \quad \text{if } \ell \nmid p-1$$

*for all pairs of distinct primes $p, \ell$ with $p > 3$.*

*Proof.* See [25, Proposition 1.14], to which we refer for explicit estimates of the $C_i$. □

We can now describe and discuss in more detail Galbraith and McKee's second heuristic argument supporting Conjecture 1. This is the type of reasoning behind all of our conjectures. Let $\ell(p)$ be the largest prime for which $\ell(p) \leqslant \sqrt{p}+1$. Let $n$ be an integer chosen uniformly at random from the Hasse interval, and let $\eta$ be $\#E_{AB}(\mathbb{F}_p)$. The aim was to estimate the ratio $P_2(p)/P_1(p)$, where $P_1(p)$ and $P_2(p)$ are as in Section 1.1. It can be rewritten as

$$\frac{P(2 \nmid \eta \text{ and } 3 \nmid \eta \text{ and } 5 \nmid \eta \text{ and } \ldots \text{ and } \ell(p) \nmid \eta)}{P(2 \nmid n \text{ and } 3 \nmid n \text{ and } 5 \nmid n \text{ and } \ldots \text{ and } \ell(p) \nmid n)}.$$

A first heuristic step is to approximate the above by

$$\frac{P(2 \nmid \eta)P(3 \nmid \eta)P(5 \nmid \eta)\ldots P(\ell(p) \nmid \eta)}{P(2 \nmid n)P(3 \nmid n)P(5 \nmid n)\ldots P(\ell(p) \nmid n)}.$$

A second heuristic step is then to estimate $P(\ell \nmid \eta)$ by

$$1 - \frac{1}{\ell-1} \text{ if } \ell \nmid p-1, \quad \text{and} \quad 1 - \frac{\ell}{\ell^2-1} \text{ if } \ell \mid p-1$$

(following Theorem 4), and $P(\ell \nmid n)$ by

$$1 - \frac{1}{\ell}.$$

One finds that

$$c_p' = \frac{\prod_{\ell \nmid p-1}(1-1/(\ell-1)) \cdot \prod_{\ell \mid p-1}(1-\ell/(\ell^2-1))}{\prod(1-1/\ell)},$$

where the products are over all primes $\ell \leqslant \ell(p)$ satisfying the stated conditions. Rearranging the expression shows that

$$\lim_{p\to\infty}(c_p - c_p') = 0,$$

where $c_p$ is the factor appearing in Conjecture 1.

It is tempting to validate the heuristics using an independence argument based on the Chinese Remainder Theorem (for $n$) and Howe's generalization of Lenstra's theorem (for $\eta$, see [19]). However, this is too naïve. By Mertens' theorem and the Prime Number Theorem, we have

$$\prod_{\ell \leqslant \sqrt{p}+1}\left(1 - \frac{1}{\ell}\right) \approx \frac{2e^{-\gamma}}{\log p} \approx 2e^{-\gamma}P_1(p).$$

Here, $\gamma \approx 0.57722$ is the Euler–Mascheroni constant ($2e^{-\gamma} \approx 1.12292$). For the heuristics to be justified, we should therefore have

$$\prod_{\ell \nmid p-1, \ell \leqslant \sqrt{p}+1}\left(1 - \frac{1}{\ell-1}\right) \cdot \prod_{\ell \mid p-1, \ell \leqslant \sqrt{p}+1}\left(1 - \frac{\ell}{\ell^2-1}\right) \approx 2e^{-\gamma}P_2(p).$$

With this in mind, the heuristics becomes very subtle: why would both naïve estimates be "equally wrong", in the words of Galbraith and McKee? We cannot give a satisfying answer, but note the following. (i) The constant $2e^{-\gamma}$, which reflects the ignored dependency between being divisible by distinct primes, is accumulated in the tail of the product, with respect to which $\eta$ and $n$ behave much alike. Stated alternatively, the 'local ratios' $P(\ell \nmid \eta)/P(\ell \nmid n)$ converge quickly to 1. By considering $c_p$ as the limiting product of these local ratios, rather than the ratio of two diverging products, one gets a more comfortable underpinning of the conjectured heuristics. (ii) The heuristics are supported by Galbraith and McKee's first argument in favor of Conjecture 1, which uses different methods (namely, the analytic Hurwitz–Kronecker class number formula). (iii) As far as computationally feasible, the conjectures that we obtain assuming this principle are confirmed by experiment in Section 11. (iv) The constant from Lemma 1 provably appeared in the dual setting of a fixed elliptic curve over $\mathbb{Q}$ reduced modulo varying primes $p$ (see [**5**, Theorem 1]).

We complete this section with a proof of Lemma 1.

*Proof of Lemma* 1. First, let us give a heuristic derivation. Let $\ell$ be a prime number. By Dirichlet's theorem, the proportion of primes $p$ satisfying $\ell \mid p-1$ is $1/(\ell-1)$. Averaging out Lenstra's result then gives

$$P(\ell \mid \eta) \approx \frac{1}{\ell-1}\frac{\ell}{\ell^2-1} + \frac{\ell-2}{\ell-1}\frac{1}{\ell-1} = \frac{\ell^2-2}{(\ell^2-1)(\ell-1)}.$$

So

$$\frac{P(\ell \nmid \eta)}{P(\ell \nmid n)} \approx 1 - \frac{\ell^2-\ell-1}{(\ell^2-1)(\ell-1)^2},$$

and applying the above heuristics yields the requested formula.

To make the argument precise, pick any $\varepsilon > 0$. It is easy to see that there is a uniform bound $L$ such that $|c_p^L - c_p| < \varepsilon/3$ for all $p$, where $c_p^L$ is defined as in Conjecture 1, but with the product restricted to primes $\ell$ that do not exceed $L$, and such that, similarly,

$$\left| \prod_{\ell \leqslant L} \left(1 - \frac{\ell^2-\ell-1}{(\ell^2-1)(\ell-1)^2}\right) - \prod_{\ell} \left(1 - \frac{\ell^2-\ell-1}{(\ell^2-1)(\ell-1)^2}\right) \right| < \varepsilon/3.$$

However, by the Dirichlet equidistribution of primes, and because we are taking finite products now, there is an $N$ such that $n \geqslant N$ implies

$$\left| \frac{1}{\pi(n)-2} \sum_{3<p\leqslant n} c_p^L - \prod_{\ell \leqslant L} \left(1 - \frac{\ell^2-\ell-1}{(\ell^2-1)(\ell-1)^2}\right) \right| < \varepsilon/3.$$

Combining the three bounds concludes the proof. □

## 4. *The random matrix model*

### 4.1. *The genus* 1 *case*

Lenstra's Theorem 4 can be understood from the following random matrix point of view. Let $\mathbb{F}_q$ be a finite field. Let $N$ be a positive integer coprime to $q$, and consider the set

$$\mathrm{GL}_2^{(q)}(\mathbb{Z}/(N)) = \{M \in \mathrm{GL}_2(\mathbb{Z}/(N)) | \det M = q\}.$$

This set is acted upon by $\mathrm{GL}_2(\mathbb{Z}/(N))$, by conjugation. To any elliptic curve $E/\mathbb{F}_q$, we can unambiguously associate an orbit of this action by collecting the matrices of $q$th power

Frobenius, considered as an endomorphism of the $\mathbb{Z}/(N)$-module $E[N]$ of $N$-torsion points, with respect to all possible bases. Denote this orbit by $\mathcal{F}_E$.

Take char $\mathbb{F}_q > 3$. For any union of orbits $\mathcal{C} \subset \mathrm{GL}_2^{(q)}(\mathbb{Z}/(N))$, let $P(\mathcal{F}_E \subset \mathcal{C})$ denote the probability that the orbit associated to the elliptic curve $y^2 = x^3 + Ax + B$, where $(A, B) \in \mathbb{F}_q$ is chosen from $\mathcal{H}_{AB}$ uniformly at random, is contained in $\mathcal{C}$.

PRINCIPLE 1. There exist $C_1 \in \mathbb{R}_{>0}$ and $c \in \mathbb{Z}_{>0}$, such that

$$\left| P(\mathcal{F}_E \subset \mathcal{C}) - \frac{\#\mathcal{C}}{\#GL_2^{(q)}(\mathbb{Z}/(N))} \right| \leqslant C_1 N^c / \sqrt{q}$$

for all choices of $q$, $N$ and $\mathcal{C}$ as above.

We use the word 'Principle', because, to our knowledge, no complete proof of this statement has been published in the literature. Nevertheless, it is commonly accepted and extensively confirmed by experiment. It is generally believed to follow from the work of Katz and Sarnak [**20**, Theorem 9.7.13]. A strategy of proof was communicated to us by Katz, and essentially matches with the approach of Achter [**2**, Theorem 3.1], who proved Principle 1 under certain mild restrictions on $q$ and $N$ (using $c = 3$). However, a more classically flavored proof of Principle 1 can be obtained by applying Chebotarev's density theorem [**13**, Proposition 6.4.8] to the function field extension $\mathbb{F}_q(j) \subset \mathbb{F}_q(\zeta_N)(j) \subset \mathbb{F}_q(\zeta_N)(X(N))$, where $\zeta_N$ is a primitive $N$th root of unity, and the latter extension corresponds to the modular cover $X(N) \to X(1)$, which is known to be defined over $\mathbb{F}_q(\zeta_N)$. This approach has recently been elaborated in a preprint of Castryck and Hubrechts [9].

Principle 1 indeed allows one to rediscover the asymptotics of Theorem 4, by counting the matrices $M \in \mathrm{GL}_2^{(p)}(\mathbb{F}_\ell)$ satisfying $p + 1 - \mathrm{Tr}(M) = 0$. We leave this as an exercise.

### 4.2. *The general case*

Let $\mathbb{F}_q$ and $N$ be as before, and let $\bar{\mathbb{F}}_q$ be an algebraic closure of $\mathbb{F}_q$. Let $C/\mathbb{F}_q$ be a complete non-singular curve of genus $g \geqslant 1$ and denote by $A = \mathrm{Jac}(C)$ its Jacobian. Then $q$th power Frobenius defines an endomorphism of the $2g$-dimensional $\mathbb{Z}/(N)$-module $A[N]$ of $N$-torsion points on $A$. Instead of considering all bases, we can make a more canonical choice by restricting to symplectic bases. We briefly review how this works.

We employ the following notation and terminology. For any $n \in \mathbb{N}$, $\mathbb{I}_n$ denotes the $n \times n$ identity matrix, and $\Omega$ denotes the $2g \times 2g$ matrix

$$\begin{pmatrix} 0 & \mathbb{I}_g \\ -\mathbb{I}_g & 0 \end{pmatrix}.$$

The group

$$\mathrm{Sp}_{2g}(\mathbb{Z}/(N)) = \{M \in \mathrm{GL}_{2g}(\mathbb{Z}/(N)) | {}^t M \Omega M = \Omega\}$$

is called the group of symplectic $2g \times 2g$ matrices, and

$$\mathrm{GSp}_{2g}(\mathbb{Z}/(N)) = \{M \in \mathrm{GL}_{2g}(\mathbb{Z}/(N)) | \exists\, d \in \mathbb{Z}/(N) \text{ such that } {}^t M \Omega M = d\Omega\},$$

is referred to as the group of symplectic similitudes. It is naturally partitioned into the sets

$$\mathrm{GSp}_{2g}^{(d)}(\mathbb{Z}/(N)) = \{M \in \mathrm{GL}_{2g}(\mathbb{Z}/(N)) | {}^t M \Omega M = d\Omega\},$$

with $d$ ranging over $(\mathbb{Z}/(N))^\times$. An element of $\mathrm{GSp}_{2g}^{(d)}(\mathbb{Z}/(N))$ is called $d$-symplectic. Note that 1-symplectic and symplectic are synonymous. A classical trick using the Pfaffian shows that the determinant of a symplectic matrix is 1. Hence the determinant of a $d$-symplectic matrix is $d^g$.

Symplectic matrices pop up in the study of skew-symmetric, non-degenerate bilinear pairings on, in our case, $2g$-dimensional $(\mathbb{Z}/(N))$-modules. Such pairings are often called symplectic forms. For any choice of basis, one can consider the standard symplectic form $\langle\cdot,\cdot\rangle$, defined by the rule

$$\langle v, w\rangle = {}^t v \Omega w.$$

Given any symplectic form, one can always choose a basis with respect to which it becomes the standard symplectic form: such a basis is called a symplectic basis or a Darboux basis. If one switches between two symplectic bases corresponding to the same symplectic form, the matrix of base change is symplectic, and conversely.

Now for each primitive $N$th root of unity $\zeta_N \in \bar{\mathbb{F}}_q$, the Weil pairing

$$e_N : A[N] \times A[N] \longrightarrow \langle\zeta_N\rangle,$$

when composed with the (non-canonical) map

$$\langle\zeta_N\rangle \longrightarrow \mathbb{Z}/(N) : \zeta_N^i \longmapsto i,$$

is a skew-symmetric and non-degenerate bilinear pairing on $A[N]$. A corresponding symplectic basis $P_1, \ldots, P_g, Q_1, \ldots, Q_g$ is characterized by the properties

$$e_N(P_i, Q_j) = \zeta_N^{\delta_{ij}}, \quad e_N(P_i, P_j) = e_N(Q_i, Q_j) = 1$$

for all $i, j \in \{1, \ldots, g\}$, where $\delta_{ij}$ is the Kronecker symbol. Because of the $\mathrm{Gal}(\bar{\mathbb{F}}_q, \mathbb{F}_q)$-invariance of the Weil pairing, one has that

$$e_N(P^\sigma, Q^\sigma) = e_N(P, Q)^q,$$

where $P$ and $Q$ are arbitrary points of $A[N]$ and $\sigma$ is $q$th power Frobenius. Then bilinearity implies that the matrix $F$ of $\sigma$ with respect to $P_1, \ldots, P_g, Q_1, \ldots, Q_g$ satisfies

$${}^t F \Omega F = q\Omega,$$

that is, $F$ is $q$-symplectic.

As mentioned above, a different choice of symplectic basis yields a matrix obtained from $F$ by $\mathrm{Sp}_{2g}(\mathbb{Z}/(N))$-conjugation. Next, if $\zeta_N$ is replaced by another $N$th root of unity $\zeta_N^j$, $j \in (\mathbb{Z}/(N))^\times$, then $P_1, \ldots, P_g, [j]Q_1, \ldots, [j]Q_g$ is a symplectic basis, and the matrix of Frobenius is $d_j F d_j^{-1}$, where

$$d_j = \begin{pmatrix} \mathbb{I}_g & 0 \\ 0 & j\mathbb{I}_g \end{pmatrix}.$$

Since $\mathrm{Sp}_{2g}(\mathbb{Z}/(N))$ and the matrices $d_j$ generate $\mathrm{GSp}_{2g}(\mathbb{Z}/(N))$, we conclude that we can unambiguously associate to $C$ an orbit of $\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/(N))$ under $\mathrm{GSp}_{2g}(\mathbb{Z}/(N))$-conjugation.

We are now ready to formulate the hyperelliptic curve analogue of Principle 1. Let char $\mathbb{F}_q > 2$ and $g \geqslant 1$. For any union of $\mathrm{GSp}_{2g}(\mathbb{Z}/(N))$-orbits $\mathcal{C} \subset \mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/(N))$, let $P(\mathcal{F}_f \subset \mathcal{C})$ denote the probability that the orbit associated to the complete non-singular model of the (hyper)elliptic curve $y^2 = f(x)$, where $f(x) \in \mathbb{F}_q[x]$ is chosen from $\mathcal{H}_{2g+2}$ uniformly at random, is contained in $\mathcal{C}$.

PRINCIPLE 2. There exist $C_1 \in \mathbb{R}_{>0}$ and $c \in \mathbb{Z}_{>0}$, such that

$$\left| P(\mathcal{F}_f \subset \mathcal{C}) - \frac{\#\mathcal{C}}{\#\mathrm{GSp}_{2g}^{(q)}(\mathbb{Z}/(N))} \right| \leqslant C_1 N^c / \sqrt{q}$$

for all choices of $q$, $N$ and $\mathcal{C}$ as above, provided that $N$ is odd as soon as $g > 2$.

The condition $N$ odd is due to the fact that we restrict to hyperelliptic curves, which as soon as $g > 2$ behave non-randomly with respect to 2-torsion (see Section 6). If instead we considered Jacobians of arbitrary curves (for example, in the sense of Section 1.8), we expect that this condition could be dropped.

Again we use the word 'Principle', because no complete proof of this statement has appeared in the literature to date. But again, this presumably follows from the work of Katz and Sarnak [**20**, Theorem 9.7.13], as elaborated by Achter [**2**, Theorem 3.1] under mild restrictions on $q$ and $N$. In his case, the exponent reads $c = 2g^2 + g$. Achter's result is sufficiently general for many of our needs below. In particular, it is sufficient for generalizing Theorem 4 to (hyper)elliptic curves of arbitrary genus $g \geqslant 1$, which is done in Section 6. Also note that Achter uses $\mathcal{H}^{\mathrm{m}}_{2g+2}$ rather than $\mathcal{H}_{2g+2}$.

## 5. *Counting matrices with eigenvalue* 1

For use in Sections 6 and 9, we study the following general question: given a prime power $q$, a prime $\ell \nmid q$, an integer $g \geqslant 0$ and $d \in \{0, \dots, 2g\}$, what is the proportion $\mathfrak{P}(q, \ell, g, d)$ of matrices in $\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)$ for which the eigenspace for eigenvalue 1 is $d$-dimensional? Lemma 3 transfers this question to the classical groups $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ and $\mathrm{GL}_g(\mathbb{F}_\ell)$. Let $\mathfrak{P}_{\mathrm{Sp}}(\ell, g, d)$ be the proportion of matrices in $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ having a $d$-dimensional eigenspace for eigenvalue 1, and let $\mathfrak{P}_{\mathrm{GL}}(\ell, g, d)$ be the corresponding proportion for the general linear group $\mathrm{GL}_g(\mathbb{F}_\ell)$, where of course $\mathfrak{P}_{\mathrm{GL}}(\ell, g, d) = 0$ as soon as $d > g$. We include $g = 0$ because of the recursive nature of the arguments below. In this, we assume that $\mathrm{GSp}_0^{(q)}(\mathbb{F}_\ell) = \mathrm{Sp}_0(\mathbb{F}_\ell) = \mathrm{GL}_0(\mathbb{F}_\ell)$ contains a unique matrix and that its 1-eigenspace is 0-dimensional. In particular, $\mathfrak{P}(q, \ell, 0, 0) = \mathfrak{P}_{\mathrm{Sp}}(\ell, 0, 0) = \mathfrak{P}_{\mathrm{GL}}(\ell, 0, 0)$ is understood to be 1.

LEMMA 3. *If* $q \equiv 1 \bmod \ell$, *then* $\mathfrak{P}(q, \ell, g, d) = \mathfrak{P}_{\mathrm{Sp}}(\ell, g, d)$. *If* $q \not\equiv 1 \bmod \ell$, *then* $\mathfrak{P}(q, \ell, g, d) = \mathfrak{P}_{\mathrm{GL}}(\ell, g, d)$.

*Proof.* The first statement is a tautology. So, assume that $q \not\equiv 1 \bmod \ell$. We follow ideas of Achter and Holden [**3**, Lemma 3.1], which in turn build upon work of Chavdarov [**10**].

First, for $r = 0, \dots, g$, let $S(q, \ell, r, d)$ be the subset of $\mathrm{GSp}_{2r}^{(q)}(\mathbb{F}_\ell)$ consisting of those matrices having characteristic polynomial $(x-1)^r(x-q)^r$ and whose 1-eigenspace has dimension $d$. Similarly, let $S_{\mathrm{GL}}(\ell, r, d)$ be the subset of $\mathrm{GL}_r(\mathbb{F}_\ell)$ consisting of the matrices having characteristic polynomial $(x-1)^r$ and whose 1-eigenspace has dimension $d$.

We will prove that

$$\#S(q, \ell, r, d) = \frac{\#\mathrm{Sp}_{2r}(\mathbb{F}_\ell)}{\#\mathrm{GL}_r(\mathbb{F}_\ell)} \cdot \#S_{\mathrm{GL}}(\ell, r, d). \tag{1}$$

By Jordan–Chevalley decomposition, every element $B \in S(q, \ell, r, d)$ can be uniquely written as the commuting product of a semisimple matrix $B_s$ and a unipotent matrix $B_u$. Necessarily, $B_s \in \mathrm{GSp}_{2r}^{(q)}(\mathbb{F}_\ell)$ has as characteristic polynomial $(x-1)^r(x-q)^r$ and $B_u \in \mathrm{Sp}_{2r}(\mathbb{F}_\ell)$ has as characteristic polynomial $(x-1)^{2r}$. By [**10**, Lemma 3.4], two such matrices $B_s$ must be conjugated by an element of $\mathrm{Sp}_{2r}(\mathbb{F}_\ell)$. It follows that for fixed $B_s$, the number of

corresponding instances of $B$ in $S(q,\ell,r,d)$ is always the same. Since one instance of $B_s$ is $\mathrm{diag}(1,1,\ldots,1,q,q,\ldots,q)$, whose centralizer in $\mathrm{Sp}_{2r}(\mathbb{F}_\ell)$ equals

$$\left\{ \begin{pmatrix} M & 0 \\ 0 & {}^t(M^{-1}) \end{pmatrix} \middle| \, M \in \mathrm{GL}_r(\mathbb{F}_\ell) \right\},$$

the number of possibilities for $B_s$ is $(\#\mathrm{Sp}_{2r}(\mathbb{F}_\ell))/(\#\mathrm{GL}_r(\mathbb{F}_\ell))$, and for each $B_s$ there are $S_{\mathrm{GL}}(\ell,r,d)$ appropriate choices for $B_u$. The claim follows.

Now, let $T(q,\ell,g,d)$ be the set of matrices of $\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)$ having a $d$-dimensional 1-eigenspace, thus $\#T(q,\ell,g,d) = \mathfrak{P}(q,\ell,g,d) \cdot \#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$. We will count the elements $M \in T(q,\ell,g,d)$ separately for each value of $r$, the order of vanishing at 1 of the characteristic polynomial $f_M$ of $M$. To $M$, one can associate a decomposition of the standard symplectic space $\mathbb{F}_\ell^{2g}, \langle\cdot,\cdot\rangle$ of the form $U_{2r} \oplus V_{2(g-r)}$, where $U_{2r}$ and $V_{2(g-r)}$ are $M$-invariant symplectic subspaces of dimensions $2r$ and $2(g-r)$, respectively, satisfying $f_{M|_{U_{2r}}} = (x-1)^r(x-q)^r$ and $f_{M|_{V_{2(g-r)}}}(1) \neq 0$. Then

$$\#T(q,\ell,g,d) = \sum_{r=0}^{g} \frac{\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)}{\#\mathrm{Sp}_{2r}(\mathbb{F}_\ell) \cdot \#\mathrm{Sp}_{2(g-r)}(\mathbb{F}_\ell)} \cdot \#S(q,\ell,r,d) \cdot \#T(q,\ell,g-r,0),$$

where the first factor corresponds to the number of ways of decomposing $\mathbb{F}_\ell^{2g}, \langle\cdot,\cdot\rangle$, the second factor counts the number of possible actions of $M$ on $U_{2r}$ and the third factor counts the number of actions of $M$ on $V_{2(g-r)}$. We conclude that

$$\mathfrak{P}(q,\ell,g,d) = \sum_{r=0}^{g} \frac{\#S(q,\ell,r,d)}{\#\mathrm{Sp}_{2r}(\mathbb{F}_\ell)} \cdot \mathfrak{P}(q,\ell,g-r,0). \tag{2}$$

Along with

$$\sum_{d=0}^{g} \mathfrak{P}(q,\ell,g,d) = 1, \tag{3}$$

one sees that, given the values $\#S(q,\ell,r,d)$, the recursive equation (2) determines all $\mathfrak{P}(q,\ell,g,d)$ by induction on $g$: first one determines $\mathfrak{P}(q,\ell,g,1),\ldots,\mathfrak{P}(q,\ell,g,g)$, during which one should use that $\#S(q,\ell,0,d) = 0$ as soon as $d > 0$, and then one uses (3) to obtain $\mathfrak{P}(q,\ell,g,0)$.

The statement then follows by noting that one similarly has

$$\mathfrak{P}_{\mathrm{GL}}(\ell,g,d) = \sum_{r=0}^{g} \frac{\#S_{\mathrm{GL}}(\ell,r,d)}{\#\mathrm{GL}_r(\mathbb{F}_\ell)} \cdot \mathfrak{P}_{\mathrm{GL}}(\ell,g-r,0),$$

along with the same initial conditions. Thus by (1), the probabilities $\mathfrak{P}(q,\ell,g,d)$ and $\mathfrak{P}_{\mathrm{GL}}(\ell,g,d)$ are solutions to the same recursive equation. By uniqueness, they must coincide. □

Now for the classical groups $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ and $\mathrm{GL}_g(\mathbb{F}_\ell)$, these proportions have been computed before. Parts of the following result have been (re)discovered by several people (see, for example, [**1**, **11**]), but the first to obtain closed formulas for both $\mathfrak{P}_{\mathrm{Sp}}(\ell,g,d)$ and $\mathfrak{P}_{\mathrm{GL}}(\ell,g,d)$ seem to be Rudvalis and Shinoda, in an unpublished work of 1988 [**30**] that was reported upon by Fulman [**14**, **15**] and, more recently, Lengler [**24**] and Malle [**26**].

THEOREM 5. *One has*

$$\mathfrak{P}_{\mathrm{GL}}(\ell,g,d)=\frac{1}{\#\mathrm{GL}_d(\mathbb{F}_\ell)}\cdot\sum_{j=0}^{g-d}\frac{(-1)^j\ell^{(j^2-j)/2}}{\ell^{dj}\cdot\#\mathrm{GL}_j(\mathbb{F}_\ell)},$$

$$\lim_{g\to\infty}\mathfrak{P}_{\mathrm{GL}}(\ell,g,d)=\frac{\ell^{-d^2}}{\prod_{j=1}^{d}(1-\ell^{-j})^2}\cdot\prod_{j=1}^{\infty}(1-\ell^{-j}),$$

$$\mathfrak{P}_{\mathrm{Sp}}(\ell,g,d)=\frac{1}{\#\mathrm{Sp}_{2k}(\mathbb{F}_\ell)}\cdot\sum_{j=0}^{g-k}\frac{(-1)^j\ell^{j^2+j}}{\ell^{2jk}\cdot\#\mathrm{Sp}_{2j}(\mathbb{F}_\ell)}\quad\text{if } d=2k \text{ is even},$$

$$\mathfrak{P}_{\mathrm{Sp}}(\ell,g,d)=\frac{1}{\ell^{2k+1}\cdot\#\mathrm{Sp}_{2k}(\mathbb{F}_\ell)}\sum_{j=0}^{g-k-1}\frac{(-1)^j\ell^{j^2+j}}{\ell^{2j(k+1)}\cdot\#\mathrm{Sp}_{2j}(\mathbb{F}_\ell)}\quad\text{if } d=2k+1 \text{ is odd},$$

$$\lim_{g\to\infty}\mathfrak{P}_{\mathrm{Sp}}(\ell,g,d)=\frac{\ell^{-d(d+1)/2}}{\prod_{j=1}^{d}(1-\ell^{-j})}\cdot\prod_{j=1}^{\infty}(1+\ell^{-j})^{-1}.$$

*Proof.* Proofs can be found in [14, Theorem 6] (for everything on the general linear group), and in [15, Corollary 1] (for the closed formulas for $\mathfrak{P}_{\mathrm{Sp}}(\ell,g,d)$) and [26, Proposition 3.1] (for the limit of the latter). The proofs of Fulman [14, 15] use the cycle index method, for which, in the symplectic case, the author assumes that $\ell$ is odd. However, in the meantime, the required theory on cycle indices has been extended to arbitrary characteristic [16]. The original proof of Rudvalis and Shinoda [30] uses integer partitions and works in full generality. □

Along with the well-known identities

$$\#\mathrm{GL}_g(\mathbb{F}_\ell)=\ell^{(g^2-g)/2}\prod_{j=1}^{g}(\ell^j-1)\quad\text{and}\quad\#\mathrm{Sp}_{2g}(\mathbb{F}_\ell)=\ell^{g^2}\prod_{j=1}^{g}(\ell^{2j}-1)\tag{4}$$

(see, for example, [22, Formula (2.9) and Theorem 3.2]), Lemma 3 and Theorem 5 yield explicit formulas for each $\mathfrak{P}(q,\ell,g,d)$.

Since the work of Rudvalis and Shinoda cannot be easily accessed, for the sake of self-containedness, we include an independent computation of $\mathfrak{P}(q,\ell,g,d)$ for the case where $d=0$. For the purposes of this article, this is the most prominent case, as we will see in Section 6. At the end of this section, we will study the convergence behavior for $g\to\infty$ in more detail.

It is convenient to consider instead $\mathfrak{Q}(q,\ell,g)=1-\mathfrak{P}(q,\ell,g,0)$, the proportion of matrices of $\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)$ for which 1 does appear as an eigenvalue. We prove the following theorem.

THEOREM 6. *With notation as above, for $g\geqslant 0$, we have*

$$\mathfrak{Q}(q,\ell,g)=\begin{cases}-\displaystyle\sum_{r=1}^{g}\ell^r\prod_{j=1}^{r}(1-\ell^{2j})^{-1} & \text{if } \ell\mid q-1,\\ -\displaystyle\sum_{r=1}^{g}\prod_{j=1}^{r}(1-\ell^{j})^{-1} & \text{if } \ell\nmid q-1.\end{cases}\tag{5}$$

*Proof.* Our starting point is the following recursion formula due to Achter and Holden [3, Lemma 3.2], the proof of which was our source of inspiration for Lemma 3: one has

$$\mathfrak{Q}(q,\ell,g)=\sum_{r=1}^{g}\frac{S(q,\ell,r)}{\#\mathrm{Sp}_{2r}(\mathbb{F}_\ell)}(1-\mathfrak{Q}(q,\ell,g-r)),$$

where

$$S(q,\ell,r) = \begin{cases} \ell^{2r^2} & \text{if } \ell \mid q-1, \\ \ell^{r^2-r}\frac{\#\mathrm{Sp}_{2r}(\mathbb{F}_\ell)}{\#\mathrm{GL}_r(\mathbb{F}_\ell)} & \text{if } \ell \nmid q-1 \end{cases}$$

and $\mathfrak{Q}(q,\ell,0) = 0$. Clearly, this determines $\mathfrak{Q}(q,\ell,g)$ uniquely for all $g$. Using (4), this can be rewritten as

$$\mathfrak{Q}(q,\ell,g) = \begin{cases} \displaystyle\sum_{r=1}^{g} \ell^{r^2}(1-\mathfrak{Q}(q,\ell,g-r))\prod_{j=1}^{r}(\ell^{2j}-1)^{-1} & \text{if } \ell \mid q-1, \\ \displaystyle\sum_{r=1}^{g} \ell^{(r^2-r)/2}(1-\mathfrak{Q}(q,\ell,g-r))\prod_{j=1}^{r}(\ell^{j}-1)^{-1} & \text{if } \ell \nmid q-1. \end{cases} \tag{6}$$

We will prove by induction on $g$ that (5) indeed solves the recursion. We only consider the case $\ell \nmid q-1$ (the necessary adaptations for the case $\ell \mid q-1$ are straightforward). Define $P_r := \prod_{j=1}^{r}(1-\ell^j)^{-1}$ for $r \geqslant 0$. After rearranging terms and using the induction hypothesis for $g-1$, one finds with some trivial computations that it suffices to prove

$$-P_g = \ell^{g(g-1)/2}\cdot(-1)^g \cdot P_g + \sum_{r=1}^{g-1} \ell^{r(r-1)/2}\cdot(-1)^r \cdot P_r \cdot P_{g-r}. \tag{7}$$

We are left with showing that with

$$S_k := \sum_{r=0}^{k} T_r \quad \text{where } T_r := (-1)^r \cdot \ell^{r(r-1)/2}\cdot P_r \cdot P_{g-r},$$

we have $S_g = 0$. This, however, follows from the observation that

$$S_k = (-1)^k \cdot \ell^{k(k+1)/2}\cdot P_k \cdot P_{g-k}\cdot(1-\ell^g)^{-1}\cdot(1-\ell^{g-k}),$$

which can be shown easily using induction on $k$. Indeed, then $S_g = 0$, because its last factor is zero. □

Next, we study the limiting behavior of $\mathfrak{Q}(q,\ell,g)$ as $g \to \infty$. Define

$$\mathcal{E}(q,\ell,g) := \begin{cases} 1-\displaystyle\prod_{j=1}^{\infty}\left(1+\frac{1}{\ell^j}\right)^{-1} - \mathfrak{Q}(q,\ell,g) & \text{if } \ell \mid q-1, \\ 1-\displaystyle\prod_{j=1}^{\infty}\left(1-\frac{1}{\ell^j}\right) - \mathfrak{Q}(q,\ell,g) & \text{if } \ell \nmid q-1. \end{cases}$$

Then we have the following theorem.

THEOREM 7. *With notation as above, we have*

$$\lim_{g\to\infty} \mathfrak{Q}(q,\ell,g) = \begin{cases} 1-\displaystyle\prod_{j=1}^{\infty}\left(1+\frac{1}{\ell^j}\right)^{-1} & \text{if } \ell \mid q-1, \\ 1-\displaystyle\prod_{j=1}^{\infty}\left(1-\frac{1}{\ell^j}\right) & \text{if } \ell \nmid q-1. \end{cases}$$

*Moreover, this convergence is alternating, that is,*

$$\lim_{g\to\infty} \mathcal{E}(q,\ell,g) = 0 \quad \text{and} \quad (-1)^g\mathcal{E}(q,\ell,g) > 0$$

*for each* $g \geqslant 0$.

*Proof.* We make use of the well-known "$q$-series" identity

$$\sum_{n\geqslant 0} \frac{z^{n(n-1)/2}x^n}{(z;z)_n} = \prod_{k=0}^{\infty}(1+xz^k) \tag{8}$$

(see, for example [**18**, II.2]). Here $(a;z)_n := \prod_{j=0}^{n-1}(1-az^j)$ is the Pochhammer symbol. Although we refer to identities from the theory of "$q$-series", we use the variable $z$ here instead, in order to distinguish with the prime power $q$ used previously. It is not hard to show that (5) is equivalent to

$$\mathfrak{Q}(q,\ell,g) = \begin{cases} -\sum_{r=1}^{g} \frac{z^{r^2}(-1)^r}{(z^2;z^2)_r} & \text{if } \ell \mid q-1, \\ -\sum_{r=1}^{g} \frac{z^{r(r+1)/2}(-1)^r}{(z;z)_r} & \text{if } \ell \nmid q-1, \end{cases}$$

where $z = \ell^{-1}$.

If $\ell \nmid q-1$, it immediately follows that

$$\lim_{g\to\infty} \mathfrak{Q}(z,\ell,g) = -\sum_{r=1}^{\infty} \frac{z^{r(r+1)/2}(-1)^r}{(z;z)_r} = 1 - \prod_{n=1}^{\infty}(1-z^n) = 1 - \prod_{n=1}^{\infty}\left(1-\frac{1}{\ell^n}\right), \tag{9}$$

where we used (8) with $x=-z$. To show the convergence is alternating, we have by definition of $\mathcal{E}(q,\ell,g)$ and Theorem 6, that

$$\mathcal{E}(q,\ell,g) = -\sum_{r=g+1}^{\infty}\prod_{j=1}^{r}(1-\ell^j)^{-1}, \tag{10}$$

which tends to 0 as $g\to\infty$. We observe that consecutive summands in (10) add to

$$-\frac{(-1)^r}{\prod_{j=1}^{r}(\ell^j-1)} - \frac{(-1)^{r+1}}{\prod_{j=1}^{r+1}(\ell^j-1)} = \frac{(-1)^{r+1}(\ell^{r+1}-2)}{\prod_{j=1}^{r+1}(\ell^j-1)}. \tag{11}$$

Now $r\geqslant 1$ and $\ell$ is prime so that (11) is positive if and only if $(-1)^{r+1}>0$, which holds if and only if $r$ is odd. The sum in (10) begins with an odd index if and only if $g$ is even or $g=0$, which shows that $(-1)^g\mathcal{E}(q,\ell,g)>0$.

If $\ell \mid q-1$, then we conclude similarly that

$$\begin{aligned}\lim_{g\to\infty} \mathfrak{Q}(q,\ell,g) &= -\sum_{r=1}^{\infty}\frac{z^{r^2}(-1)^r}{(z^2;z^2)_r} = 1-\prod_{n=1}^{\infty}(1-z^{2n-1}) \\ &= 1-\prod_{n=1}^{\infty}(1+z^n)^{-1} = 1-\prod_{n=1}^{\infty}\left(1+\frac{1}{\ell^n}\right)^{-1},\end{aligned}$$

by replacing $z$ by $z^2$, and setting $x=-z$. To show the convergence is alternating, we have by definition of $\mathcal{E}(q,\ell,g)$ and Theorem 6 that

$$\mathcal{E}(q,\ell,g) = -\sum_{r=g+1}^{\infty}\ell^r\prod_{j=1}^{r}(1-\ell^{2j})^{-1}, \tag{12}$$

which tends to 0 as $g\to\infty$. We observe that consecutive summands in (12) add to

$$-\frac{(-\ell)^r}{\prod_{j=1}^{r}(\ell^{2j}-1)} - \frac{(-\ell)^{r+1}}{\prod_{j=1}^{r+1}(\ell^{2j}-1)} = \frac{(-\ell)^{r+1}(\ell^{2r+2}-1-\ell)}{\prod_{j=1}^{r+1}(\ell^{2j}-1)}. \tag{13}$$

Again because $r\geqslant 1$ and $\ell$ is prime, we find that (13) is positive if and only if $(-1)^{r+1}>0$, so by the argument given in the previous case when $\ell\nmid q-1$, we have that $(-1)^g\mathcal{E}(q,\ell,g)>0$ in this case as well. □

## 6. *A generalization of Lenstra's theorem*

With Principle 2 in mind, generalizing Lenstra's Theorem 4 boils down to counting matrices $M \in \mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)$ having 1 as an eigenvalue. Indeed, the Jacobian of a curve $C/\mathbb{F}_q$ will have a rational $\ell$-torsion point if and only if Frobenius acting on $\mathrm{Jac}(C)[\ell]$ has a fixed point, that is, an eigenvector with eigenvalue 1.

More formally, for every positive integer $g \geqslant 1$, and for each pair of distinct primes $p > 2$ and $\ell$, let $P(p, \ell, g)$ be the probability that the Jacobian of the (hyper)elliptic curve $y^2 = f(x)$, with $f(x) \in \mathbb{F}_p[x]$ uniformly randomly chosen from $\mathcal{H}_{2g+2}$, has rational $\ell$-torsion. Assume that $\ell$ is odd. Then according to Principle 2, there exist $C_1 \in \mathbb{R}_{>0}$ and $c \in \mathbb{Z}_{>0}$, independent of $p$ and $\ell$ (but depending on $g$), such that

$$|P(p, \ell, g) - \mathfrak{Q}(p, \ell, g)| \leqslant C_1 \ell^c / \sqrt{p},$$

where $\mathfrak{Q}(p, \ell, g)$ is defined in Section 5. This can be considered a proven statement: Achter's proof [2, Theorem 3.1] covers the case where $\mathbb{F}_q$ is a large prime field. Therefore, we conclude the following.

THEOREM 8. *There exist $C_1 \in \mathbb{R}_{>0}$ and $c \in \mathbb{Z}_{>0}$, such that*

$$\left| P(p, \ell, g) + \sum_{r=1}^{g} \ell^r \prod_{j=1}^{r} (1 - \ell^{2j})^{-1} \right| \leqslant C_1 \ell^c / \sqrt{p} \quad \text{if } \ell \mid p - 1$$

*and*

$$\left| P(p, \ell, g) + \sum_{r=1}^{g} \prod_{j=1}^{r} (1 - \ell^{j})^{-1} \right| \leqslant C_1 \ell^c / \sqrt{p} \quad \text{if } \ell \nmid p - 1$$

*for all pairs of distinct primes $p, \ell > 2$.*

Theorem 8 is invalid for $\ell = 2$: as soon as $g > 2$, hyperelliptic curves behave unlike general curves with respect to 2-torsion. But we can estimate $P(p, 2, g)$ using the following slightly simplified result of Cornelissen [12, Theorem 1.4].

THEOREM 9 (Cornelissen). *Let $f(x) \in \mathcal{H}_{2g+2}$. Then the Jacobian of the hyperelliptic curve defined by $y^2 = f(x)$ does* not *have $\mathbb{F}_p$-rational 2-torsion if and only if*

(i) *($g$ odd) $f(x)$ factors as a product of two irreducible polynomials of odd degree;*
(ii) *($g$ even) $f(x)$ factors as a product of two irreducible polynomials of odd degree, or $f(x)$ is irreducible itself.*

Using that a polynomial of degree $d \geqslant 1$ over $\mathbb{F}_p$ is irreducible with probability approximately $1/d$, we obtain the following estimates.

COROLLARY 1. *If $g$ is odd, then*

$$P(p, 2, g) \longrightarrow 1 - \sum_{j=0}^{(g-1)/2} \frac{1}{2j+1} \cdot \frac{1}{2g+2-(2j+1)} \quad \text{as } p \longrightarrow \infty,$$

*whereas if $g$ is even, we have*

$$P(p,2,g) \longrightarrow 1 - \frac{2g}{(2g+2)^2} - \sum_{j=0}^{g/2} \frac{1}{2j+1} \cdot \frac{1}{2g+2-(2j+1)} \quad \text{as } p \longrightarrow \infty.$$

*In particular, we have*

$$\lim_{g,p\to\infty} P(p,2,g) = 1,$$

*hence Theorem 2 holds.*

Note again that for $g \in \{1,2\}$, where the random matrix heuristics are assumed to apply (and in fact provably do for $\ell = 2$ (see Corollary 2 for $g = 2$, exercise for $g = 1$)), we obtain $P(p,2,1) = \frac{2}{3}$ and $P(p,2,2) \approx 26/45$, which is the same as if we would have evaluated the second formula of Theorem 6 in $\ell = 2$.

We are now ready to derive Conjectures 2 and 8 and to prove Lemma 2.

*Derivation of Conjecture* 2. Let $\mathbb{F}_p$ be a large prime field and let $\ell$ be a prime different from its characteristic $p$. From Theorem 6, we see that the probability that the Jacobian of $y^2 = f(x)$, with $f(x)$ chosen from $\mathcal{H}_6$ uniformly at random, has a rational point of order $\ell$ is approximately

$$\frac{\ell(\ell^4-\ell-1)}{(\ell^4-1)(\ell^2-1)} \text{ if } \ell \mid p-1 \quad \text{and} \quad \frac{\ell^2-2}{(\ell^2-1)(\ell-1)} \text{ if } \ell \nmid p-1.$$

Note that because $g = 2$, these limiting probabilities are also valid for $\ell = 2$. Applying the heuristics from Section 3 then yields the requested formula for $c_p$. One new point of concern is that $\ell(p)$, which should now be the largest prime for which $\ell(p) \leqslant (\sqrt{p}+1)^2$, exceeds $p$. Therefore, we should take into account the contribution of $\ell = p$. But since we take $p \to \infty$, it suffices that the probability of not having $p$-torsion tends to 1. This follows from Principle 3 (Section 10).

*Proof of Lemma* 2. This is entirely analogous to the proof of Lemma 1. □

*Derivation of Conjecture* 8. Applying our heuristics, using the probabilities given in Theorem 7, we obtain

$$c_p = \prod_{\ell \nmid p-1} \frac{\prod_{j=1}^{\infty}(1-1/\ell^j)}{1-1/\ell} \cdot \prod_{\ell \mid p-1} \frac{\prod_{j=1}^{\infty}(1+1/\ell^j)^{-1}}{1-1/\ell}.$$

Note that we also use these probabilities for $\ell = 2$, since we expect the random matrix statement from Pinciple 2 to apply in arbitrary level $N$ (in the current, more general framework of selecting curves from $\mathcal{M}_g$ uniformly at random). Rearranging factors gives

$$c_p = \prod_{\ell} \prod_{j=2}^{\infty} \left(1 - \frac{1}{\ell^j}\right) \cdot \prod_{\ell \mid p-1} \prod_{j=1}^{\infty} \left(1 - \frac{1}{\ell^{2j}}\right)^{-1},$$

from which the requested formula follows.

We remark that the average setups (Lemmas 1 and 2) can be thought of as taking matrices at random from $\mathrm{GSp}_{2g}(\mathbb{F}_\ell)$, rather than $\mathrm{GSp}_{2g}^{(p)}(\mathbb{F}_\ell)$.

It is interesting to note, using Theorem 7, that as the genus $g$ grows, the average value $\bar{c}_p$ oscillates, but converges rapidly to its limiting value. This is illustrated numerically in Table 1. Of all genera, elliptic curves disfavor prime orders to the biggest extent, and the Jacobians of genus 2 curves disfavor prime orders to the least extent.

TABLE 1. *Value of $\bar{c}_p$ for growing genus, that is, the constants appearing in Lemmas* 1 *and* 2*, and their higher genus analogues.*

| $g$ | $\bar{c}_p$ |
|---|---|
| 1 | 0.50516617 |
| 2 | 0.69463828 |
| 3 | 0.68851794 |
| 4 | 0.68857163 |
| 5 | 0.68857149 |
| 6 | 0.68857149 |
| 7 | 0.68857149 |

## 7. *The case of a rational Weierstrass point*

In many applications, often cryptographic, one restricts to genus 2 curves of the form $y^2 = f(x)$, where $f(x)$ is chosen from

$$\mathcal{H}_5^{\mathrm{m}} = \{f \in \mathbb{F}_q[x] | f \text{ monic and square-free}, \deg f = 5\}$$

uniformly at random. Stated more geometrically, one restricts to genus 2 curves having a rational Weierstrass point. However, the latter description is not free of ambiguities. Namely, consider the notion of randomness in which $f(x)$ is taken from

$$\mathcal{H}_6^{(>0)} = \{f \in \mathbb{F}_q[x] | f \text{ square-free}, \deg f = 6, \exists a \in \mathbb{F}_q : f(a) = 0\}$$

uniformly at random. Then this is fundamentally different from the $\mathcal{H}_5^{\mathrm{m}}$ setting. To illustrate this: the probability that the Jacobian of a randomly chosen curve has even order tends to $\frac{4}{5} = 0.8$ with respect to $\mathcal{H}_5^{\mathrm{m}}$, whereas it tends to $\frac{311}{455} \approx 0.68$ with respect to $\mathcal{H}_6^{(>0)}$. Both statements will be proved below.

The main conclusion of this section will be, however, that the distribution of Frobenius acting on any *odd*-torsion subgroup of the Jacobian is barely affected by this ambiguity. In Section 7.2, we will show the following.

THEOREM 10. *Let $N$ be an odd positive integer, let $q$ be an odd prime power coprime to $N$ and let $\mathcal{H}$ be either $\mathcal{H}_5^{\mathrm{m}}$, $\mathcal{H}_6^{(>0)}$ or $\mathcal{H}_6$. For any subset $\mathcal{C} \subset \mathrm{GSp}_4^{(q)}(\mathbb{Z}/(N))$ that is closed under $\mathrm{GSp}_4(\mathbb{Z}/(N))$-conjugation, let $P(\mathcal{F}_f \subset \mathcal{C})$ be defined as in Section* 4.2*, where now $f$ is chosen from $\mathcal{H}$ uniformly at random. If Principle* 2 *holds, then there exist $C_1 \in \mathbb{R}_{>0}$ and $c \in \mathbb{Z}_{>0}$ such that*

$$\left| P(\mathcal{F}_f \subset \mathcal{C}) - \frac{\#\mathcal{C}}{\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(N))} \right| \leqslant C_1 N^c / \sqrt{q}$$

*for all choices of $q$ and $\mathcal{C}$ as above.*

For $\mathcal{H}_5^{\mathrm{m}}$, we remark that it is presumably possible to prove Theorem 10 directly from Katz–Sarnak [**20**, Theorem 9.7.13], that is, independently of Principle 2, in the same way as a proof of Principle 2 is expected to work, using that the family corresponding to $\mathcal{H}_5^{\mathrm{m}}$ has the largest possible monodromy group [**20**, 10.1.18].

As an immediate application, one obtains:

*Heuristic derivation of Conjecture* 3. By Theorem 10, we only need to replace the factor $\frac{38}{45}$, corresponding to the prime $\ell = 2$, by $\frac{2}{5}$. So the correcting factor is $\frac{9}{19}$.

### 7.1. *Rational 2-torsion in genus 2*

Some material in this section has appeared in the literature before, see, for example, [**6**, Section 2].

LEMMA 4. *Every non-trivial 2-torsion point on the Jacobian of a genus 2 curve over $\mathbb{F}_q$ (thought of as a divisor class) contains a unique pair of divisors $\{P_i - P_j, P_j - P_i\}$, where $P_i$ and $P_j$ are distinct Weierstrass points.*

*Proof.* It is obvious that $P_i - P_j$ and $P_j - P_i$ are linearly equivalent and that they map to a 2-torsion point on the Jacobian. By Riemann–Roch, this point is non-trivial and two different pairs give rise to distinct 2-torsion points. Since there are 15 non-trivial 2-torsion points on the Jacobian of a genus 2 curve, and since there are 15 pairs in a set of 6 elements, the correspondence must be one to one. □

We immediately obtain (compare with Theorem 9) the following.

LEMMA 5. *The Jacobian of a genus 2 curve over $\mathbb{F}_q$ defined by an equation of the form $y^2 = f(x)$ with $f \in \mathcal{H}_5^{\mathrm{m}}$ (resp. $f \in \mathcal{H}_6$) has a non-trivial rational 2-torsion point if and only if $f$ is reducible (resp. $f$ has a factor of degree 2).*

*Proof.* By Lemma 4, there exists a non-trivial rational 2-torsion point if and only if there are Weierstrass points $P_1$ and $P_2$ such that $\{P_1, P_2\}$ is closed under $q$th power Frobenius. □

This allows us to estimate the probability that the Jacobian has even order.

LEMMA 6. *Let $f_5^{\mathrm{m}} \in \mathcal{H}_5^{\mathrm{m}}$, $f_6^{(>0)} \in \mathcal{H}_6^{(>0)}$ and $f_6 \in \mathcal{H}_6$ be chosen uniformly at random. Let $C_5^{\mathrm{m}}$, $C_6^{(>0)}$ and $C_6$ denote the corresponding genus 2 curves. Then as $q \to \infty$*

(i) $P(\#\mathrm{Jac}(C_5^{\mathrm{m}})(\mathbb{F}_q)$ *is even*$) \to \frac{4}{5}$;
(ii) $P(\#\mathrm{Jac}(C_6)(\mathbb{F}_q)$ *is even*$) \to \frac{26}{45}$;
(iii) $P(\#\mathrm{Jac}(C_6^{(>0)})(\mathbb{F}_q)$ *is even*$) \to \frac{311}{455}$.

*Proof.* We leave this as an exercise, or refer to Table 2. □

We will now describe the symplectic structure of the 2-torsion subgroup in more detail. Fix a genus 2 curve $C/\mathbb{F}_q$ and let $P_1, \dots, P_6$ be its Weierstrass points. Following Lemma 4, every non-trivial element of $\mathrm{Jac}(C)[2]$ can be identified with a unique pair of distinct points $\{P_i, P_j\}$, and the group structure can be described by the rules

$$\begin{cases} \{P_i, P_j\} + \{P_i, P_j\} = 0 \\ \{P_i, P_j\} + \{P_i, P_k\} = \{P_j, P_k\} \quad \text{if } j \neq k \\ \{P_i, P_j\} + \{P_k, P_\ell\} = \{\text{remaining two points}\} \quad \text{if } \{i,j\} \cap \{k,\ell\} = \emptyset. \end{cases}$$

The Weil pairing can be seen to satisfy

$$e_2(\{P_i, P_j\}, \{P_k, P_\ell\}) = (-1)^{\#\{i,j,k,\ell\}}$$

for all $i, j, k, \ell \in \{1, \dots, 6\}$.

We use this to prove the following.

TABLE 2. *Factorization patterns of $f(x) \in \mathcal{H}_6, \mathcal{H}_5^{\mathrm{m}}$ and the corresponding Frobenius conjugacy classes.*

| $\mathcal{H}_6$ | | $\mathcal{H}_5^{\mathrm{m}}$ | | Conjugacy classes of $\mathrm{Sp}_4(\mathbb{F}_2)$ | | | | |
|---|---|---|---|---|---|---|---|---|
| Pattern | Probability | Pattern | Probability | Representant | Size | Order | $\mathbb{F}_q$-rank | Trace |
| 6 | $\approx\frac{1}{6}$ | | | $\left(\begin{smallmatrix}1&1&0&1\\0&1&0&1\\1&1&1&1\\0&0&1&1\end{smallmatrix}\right)$ | 120 | 6 | 0 | 0 |
| 5,1 | $\approx\frac{1}{5}$ | 5 | $\approx\frac{1}{5}$ | $\left(\begin{smallmatrix}0&1&1&0\\0&0&1&0\\0&1&0&1\\1&1&0&1\end{smallmatrix}\right)$ | 144 | 5 | 0 | 1 |
| 4,2 | $\approx\frac{1}{8}$ | | | $\left(\begin{smallmatrix}0&1&0&0\\1&0&0&0\\0&0&0&1\\1&0&1&0\end{smallmatrix}\right)$ | 90 | 4 | 1 | 0 |
| 4,1,1 | $\approx\frac{1}{8}$ | 4,1 | $\approx\frac{1}{4}$ | $\left(\begin{smallmatrix}1&0&1&1\\1&0&0&1\\0&1&0&1\\1&1&1&1\end{smallmatrix}\right)$ | 90 | 4 | 1 | 0 |
| 3,3 | $\approx\frac{1}{18}$ | | | $\left(\begin{smallmatrix}1&0&1&1\\0&1&1&0\\0&1&0&0\\1&1&0&0\end{smallmatrix}\right)$ | 40 | 3 | 0 | 0 |
| 3,2,1 | $\approx\frac{1}{6}$ | 3,2 | $\approx\frac{1}{6}$ | $\left(\begin{smallmatrix}1&1&0&0\\0&1&1&1\\0&1&0&1\\1&1&1&1\end{smallmatrix}\right)$ | 120 | 6 | 1 | 1 |
| 3,1,1,1 | $\approx\frac{1}{18}$ | 3,1,1 | $\approx\frac{1}{6}$ | $\left(\begin{smallmatrix}1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&1\end{smallmatrix}\right)$ | 40 | 3 | 2 | 1 |
| 2,2,2 | $\approx\frac{1}{48}$ | | | $\left(\begin{smallmatrix}0&0&0&1\\1&0&1&0\\0&1&0&1\\1&0&0&0\end{smallmatrix}\right)$ | 15 | 2 | 2 | 0 |
| 2,2,1,1 | $\approx\frac{1}{16}$ | 2,2,1 | $\approx\frac{1}{8}$ | $\left(\begin{smallmatrix}0&0&1&0\\0&1&0&0\\1&0&0&0\\0&1&0&1\end{smallmatrix}\right)$ | 45 | 2 | 2 | 0 |
| 2,1,1,1,1 | $\approx\frac{1}{48}$ | 2,1,1,1 | $\approx\frac{1}{12}$ | $\left(\begin{smallmatrix}0&1&1&0\\0&1&0&0\\1&1&0&0\\1&1&1&1\end{smallmatrix}\right)$ | 15 | 2 | 3 | 0 |
| 1,1,1,1,1,1 | $\approx\frac{1}{720}$ | 1,1,1,1,1 | $\approx\frac{1}{120}$ | $\left(\begin{smallmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{smallmatrix}\right)$ | 1 | 1 | 4 | 0 |

For instance, the pattern $3,1,1,1$ means that $f(x) \in \mathcal{H}_6$ factors into three linear polynomials and one irreducible cubic polynomial. The probability of this event is approximately $\frac{1}{3} \cdot \frac{1}{3!}\frac{1}{1} = \frac{1}{18}$. The corresponding conjugacy class of Frobenius is generated by the depicted matrix and contains 40 elements. Every such element has order 3 and trace 1, and its eigenspace for eigenvalue 1 is two-dimensional (that is, $\dim \mathrm{Jac}(C)[2](\mathbb{F}_q) = 2$).

THEOREM 11. *Let $q$ be an odd prime power. There exist $\mathcal{W}_0, \ldots, \mathcal{W}_6 \subset \mathrm{Sp}_4(\mathbb{F}_2)$ such that for any curve $C/\mathbb{F}_q$ of genus 2, any symplectic basis of $\mathrm{Jac}(C)[2]$, and any $r \in \{0, \ldots, 6\}$, the matrix $F$ of $q$th power Frobenius with respect to this basis satisfies*

$$F \in \mathcal{W}_r \text{ if and only if } C \text{ has } r \text{ rational Weierstrass points.}$$

*The cardinalities of the $\mathcal{W}_r$ are $265, 264, 135, 40, 15, 0$ and $1$, respectively.*

*Proof.* There exist six subsets $U \subset \mathrm{Jac}(C)[2]$ that are maximal with respect to the condition that $u_1, u_2 \in U$ and $u_1 \neq u_2$ implies $e_2(u_1, u_2) = -1$, namely

$$U_i = \{\{P_i, P_j\} | j \in \{1, 2, \ldots, 6\} \setminus \{i\}\} \quad \text{for } i = 1, \ldots, 6.$$

Since $N = 2$, the choice of a primitive $N$th root of unity is canonical, hence the Weil pairing defines unambiguously a symplectic pairing on $\mathrm{Jac}(C)[2]$. After having fixed a symplectic basis, every symplectic matrix induces a permutation of $\{U_1, \ldots, U_6\}$. In fact, this induces a group isomorphism $\mathrm{Sp}_4(\mathbb{F}_2) \to \mathrm{Sym}(6)$. Indeed, it is easy to see that the above induces an injective group homomorphism, and surjectivity follows from $\#\mathrm{Sp}_4(\mathbb{F}_2) = \#\mathrm{Sym}(6) = 720$. Then the sets $\mathcal{W}_r$ are the pre-images under this isomorphism of the set of permutations having exactly

$r$ fixed points. While the isomorphism depends on the choice of symplectic basis, the sets $\mathcal{W}_r$ do not, because they are invariant under conjugation. □

Pushing the argument a little further, one actually sees that the conjugacy class of Frobenius, which under the above group isomorphism corresponds to a conjugacy class of $\mathrm{Sym}(6)$, is completely determined by the factorization pattern of $f(x)$, and conversely. Note that there are 11 conjugacy classes in $\mathrm{Sym}(6) \cong \mathrm{Sp}_4(\mathbb{F}_2)$ and that there are 11 ways to partition the number 6. Since the probability of having a certain factorization pattern is easily estimated using the well-known fact that a polynomial of degree $d$ is irreducible with probability about $1/d$, this unveils the complete stochastic picture of $\mathrm{Jac}(C)[2]$, as shown in Table 2.

COROLLARY 2. *Principle* 2 *holds for* $g = N = 2$.

*Proof.* This can be read off from Table 2. The only additional concern is the bound on the error term, but this is easily verified. □

### 7.2. *Equidistribution in odd level*

In this section, we will prove Theorem 10. Consider $f \in \mathcal{H}_6^{(>0)}$, so that $y^2 = f(x)$ defines a genus 2 curve having a rational Weierstrass point $(a, 0)$. Then the birational change of variables

$$x \longleftarrow \frac{1}{x} + a \quad \text{and} \quad y \longleftarrow \frac{y}{x^3},$$

transforms this into $y^2 = f'(x)$ with $f' \in \mathcal{H}_5$. This leads us to defining a relation

$$\rho \subset \mathcal{H}_6^{(>0)} \times \mathcal{H}_5$$

associating to $f \in \mathcal{H}_6^{(>0)}$ all polynomials of $\mathcal{H}_5$, that can be obtained through the above procedure. However, this correspondence is not uniform, because of the number of choices that can be made for $a$, that is, the number of rational roots of $f$. This is the reason why the notions of randomness with respect to $\mathcal{H}_5$ (or $\mathcal{H}_5^{\mathrm{m}}$) and $\mathcal{H}_6^{(>0)}$ are fundamentally different, as reflected in Lemma 6.

We are led to introducing the following notation. For $r \in \{0, \dots, 6\}$, define

$$\mathcal{H}_6^{(r)} = \{f \in \mathbb{F}_q[x] | f \text{ square-free}, \deg f = 6, f \text{ has precisely } r \text{ rational zeroes}\}$$

so that

$$\mathcal{H}_6 = \bigsqcup_{r=0}^{6} \mathcal{H}_6^{(r)} \quad \text{and} \quad \mathcal{H}_6^{(>0)} = \bigsqcup_{r=1}^{6} \mathcal{H}_6^{(r)}. \tag{14}$$

Similarly, for $r \in \{0, \dots, 5\}$ we introduce

$$\mathcal{H}_5^{(r)} = \{f \in \mathbb{F}_q[x] | f \text{ square-free of degree } 5,\ f \text{ has precisely } r \text{ rational zeroes}\},$$

so that

$$\mathcal{H}_5 = \bigsqcup_{r=0}^{5} \mathcal{H}_5^{(r)}.$$

Note that $\mathcal{H}_6^{(5)}$ and $\mathcal{H}_5^{(4)}$ are empty. We implicitly omit these sets to avoid probabilities of the type $\frac{0}{0}$. Similarly, we assume that $q > 6$ so that none of the other sets is empty.

Now because of (14), to prove Theorem 10 for $\mathcal{H}_6^{(>0)}$, it suffices to do so for each $\mathcal{H}_6^{(r)}$ $(r = 1, \dots, 6)$. Similarly, by the discussion in Section 2, we can use $\mathcal{H}_5$ instead of $\mathcal{H}_5^{\mathrm{m}}$, and it

is sufficient to prove Theorem 10 for $\mathcal{H}_5^{(r)}$ $(r = 0, \ldots, 5)$ in this case. Finally, by Lemma 7, the cases $\mathcal{H}_5^{(r)}$ can in turn be reduced to the cases $\mathcal{H}_6^{(r)}$.

LEMMA 7. *Let* $S_0 = \{f \in \mathcal{H}_5 | f(0) \neq 0\}$. *For each* $r = 1, \ldots, 6$, *the restriction of* $\rho$ *to*

$$\mathcal{H}_6^{(r)} \times (\mathcal{H}_5^{(r-1)} \cap S_0)$$

*is uniform.*

*Proof.* This is immediate. □

We are now ready to prove Theorem 10.

*Proof of Theorem* 10. By the above discussion, it suffices to estimate the conditional probabilities

$$P(\mathcal{F}_f \subset \mathcal{C} | f \in \mathcal{H}_6^{(r)}) = \frac{P(\mathcal{F}_f \subset \mathcal{C} \text{ and } f \in \mathcal{H}_6^{(r)})}{P(f \in \mathcal{H}_6^{(r)})}$$

for $r = 1, \ldots, 6$. By Theorem 11, $f \in \mathcal{H}_6^{(r)}$ is equivalent to saying that the conjugacy class of Frobenius, acting on the 2-torsion points of the Jacobian of $y^2 = f(x)$, is contained in $\mathcal{W}_r$. Denote this conjugacy class by $\mathcal{F}_{f,2}$. Similarly, let $\mathcal{F}_{f,2N}$ denote the conjugacy class of Frobenius acting on the $2N$-torsion points.

Since $N$ is odd, we have a canonical isomorphism

$$\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(2N)) \cong \mathrm{GSp}_4^{(q)}(\mathbb{F}_2) \oplus \mathrm{GSp}_4^{(q)}(\mathbb{Z}/(N)),$$

allowing us to consider $\mathcal{W}_r \oplus \mathcal{C}$ as a subset of $\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(2N))$. Because it is the union of a number of orbits under $\mathrm{GSp}_4(\mathbb{Z}/(2N))$-conjugation, there exist $C_1 \in \mathbb{R}_{>0}$ and $c \in \mathbb{Z}_{>0}$, such that

$$\left| P(\mathcal{F}_{f,2N} \subset \mathcal{W}_r \oplus \mathcal{C}) - \frac{\#(\mathcal{W}_r \oplus \mathcal{C})}{\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(2N))} \right| \leqslant C_1 N^c / \sqrt{q} \tag{15}$$

for all choices of $q$, $N$ and $\mathcal{C}$. In particular, for $N = 1$, this gives

$$\left| P(f \in \mathcal{H}_6^{(r)}) - \frac{\#\mathcal{W}_r}{\#\mathrm{GSp}_4^{(q)}(\mathbb{F}_2)} \right| \leqslant C_1 / \sqrt{q}. \tag{16}$$

Since

$$P(\mathcal{F}_{f,2N} \subset \mathcal{W}_r \oplus \mathcal{C}) = P(\mathcal{F}_f \subset \mathcal{C} \text{ and } \mathcal{F}_{f,2} \subset \mathcal{W}_r) = P(\mathcal{F}_f \subset \mathcal{C} \text{ and } f \in \mathcal{H}_6^{(r)})$$

and

$$\frac{\#(\mathcal{W}_r \oplus \mathcal{C})}{\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(2N))} = \frac{\#\mathcal{W}_r}{\#\mathrm{GSp}_4^{(q)}(\mathbb{F}_2)} \cdot \frac{\#\mathcal{C}}{\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(N))},$$

inequality (15) can be rewritten as

$$\left| P(\mathcal{F}_f \subset \mathcal{C} | f \in \mathcal{H}_6^{(r)}) - \frac{\#\mathcal{W}_r / \#\mathrm{GSp}_4^{(q)}(\mathbb{F}_2)}{P(f \in \mathcal{H}_6^{(r)})} \cdot \frac{\#\mathcal{C}}{\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(N))} \right| \leqslant \frac{C_1 N^c / \sqrt{q}}{P(f \in \mathcal{H}_6^{(r)})}.$$

It follows from (16) that there is a $C_2 \in \mathbb{R}^+$ such that

$$\left| P(\mathcal{F}_f \subset \mathcal{C} | f \in \mathcal{H}_6^{(r)}) - \frac{\#\mathcal{C}}{\#\mathrm{GSp}_4^{(q)}(\mathbb{Z}/(N))} \right| \leqslant C_2 N^c / \sqrt{q}$$

for all choices of $q$, $N$ and $\mathcal{C}$. This completes the proof. □

## 8. *The number of points on the curve itself*

Up to now we have focused entirely on the number of rational points on the Jacobian of a curve. However, the random matrix framework allows us to consider the number of rational points on the curve itself as well.

For any pair of distinct primes $p > 2$ and $\ell$, and any $t \in \mathbb{F}_\ell$, we define the following constants:

$$\begin{aligned} a_{\ell,t,p} &:= \#\{(x,y) \in \mathbb{F}_\ell^\times \times (\mathbb{F}_\ell^\times \backslash \{-p\}) | (x + y/x)(1 + p/y) = t\}, \\ A_{\ell,t,p} &:= \ell^4((\ell-1)(\ell-2) + a_{\ell,t,p}) + \begin{cases} \ell^6 - \ell^4 & \text{if } t = 0, \\ 0 & \text{otherwise,} \end{cases} \\ B_\ell &:= \ell^4(\ell^2-1)^2, \\ C_{\ell,t} &:= \ell^5(\ell-1)(\ell^3-\ell-1) + \begin{cases} \ell^7 - \ell^6 & \text{if } t = 0, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

Note that, in general, it is impossible to find a closed formula for $a_{\ell,t,p}$ since it typically describes the number of points on an elliptic curve over $\mathbb{F}_\ell$ (though it is clear that $a_{\ell,t,p}$ lies close to $\ell$). Let $P(p,\ell,t)$ be the probability that the number of rational points on the non-singular complete model of the curve $C : y^2 = f(x)$, with $f(x)$ chosen uniformly at random from $\mathcal{H}_6$, is congruent to $p + 1 - t$ modulo $\ell$.

THEOREM 12. *There exist $C_1 \in \mathbb{R}_{>0}$ and $c \in \mathbb{Z}_{>0}$, such that*

$$\left| P(p,\ell,t) - \frac{A_{\ell,t,p} + B_\ell + C_{\ell,t}}{\ell^4 \cdot (\ell^4-1) \cdot (\ell^2-1)} \right| \leqslant C_1 \ell^c / \sqrt{p}$$

*for all $p, \ell, t$ as above.*

*Proof.* Because the trace of a matrix is invariant under conjugation, it suffices by Principle 2 (proved for $\ell$ odd by Achter [2, Theorem 3.1], and for $\ell = 2$ in Corollary 2) to count the number of matrices $M$ in $\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$ with trace $t$, and show that it equals $A_{\ell,t,p} + B_\ell + C_{\ell,t}$. Our main tool is the following Bruhat decomposition of $\mathrm{Sp}_4(\mathbb{F}_\ell)$, proved by Kim [22]. Consider the group

$$P = \left\{ \begin{pmatrix} A & AB \\ 0 & {}^tA^{-1} \end{pmatrix} \middle| \, A, B \in \mathbb{F}_\ell^{2\times 2}, A \text{ invertible, } B \text{ symmetric} \right\}, \tag{17}$$

then we have the disjoint union

$$\mathrm{Sp}_4(\mathbb{F}_\ell) = P \sqcup P\sigma_1 P \sqcup P\sigma_2 P,$$

where

$$\sigma_1 = \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \sigma_2 = \Omega = \begin{pmatrix} 0 & \mathbb{I}_2 \\ -\mathbb{I}_2 & 0 \end{pmatrix}.$$

For $r \in \{1, 2\}$, consider the subgroup

$$A_r = \{M \in P | \sigma_r M \sigma_r^{-1} \in P\}.$$

Then one can find unique representatives for the elements of $P\sigma_r P$ by rewriting

$$P\sigma_r P = P\sigma_r(A_r \backslash P),$$

where $A_r \backslash P$ should be seen as a set of representatives of the right cosets of $A_r$ in $P$. This implies that

$$|P\sigma_r P| = |P| \cdot |A_r \backslash P|.$$

One can prove (see [22]) that $|A_1\backslash P| = \ell^2 + \ell$ and $|A_2\backslash P| = \ell^3$. Taking $\sigma_0 = \mathbb{I}_4$, the Bruhat decomposition of $\mathrm{Sp}_4(\mathbb{F}_\ell)$ implies the following partition of $\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell)$:

$$\mathrm{GSp}_4^{(p)}(\mathbb{F}_\ell) = \bigsqcup_{r=0}^{2} d_p P \sigma_r P.$$

We will do a component-wise count of the number of matrices having trace $t$. First we observe that

$$|\{M \in d_p P \sigma_r P | \mathrm{Tr}(M) = t\}| = |A_r\backslash P| \cdot |\{M \in d_p P \sigma_r | \mathrm{Tr}(M) = t\}|$$

for $r = 1, 2$. Indeed, every element of $d_p P \sigma_r P$ has a unique representation of the form

$$d_p M \sigma_r N$$

with $M \in P$ and $N \in A_r\backslash P$ (where $A_r\backslash P$ is thought of as a set of representatives of the right cosets of $A_r$). Using this representation, the map

$$d_p P \sigma_r P \longrightarrow d_p P \sigma_r : d_p M \sigma_r N \longmapsto d_p (d_p^{-1} N d_p M) \sigma_r$$

is surjective and $|A_r\backslash P|$-to-1. Since $d_p M \sigma_r N$ and $d_p(d_p^{-1} N d_p M)\sigma_r$ are conjugated, the observation follows.

A matrix $M \in d_p P$ can be written as $\left(\begin{smallmatrix} A & AB \\ 0 & p\cdot {}^tA^{-1} \end{smallmatrix}\right)$ with $A \in \mathrm{GL}_2(\mathbb{F}_\ell)$ and $B \in \mathbb{F}_\ell^{2\times 2}$ symmetric.

First, we consider $M\sigma_1$, whose trace equals $-(AB)_{1,1} + A_{2,2} + (p \cdot {}^tA^{-1})_{2,2}$, where the index notation refers to the corresponding entries. Fix $A$ and let $B$ vary. Then because $(AB)_{1,1} = A_{1,1}B_{1,1} + A_{1,2}B_{2,1}$ and not both $A_{1,1}$ and $A_{1,2}$ can be zero, we find that each trace occurs equally often. We conclude that traces are uniformly distributed in $d_p P \sigma_1$. Next, for $M\sigma_2$ we find that $\mathrm{Tr}(M\sigma_2) = -\mathrm{Tr}(AB)$, which is uniformly distributed for all $A$ not of the form $\left(\begin{smallmatrix} 0 & a \\ -a & 0 \end{smallmatrix}\right)$, and which is zero if $A$ does have this form. Using the above formulas for $|A_r\backslash P|$ and using $|\mathrm{GL}_2(\mathbb{F}_\ell)| = \ell(\ell^2-1)(\ell-1)$, we find that the number of matrices in $d_p P\sigma_1 \sqcup d_p P \sigma_2$ having trace $t$ equals $B_\ell + C_{\ell,t}$.

Finally, we consider $M \in d_p P$ when $\mathrm{Tr}(M) = \mathrm{Tr}(A) + \mathrm{Tr}(pA^{-1})$. We write $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and let $\delta = ad - bc$ be its determinant. Clearly $\mathrm{Tr}(M) = \mathrm{Tr}(A)\cdot(1 + p/\delta)$. There are $\ell(\ell^2-1)$ matrices $A$ with determinant $-p$, in which case this trace equals 0. So suppose that $\delta \neq -p$. When $a = 0$ it is easy to see that we have uniform distribution, so we also suppose that $a \neq 0$. We can replace $d$ by $(\delta + bc)/a$ and again, if $b \neq 0$ we will find uniformity. Finally the case $b = 0$ gives as trace

$$(a + \delta/a)(1 + p/\delta),$$

so that an easy calculation shows that the number of matrices in $d_p P$ with trace $t$ equals $A_{\ell,t,p}$. □

Table 3 gives the respective probabilities for various small $\ell$. Note that the probabilities of $C$ and $\mathrm{Jac}(C)$ having an even number of rational points are the same, despite the fact that these events do not coincide. Also note from Table 3 that trace 0 is favored. This is a general phenomenon that can be seen as follows. It is not hard to verify that if $2t(t^2 - 16p) \equiv 0 \bmod \ell$, the curve $(x + y/x)(1 + p/y) = t$ in the definition of $a_{\ell,t,p}$ is reducible or has genus 0, in which case $a_{\ell,t,p}$ can be explicitly computed. It is equal to zero if $\ell = 2$. For $t \equiv 0 \bmod \ell$ and $\ell > 2$ we can compute the following estimate for $P(p, \ell, t)$:

$$\frac{\ell^9 - \ell^6 - \ell^5 - \ell^4}{\ell^4(\ell^4-1)(\ell^2-1)} = \frac{\ell^3 - \ell - 1}{(\ell^2-1)^2}$$

if $p$ is a square modulo $\ell$ and

$$\frac{\ell^9 - \ell^6 - \ell^5 + \ell^4}{\ell^4(\ell^4-1)(\ell^2-1)} = \frac{\ell^3 + \ell - 1}{\ell^4 - 1}$$

TABLE 3. *Distribution of Frobenius traces modulo small $\ell$ for $y^2 = f(x)$, with $f(x) \in \mathcal{H}_6$ chosen at random.*

| | $p \bmod \ell \setminus t$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|---|
| $\ell = 2$ | 1 | $\frac{26}{45}$ | $\frac{19}{45}$ | | | |
| $\ell = 3$ | 1 | $\frac{46}{128}$ | $\frac{41}{128}$ | $\frac{41}{128}$ | | |
| | 2 | $\frac{58}{160}$ | $\frac{51}{160}$ | $\frac{51}{160}$ | | |
| $\ell = 5$ | 1 | $\frac{3094}{14976}$ | $\frac{2969}{14976}$ | $\frac{2972}{14976}$ | $\frac{2972}{14976}$ | $\frac{2969}{14976}$ |
| | 2 | $\frac{774}{3744}$ | $\frac{743}{3744}$ | $\frac{742}{3744}$ | $\frac{742}{3744}$ | $\frac{743}{3744}$ |
| | 3 | $\frac{774}{3744}$ | $\frac{742}{3744}$ | $\frac{743}{3744}$ | $\frac{743}{3744}$ | $\frac{742}{3744}$ |
| | 4 | $\frac{3094}{14976}$ | $\frac{2972}{14976}$ | $\frac{2969}{14976}$ | $\frac{2969}{14976}$ | $\frac{2972}{14976}$ |

otherwise. Both probabilities are indeed larger than $1/\ell$. If $p \equiv t^2/16 \bmod \ell$, and hence $t \not\equiv 0 \bmod \ell$, we obtain

$$\frac{\ell^9 - \ell^7 - \ell^6 - \ell^5 - \ell^4}{\ell^4(\ell^4 - 1)(\ell^2 - 1)} = \frac{\ell^5 - \ell^3 - \ell^2 - \ell - 1}{(\ell^4 - 1)(\ell^2 - 1)}$$

if $\ell \equiv 1 \bmod 4$, and when $\ell \equiv 3 \bmod 4$ we find

$$\frac{\ell^9 - \ell^7 - \ell^6 - \ell^5 + \ell^4}{\ell^4(\ell^4 - 1)(\ell^2 - 1)} = \frac{\ell^5 - \ell^3 - \ell^2 - \ell + 1}{(\ell^4 - 1)(\ell^2 - 1)}.$$

*Heuristic derivation of Conjecture* 4. The number of rational points on the curve defined by $y^2 = f(x)$ is divisible by $\ell$ if and only if its trace $t$ is congruent to $p + 1 \bmod \ell$. Thus, by Theorem 12, the probability that this number of points is not divisible by $\ell$ can be estimated by

$$\frac{\beta_{\ell,p}}{(\ell^4 - 1)(\ell^2 - 1)},$$

where $\beta_{\ell,p}$ is as in Section 1.5. Dividing by $1 - 1/\ell$ and taking the product then gives the constant $c_p$ from Conjecture 4. The factor corresponding to $\ell = 2$ can be read off from Table 3 (or from Table 2). When switching from $\mathcal{H}_6$ to $\mathcal{H}_5$, following Theorem 10 and using Table 2, we should replace the factor $\frac{38}{45}$ by $\frac{16}{15}$.

## 9. *The probability of cyclicity*

In this section, we will estimate the probability $P(p, g)$ that the group of rational points of the Jacobian of the (hyper)elliptic curve $C : y^2 = f(x)$, with $f(x)$ chosen from $\mathcal{H}_{2g+2}$ uniformly at random, is cyclic. This question is of a different type than those we have considered so far. We use the following heuristic reasoning. Note that $\mathrm{Jac}(C)(\mathbb{F}_p)$ is cyclic if and only if $\mathrm{Jac}(C)[\ell](\mathbb{F}_p)$ is cyclic for each prime $\ell$. The probabilities of the latter events can be estimated using Principle 2: for each $\ell \neq p$, this is approximately

$$\mathfrak{P}(p, \ell, g, 0) + \mathfrak{P}(p, \ell, g, 1),$$

where the notation from Section 5 is used. For a reason similar to the one explained in the derivation of Conjecture 2 in Section 6, we will omit the contribution of $\ell = p$. Then the

TABLE 4. *Average conjectured probability of being cyclic for growing genus.*

| $g$ | Factor |
|---|---|
| 1 | 0.81375191 |
| 2 | 0.80882586 |
| 3 | 0.80924272 |
| 4 | 0.80923674 |
| 5 | 0.80923677 |
| 6 | 0.80923677 |
| 7 | 0.80923677 |

idea is to assume independence and naïvely multiply these proportions. As suggested by our experiments in Section 11, this gives accurate predictions for $g \in \{1, 2\}$. In particular, an effect of the type reflected in Mertens' theorem seems absent in this non-relative setting. For $g = 1$, the heuristics confirm a formula proven by Vlăduţ [**34**, Theorem 6.1].

*Heuristic derivation of Conjecture* 5. The formulas of Theorem 5 for $g = 2$ give

$$\mathfrak{P}(p, \ell, 2, 0) + \mathfrak{P}(p, \ell, 2, 1) = \begin{cases} \dfrac{\ell^8 - \ell^6 - \ell^5 - \ell^4 + \ell^2 + \ell + 1}{\ell^2(\ell^4 - 1)(\ell^2 - 1)} & \text{if } \ell \mid p - 1, \\ 1 - \dfrac{1}{\ell(\ell^2 - 1)(\ell - 1)} & \text{if } \ell \nmid p - 1. \end{cases}$$

Multiplying gives the conjectured formula. If we switch from $\mathcal{H}_6$ to $\mathcal{H}_5^{\mathrm{m}}$, the leading factor $\frac{151}{180}$ should be replaced by $\frac{37}{60}$, as can be read off from Table 2.

*Proof of Theorem* 3. This is analogous to the proof of Theorem 2 (see Corollary 1). In fact, the original version of Cornelissen's Theorem 9 [**12**, Theorem 1.4] is much stronger and describes the rank of $\mathrm{Jac}(C)[2](\mathbb{F}_p)$ in terms of the factorization pattern of $f(x)$. For example, it suffices that $f(x)$ has at least four distinct factors for the rank to be at least 2. From this, one verifies that for $g \to \infty$, this rank will be 2 or larger with a probability converging to 1. □

*Heuristic derivation of Conjecture* 9. This is a combination of the derivations of Conjectures 5 and 8, the details of which we leave to the reader.

As in the case of primality, we list the average values (in the sense of Conjecture 1.3) of the probabilities of cyclicity for growing genus in Table 4. Again one notices that the convergence is alternating (although we did not elaborate the details of a proof of this) and fast.

## 10. *Extension fields*

In this section, we briefly discuss how our heuristics can be adapted to the setting of finite fields $\mathbb{F}_{p^k}$ of growing extension degree, over a fixed prime field $\mathbb{F}_p$. In this situation, one can no longer neglect the contribution of the prime $\ell = p$.

Let $C/\mathbb{F}_{p^k}$ be a complete non-singular curve of genus $g \geqslant 1$ and, as before, denote by $A = \mathrm{Jac}(C)$ its Jacobian. One has

$$A[p] \cong (\mathbb{F}_p)^r$$

for some $0 \leqslant r \leqslant g$. We assume that if $k$ is large and one picks $C$ at random (for example, from

$$\mathcal{M}_g = \{\text{curves of genus } g \text{ over } \mathbb{F}_{p^k}\}/\cong_{\mathbb{F}_{p^k}}$$

uniformly at random), one has $r = g$ with probability $\approx 1$. This is reasonable, because the moduli space $\mathcal{A}_g$ of abelian varieties of dimension $g$ is stratified by rank, the stratum corresponding to $r = g$ having the biggest dimension [28, Theorem 4.1]. We do not claim a proof of this assumption however, although for hyperelliptic curves this is a known fact [4, 29]. If $r = g$, then the matrix of the $p^k$th power Frobenius acting on $A[p]$ with respect to any $\mathbb{F}_p$-basis is an element of $\mathrm{GL}_g(\mathbb{F}_p)$. Thus, in that case, we can unambiguously associate to $C$ a conjugacy class of matrices of $p^k$th power Frobenius, denoted by $\mathcal{F}_C$. The expectation is that for every union of conjugacy classes $\mathcal{C} \subset \mathrm{GL}_g(\mathbb{F}_p)$, the probability that $\mathcal{F}_C \subset \mathcal{C}$ becomes proportional to $\#\mathcal{C}$ (as $k \to \infty$).

Returning to hyperelliptic curves, let $P(\mathcal{F}_{f,h} \subset \mathcal{C})$ be the probability that the conjugacy class of Frobenius associated to the hyperelliptic curve $y^2 + h(x)y = f(x)$, where $(f, h)$ is chosen from $\mathcal{H}_{g+1,2g+2}$ uniformly at random, is contained in $\mathcal{C}$. As explained in Section 2, for $p > 2$, one can assume $h(x) = 0$ and $f(x)$ chosen from $\mathcal{H}_{2g+2}$ if desired.

PRINCIPLE 3. Let $g \in \{1, 2\}$. There exist $C_1 \in \mathbb{R}_{>0}$ and $c \in \mathbb{Z}_{>0}$ such that

$$\left| P(\mathcal{F}_{f,h} \subset \mathcal{C}) - \frac{\#\mathcal{C}}{\#GL_g(\mathbb{F}_p)} \right| \leqslant C_1 p^c / \sqrt{p^k}$$

for all choices of $p, k$ and $\mathcal{C}$ as above.

The assumption $g \in \{1, 2\}$ is a 'safety' measure, because we do not feel comfortable with the behavior of the hyperelliptic locus inside $\mathcal{A}_g$ as soon as $g > 2$. In fact, even for $g = 2$ some prudence is needed with respect to Principle 3: the literature seems to contain much less evidence in its favor than in the cases of Principles 1 and 2.

In contrast, for $g = 1$, Principle 3 can be proved by applying the Hasse–Weil bound to the Igusa curve $\mathrm{Ig}(p)$, whose $\mathbb{F}_{p^k}$-rational points essentially parameterize pairs $(E, P)$, where $E/\mathbb{F}_{p^k}$ is an elliptic curve and $P \in E[p](\mathbb{F}_{p^k})$. A more elementary but longer proof is given below. We include it because we believe some intermediate statements are interesting in their own right (in fact, we develop a version of [32, Theorem V.4.1], which is on the Legendre family, for Weierstrass equations). First note that Principle 3 is trivial for $p = 2$ and for $p = 3$; in the latter case because quadratic twisting provides a bijection between the set of elliptic curves having trace 1 mod 3 and the set of elliptic curves with trace 2 mod 3.

THEOREM 13. *Let $p \geqslant 5$ be a prime number, let $k \geqslant 1$ be an integer and let $t \in \{1, \ldots, p-1\}$. Let $S_t$ be the set of couples in*

$$S = \mathcal{H}_{A,B} = \{(A, B) \in (\mathbb{F}_{p^k})^2 | 4A^3 + 27B^2 \neq 0\}$$

*for which the trace $T$ of the $p^k$th power Frobenius of the elliptic curve given by $y^2 = x^3 + Ax + B$ satisfies $T \equiv t \mod p$. Then $\#S = p^{2k} - p^k$ and*

$$\left| \#S_t - \frac{\#S}{p-1} \right| \leqslant 3p^{3k/2+1}.$$

*Proof.* We leave it as an exercise to show that $\#S = p^{2k} - p^k$.

For each $(A, B) \in S$, one has that $T \bmod p$ equals the norm (with respect to $\mathbb{F}_{p^k}/\mathbb{F}_p$) of the coefficient $c_{A,B}$ of $x^{p-1}$ in

$$(x^3 + Ax + B)^{(p-1)/2}$$

(see the proof of [32, Theorem V.4.1(a)]). Lemma 8 shows that for every $\gamma \in \mathbb{F}_{p^k}^{\times}$, the polynomial $c_{A,B} - \gamma$ is absolutely irreducible when $A$ and $B$ are considered to be variables.

Now write $S'_t$ for the set of couples $(A,B) \in (\mathbb{F}_{p^k})^2$ in which $c_{A,B}$ evaluates to an element $\gamma \in \mathbb{F}_{p^k} \setminus \{0\}$ with norm $t$ (regardless of the condition $4A^3 + 27B^2 \neq 0$). There are

$$\frac{p^k - 1}{p - 1}$$

such $\gamma$ elements. For each of these, the polynomial $c_{A,B} - \gamma$ defines a plane affine curve, by the claimed irreducibility. Its degree is bounded by $d = 3(p-1)/2$, hence its (geometric) genus is at most $(d-1)(d-2)/2$, and the number of points at infinity is at most $d$. Therefore, the set $S'_\gamma \subset S'_t$ of couples satisfying $c_{A,B} = \gamma$ is subject to

$$|\#S'_\gamma - (p^k + 1)| \leqslant (d-1)(d-2)\sqrt{p^k} + d \leqslant \tfrac{9}{4}p^{k/2+2}$$

by the Hasse–Weil bound. Note that $c_{A,B} = \gamma$ defines an affine, possibly singular curve, so some caution is needed when applying the Hasse–Weil bound (see [**13**, Theorem 5.4.1] for details).

Summing up, and using $(p^k - 1)/(p-1) \leqslant \frac{5}{4}p^{k-1}$ (since $p \geqslant 5$),

$$\left| \#S'_t - \frac{p^{2k} - 1}{p - 1} \right| \leqslant \frac{45}{16} p^{3k/2+1}.$$

Because $\#(S'_t \setminus S_t) \leqslant p^k$ and $5p^{k-1} \leqslant p^k \leqslant \frac{1}{11}p^{(3/2)k+1}$, we obtain

$$\left| \#S_t - \frac{p^{2k} - p^k}{p-1} \right| \leqslant \left| \#S_t - \frac{p^{2k}-1}{p-1} \right| + \frac{p^k - 1}{p-1} \leqslant \left( \frac{45}{16} + \frac{1}{11} + \frac{5}{4} \cdot \frac{1}{55} \right) p^{(3k/2)+1},$$

which completes the proof. □

LEMMA 8. *Let $p \geqslant 5$ be a prime number and let $c_{A,B} \in \mathbb{F}_p[A,B]$ be the coefficient of $x^{p-1}$ in*

$$(x^3 + Ax + B)^{(p-1)/2} \quad \in \mathbb{F}_p[A,B][x].$$

*Then $c_{A,B}$ is homogeneous of $(2,3)$-weighted degree $(p-1)/2$, non-zero and absolutely square-free. As a consequence, for any $\gamma \in \bar{\mathbb{F}}_p^\times$, the polynomial*

$$c_{A,B} - \gamma \quad \in \bar{\mathbb{F}}_p[A,B]$$

*is irreducible.*

*Proof.* One verifies that

$$c_{A,B} = \sum_{i=\lceil (p-1)/6 \rceil}^{\lfloor (p-1)/4 \rfloor} \binom{\frac{p-1}{2}}{i} \binom{i}{3i - \frac{p-1}{2}} A^{3i-(p-1)/2} B^{(p-1)/2-2i}, \tag{18}$$

from which it immediately follows that $c_{A,B}$ is non-zero and homogeneous of degree $(p-1)/2$ if we equip $A$ and $B$ with weights 2 and 3, respectively. It is easy to verify that $A$ and $B$ appear as a factor at most once.

Let $c'_{A,B}$ be obtained from $c_{A,B}$ by deleting the factors $A$ and $B$ when possible. Define $\varepsilon_A$ and $\varepsilon_B$ to be 1 if a factor $A$ and $B$ was deleted, respectively, and 0 otherwise. Then $c'_{A,B}$ is still homogeneous, of degree $(p-1)/2 - 2\varepsilon_A - 3\varepsilon_B$. After dividing by a suitable power of $A$ and considering the resulting polynomial in the single variable $B^2/A^3$, one verifies that $c'_{A,B}$ splits (over $\bar{\mathbb{F}}_p$) as

$$c(B^2 - a_1 A^3)(B^2 - a_2 A^3) \dots (B^2 - a_r A^3), \tag{19}$$

with $r = \frac{1}{6}((p-1)/2 - 2\varepsilon_A - 3\varepsilon_B)$ and all $c, a_i \neq 0$. Each of these factors corresponds to a $j_i \neq 0, 1728$ for which the elliptic curve over $\bar{\mathbb{F}}_p$ with $j$-invariant $j_i$ is supersingular, and

conversely, all supersingular $j$-invariants different from 0 and 1728 must be represented this way. Now the number of supersingular $j$-invariants different from 0 and 1728 is precisely given by $r$ (see the proof of [**32**, Theorem V.4.1(c)]). Therefore, all factors in (19) must be different, and in particular $c_{A,B}$ must be square-free.

Now let $\gamma \in \overline{\mathbb{F}}_p^\times$ and suppose we had a non-trivial factorization

$$c_{A,B} - \gamma = (F_1 + X_1)(F_2 + X_2),$$

where $F_1$ and $F_2$ are the components of highest (weighted) degree of the respective factors. Then it follows that $F_1F_2 = c_{A,B}$, so $F_1$ and $F_2$ cannot have a common factor. It also follows that

$$X_1F_2 + X_2F_1 + X_1X_2 + \gamma = 0. \tag{20}$$

Let $X_1'$ and $X_2'$ be the components of highest degree of $X_1$ and $X_2$, respectively. Suppose $\deg X_1F_2 > \deg X_2F_1$. Then $X_1'F_2$ is zero, because it cannot be cancelled in (20). But then $X_1' = X_1 = 0$ and we run into a contradiction. By symmetry, we conclude that $\deg X_1F_2 = \deg X_2F_1$. But then $X_1'F_2 + X_2'F_1 = 0$. So all factors of $F_1$ must divide $X_1'F_2$, which is impossible unless $X_1' = 0$, and we again run into a contradiction. □

TABLE 5. *$\ell$-torsion frequencies and $c_p$ values for $C(\mathbb{F}_p)$ using random elliptic curves $C : y^2 = f(x)$ with $f \in \mathcal{H}_3^m$.*

| $p$ | | $\ell = 2$ | $\ell = 3$ | $\ell = 5$ | $\ell = 7$ | $c_p$ |
|---|---|---|---|---|---|---|
| $10^{12} + 39$ | Observed | 0.6654 | 0.3749 | 0.2507 | 0.1664 | 0.5492 |
| | Predicted | 0.6667 | 0.3750 | 0.2500 | 0.1667 | 0.5564 |
| $10^{12} + 61$ | Observed | 0.6662 | 0.5003 | 0.2083 | 0.1664 | 0.4686 |
| | Predicted | 0.6667 | 0.5000 | 0.2083 | 0.1667 | 0.4646 |
| $10^{12} + 63$ | Observed | 0.6672 | 0.3756 | 0.2503 | 0.1460 | 0.5600 |
| | Predicted | 0.6667 | 0.3750 | 0.2500 | 0.1458 | 0.5642 |
| $10^{12} + 91$ | Observed | 0.6660 | 0.4989 | 0.2089 | 0.1454 | 0.4818 |
| | Predicted | 0.6667 | 0.5000 | 0.2083 | 0.1458 | 0.4794 |
| $[10^{12}, 10^{12} + 4 \times 10^6]$ | Observed | 0.6666 | 0.4374 | 0.2396 | 0.1631 | 0.5044 |
| | Predicted | 0.6667 | 0.4375 | 0.2396 | 0.1632 | 0.5052 |

Sample size is $10^6$ (or $10^2$ for $p$ ranging over the interval $[10^{12}, 10^{12} + 4 \times 10^6]$).

TABLE 6. *$\ell$-torsion frequencies and $c_p$ values for $\mathrm{Jac}(C)(\mathbb{F}_p)$ using random genus 2 curves $C : y^2 = f(x)$ with $f \in \mathcal{H}_5^m$.*

| $p$ | | $\ell = 2$ | $\ell = 3$ | $\ell = 5$ | $\ell = 7$ | $c_p$ |
|---|---|---|---|---|---|---|
| $10^6 + 3$ | Observed | 0.7991 | 0.3616 | 0.2395 | 0.1628 | 0.3426 |
| | Predicted | 0.8000 | 0.3609 | 0.2396 | 0.1632 | 0.3444 |
| $10^6 + 37$ | Observed | 0.8000 | 0.4376 | 0.2393 | 0.1626 | 0.3056 |
| | Predicted | 0.8000 | 0.4375 | 0.2396 | 0.1632 | 0.3037 |
| $10^6 + 81$ | Observed | 0.8001 | 0.3619 | 0.2066 | 0.1632 | 0.3571 |
| | Predicted | 0.8000 | 0.3609 | 0.2067 | 0.1632 | 0.3593 |
| $10^6 + 121$ | Observed | 0.8003 | 0.4376 | 0.2059 | 0.1637 | 0.3197 |
| | Predicted | 0.8000 | 0.4375 | 0.2067 | 0.1632 | 0.3189 |
| $[10^6, 2 \times 10^6]$ | Observed | 0.8000 | 0.3992 | 0.2314 | 0.1604 | 0.3285 |
| | Predicted | 0.8000 | 0.3992 | 0.2314 | 0.1602 | 0.3290 |

Sample size is $10^6$ (or $10^2$ for $p$ ranging over the interval $[10^6, 2 \times 10^6]$).

We conclude this section with a derivation of Conjectures 6 and 7. To apply our heuristics, we need to generalize the material from Section 6. In analogy with the notation employed there, for any prime power $q$, any prime number $\ell$ and any integer $g \geqslant 1$, let $P(q,\ell,g)$ be the probability that the Jacobian of the hyperelliptic curve $y^2 + h(x)y = f(x)$, with $(f,h)$ chosen from $\mathcal{H}_{g+1,2g+2}$ uniformly at random, has an $\mathbb{F}_q$-rational $\ell$-torsion point. Let $\mathfrak{Q}(q,\ell,g)$ be the proportion of matrices of $\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)$ having 1 as an eigenvalue if $\ell \nmid q$, and the proportion of matrices of $\mathrm{GL}_g(\mathbb{F}_\ell)$ if $\ell \mid q$. Then according to Principles 2 and 3, if $g \in \{1,2\}$, we have that $P(q,\ell,g) \to \mathfrak{Q}(q,\ell,g)$ as $q \to \infty$. Recall from Theorem 6 that one has

$$\mathfrak{Q}(q,\ell,g) = \begin{cases} -\sum_{r=1}^{g} \ell^r \prod_{j=1}^{r} (1-\ell^{2j})^{-1} & \text{if } \ell \mid q-1, \\ -\sum_{r=1}^{g} \prod_{j=1}^{r} (1-\ell^{j})^{-1} & \text{if } \ell \nmid q-1 \end{cases} \tag{21}$$

TABLE 7. *$c_p$ values for the number of points on random genus 2 curves $y^2 = f(x)$ with $f \in \mathcal{H}_5^m$.*

| | $10^9+7$ | $10^9+9$ | $10^9+21$ | $10^9+33$ |
|---|---|---|---|---|
| Observed | 1.0162 | 1.0738 | 1.0892 | 1.0945 |
| Predicted | 1.0194 | 1.0790 | 1.0865 | 1.0898 |

Sample size is $10^6$. The deviations are larger here due to the shorter intervals (of width approximately $8 \times 10^{9/2}$ versus $8 \times 10^6$ and $4 \times 10^6$ in Tables 5 and 6).

TABLE 8. *Trace distributions modulo $\ell$ for random genus 2 curves $y^2 = f(x)$ with $f \in \mathcal{H}_5^m$.*

| $p$ | $\ell$ | | $t \equiv 0$ | $t \equiv 1$ | $t \equiv 2$ | $t \equiv 3$ | $t \equiv 4$ |
|---|---|---|---|---|---|---|---|
| $10^6+3$ | 2 | Observed | 0.4658 | 0.5342 | | | |
| | | Predicted | 0.4667 | 0.5333 | | | |
| | 3 | Observed | 0.3598 | 0.3205 | 0.3197 | | |
| | | Predicted | 0.3594 | 0.3203 | 0.3203 | | |
| | 5 | Observed | 0.2072 | 0.1988 | 0.1978 | 0.1981 | 0.1981 |
| | | Predicted | 0.2067 | 0.1982 | 0.1985 | 0.1985 | 0.1982 |
| $10^6+37$ | 2 | Observed | 0.4653 | 0.5346 | | | |
| | | Predicted | 0.4667 | 0.5333 | | | |
| | 3 | Observed | 0.3628 | 0.3185 | 0.3186 | | |
| | | Predicted | 0.3625 | 0.3188 | 0.3188 | | |
| | 5 | Observed | 0.2070 | 0.1982 | 0.1981 | 0.1983 | 0.1984 |
| | | Predicted | 0.2067 | 0.1985 | 0.1982 | 0.1982 | 0.1985 |
| $10^6+39$ | 2 | Observed | 0.4667 | 0.5332 | | | |
| | | Predicted | 0.4667 | 0.5333 | | | |
| | 3 | Observed | 0.3593 | 0.3206 | 0.3202 | | |
| | | Predicted | 0.3594 | 0.3203 | 0.3203 | | |
| | 5 | Observed | 0.2068 | 0.1978 | 0.1983 | 0.1989 | 0.1982 |
| | | Predicted | 0.2066 | 0.1985 | 0.1983 | 0.1983 | 0.1985 |
| $[10^6, 2\times10^6]$ | 2 | Observed | 0.4669 | 0.5331 | | | |
| | | Predicted | 0.4667 | 0.5333 | | | |
| | 3 | Observed | 0.3609 | 0.3194 | 0.3197 | | |
| | | Predicted | 0.3625 | 0.3203 | 0.3203 | | |
| | 5 | Observed | 0.2068 | 0.1982 | 0.1984 | 0.1981 | 0.1985 |
| | | Predicted | 0.2067 | 0.1984 | 0.1984 | 0.1985 | 0.1984 |

Sample size is $10^6$ (or $10^2$ for $p$ ranging over the interval $[10^6, 2\times10^6]$).

if $\ell \nmid q$. However, the same formula applies for $\ell \mid q$, because in case $\ell \nmid q-1$, the proportion of matrices of $\mathrm{GSp}_{2g}^{(q)}(\mathbb{F}_\ell)$ having 1 as an eigenvalue equals the corresponding proportion for $\mathrm{GL}_g(\mathbb{F}_\ell)$ anyway, due to Lemma 3. In other words, one can blindly adapt Theorem 6 to this more general setting. Therefore, we have the following.

*Heuristic derivation of Conjectures* 6 *and* 7. This is a copy of the heuristic derivations of Conjectures 1 and 2.

## 11. *Experimental evidence*

Tables 5–11 present experimental data in support of Conjectures 1–5. Table 5 lists $\ell$-torsion frequency data and $c_p$ values for elliptic curves, which is relevant to Conjecture 1 and the corresponding Lemma 1. Table 6 lists similar data for Jacobians of genus 2 curves (see Conjectures 2 and 3, and Lemma 2). Table 7 lists $c_p$ values for the number of points on the curves themselves, related to Conjecture 4, while Table 8 gives experimental trace distributions of genus 2 curves modulo $\ell$ (see Table 3). Tables 9 and 10 relate to Theorem 1 and Conjecture 5, concerning the rank of the Jacobians of curves of genus 1 and 2, respectively. Finally, Table 11 supports Conjecture 6 on the case of extension fields in genus 1.

TABLE 9. *Rank frequencies for $C(\mathbb{F}_p)$ for random elliptic curves $C : y^2 = f(x)$ with $f \in \mathcal{H}_3^m$.*

| $p$ | $\ell$ | | Rank 0 | Rank 1 | Rank 2 |
|---|---|---|---|---|---|
| $10^{12}+39$ | 2 | Observed | 0.3346 | 0.4993 | 0.1661 |
| | | Predicted | 0.3333 | 0.5000 | 0.1667 |
| | 3 | Observed | 0.6251 | 0.3334 | 0.0415 |
| | | Predicted | 0.6250 | 0.3333 | 0.0417 |
| | 5 | Observed | 0.7492 | 0.2507 | |
| | | Predicted | 0.7500 | 0.2500 | |
| | $\infty$ | Observed | | 0.7988 | 0.2013 |
| | | Predicted | | 0.7980 | 0.2020 |
| $10^{12}+61$ | 2 | Observed | 0.3338 | 0.4996 | 0.1666 |
| | | Predicted | 0.3333 | 0.5000 | 0.1667 |
| | 3 | Observed | 0.4997 | 0.5003 | |
| | | Predicted | 0.5000 | 0.5000 | |
| | 5 | Observed | 0.7917 | 0.1999 | 0084 |
| | | Predicted | 0.7917 | 0.2000 | 0083 |
| | $\infty$ | Observed | | 0.8263 | 0.1737 |
| | | Predicted | | 0.8264 | 0.1736 |
| $10^{12}+63$ | 2 | Observed | 0.3328 | 0.4995 | 0.1677 |
| | | Predicted | 0.3333 | 0.5000 | 0.1667 |
| | 3 | Observed | 0.6244 | 0.3339 | 0.0416 |
| | | Predicted | 0.6250 | 0.3333 | 0.0417 |
| | 5 | Observed | 0.7497 | 0.2503 | |
| | | Predicted | 0.7500 | 0.2500 | |
| | $\infty$ | Observed | | 0.7953 | 0.2047 |
| | | Predicted | | 0.7962 | 0.2038 |
| $[10^{12}, 2\times10^{12}+4\times10^6]$ | 2 | Observed | 0.3334 | 0.4999 | 0.1666 |
| | | Predicted | 0.3333 | 0.5000 | 0.1667 |
| | 3 | Observed | 0.5626 | 0.4166 | 0.0208 |
| | | Predicted | 0.5635 | 0.4167 | 0.0208 |
| | 5 | Observed | 0.7604 | 0.2375 | 0.0021 |
| | | Predicted | 0.7604 | 0.2375 | 0.0021 |
| | $\infty$ | Observed | | 0.8138 | 0.1862 |
| | | Predicted | | 0.8138 | 0.1862 |

Sample size is $10^6$ (or $10^2$ for $p$ ranging over the interval $[10^{12}, 2\times10^{12}]$). Rows with $\ell=\infty$ indicate maximum $\ell$-rank over all primes $\ell$.

The data in Tables 5–10 were obtained using the SMALLJAC library [33], based on the algorithms described in [21]. Table 11 was obtained using the intrinsic MAGMA [7] point counting function. We conducted our tests by sampling random curves $C$ over finite fields $\mathbb{F}_p$. We collected data both using fixed primes $p$, and for all primes in a given interval. For genus 1,

TABLE 10. *Rank frequencies for $Jac(C)(\mathbb{F}_p)$ for random genus 2 curves $C : y^2 = f(x)$ with $f \in \mathcal{H}_5^m$.*

| $p$ | $\ell$ | | Rank 0 | Rank 1 | Rank 2 | Rank 3 | Rank 4 |
|---|---|---|---|---|---|---|---|
| $10^6 + 3$ | 2 | Observed | 0.200113 | 0.416313 | 0.291528 | 0.083775 | 0.008271 |
| | | Predicted | 0.200000 | 0.416667 | 0.291667 | 0.083333 | 0.008333 |
| | 3 | Observed | 0.637964 | 0.320212 | 0.040254 | 0.001548 | 0.000022 |
| | | Predicted | 0.639063 | 0.319444 | 0.039931 | 0.001543 | 0.000019 |
| | 5 | Observed | 0.761095 | 0.236804 | 0.002101 | | |
| | | Predicted | 0.760417 | 0.237500 | 0.002083 | | |
| | $\infty$ | Observed | | 0.589030 | 0.317489 | 0.085188 | 0.008293 |
| | | Predicted | | 0.589471 | 0.317443 | 0.084733 | 0.008352 |
| $10^6 + 81$ | 2 | Observed | 0.200794 | 0.416446 | 0.290857 | 0.083593 | 0.008310 |
| | | Predicted | 0.200000 | 0.416667 | 0.291667 | 0.083333 | 0.008333 |
| | 3 | Observed | 0.637636 | 0.320698 | 0.040107 | 0.001533 | 0.000026 |
| | | Predicted | 0.639063 | 0.319444 | 0.039931 | 0.001543 | 0.000019 |
| | 5 | Observed | 0.793657 | 0.198090 | 0.008186 | 0.000067 | 0.000000 |
| | | Predicted | 0.793336 | 0.198333 | 0.008264 | 0.000067 | 0.000000 |
| | $\infty$ | Observed | | 0.586416 | 0.320192 | 0.085056 | 0.008336 |
| | | Predicted | | 0.585781 | 0.321073 | 0.084794 | 0.008353 |
| $10^6 + 133$ | 2 | Observed | 0.199300 | 0.416997 | 0.292156 | 0.083233 | 0.008314 |
| | | Predicted | 0.200000 | 0.416667 | 0.291667 | 0.083333 | 0.008333 |
| | 3 | Observed | 0.562514 | 0.416732 | 0.020754 | | |
| | | Predicted | 0.562500 | 0.416667 | 0.020833 | | |
| | 5 | Observed | 0.760019 | 0.237919 | 0.002062 | | |
| | | Predicted | 0.760417 | 0.237500 | 0.002083 | | |
| | $\infty$ | Observed | | 0.600296 | 0.308148 | 0.083242 | 0.008314 |
| | | Predicted | | 0.600635 | 0.307690 | 0.083341 | 0.008333 |
| $[10^6, 2 \times 10^6]$ | 2 | Observed | 0.200039 | 0.416528 | 0.291761 | 0.083320 | 0.008353 |
| | | Predicted | 0.200000 | 0.416667 | 0.291667 | 0.083333 | 0.008333 |
| | 3 | Observed | 0.600830 | 0.368047 | 0.030337 | 0.000777 | 0.000009 |
| | | Predicted | 0.600781 | 0.368056 | 0.030382 | 0.000772 | 0.000010 |
| | 5 | Observed | 0.768609 | 0.227739 | 0.003637 | 0.000016 | 0.000000 |
| | | Predicted | 0.768647 | 0.227708 | 0.003629 | 0.000017 | 0.000000 |
| | $\infty$ | Observed | | 0.594471 | 0.313125 | 0.084043 | 0.008362 |
| | | Predicted | | 0.594567 | 0.313040 | 0.084050 | 0.008343 |

Sample size is $10^6$ (or $10^2$ $p$ ranging over the interval $[10^6, 2 \times 10^6]$). Rows with $\ell = \infty$ indicate maximum $\ell$-rank over all primes $\ell$.

TABLE 11. *$\ell$-torsion frequencies and $c_k$ values for $C(\mathbb{F}_{p^k})$ using random elliptic curves $C : y^2 = f(x)$ with $f \in \mathcal{H}_3^m$.*

| $p^k$ | | $\ell = 2$ | $\ell = 3$ | $\ell = 5$ | $\ell = 7$ | $\ell = 11$ | $c_k$ |
|---|---|---|---|---|---|---|---|
| $3^{26}$ | Observed | 0.6669 | 0.4999 | 0.2501 | 0.1666 | 0.1000 | 0.4387 |
| | Predicted | 0.6667 | 0.5000 | 0.2500 | 0.1667 | 0.1000 | 0.4401 |
| $5^{18}$ | Observed | 0.6667 | 0.3748 | 0.2501 | 0.1458 | 0.1000 | 0.5659 |
| | Predicted | 0.6667 | 0.3750 | 0.2500 | 0.1458 | 0.1000 | 0.5662 |
| $7^{15}$ | Observed | 0.6667 | 0.3751 | 0.2499 | 0.1667 | 0.1001 | 0.5541 |
| | Predicted | 0.6667 | 0.3750 | 0.2500 | 0.1667 | 0.1000 | 0.5523 |
| $11^{12}$ | Observed | 0.6665 | 0.3749 | 0.2083 | 0.1457 | 0.1002 | 0.6020 |
| | Predicted | 0.6667 | 0.3750 | 0.2083 | 0.1458 | 0.1000 | 0.6015 |

Sample size is $10^7$.

we used $p \approx 10^{12}$ and for genus 2 we used $p \approx 10^6$ (except for Table 7) so that in both cases $\#\mathrm{Jac}(C)(\mathbb{F}_p) \approx 10^{12}$. Each test with a fixed prime used a sample size of approximately $10^6$, while our interval tests used $10^2$ curves for each of at least $10^4$ primes. In order to maximize the performance of the algorithms used to collect the data, we restricted our tests to curves of the form $y^2 = f(x)$, where $f$ is a monic polynomial of degree $2g + 1$. Therefore, in genus 2, our experimental data should be compared with the $\mathcal{H}_5^m$ analogues of the conjectures that deal with $\mathcal{H}_6$ (which according to Theorem 10 only affects the contribution of $\ell = 2$, the necessary adaptations to which can be made using Table 2).

*Acknowledgements.* We thank Steven Galbraith for proposing this research, and Jeff Achter, Jason Fulman, Frans Oort, Bjorn Poonen, Alessandra Rigato, Igor Shparlinski, Marco Streng and the anonymous referee for some helpful comments. The first author is grateful to the Massachusetts Institute of Technology for its hospitality.

## *References*

**1.** J. Achter, 'The distribution of class groups of function fields', *J. Pure Appl. Algebra* 204 (2006) 316–333.
**2.** J. Achter, 'Results of Cohen-Lenstra type for quadratic function fields', *Computational Arithmetic Geometry*, American Mathematical Society Contemporary Mathematics 463 (American Mathematical Society, Providence, RI, 2008) 1–7.
**3.** J. Achter and J. Holden, 'Notes on an analogue of the Fontaine–Mazur conjecture', *J. Théor. Nombres Bordeaux* 15 (2003) 627–637.
**4.** J. Achter and R. Pries, 'The $p$-rank strata of the moduli space of hyperelliptic curves', *Adv. Math.* (5) 227 (2011) 1846–1872.
**5.** A. Balog, A.-C. Cojocaru and C. David, 'Average twin prime conjecture for elliptic curves', *Amer. J. Math.* (5) 133 (2011) 1179–1229.
**6.** J. Bergström, C. Faber and G. van der Geer, 'Siegel modular forms of genus 2 and level 2: cohomological computations and conjectures', *Int. Math. Res. Not.* (2008) 20.
**7.** W. Bosma, J. Cannon and C. Playoust, 'The Magma algebra system I: The user language', *J. Symbolic Comput.* 24 (1997) 235–265.
**8.** R. Bröker, 'Constructing elliptic curves of prescribed order', Ph.D. thesis, Universiteit Leiden (2006).
**9.** W. Castryck and H. Hubrechts, 'The distribution of the number of points modulo an integer on elliptic curves over finite fields', Preprint, http://arxiv.org/abs/0902.4332.
**10.** N. Chavdarov, 'The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy', *Duke Math. J.* 87 (1997) 151–180.
**11.** H. Cohen and H. W. Lenstra, Jr., 'Heuristics on class groups of number fields', *Number theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, Lecture Notes in Mathematics 1068 (Springer, Berlin, 1984) 33–62.
**12.** G. Cornelissen, 'Two-torsion in the Jacobian of hyperelliptic curves over finite fields', *Arch. Math.* 77 (2001) 241–246.
**13.** M. Fried and M. Jarden, *Field arithmetic, Ergebnisse der Mathematik und ihrer Grenzgebiete*, 3. Folge, Bd. 11 3rd edn (Springer, Berlin, 1986).
**14.** J. Fulman, 'A probabilistic approach toward conjugacy classes in the finite general linear and unitary groups', *J. Algebra* 212 (1999) 557–590.
**15.** J. Fulman, 'A probabilistic approach to conjugacy classes in the finite symplectic and orthogonal groups', *J. Algebra* 234 (2000) 207–224.
**16.** J. Fulman and R. Guralnick, 'Conjugacy class properties of the extension of $\mathrm{GL}(n, q)$ generated by the inverse transpose involution', *J. Algebra* 275 (2004) 356–396.
**17.** S. Galbraith and J. McKee, 'The probability that the number of points on an elliptic curve over a finite field is prime', *J. London Math. Soc.* 62 (2000) 671–684.
**18.** G. Gasper and M. Rahman, *Basic hypergeometric series*, (Cambridge University Press, Cambridge 1990).
**19.** E. Howe, 'On the group orders of elliptic curves over finite fields', *Compos. Math.* 85 (1993) 229–247.
**20.** N. Katz and P. Sarnak, *Random matrices, Frobenius eigenvalues, and monodromy* AMS Colloquium Publications (American Mathematical Society, Providence, RI, 1999).
**21.** K. Kedlaya and A. V. Sutherland, 'Computing L-series of hyperelliptic curves', Algorithmic Number Theory 8th International Symposium (ANTS VIII), Lecture Notes in Computer Science 5011 (Springer, Berlin, 2008) 312–326.
**22.** D. S. Kim, 'Gauss sums for symplectic groups over a finite field', *Monatsh. Math.* 126 (1998) 55–71.
**23.** N. Koblitz, 'Primality of the number of points on an elliptic curve over a finite field', *Pacific J. Math.* 131 (1988) 157–165.
**24.** J. Lengler, 'The Cohen-Lenstra heuristic: methodology and results', *J. Algebra* 323 (2010) 2960–2976.

**25.** H. Lenstra, 'Factoring integers with elliptic curves', *Ann. Math.* 126 (1987) 649–673.
**26.** G. Malle, 'On the distribution of class groups of number fields', *Experiment. math.* 19 (2010) 465–474.
**27.** E. Nart, 'Counting hyperelliptic curves', *Adv. Math.* 221 (2009) 774–787.
**28.** P. Norman and F. Oort, 'Moduli of abelian varieties', *Ann. of Math.* 112 (1980) 413–439.
**29.** R. Pries and H. J. Zhu, 'The $p$-rank stratification of Artin-Schreier curves', Preprint, http://www.math.colostate.edu/∼pries/Preprints/paper34fourier610.pdf.
**30.** A. Rudvalis and K. Shinoda, 'An enumeration in finite classical groups', unpublished report, Department of Mathematics, University of Massachusetts, Amherst, 1988.
**31.** R. Schoof, 'Counting points on elliptic curves over finite fields', *J. Théor. Nombres Bordeaux* 7 (1995) 219–254.
**32.** J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics 106 (Springer, New York 1986).
**33.** A. V. Sutherland, smalljac library, version 3.0, available at http://math.mit.edu/ drew (2008).
**34.** S. G. Vlăduţ, 'Cyclicity statistics for elliptic curves over finite fields', *Finite Fields Appl.* 5 (1999) 13–25.
**35.** A. Weng, 'Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation', Ph.D. thesis, Universität Essen (2001), available at http://www.iem.uni-due.de/zahlentheorie/preprints/wengthesis.pdf

*Wouter Castryck*
*Departement Wiskunde*
*Katholieke Universiteit Leuven*
*Celestijnenlaan 200B*
*3001 Leuven (Heverlee)*
*Belgium*

wouter.castryck@gmail.com

*Hendrik Hubrechts*
*Departement Wiskunde*
*Katholieke Universiteit Leuven*
*Celestijnenlaan 200B*
*3001 Leuven (Heverlee)*
*Belgium*
*and*
*Département de Mathématique*
*Université Libre de Bruxelles*
*Boulevard du Triomphe*
*1050 Brussels*
*Belgium*

hendrik.hubrechts@wis.kuleuven.be

*Amanda Folsom*
*Department of Mathematics*
*Yale University*
*PO Box 208283*
*New Haven, CT 06520-8283*
*USA*

amanda.folsom@yale.edu

*Andrew V. Sutherland*
*Department of Mathematics*
*Massachusetts Institute of Technology*
*77 Massachusetts Avenue*
*Cambridge, MA 02139-4307*
*USA*

drew@math.mit.edu