

The distribution of the number of points modulo an integer on elliptic curves over finite fields

Wouter Castryck* and Hendrik Hubrechts*

Abstract

Let \mathbb{F}_q be a finite field and let b and N be integers. We prove explicit estimates for the probability that the number of rational points on a randomly chosen elliptic curve E over \mathbb{F}_q equals b modulo N . The underlying tool is an equidistribution result on the action of Frobenius on the N -torsion subgroup of E . Our results subsume and extend previous work by Achter and Gekeler.

Keywords: elliptic curves, finite fields, Frobenius statistics, modular curves

MSC 2010: 14H52, 14K10

1 Introduction

If one writes the number of rational points on an elliptic curve E over a finite field \mathbb{F}_q as $q + 1 - T_E$, then the integer T_E is called the trace of Frobenius of E . Hasse proved that $T_E \in [-2\sqrt{q}, 2\sqrt{q}]$, but within this interval the trace of Frobenius is an unpredictable number, seemingly picked at random. Since the 1960's, its statistical behavior has become subject to extensive study.

To make the problem well-defined, the best-known approach is to fix an elliptic curve E over a number field K and to consider it modulo various prime ideals $\mathfrak{p} \subset \mathcal{O}_K$ of good reduction. Based on experimental evidence, Sato and Tate conjecturally described how the traces of Frobenius of $E \bmod \mathfrak{p}$ are (after being normalized by $2\sqrt{N(\mathfrak{p})}$) distributed along the interval $[-1, 1]$. We refer to [5] for the details and an introduction to the recent progress on this matter.

Another approach is to fix the finite field \mathbb{F}_q and to consider all \mathbb{F}_q -isomorphism classes of elliptic curves E over it. Their traces of Frobenius T_E define a discrete probability measure μ_q on $\{-\lfloor 2\sqrt{q} \rfloor, \dots, \lfloor 2\sqrt{q} \rfloor\}$. As above, one can normalize to obtain a distribution $\tilde{\mu}_q$ on $[-1, 1]$. Birch [4], Deligne [9, 3.5.7] and Yoshida [24] proved results on the limiting behavior of $\tilde{\mu}_q$ as q tends to infinity,

*Address: Katholieke Universiteit Leuven, Departement Wiskunde, Celestijnenlaan 200B, 3001 Leuven (Heverlee), Belgium; E-mail: firstname.lastname@wis.kuleuven.be;

thereby lending indirect support for the Sato-Tate conjecture. However, some interesting properties that are related to the discrete nature of μ_q become dissolved in the limit procedure. As an introductory exercise, the reader is invited to show that when q is odd, T_E favors even numbers. This is related to the fact that a randomly chosen cubic polynomial $f(x) \in \mathbb{F}_q[x]$ has a rational root with a probability that tends to $\frac{2}{3}$ as q tends to infinity. More generally, for any integer $N \geq 2$, the probability that $\#E(\mathbb{F}_q) = q + 1 - T_E$ is divisible by N tends to be strictly bigger than $\frac{1}{N}$. Lenstra was the first to observe this phenomenon in his famous paper [20, Prop. 1.14] — which has implications for integer factorization [20] and cryptography [12] — and he proved explicit estimates in the situation where N is a prime number different from $p = \text{char}(\mathbb{F}_q)$. The proof uses modular curves and was generalized to arbitrary N by Howe [16, Thm. 1.1].

In this article, we study the more general question of how $\#E(\mathbb{F}_q)$ modulo N is distributed along $\{0, 1, \dots, N-1\}$. For an arbitrary integer $N \geq 2$ and $t \in \mathbb{Z}_{\geq 0}$, write $P_{q,N}(t)$ for the probability that $T_E \equiv t \pmod{N}$. We prove:

Theorem 1 *Let $Q = \{p^k \mid p \text{ prime}, k \in \mathbb{Z}_{\geq 1}\}$, and let $r : Q \times \mathbb{Z}_{\geq 1} \times \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Q}_{>0}$ be the unique function satisfying the following rules.*

- (i) *r is a multiplicative arithmetic function in the second argument, i.e. for all $q \in Q$, $t \in \mathbb{Z}_{\geq 0}$ and coprime $M, N \in \mathbb{Z}_{\geq 1}$ one has*

$$r(q, MN, t) = r(q, M, t) \cdot r(q, N, t).$$

- (ii) *If $N = \ell^n$ for an integer $n \geq 1$ and a prime number ℓ , then for all $q \in Q$ that are coprime to ℓ and all $t \in \mathbb{Z}_{\geq 0}$ one has*

$$r(q, N, t) = \frac{\Psi(t^2 - 4q)}{\ell^{3n} - \ell^{3n-2}}$$

for the function $\Psi : \mathbb{Z} \rightarrow \mathbb{Z}$ that is described explicitly in Section 3 below. In case $\ell \geq 3$ and $n = 1$ we have $\Psi : x \mapsto \ell^2 + \left(\frac{x}{\ell}\right)\ell$, where (\cdot) is the Legendre symbol.

- (iii) *If $N = p^e$ for an integer $e \geq 1$ and a prime number p , then for all $q \in Q$ that are a power of p and all $t \in \mathbb{Z}_{\geq 0}$ one has*

$$r(q, N, t) = \begin{cases} \frac{1}{p^e - p^{e-1}} & \text{if } t \not\equiv 0 \pmod{p}, \\ 0 & \text{if } t \equiv 0 \pmod{p}. \end{cases}$$

Then there exists an absolute and explicitly computable constant $C \in \mathbb{R}_{>0}$ such that for all $q \in Q$, $N \in \mathbb{Z}_{\geq 1}$ and $t \in \mathbb{Z}_{\geq 0}$ one has

$$|P_{q,N}(t) - r(q, N, t)| \leq C \cdot \frac{N^2 \ln \ln N}{\sqrt{q}}.$$

Theorem 1 is essentially obtained from an equidistribution result on the action of q th power Frobenius on the N -torsion group $E[N]$ of E . Throughout this article, for any integer A we will write Z_A for the ring of residues $\mathbb{Z}/(A)$. Factor N as $N'p^e$, where N' is coprime to p . In case $e \geq 1$, we suppose that E is taken from the set of ordinary elliptic curves. Then $E[N] \cong E[N'] \oplus E[p^e] \cong Z_{N'} \oplus Z_{N'} \oplus Z_{p^e}$. With respect to a $Z_{N'}$ -module basis of $E[N']$ and a generator of $E[p^e]$, the action of q th power Frobenius is given by a pair

$$(F, T) \in \mathrm{GL}_2(Z_{N'}) \oplus Z_{p^e}^\times$$

satisfying $\det F \equiv q \pmod{N'}$, $\mathrm{Tr} F \equiv T_E \pmod{N'}$, and $T \equiv T_E \pmod{p^e}$. When considering all bases of $E[N']$, the corresponding matrices F yield a conjugacy class of $\mathrm{GL}_2(Z_{N'})$ which we denote by \mathcal{F}_E . In contrast, the element T does not depend on the generator of $E[p^e]$; for sake of consistency, we will denote it by \mathcal{T}_E . Note that $(\mathcal{F}_E, \mathcal{T}_E)$ can in fact be seen as a conjugacy class of $\mathrm{GL}_2(Z_{N'}) \oplus Z_{p^e}^\times$. Denote the subset of $\mathrm{GL}_2(Z_{N'})$ consisting of all matrices of determinant q by $\mathcal{M}_{q, N'}$. Then the equidistribution theorem reads:

Theorem 2 *There exists an absolute and explicitly computable constant $C \in \mathbb{R}_{>0}$ such that for every conjugacy class $\mathcal{F} \subset \mathrm{GL}_2(Z_{N'})$ of matrices of determinant q and every element $T \in Z_{p^e}^\times$ one has*

$$\left| P_{\mathcal{F}, T} - \frac{\#\mathcal{F}}{\#\mathcal{M}_{q, N'}} \cdot \frac{1}{\varphi(p^e)} \right| \leq C \cdot \frac{p^e N'^2 \ln \ln N'}{\sqrt{q}},$$

where φ is Euler's totient function and $P_{\mathcal{F}, T}$ is the probability that

- $\mathcal{F}_E = \mathcal{F}$ if $e = 0$;
- E is ordinary and $(\mathcal{F}_E, \mathcal{T}_E) = (\mathcal{F}, T)$ if $e \geq 1$.

Loosely stated: if q gets big, a Frobenius conjugacy class becomes as likely as its own relative size.

Theorem 2 fits within the random matrix philosophy that dominates nowadays research on the statistical behavior of Frobenius, both in the Sato-Tate setting (fixed curve, varying field) as in the setting of a fixed field and a varying curve. This was initialized by Deligne, who obtained his earlier-mentioned result as a consequence to an equidistribution theorem in étale cohomology. The random matrix idea has proven to provide well-working models for higher genus analogues of the Frobenius distribution problem [18, 19], although many statements remain conjectural. The standard reference has become the book by Katz and Sarnak [18], who also refined Deligne's equidistribution theorem to a version [18, 9.7] that was used by Achter to prove a variant of Theorem 2 that works in arbitrary genus [2, Thm. 3.1]. However, Achter's result involves certain mild restrictions on q and N , the main one being that q and N should be coprime. Our attention will be devoted to a slightly more elementary approach, based on the modular covering $X(p^e; \zeta_{N'}) \rightarrow X(1; 1)$ and Chebotarev's density theorem for function fields. Apart from resolving the conditions on q and N ,

this has the additional advantage of yielding a tighter error bound: in Achter's case it is of the form $C \cdot N^3/\sqrt{q}$. There is no doubt that several specialists in the field expected an approach using Chebotarev's density theorem to work, but up to our knowledge, a complete proof of Theorem 2 did not appear in the literature before.

Given Theorem 2, the proof of Theorem 1 then comes down to determining the number of matrices in $\mathcal{M}_{q,N}$ with trace t . This is elaborated in Section 3. Again, large parts of this matrix count have been carried out before, now by Gekeler [13], who worked towards estimating $P_{q,N}(t)$ under certain mild conditions on q and N , while assuming the random matrix principle as a black box. The current article can therefore be viewed as a self-contained subsumption of both Achter's result in genus 1 and Gekeler's count, providing more elementarily flavored proofs and removing the restrictions on q and N .

It is worth noting that Theorem 2 can be used to study a number of alternative questions, various of which have been addressed in the literature before, albeit often conjecturally. E.g., in the weaker set-up where \mathbb{F}_q is a large prime field that is chosen at random, Gekeler studied the probability that $E[\ell^\infty](\mathbb{F}_q)$ has a given structure and the probability that $E(\mathbb{F}_q)$ is cyclic [14, 15]. The latter probability has also been investigated by Vlăduț in case \mathbb{F}_q is fixed [23], building on Howe's aforementioned work. Still for \mathbb{F}_q fixed, Galbraith and McKee conjecturally estimated the chance that $E(\mathbb{F}_q)$ is a prime number [12]. Achter and Sadornil studied the probability that E has a given number of rational isogenies of given prime degree emanating from it [3]. For higher genus curves C/\mathbb{F}_q , Achter gave explicit estimates for the chance that $\text{Jac}(C)[N](\mathbb{F}_q)$ has a given structure [1, 2], and Chavdarov proved that the numerator of the zeta function $Z_C(T)$ is generically irreducible [7]. Recently, the current authors, Folsom and Sutherland [6] studied the probabilities of having prime order and of cyclicity of $\text{Jac}(C)[N](\mathbb{F}_q)$.

One interesting question that did not see explicit study so far is on the probability $P'_q(N)$ that E contains a rational point of given order N . In Section 4 we prove:

Theorem 3 *Let $r' : Q \times \mathbb{Z}_{\geq 1} \rightarrow \mathbb{Q}_{\geq 0}$ be the unique function satisfying the following rules.*

- (i) *r' is a multiplicative arithmetic function in the second argument, i.e. for all $q \in Q$ and coprime $M, N \in \mathbb{Z}_{\geq 1}$ one has*

$$r'(q, MN) = r'(q, M) \cdot r'(q, N).$$

- (ii) *If $N = \ell^n$ for an integer $n \geq 1$ and a prime number ℓ , then for all $q \in Q$ that are coprime to ℓ one has*

$$r'(q, N) = \begin{cases} 1/(\ell^n - \ell^{n-2}) & \text{if } \nu \geq n, \\ (\ell^{2\nu+1} + 1)/(\ell^{n+2\nu-1}(\ell^2 - 1)) & \text{if } \nu < n, \end{cases}$$

where ν is the ℓ -adic valuation of $(q-1)$.

(iii) If $N = p^e$ for an integer $e \geq 1$ and a prime number p , then for all $q \in Q$ that are a power of p one has

$$r'(q, N) = 1/(p^e - p^{e-1}).$$

Then there exists an absolute and explicitly computable constant $C \in \mathbb{R}_{>0}$ such that for all $q \in Q$ and $N \in \mathbb{Z}_{\geq 1}$ one has

$$|P'_q(N) - r'(q, N)| \leq C \cdot \frac{N^2 \ln \ln N}{\sqrt{q}}.$$

In fact, this theorem can be derived directly from the work of Howe [16, Thm. 1.1], instead of Theorem 2.

2 Equidistribution of Frobenius

In this section, we will prove Theorem 2. The two main theoretical ingredients are the modular curve $X(p^e; \zeta_{N'})$ and Chebotarev's density theorem for function fields.

We first recall some facts on modular curves. Let \mathbb{F}_q be a finite field of characteristic p having q elements, let N be a positive integer, and write $N = N'p^e$ with N' coprime to p . Assume throughout that $N' > 2$. Fix an algebraic closure $\overline{\mathbb{F}}_q$ of \mathbb{F}_q and a primitive N' th-root of unity $\zeta_{N'} \in \overline{\mathbb{F}}_q$. Consider all quartets (E, P, Q, R) for which E is an elliptic curve over $\overline{\mathbb{F}}_q$ and

- $P, Q \in E[N']$ satisfy $e_{N'}(P, Q) = \zeta_{N'}$, where

$$e_{N'} : E[N'] \times E[N'] \rightarrow \{N'\text{th-roots of unity}\}$$

is the Weil pairing [22, III.§8];

- $R \in E^{(p^e)}$ is a generator of the kernel of the Verschiebung $V_{p^e} : E^{(p^e)} \rightarrow E$, where $E^{(p^e)}$ is the elliptic curve obtained by raising all coefficients of a model of E to the p^e th power.

Two quartets (E, P, Q, R) and (E', P', Q', R') are called equivalent if there exists an $\overline{\mathbb{F}}_q$ -isomorphism $E \rightarrow E'$ mapping P to P' and Q to Q' , such that the induced isomorphism $E^{(p^e)} \rightarrow E'^{(p^e)}$ takes R to R' . As a special instance, using multiplication by -1 , we have that (E, P, Q, R) is equivalent to $(E, -P, -Q, -R)$. Denote the set of equivalence classes of such quartets by $Y(p^e; \zeta_{N'})$. Then there exists an irreducible nonsingular projective curve $X(p^e; \zeta_{N'})$ over $\overline{\mathbb{F}}_q$, along with a morphism

$$J : X(p^e; \zeta_{N'}) \rightarrow \mathbb{P}^1 \supset \text{Spec } \overline{\mathbb{F}}_q[j]$$

such that

- the points of $J^{-1}(\text{Spec } \overline{\mathbb{F}}_q[j])$ are in bijective correspondence with $Y(p^e; \zeta_{N'})$, giving the latter the structure of an irreducible nonsingular affine curve over $\overline{\mathbb{F}}_q$;

- if $x \in J^{-1}(\text{Spec } \overline{\mathbb{F}}_q[j])$ corresponds to a quartet (E, P, Q, R) , then $J(x) = j(E)$, the j -invariant of E ;
- J is a Galois covering with Galois group $(\text{SL}_2(Z_{N'}) \oplus Z_{p^e}^\times) / \{\pm 1\}$, where $\{\pm 1\}$ is understood to be diagonally embedded; the action is such that an element

$$\pm \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, u \right)$$

takes the point corresponding to the class $(E, P, Q, R) \in Y(p^e; \zeta_{N'})$ to the point corresponding to $(E, aP + cQ, bP + dQ, uR)$.

Moreover, $X(p^e; \zeta_{N'})$ and J are naturally defined over $\mathbb{F}_q(\zeta_{N'})$, and for $k = [\mathbb{F}_q(\zeta_{N'}) : \mathbb{F}_q]$ the action of q^k th power Frobenius on $X(p^e; \zeta_{N'})$ commutes with the action of the Galois group. When restricted to $Y(p^e; \zeta_{N'})$, the Frobenius action is given by $(E, P, Q, R) \mapsto (E^{(q^k)}, P^{(q^k)}, Q^{(q^k)}, R^{(q^k)})$. The genus of $X(p^e; \zeta_{N'})$ equals

$$\begin{cases} 1 + \frac{1}{24}(N-6)\varphi(N)\tilde{\varphi}(N) & \text{if } e = 0 \\ 1 + \frac{1}{48}(N-12)\varphi(N)\tilde{\varphi}(N') & \text{if } e \geq 1. \end{cases} \quad (1)$$

Here $\varphi : x \mapsto x \prod_{p|x} (1 - 1/p)$ is Euler's totient function, and $\tilde{\varphi}$ is, somehow dually, defined by $x \mapsto x \prod_{p|x} (1 + 1/p)$.

For a proof of the above statements, we refer to the notes by Deligne and Rapoport [10], the article of Howe [16, Prop. 3.1 and 3.2] and the many references therein to the book of Katz and Mazur [17]. In the latter, the curve $X(p^e; \zeta_{N'})$ is denoted $\mathfrak{M}(\mathcal{P})$, where \mathcal{P} is the moduli problem $([\Gamma(N')]^{\text{can}}, [\text{Ig}(p^e)])$ over $(\text{Ell}/\overline{\mathbb{F}}_q)$. Howe denotes this curve by $\overline{X}(N', N)$. The condition $N' > 2$ is necessary for $[\Gamma(N')]^{\text{can}}$ to be representable in the sense of [17, (4.3)]; see also [17, (10.9.3)]. It is possible to construct similar modular curves for $N' \leq 2$, as illustrated by Howe [16, Prop. 3.1], but we will not need this.

The $\mathbb{F}_q(\zeta_{N'})$ -rational morphism J gives rise to a field extension

$$\mathbb{F}_q(\zeta_{N'})(j) \subset \mathbb{F}_q(\zeta_{N'})(X(p^e; \zeta_{N'})) =: L.$$

Our central object of interest will be the larger extension

$$K := \mathbb{F}_q(j) \subset \mathbb{F}_q(\zeta_{N'})(j) \subset L.$$

It allows a modular interpretation as follows. Let $H \subset Z_{N'}^\times$ be the group generated by $q \bmod N'$. Under the map $h \mapsto \zeta_{N'}^h$, its elements are in bijective correspondence with the $\text{Gal}(\mathbb{F}_q(\zeta_{N'}), \mathbb{F}_q)$ -orbit of $\zeta_{N'}$. Then similar to before, using $[\Gamma(N')]^{\mathbb{Z}[\zeta_{N'}]^H\text{-can}}$ instead of $[\Gamma(N')]^{\text{can}}$, we can define a complete nonsingular (but possibly reducible) curve $X^H(p^e; \zeta_{N'})$ over $\overline{\mathbb{F}}_q$ along with a morphism J^H to \mathbb{P}^1 , such that

- $(J^H)^{-1}(\text{Spec } \overline{\mathbb{F}}_q[j])$ can be identified with

$$Y^H(p^e; \zeta_{N'}) := Y(p^e; \zeta_{N'}) \sqcup Y(p^e; \zeta_{N'}^q) \sqcup \dots \sqcup Y(p^e; \zeta_{N'}^{q^{k-1}});$$

- if $x \in (J^H)^{-1}(\text{Spec } \overline{\mathbb{F}}_q[j])$ corresponds to a quartet (E, P, Q, R) , then $J^H(x) = j(E)$;
- J^H is a Galois covering with Galois group $G = (\text{GL}_2^H(Z_{N'}) \oplus Z_{p^e}^\times) / \{\pm 1\}$, where $\text{GL}_2^H(Z_{N'})$ is the group of matrices of $\text{GL}_2(Z_{N'})$ taking determinants in H ; on $Y^H(p^e; \zeta_{N'})$, the action of an element

$$\pm \left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, u \right) \quad (2)$$

is such that it takes the point corresponding to the class (E, P, Q, R) to the point corresponding to $(E, aP + cQ, bP + dQ, uR)$.

Moreover, $X^H(p^e; \zeta_{N'})$ and J^H can be defined over \mathbb{F}_q , and the action of q th power Frobenius on $Y^H(p^e; \zeta_{N'})$ is given by $(E, R, P, Q) \mapsto (E^{(q)}, R^{(q)}, P^{(q)}, Q^{(q)})$. This action commutes with the action of the Galois group. Considered as a scheme over \mathbb{F}_q , the curve $X^H(N'; \zeta_{N'})$ is irreducible, and the function field extension corresponding to the rational morphism J^H to \mathbb{P}^1 is nothing else than $K \subset L$. In particular, this extension is Galois.

We now start working towards an application of Chebotarev's density theorem to $K \subset L$. Let $R = \mathbb{F}_q[j]$ and let S be its integral closure inside L . Then S is the coordinate ring of $Y^H(p^e; \zeta_{N'})$ considered as an \mathbb{F}_q -scheme. Let $j_0 \in \mathbb{F}_q$ and let E_{j_0}/\mathbb{F}_q be an elliptic curve with j -invariant j_0 . A quartet $\mathcal{E} = (E_{j_0}, P, Q, R)$ on $Y^H(p^e; \zeta_{N'})$ corresponds to a maximal ideal $\mathfrak{m}_{\mathcal{E}}$ in $S \otimes_{\mathbb{F}_q} R$. Define $\mathbf{P}_{\mathcal{E}} := \mathfrak{m}_{\mathcal{E}} \cap S$, which can be viewed as a closed point of $Y^H(p^e; \zeta_{N'})$ as an \mathbb{F}_q -scheme. Suppose that $\mathbf{P}_{\mathcal{E}}$ is unramified over K , which is equivalent to

$$j_0 \notin \begin{cases} \{0, 1728\} & \text{if } e = 0 \\ \mathcal{J}_{\text{ss}} \cup \{0, 1728\} & \text{if } e \geq 1, \end{cases} \quad (3)$$

where $\mathcal{J}_{\text{ss}} \subset \overline{\mathbb{F}}_q$ is the set of supersingular j -invariants. As explained in [11, Section 6.2] we can associate to $\mathbf{P}_{\mathcal{E}}$ its Frobenius automorphism $\left[\frac{L/K}{\mathbf{P}_{\mathcal{E}}} \right] \in G = \text{Gal}(L/K)$. With $\mathbf{p}_{\mathcal{E}} := \mathbf{P}_{\mathcal{E}} \cap R$, this automorphism is uniquely determined by the condition

$$\left[\frac{L/K}{\mathbf{P}_{\mathcal{E}}} \right] x \equiv x^{N(\mathbf{p}_{\mathcal{E}})} \pmod{\mathbf{P}_{\mathcal{E}}}, \quad \text{for all } x \in S. \quad (4)$$

We note that $j_0 \in \mathbb{F}_q$ implies that $\mathbf{p}_{\mathcal{E}} = (j - j_0)$ and hence $N(\mathbf{p}_{\mathcal{E}}) = q$. Geometrically, condition (4) just means that if

$$\{(E_{j_0}, P_1, Q_1, R_1), (E_{j_0}, P_2, Q_2, R_2), \dots, (E_{j_0}, P_{\deg \mathbf{P}_{\mathcal{E}}}, Q_{\deg \mathbf{P}_{\mathcal{E}}}, R_{\deg \mathbf{P}_{\mathcal{E}}})\}$$

is the set of points of $Y^H(p^e; \zeta_{N'})$ (maximal ideals of $S \otimes_{\mathbb{F}_q} R$) above $\mathbf{P}_{\mathcal{E}}$, then $\left[\frac{L/K}{\mathbf{P}_{\mathcal{E}}} \right] \in G$ permutes this set in the same manner as described in (2) above. If \mathbf{P}'

is another prime ideal of S above $\mathfrak{p}_\mathcal{E}$, we have that the Frobenius automorphism $\left[\frac{L/K}{\mathfrak{P}'}\right]$ is conjugated to $\left[\frac{L/K}{\mathfrak{P}_\mathcal{E}}\right]$. The Artin symbol

$$\left(\frac{L/K}{\mathfrak{p}_\mathcal{E}}\right)$$

of $\mathfrak{p}_\mathcal{E}$ is then defined as the conjugacy class of $\left[\frac{L/K}{\mathfrak{P}_\mathcal{E}}\right]$ in G . Thus, the Artin symbol associated to a prime ideal $\mathfrak{p}_\mathcal{E} = (j - j_0) \subset \bar{R}$ with j_0 satisfying (3) is the conjugacy class of $G = (\mathrm{GL}_2^H(Z_{N'}) \oplus Z_{p^e}^\times) / \{\pm 1\}$ obtained by considering for an elliptic curve E/\mathbb{F}_q with j -invariant j_0 the action of q th power Frobenius with respect to

- all generators R of $\ker V_{p^e}$;
- all bases P, Q of $E[N']$ for which $e_{N'}(P, Q) = \zeta_{N'}^h$, for some $h \in H$.

Chebotarev's density theorem, in the following version of Fried and Jarden [11, Prop. 6.4.8], states:

Theorem 4 (Fried–Jarden) *Let $R = \mathbb{F}_q[j]$, let K be its field of fractions, let L be a finite Galois extension of K with Galois group G , and let $\mathcal{C} \subset G$ be a conjugacy class. Let \mathbb{F} be the algebraic closure of \mathbb{F}_q in L and let a be a positive integer such that $\tau|_{\mathbb{F}}$ acts as q^a th power Frobenius for each $\tau \in \mathcal{C}$. Let $C_1(L/K, \mathcal{C})$ be the set of prime ideals of degree 1 of R that do not ramify in L and for which the associated Artin symbol equals \mathcal{C} . If $a \not\equiv 1 \pmod{[\mathbb{F} : \mathbb{F}_q]}$ then $C_1(L/K, \mathcal{C}) = \emptyset$. If not, we have*

$$\left| \#C_1(L/K, \mathcal{C}) - \frac{\#\mathcal{C}}{m} q \right| < \frac{2\#\mathcal{C}}{m} [(m + g_L)\sqrt{q} + m\sqrt[4]{q} + g_L + m]$$

where $m = [L : K\mathbb{F}]$ and g_L is the genus of L as a function field over $K\mathbb{F}$.

For our choice of R and L , we have that $\mathbb{F} = \mathbb{F}_q(\zeta_{N'})$. Then $m = [L : \mathbb{F}_q(\zeta_{N'})(j)]$ is the degree of J , i.e.

$$m = \#(\mathrm{SL}_2(Z_{N'}) \oplus Z_{p^e}^\times) / \{\pm 1\},$$

and g_L is the genus of $X(p^e; \zeta_{N'})$, which is given by formula (1) above. An element $\pm(M, u) \in G$ acts as q th power Frobenius on $\mathbb{F}_q(\zeta_{N'})$ if and only if $\det M = q$.

Let $\mathcal{F} \subset \mathrm{GL}_2(Z_{N'})$ and $\mathcal{T} \in Z_{p^e}^\times$ be as in the énoncé of Theorem 2, with the extra condition that we are still assuming $N' > 2$. Then \mathcal{F} and \mathcal{T} determine a conjugacy class of $\mathrm{GL}_2(Z_{N'}) \oplus Z_{p^e}$ which we abusively denote by $(\mathcal{F}, \mathcal{T})$ and which is actually contained in $\mathrm{GL}_2^H(Z_{N'}) \oplus Z_{p^e}$. In this smaller group, $(\mathcal{F}, \mathcal{T})$ splits into a union of conjugacy classes $(\mathcal{F}_1, \mathcal{T}), \dots, (\mathcal{F}_r, \mathcal{T})$ for some $r \in \mathbb{Z}_{\geq 1}$. Each $(\mathcal{F}_i, \mathcal{T})$ reduces modulo $\{\pm 1\}$ to a conjugacy class $(\overline{\mathcal{F}}_i, \overline{\mathcal{T}})$ of G . Let $(\overline{\mathcal{F}}, \overline{\mathcal{T}})$ denote the union of these conjugacy classes, and let $B = C_1(L/K, (\overline{\mathcal{F}}, \overline{\mathcal{T}}))$ be

the set of $j_0 \in \overline{\mathbb{F}}_q$ for which j_0 satisfies (3) and the Artin symbol of $(j - j_0)$ is contained in $(\overline{\mathcal{F}}, \overline{\mathcal{T}})$. Then by applying Theorem 4 to each $(\overline{\mathcal{F}}_i, \overline{\mathcal{T}})$ and taking the sum of the resulting inequalities, we find

$$\left| \#B - \frac{\#(\overline{\mathcal{F}}, \overline{\mathcal{T}})}{m} q \right| < \frac{2\#(\overline{\mathcal{F}}, \overline{\mathcal{T}})}{m} [(m + g_L)\sqrt{q} + m\sqrt[4]{q} + g_L + m]. \quad (5)$$

Now let A denote the set of \mathbb{F}_q -isomorphism classes of elliptic curves E/\mathbb{F}_q for which

- $j(E) \notin \begin{cases} \{0, 1728\} & \text{if } e = 0 \\ \mathcal{J}_{\text{ss}} \cup \{0, 1728\} & \text{if } e \geq 1; \end{cases}$
- the conjugacy class of $\text{GL}_2(Z_{N'}) \oplus Z_{p^e}^\times$ obtained by considering the action of q th power Frobenius with respect to all bases P, Q of $E[N']$ equals \mathcal{F} ;
- q th power Frobenius maps every generator R of $E[p^e]$ to $\mathcal{T} \cdot R$.

Lemma 5 *One has*

$$\left| \#A - \frac{\#(\mathcal{F}, \mathcal{T})}{m} q \right| < \frac{4\#(\mathcal{F}, \mathcal{T})}{m} [(m + g_L)\sqrt{q} + m\sqrt[4]{q} + g_L + m].$$

PROOF. First note that q th power Frobenius acts on $E[p^e]$ as multiplication by \mathcal{T} if and only if it acts on $\ker V_{p^e}$ as multiplication by \mathcal{T} . By the lemma below, the natural map $A \rightarrow B : E \mapsto j(E)$ is onto and 2-to-1, and for each $j_0 \in B$, Frobenius acts on the two pre-images with opposite signs. Thus if $(\mathcal{F}, \mathcal{T}) \cap (-\mathcal{F}, -\mathcal{T}) = \emptyset$, then $\#A = \#B$ and $\#(\mathcal{F}, \mathcal{T}) = \#(\overline{\mathcal{F}}, \overline{\mathcal{T}})$ and the statement follows from (5). If $(\mathcal{F}, \mathcal{T}) = (-\mathcal{F}, -\mathcal{T})$ then $\#A = 2 \cdot \#B$ and $\#(\mathcal{F}, \mathcal{T}) = 2 \cdot \#(\overline{\mathcal{F}}, \overline{\mathcal{T}})$ and the statement again follows. \blacksquare

Lemma 6 *Let E/\mathbb{F}_q be an elliptic curve and let $[E]_{\mathbb{F}_q}$ be the set of \mathbb{F}_q -isomorphism classes of elliptic curves that are $\overline{\mathbb{F}}_q$ -isomorphic to E . Then $\#[E]_{\mathbb{F}_q} \geq 2$. More precisely,*

- if $j(E) \neq 0, 1728$, then $\#[E]_{\mathbb{F}_q} = 2$ and $[E]_{\mathbb{F}_q}$ consists of E and its quadratic twist E^t ; if $\mathcal{F} \subset \text{GL}_2(Z_{N'})$ is the conjugacy class determined by q th power Frobenius acting on $E[N']$, then $-\mathcal{F}$ is the conjugacy class determined by q th power Frobenius acting on $E^t[N']$; similarly, if q th power Frobenius acts on $E[p^e]$ as multiplication by $\mathcal{T} \in Z_{p^e}^\times$, then it acts on $E^t[p^e]$ as multiplication by $-\mathcal{T}$;
- otherwise, we have the following upper bounds: if $j(E) = 1728$ and $p \neq 2, 3$ then $\#[E]_{\mathbb{F}_q} \leq 4$; if $j(E) = 0$ and $p \neq 2, 3$ then $\#[E]_{\mathbb{F}_q} \leq 6$; if $j(E) = 0 = 1728$ and $p = 3$ then $\#[E]_{\mathbb{F}_q} \leq 12$; if $j(E) = 0 = 1728$ and $p = 2$ then $\#[E]_{\mathbb{F}_q} \leq 24$.

PROOF. We first recall some facts on quadratic twisting, because the existing literature contains certain ambiguities here. We follow [22, X.2.4, Exercise A.2]. First suppose that $p > 2$. Let E be an elliptic curve over \mathbb{F}_q , take a short Weierstrass model $E : y^2 = f(x)$ and a nonsquare $d \in \mathbb{F}_q$. Then E^t is defined by $dy^2 = f(x)$. Its \mathbb{F}_q -isomorphism class does not depend on the choice of the model, nor on the choice of d . We have an $\overline{\mathbb{F}}_q$ -isomorphism $\iota : E^t \rightarrow E : (x, y) \mapsto (x, \sqrt{d}y)$. If $p = 2$ and $j(E) \neq 0$ then E allows a model $y^2 + xy = x^3 + ax^2 + b$ (see [22, Appendix A]). Let $d \in \mathbb{F}_q$ have trace 1, then it is of the form $\beta^2 + \beta$ for some $\beta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$. The quadratic twist E^t is then given by

$$y^2 + xy = x^3 + (a + d)x^2 + b.$$

This is again well-defined and we have an $\overline{\mathbb{F}}_q$ -isomorphism $\iota : E^t \rightarrow E : (x, y) \mapsto (x, y + \beta x)$. Note that E can a priori be \mathbb{F}_q -isomorphic to its quadratic twist, take for instance $q \equiv 3 \pmod{4}$, $E : y^2 = x^3 + x$ and $d = -1$. Now it is an easy exercise to verify that if F is the matrix of q th power Frobenius acting on $E[N']$ with respect to a basis P, Q , then $-F$ is the matrix of q th power Frobenius acting on $E^t[N']$ with respect to $\iota^{-1}(P), \iota^{-1}(Q)$, and similarly for $\ker V_{p^e}$.

For the remaining statements, we analyze the formula

$$\sum_{E' \in [E]_{\mathbb{F}_q}} \frac{1}{\#\text{Aut}_{\mathbb{F}_q}(E')} = 1,$$

a proof of which can be found in [16, Prop. 2.1]. Since $\{\pm 1\} \subset \text{Aut}_{\mathbb{F}_q}(E')$, we have that $\#[E]_{\mathbb{F}_q} \geq 2$. The upper bounds follow from $\text{Aut}_{\mathbb{F}_q}(E') \subset \text{Aut}_{\overline{\mathbb{F}}_q}(E')$ and [22, Thm. III.10.1]. Finally, if $j(E) \neq 0, 1728$, then E cannot be \mathbb{F}_q -isomorphic to its quadratic twist: such an isomorphism would yield a non-rational automorphism of E , which cannot exist since $\text{Aut}_{\overline{\mathbb{F}}_q}(E) = \{\pm 1\}$. ■

We are now ready to prove Theorem 2.

Still assuming $N' > 2$, Lemma 5 immediately implies

$$\left| \#A - \frac{\#\mathcal{F}}{\#\mathcal{M}_{q, N'}} \cdot \frac{1}{\varphi(p^e)} \cdot 2q \right| \leq \frac{8 \cdot \#\mathcal{F}}{\varphi(p^e) \cdot \#\mathcal{M}_{q, N'}} [(m + g_L)\sqrt{q} + m\sqrt[3]{q} + g_L + m].$$

By Lemma 6, the number of \mathbb{F}_q -isomorphism classes of elliptic curves over \mathbb{F}_q is contained in $[2q, 2q + 22]$. Taking into account the ramifying j -invariants 0 and 1728, corresponding to at most 24 \mathbb{F}_q -isomorphism classes, we find

$$\begin{aligned} & \left| P_{\mathcal{F}, \mathcal{T}} - \frac{\#\mathcal{F}}{\#\mathcal{M}_{q, N'}} \cdot \frac{1}{\varphi(p^e)} \right| \\ & \leq \frac{8 \cdot \#\mathcal{F}}{\varphi(p^e) \cdot \#\mathcal{M}_{q, N'}} \cdot \frac{(m + g_L)\sqrt{q} + m\sqrt[3]{q} + g_L + m + \frac{22}{8}}{2q} + \frac{24}{2q}. \end{aligned} \quad (6)$$

Note that, in the case $e \geq 1$, both the definition of A and the definition of $P_{\mathcal{F}, \mathcal{T}}$ ruled out all supersingular curves. Therefore, this has no influence. This is an important difference with the proof of Theorem 1 in Section 3 below.

Next, we analyze the asymptotical behavior of the error term. From (1) we see that $g_L \leq \frac{p^e \varphi(p^e) N'^3}{24}$, and it is easy to verify that if N' factors as $\ell_1^{n_1} \cdots \ell_t^{n_t}$ for distinct primes ℓ_i , then

$$m = \#(\mathrm{SL}_2(Z_{N'}) \oplus Z_{p^e}^\times) / \{\pm 1\} = \frac{\varphi(p^e)}{2} \cdot \prod_{i=1}^t \ell_i^{3n_i-2} (\ell_i^2 - 1) \leq \frac{\varphi(p^e) N'^3}{2}.$$

Finally,

$$\#\mathcal{F} \leq \#\{\text{matrices with trace } \mathrm{Tr}(\mathcal{F})\} \leq \prod_{i=1}^t \ell_i^{2n_i-1} (\ell_i + 1)$$

by the results of Section 3 below. Hence

$$\frac{\#\mathcal{F}}{\#\mathcal{M}_{q,N'}} \leq \frac{1}{N'} \prod_{i=1}^t \frac{\ell_i}{\ell_i - 1} \leq \frac{1}{N'} \prod_{\ell \leq 2^{\lceil \log_2 N' \rceil}} \frac{\ell}{\ell - 1}$$

where the latter product is over all primes ℓ . The first inequality follows from the formula for the size of $\mathcal{M}_{q,N'}$ given in Section 3, the second inequality follows from the estimate $\prod_{\ell \leq 2^x} \ell \geq 2^x$ (see e.g. [8, Exercise 1.28]). Mertens' theorem (see [21, Corollary 1] for an effective version) then shows that this product is $\mathcal{O}(\ln \ln N')$.

Theorem 2 then follows by noting that the case $N' \leq 2$ is a mere consequence of the case $N' = 4$ (possibly yielding an increase of C , though).

3 The distribution of Frobenius traces

In this section, we will prove Theorem 1 and provide an explicit description of the function Ψ .

For each prime number p and each pair of integers $N' \geq 1$, $e \geq 0$, write $N = N' p^e$ and define the trace $\mathrm{Tr}(x)$ of an element $x = (M, u)$ of

$$G = \mathrm{GL}_2(Z_{N'}) \oplus Z_{p^e}^\times$$

to be the unique element of Z_N that is congruent both to $\mathrm{Tr}(M) \bmod N'$ and to $u \bmod p^e$. As before, for each power q of p , let $\mathcal{M}_{q,N'} \subset \mathrm{GL}_2(Z_{N'})$ be the set of matrices having determinant q . Let Q be as in the introduction and define

$$r : Q \times \mathbb{Z}_{\geq 1} \times \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Q}_{\geq 0} : (q, N, t) \mapsto \frac{\#\{x \in \mathcal{M}_{q,N'} \times Z_{p^e}^\times \mid \mathrm{Tr}(x) \equiv t \bmod N\}}{\varphi(p^e) \cdot \#\mathcal{M}_{q,N'}}.$$

Then it is easy to verify that r satisfies conditions (i) and (iii) of Theorem 1. Moreover, there exists an absolute and explicitly computable constant $C \in \mathbb{R}_{>0}$ such that, for all $q \in Q$, $N \in \mathbb{Z}_{\geq 1}$ and $t \in \mathbb{Z}_{\geq 0}$,

$$|P_{q,N}(t) - r(q, N, t)| \leq C \cdot \frac{p^e N'^2 \ln \ln N'}{\sqrt{q}}$$

Indeed, let $(\mathcal{F}_t, \mathcal{T}_t)$ denote the set of elements of $\mathcal{M}_{q,N'} \times Z_{p^e}^\times$ having trace $t \bmod N$. It is a union of conjugacy classes of G . By applying Lemma 5 to each of these conjugacy classes, taking the sum of the resulting inequalities, and following a reasoning similar to the one at the end of Section 2, we obtain

$$|P_{q,N}(t) - r(q, N, t)| \leq \frac{8 \cdot \#(\mathcal{F}_t, \mathcal{T}_t)}{\varphi(p^e) \cdot \#\mathcal{M}_{q,N'}} \cdot \frac{(m + g_L)\sqrt{q} + m\sqrt[4]{q} + g_L + m + \frac{22}{8}}{2q} + \frac{24}{2q} + \bar{\delta}_{e,0} \frac{p/6}{2q}, \quad (7)$$

where $\bar{\delta}_{e,0} = 1 - \delta_{e,0}$, with $\delta_{e,0}$ the Kronecker delta. In contrast with $\mathcal{P}_{\mathcal{F},\mathcal{T}}$, the definition of $P_{q,N}(t)$ does include supersingular curves, whereas the set A from Lemma 5 does not as soon as $e \geq 1$. Therefore, the error term $\frac{24}{2q}$, which in (6) accounted for the j -invariants 0 and 1728, should be replaced by an error term accounting in addition for all supersingular j -invariants. For this one can use that there are at most $p/12 + 2$ supersingular j -invariants in $\overline{\mathbb{F}}_q$, and that that for $p = 2, 3$ the unique supersingular j -invariant is in fact $0 = 1728$. See [22, V.4]. An error term analysis as in Section 2 then proves the estimate.

It remains to show that, for the function Ψ that is described below, the function r satisfies condition (ii) of Theorem 1. So assume that $N = \ell^n$ for some integer $n \geq 1$ and a prime number ℓ , and let $q \in Q$ be coprime to ℓ . Then

$$r(q, \ell^n, t) = \frac{\#\{M \in \mathcal{M}_{q,\ell^n} \mid \text{Tr}(M) \equiv t \bmod \ell^n\}}{\#\mathcal{M}_{q,\ell^n}}.$$

It is easy to verify that $\#\mathcal{M}_{q,\ell^n} = \#\text{SL}_2(Z_{\ell^n}) = \ell^{3n-2}(\ell^2 - 1)$. With $\alpha \in Z_{\ell^n} \setminus \{0\}$, we define the valuation $\text{ord}(\alpha)$ as the ℓ -adic valuation of α embedded in \mathbb{Z} , whereas we will put $\text{ord}(0) = +\infty$. Let for $\ell \geq 3$ the map $\Psi : \mathbb{Z} \rightarrow \mathbb{Z}$ be defined as $\Psi = \psi \circ \chi$, where $\chi : \mathbb{Z} \rightarrow Z_{\ell^n}$ is the natural projection and $\psi : Z_{\ell^n} \rightarrow \mathbb{Z}$ is given by

$$\Delta \mapsto \begin{cases} \ell^{2n} + \ell^{2n-1} & \text{if } \Delta \text{ is a nonzero square,} \\ \ell^{2n} + \ell^{2n-1} - 2\ell^{2n-\frac{k}{2}-1} & \text{if } \Delta \text{ is no square, } k := \text{ord}(\Delta) \text{ is even,} \\ \ell^{2n} + \ell^{2n-1} - (\ell + 1)\ell^{2n-\frac{k+3}{2}} & \text{if } k := \text{ord}(\Delta) \text{ is odd,} \\ \ell^{2n} + \ell^{2n-1} - \ell^{\frac{3n}{2}-1} & \text{if } \Delta = 0 \text{ and } n \text{ is even,} \\ \ell^{2n} + \ell^{2n-1} - \ell^{\frac{3n-1}{2}} & \text{if } \Delta = 0 \text{ and } n \text{ is odd.} \end{cases}$$

We refer to the end of this section for the definition of Ψ in case $\ell = 2$. Below we prove that indeed:

Theorem 7 *Let q, t and ℓ^n be as above and define $\Delta_t := t^2 - 4q$. Then*

$$r(q, \ell^n, t) = \frac{\Psi(\Delta_t)}{\ell^{3n} - \ell^{3n-2}}.$$

Let us first discuss some corollaries. The number of rational points on an elliptic curve E over \mathbb{F}_q with trace of Frobenius T equals $q + 1 - T$. Hence

we can estimate the probability that $\ell^n \mid \#E(\mathbb{F}_q)$ by applying Theorem 7 with $t = q + 1$. Note that then $t^2 - 4q \equiv (q - 1)^2 \pmod{\ell^n}$. Using this, we recover the estimates obtained by Howe [16, Thm. 1.1].

If we suppose $\ell \geq 3$ and $n = 1$, then the above formulas become quite pretty, namely

$$P(t) \sim \begin{cases} \frac{\ell}{\ell^2 - 1} & \text{if } t^2 - 4q = 0 \text{ in } \mathbb{F}_\ell, \\ \frac{1}{\ell - 1} & \text{if } t^2 - 4q \text{ is a square in } \mathbb{F}_\ell^\times, \\ \frac{1}{\ell + 1} & \text{if } t^2 - 4q \text{ is a nonsquare in } \mathbb{F}_\ell. \end{cases}$$

The combination of these two corollaries generalizes Lenstra's result [20, Prop. 1.14] which states that the probability of ℓ -torsion approaches $\ell/(\ell^2 - 1)$ if $q \equiv 1 \pmod{\ell}$ and $1/(\ell - 1)$ otherwise.

The remainder of this section is devoted to the proof of Theorem 7. We note that the counting of matrices described below was already done by Gekeler [13, Thm. 4.4] for the case $n \geq 2 \cdot \lfloor \frac{\text{ord}(\Delta_t)}{2} \rfloor + 2$, using different techniques.

Let $\begin{pmatrix} u & x \\ -y & z \end{pmatrix} \in \text{GL}_2(Z_{\ell^n})$ have determinant q and trace t . A trivial computation yields that these conditions are equivalent to the system of equations

$$u = t - z, \quad xy = z^2 - tz + q. \quad (8)$$

By completing the square, the above system has as many solutions as

$$u = t - z, \quad xy = z^2 - \Delta_t/4, \quad (9)$$

provided that $t/2$ exists modulo ℓ^n . Suppose for the rest of the proof that $\ell \geq 3$ and $\Delta_t \in Z_{\ell^n}$; we refer to the end of this section for the situation $\ell = 2$. Clearly all relevant properties (valuation, being a square or not) of Δ_t and $\Delta_t/4$ are the same, hence if we can show that the number of solutions to $xy = z^2 - \Delta_t$ equals $\Psi(\Delta_t)$, we are done. For each value of z , we will determine the valuation of $z^2 - \Delta_t$. Then the number of corresponding solutions (x, y) can be computed using the following lemma.

Lemma 8 *Let ℓ be any prime number, let $n \in \mathbb{Z}_{\geq 1}$ and $\alpha \in Z_{\ell^n}$. Write $k := \text{ord}(\alpha)$. Then the equation $xy = \alpha$ has the following number of solutions (x, y) in $(Z_{\ell^n})^2$:*

$$\begin{cases} (k + 1)(\ell^n - \ell^{n-1}) & \text{if } \alpha \neq 0, \\ (n + 1)(\ell^n - \ell^{n-1}) + \ell^{n-1} & \text{if } \alpha = 0. \end{cases}$$

PROOF. Suppose $\alpha \neq 0$, the other case works similarly. We can take x to be any number with valuation $i \in \{0, 1, \dots, k\}$. For each i , the number of such x is $\ell^{n-i} - \ell^{n-i-1}$. Every choice of x fixes all but the last i ℓ -adic digits of y , hence we have ℓ^i possibilities for y . In total this amounts to

$$\sum_{i=0}^k (\ell^{n-i} - \ell^{n-i-1}) \ell^i = \sum_{i=0}^k (\ell^n - \ell^{n-1}) = (k + 1)(\ell^n - \ell^{n-1})$$

solutions (x, y) . ■

Another tool will be the following formula, which is easily proven by induction:

Lemma 9 *Let ℓ be any prime number, let $n \geq 1$ be an integer and $k \in \{0, 1, \dots, n\}$. Then*

$$\sum_{i=0}^k (\ell^{n-i} - \ell^{n-i-1})(2i+1)(\ell^n - \ell^{n-1}) = \ell^{2n} + \ell^{2n-1} - (2k+3)\ell^{2n-k-1} + (2k+1)\ell^{2n-k-2}.$$

Suppose first that $\Delta_t = 0$ and n even. Then $\text{ord}(z^2 - \Delta_t) = \text{ord}(z^2)$ for all z , and the number of solutions to $xy = z^2 - \Delta_t$ with $\text{ord}(z) < n/2$ equals

$$\sum_{i=0}^{n/2-1} (\ell^{n-i} - \ell^{n-i-1})(2i+1)(\ell^n - \ell^{n-1}),$$

by Lemma 8. For $\text{ord}(z) \geq n/2$, we find

$$\ell^{n/2} ((n+1)(\ell^n - \ell^{n-1}) + \ell^{n-1})$$

additional solutions. Using Lemma 9 one verifies that the sum of these expressions equals $\Psi(0)$. If n is odd, then the reasoning is similar.

Let us now assume that Δ_t is a nonzero square, i.e. $\Delta_t = \ell^{2k} \Delta^2$, where $2k < n$ and Δ is a unit. Under the change of variables $(x, y, z) \leftarrow (\Delta x, \Delta y, \Delta z)$ our equation becomes

$$xy = z^2 - \ell^{2k}. \tag{10}$$

We will use induction on k to show that (10) has $\Psi(\Delta_t) = \ell^{2n} + \ell^{2n-1}$ solutions. For $k = 0$ we have $xy = z^2 - 1$. If x is any unit, we have $y = x^{-1}(z^2 - 1)$ and z can be chosen arbitrarily. If x is a nonunit and y is arbitrary, we have 2 different solutions $z \equiv \pm 1$ modulo ℓ , which can both be lifted to Z_{ℓ^n} . In total this gives

$$(\ell^n - \ell^{n-1})\ell^n + 2\ell^{n-1}\ell^n = \ell^{2n} + \ell^{2n-1}.$$

Suppose now that $k \geq 1$. There are $\ell^{2n} - \ell^{2n-1}$ solutions for which x is a unit. There are $(\ell^n - \ell^{n-1})\ell^{n-1}$ solutions for which y is a unit and z — and hence x — are nonunits. The solutions for which x and y are both nonunits can be determined using the induction hypothesis. Indeed, a triplet $(x, y, z) = (\ell x', \ell y', \ell z')$ satisfies (10) if and only if (x', y', z') satisfies

$$x'y' = z'^2 - \ell^{2k-2} \quad \text{over } Z_{\ell^{n-2}},$$

which has $\ell^{2n-4} + \ell^{2n-5}$ solutions. For each $x' \in Z_{\ell^{n-2}}$ there are ℓ corresponding values for $x = \ell x' \pmod{\ell^n}$, and similar for y and z . In total we find then

$$\ell^{2n} - \ell^{2n-1} + (\ell^n - \ell^{n-1})\ell^{n-1} + \ell^3(\ell^{2n-4} + \ell^{2n-5}) = \ell^{2n} + \ell^{2n-1}.$$

Next, if $k = \text{ord}(\Delta_t) < +\infty$ is odd, we find the following sum for the number of solutions

$$\sum_{i=0}^{(k-1)/2} (\ell^{n-i} - \ell^{n-i-1})(2i+1)(\ell - \ell^{n-1}) + \ell^{n-(k+1)/2}(k+1)(\ell^n - \ell^{n-1}),$$

which by Lemma 9 equals $\Psi(\Delta_t)$.

Finally, with k even but Δ_t nonsquare we get

$$\sum_{i=0}^{k/2-1} (\ell^{n-i} - \ell^{n-i-1})(2i+1)(\ell - \ell^{n-1}) + \ell^{n-k/2}(k+1)(\ell^n - \ell^{n-1}),$$

and again the result follows from Lemma 9. This completes the proof for $\ell \geq 3$.

We end this section by considering the case $\ell = 2$. The appropriate description of Ψ depends now on its argument mod 2^{n+2} rather than mod 2^n . More precisely, $\Psi = \psi \circ \chi$ where $\chi : \mathbb{Z} \rightarrow Z_{2^{n+2}}$ is the natural projection and $\psi : Z_{2^{n+2}} \rightarrow \mathbb{Z}$ is partially given by

$$\Delta \mapsto \begin{cases} 2^{2n-1} & \text{if } \Delta \text{ is odd,} \\ 2^{2n} + 2^{2n-1} - 3 \cdot 2^{2n-\frac{k+1}{2}} & \text{if } \Delta \neq 0 \text{ is even and } k := \text{ord}(\Delta) \text{ is odd,} \\ 2^{2n} + 2^{2n-1} - 2^{\frac{3n}{2}-1} & \text{if } \Delta \equiv 0 \pmod{2^{n+2}} \text{ and } n \text{ is even,} \\ 2^{2n} + 2^{2n-1} - 2^{\frac{3n-1}{2}} & \text{if } \Delta \equiv 0 \pmod{2^{n+2}} \text{ and } n \text{ is odd.} \end{cases}$$

In case $\Delta \neq 0$ is even and $\text{ord}(\Delta) = 2k > 0$ is even as well, the definition of ψ is more complicated. Let D be such that $\Delta = 2^{2k}D$. Then:

$$\begin{aligned} \text{if } n = 2k - 1: & \quad \psi(\Delta) := 2^{2n} + 2^{2n-1} - 2^{\frac{3n-1}{2}}, \\ \text{if } n = 2k, & \quad D \equiv 1 \pmod{4}: \quad \psi(\Delta) := 2^{2n} + 2^{2n-1} - 2^{\frac{3n}{2}-1}, \\ & \quad D \equiv 3 \pmod{4}: \quad \psi(\Delta) := 2^{2n} + 2^{2n-1} - 3 \cdot 2^{\frac{3n}{2}-1}, \\ \text{if } n \geq 2k + 1, & \quad D \equiv 3 \pmod{4}: \quad \psi(\Delta) := 2^{2n} + 2^{2n-1} - 3 \cdot 2^{2n-k-1}, \\ & \quad D \equiv 5 \pmod{8}: \quad \psi(\Delta) := 2^{2n} + 2^{2n-1} - 2^{2n-k}, \\ & \quad D \equiv 1 \pmod{8}: \quad \psi(\Delta) := 2^{2n} + 2^{2n-1}. \end{aligned}$$

We will now prove that for any $t \in \mathbb{Z}$, the number of solutions (over Z_{2^n}) to the system (8) is precisely $\Psi(\Delta_t)$, where $\Delta_t = t^2 - 4q$. Note first that if t (or equivalently Δ_t) is odd, we have that $\text{ord}(z^2 - tz + q) = 0$ for all z . Then Lemma 8 gives a total of

$$2^n(2^n - 2^{n-1}) = 2^{2n-1} = \Psi(\Delta_t)$$

solutions.

Therefore suppose that t is even. Then $\Delta_t \equiv 0 \pmod{4}$, and it makes sense to complete the square in (8) and analyze the system (9) instead. As we are interested in solutions modulo 2^n , from now on we will consider $\Delta_t/4$ as an element of Z_{2^n} . Note that this depends on $\Delta_t \pmod{2^{n+2}}$. Copying the proofs of

the corresponding cases above, the system (9) has $\Psi(\Delta_t)$ solutions if $\Delta_t/4 = 0$ (in Z_{2^n}) or if $\text{ord}(\Delta_t/4) < n$ is odd. Hence we assume that $\text{ord}(\Delta_t/4) = 2\kappa < n$ is even. Let $D \in Z_{2^n}$ be such that $2^{2\kappa}D = \Delta_t/4$. If $i = \text{ord}(z) < \kappa$ we have $\text{ord}(z^2 - \Delta_t/4) = 2i$, so by Lemma 8 and Lemma 9 all such z together account for

$$S := \sum_{i=0}^{\kappa-1} (2^{n-i} - 2^{n-i-1})(2i+1)(2^n - 2^{n-1}) = 2^{2n} + 2^{2n-1} - (2\kappa+3)2^{2n-\kappa-1}$$

solutions (x, y, z) . From now on we assume $\text{ord}(z) \geq \kappa$ and put $z = 2^\kappa z'$, so that our equation becomes

$$xy = 2^{2\kappa}(z'^2 - D).$$

Note that z' is only well-determined modulo $2^{n-\kappa}$, and that we are interested in $z'^2 - D \pmod{2^{n-2\kappa}}$.

If $n = 2\kappa + 1$ we have two possibilities: either $z' \equiv 0 \pmod{2}$, which gives $2^{n-\kappa-1}(2\kappa+1)2^{n-1}$ solutions $(x, y, z' \pmod{2^{n-\kappa}})$, or $z' \equiv 1 \pmod{2}$, which gives $2^{n-\kappa-1}((n+1)2^{n-1} + 2^{n-1})$ solutions. If we add S to these two numbers, we find the requested result.

Let $n = 2\kappa + 2$, then we have to distinguish between $D \equiv 1 \pmod{4}$ and $D \equiv 3 \pmod{4}$. For example, if $D \equiv 3 \pmod{4}$ and z' is odd, the valuation of $2^{2\kappa}(z'^2 - D)$ equals $2\kappa + 1$, since 3 is not a quadratic residue modulo 4. We leave further details to the reader.

Finally we assume that $n \geq 2\kappa + 3$. The cases $D \equiv 3 \pmod{4}$ and $D \equiv 5 \pmod{8}$ are similar to the situation $n = 2\kappa + 2$ above, so we only go into more details for $D \equiv 1 \pmod{8}$. Then we know that D is a square modulo $2^{n-2\kappa}$ and we can proceed as in the case $\ell \geq 3$ and Δ_t a nonzero square. However, things work differently for the induction step $\kappa = 0$, i.e. $xy = z^2 - 1 \pmod{2^n}$, $n \geq 3$. As the valuation of $z^2 - 1$ cannot be 1 or 2, we have to consider four situations. Firstly, $\text{ord}(x) = 0$, then z can be chosen arbitrarily and we find $2^{n-1} \cdot 2^n$ solutions. Secondly, $\text{ord}(x) = 1$, then $\text{ord}(y) \geq 2$ and we can lift the four solutions $z \equiv 1, 3, 5, 7 \pmod{8}$ to Z_{2^n} , which gives a total of $4 \cdot 2^{n-2} 2^{n-2}$ solutions. Third, $\text{ord}(x) = 2$ and $\text{ord}(y) \geq 1$ which gives again 2^{2n-2} solutions. Finally, $\text{ord}(x) \geq 3$ and y is arbitrary, which gives $4 \cdot 2^{n-3} 2^n$ solutions. Adding all these terms together gives $2^{2n} + 2^{2n-1}$ solutions.

4 The probability of a point of order N

In this section, we prove Theorem 3. Recall that we defined $P'_q(N)$ as the probability that an elliptic curve over \mathbb{F}_q contains a point of order N .

Let \mathbb{F}_q be a finite field of characteristic p with q elements. Let E be an elliptic curve over \mathbb{F}_q . It is well-known (see e.g. [22, Exercise 5.6]) that

$$E(\mathbb{F}_q) \cong Z_A \oplus Z_B$$

for integers A, B such that $A|B$ and $A|q-1$. Hence if $\gcd(N, q-1) = 1$, then $P'_q(N)$ equals the probability $P_{q,N}(q+1)$ that $N|\#E(\mathbb{F}_q)$, which can be computed using Theorem 1. However, if $\gcd(N, q-1) > 1$, both probabilities are fundamentally different. The following small example might shed some light on this difference. Let $\ell^n = 9$, $q \equiv 1 \pmod{9}$ and E a random elliptic curve over \mathbb{F}_q . The probability that $\#E(\mathbb{F}_q) \equiv 0 \pmod{9}$ approaches (for $q \rightarrow \infty$) $11/72$. However, the approximate probability that E has a point of order 9 is smaller, namely $9/72$. A corollary is that the probability that $E(\mathbb{F}_q)[9] \cong Z_3 \oplus Z_3$ tends to $2/72$.

Entirely analogous to the proof of Theorem 1 in Section 3, one sees that it suffices to consider the case $N = \ell^n$ for some prime $\ell \neq p$ and some integer $n \geq 1$. Moreover, it suffices to prove that the number of matrices in $\mathrm{GL}_2(Z_{\ell^n})$ that are conjugated to a matrix of the form $\begin{pmatrix} 1 & w \\ 0 & q \end{pmatrix}$ for a certain $w \in Z_{\ell^n}$ is given by $\theta_{\ell^n} \cdot \#\mathrm{SL}_2(Z_{\ell^n})$, with

$$\theta_{\ell^n} := \begin{cases} \frac{1}{\ell^n - \ell^{n-2}} & \text{if } q \equiv 1 \pmod{\ell^n}, \text{ i.e. } \nu \geq n, \\ \frac{\ell^{2\nu+1} + 1}{\ell^{n+2\nu-1}(\ell^2 - 1)} & \text{elsewhere,} \end{cases}$$

where ν is the ℓ -adic valuation of $q-1$. Indeed, E will have an \mathbb{F}_q -rational point of order ℓ^n if and only if \mathcal{F}_E is conjugated to an upper diagonal matrix of the above form.

The conjugacy classes of matrices of the form $\begin{pmatrix} 1 & w \\ 0 & q \end{pmatrix}$ are determined by their representants M_a in Lemma 10 below. The size of the conjugacy class Cl_a of M_a can be computed as follows. Let St_a be the stabilizer subgroup of M_a , then the classical orbit-stabilizer theorem states that $\#\mathrm{St}_a \cdot \#\mathrm{Cl}_a = \#\mathrm{GL}_2(Z_{\ell^n})$. Hence it suffices to compute the size of St_a . We know that $\begin{pmatrix} x & y \\ s & t \end{pmatrix} \in \mathrm{St}_a$ if and only if $\begin{pmatrix} x & y \\ s & t \end{pmatrix}$ is invertible and

$$\begin{pmatrix} 1 & \ell^a \\ 0 & q \end{pmatrix} \cdot \begin{pmatrix} x & y \\ s & t \end{pmatrix} = \begin{pmatrix} x & y \\ s & t \end{pmatrix} \cdot \begin{pmatrix} 1 & \ell^a \\ 0 & q \end{pmatrix}. \quad (11)$$

This condition is equivalent to the system (using $a \leq \nu$)

$$\begin{cases} \ell^a s \equiv 0 \pmod{\ell^n} \\ \ell^a(t-x) \equiv y(q-1) \pmod{\ell^n}. \end{cases} \quad (12)$$

We can choose x and y at random, so that $t \equiv y(q-1)\ell^{-a} + x \pmod{\ell^{n-a}}$ and $s \equiv 0 \pmod{\ell^{n-a}}$; we find a total of ℓ^{2n+2a} matrices satisfying (11). From these we have to remove the singular matrices, which adds the condition $xt \equiv sy \pmod{\ell}$. If $a < \nu$ we have by (12) that $s \equiv 0 \pmod{\ell}$ and $t \equiv x \pmod{\ell}$, hence the only additional restriction is that $x \equiv 0 \pmod{\ell}$. This gives $\ell^{2n+2a-1}$ singular matrices and hence $\#\mathrm{St}_a = \ell^{2n+2a} - \ell^{2n+2a-1}$ for $a < \nu$. If $\nu = n$ it is obvious that $\#\mathrm{Cl}_n = 1$, so we are left with considering St_ν for $\nu < n$. As shown in the proof

of Lemma 10, the matrix $\begin{pmatrix} 1 & \ell^\nu \\ 0 & q \end{pmatrix}$ is conjugated to $\begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$, and now it is an easy exercise to compute the number $\#\text{St}_\nu = \ell^{2n+2\nu} - (2\ell^{2n-1} - \ell^{2n-2})\ell^{2\nu}$. Combined this gives that the number of matrices conjugated to some $\begin{pmatrix} 1 & w \\ 0 & q \end{pmatrix}$ where $\nu < n$ equals (note that $\#\text{GL}_2(Z_{\ell^n}) = \ell^{4n-4}(\ell^2 - \ell)(\ell^2 - 1)$):

$$\sum_{a=0}^{\nu-1} \frac{\ell^{4n-4}(\ell^2 - \ell)(\ell^2 - 1)}{\ell^{2n+2a} - \ell^{2n+2a-1}} + \frac{\ell^{4n-4}(\ell^2 - \ell)(\ell^2 - 1)}{\ell^{2n+2\nu} - 2\ell^{2n+2\nu-1} + \ell^{2n+2\nu-2}} = \ell^{2n} + \ell^{2n-2\nu-1}.$$

Dividing this number by $\#\text{SL}_2(Z_{\ell^n})$ gives the theorem for $\nu < n$. If $q \equiv 1 \pmod{\ell^n}$ we similarly find

$$\sum_{a=0}^{n-1} \frac{\ell^{4n-4}(\ell^2 - \ell)(\ell^2 - 1)}{\ell^{2n+2a} - \ell^{2n+2a-1}} + 1 = \ell^{2n}.$$

This concludes the proof of Theorem 3.

Lemma 10 *Let $\nu = \text{ord}_\ell(q - 1)$. Each matrix over Z_{ℓ^n} of the form $\begin{pmatrix} 1 & w \\ 0 & q \end{pmatrix}$ is conjugated to precisely one matrix of the set*

$$\left\{ M_a := \begin{pmatrix} 1 & \ell^a \\ 0 & q \end{pmatrix} \mid 0 \leq a \leq \nu \right\}.$$

PROOF. First we show that $\begin{pmatrix} 1 & \ell^a \\ 0 & q \end{pmatrix}$ with $a \geq \nu$ is conjugated to $\begin{pmatrix} 1 & \ell^\nu \\ 0 & q \end{pmatrix}$. Write $q = 1 + \ell^\nu q'$, then

$$\begin{pmatrix} 1 & q'^{-1}(\ell^{a-\nu} - 1) \\ 0 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & \ell^a \\ 0 & q \end{pmatrix} \cdot \begin{pmatrix} 1 & q'^{-1}(\ell^{a-\nu} - 1) \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \ell^\nu \\ 0 & q \end{pmatrix}.$$

Let $w = \ell^a w'$ with w' a unit in Z_{ℓ^n} , then

$$\begin{pmatrix} w' & 0 \\ 0 & 1 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & \ell^a w' \\ 0 & q \end{pmatrix} \cdot \begin{pmatrix} w' & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \ell^a \\ 0 & q \end{pmatrix},$$

which implies that at least one matrix of the above set is conjugated to $\begin{pmatrix} 1 & w \\ 0 & q \end{pmatrix}$. The fact that all matrices M_a define different conjugacy classes follows either from a direct reasoning (assuming that two of them are conjugated, the transformation matrix will have determinant 0 modulo ℓ) or from the computations above which show that the conjugacy classes have different size. \blacksquare

Note. It is possible to determine the probability of all kinds of group structures in a similar way. For example, let $0 \leq a \leq b$ be integers, ℓ a prime coprime to q and suppose we want to know the probability that

$$E[\ell^\infty](\mathbb{F}_q) \cong Z_{\ell^a} \oplus Z_{\ell^b}.$$

This can be done as follows. Let \mathcal{S} be the set of matrices M in $\text{GL}_2(Z_{\ell^{a+b+1}})$ with determinant q for which the following conditions hold:

- (i) $\text{Tr}(M) \not\equiv q + 1 \pmod{\ell^{a+b+1}}$,
- (ii) $\text{Tr}(M) \equiv q + 1 \pmod{\ell^{a+b}}$,
- (iii) M is conjugated to some $\begin{pmatrix} 1 & w \\ 0 & q \end{pmatrix} \pmod{\ell^b}$, and
- (iv) $M \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{\ell^a}$.

Then the requested probability tends to $\#\mathcal{S}/\#\text{SL}_2(Z_{\ell^{a+b+1}})$. Note that this question was also considered by Gekeler in [14] in the alternative setting mentioned in the introduction.

Note. As pointed out by the anonymous referee of a prior submission of this article, an alternative proof of Theorem 3 can be obtained by using intermediate results of Howe [16, Section 4]. For each pair of integers (M, N) for which $M \mid N$, Howe provides a closed formula for the number of \mathbb{F}_q -isomorphism classes of elliptic curves, counted with a weight that is inversely proportional to the size of the automorphism group, for which

$$E[N](\mathbb{F}_q) \cong Z_M \oplus Z_N.$$

By letting M range over the divisors of N and summing up the corresponding formulas, one recovers the estimates from Theorem 3.

Acknowledgements

The authors are very grateful to the anonymous referee of a prior submission of this document, to Hendrik W. Lenstra for suggesting the use of Chebotarev's density theorem, and to Barry Mazur and Bjorn Poonen for their helpful comments on modular curves. Both authors thank F.W.O.-Vlaanderen for its financial support. The first author thanks the Massachusetts Institute of Technology for its hospitality.

References

- [1] Achter, J.: The distribution of class groups of function fields. *J. Pure Appl. Alg.* 204(2), 316-333 (2006)
- [2] Achter, J.: Results of Cohen-Lenstra type for quadratic function fields. In: Lauter, K., Ribet, K. (eds.) *Computational Arithmetic Geometry*, *Contemporary Mathematics* 463, pp. 1-8. American Mathematical Society (2008)
- [3] Achter, J., Sadornil, D.: On the probability of having rational ℓ -isogenies. *Arch. Math.* 90, 511-519 (2008)
- [4] Birch, B.: How the number of points of an elliptic curve over a fixed prime field varies. *J. London Math. Soc.* 43, 57-60 (1968)

- [5] Carayol, H.: La conjecture de Sato-Tate. Séminaire Bourbaki 977, 59^{ème} année (2006-2007)
- [6] Castryck, W., Folsom, A., Hubrechts, H., Sutherland A.V.: The probability that the number of points on the Jacobian of a genus 2 curve is prime. Preprint (2011)
- [7] Chavdarov, N.: The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy. *Duke Math. J.* 87(1), 151-180 (1997)
- [8] Crandall, R., Pomerance, C.: Prime numbers: a computational perspective (second edition). Springer Science (2005)
- [9] Deligne, P.: La conjecture de Weil: II. *Publ. Math. IHES* 52, 137-252 (1980)
- [10] Deligne, P., Rapoport, M.: Les schémas de modules de courbes elliptiques. In: *Modular functions of one variable, II (Proc. Int. Summer School Antwerp)*, *Lecture Notes in Math.* 349, 143-174. Springer-Verlag (1973)
- [11] Fried, M., Jarden, M.: *Field Arithmetic* (third edition). *Ergebnisse der Mathematik und ihrer Grenzgebiete, 3. Folge, Bd. 11.* Springer-Verlag (1986)
- [12] Galbraith, S., McKee, J.: The probability that the number of points on an elliptic curve over a finite field is prime. *J. London Math. Soc.* 62(3), 671-684 (2000)
- [13] Gekeler, E.-U.: Frobenius distributions of elliptic curves over finite prime fields. *Int. Math. Res. Not.* 37, 1999-2018 (2003)
- [14] Gekeler, E.-U.: The distribution of group structures on elliptic curves over finite prime fields. *Documenta Math.* 11, 119-142 (2006)
- [15] Gekeler, E.-U.: Statistics about elliptic curves over finite prime fields. *Manuscripta Math.* 127, 55-67 (2008)
- [16] Howe, E.: On the group orders of elliptic curves over finite fields. *Compositio Math.* 85, 229-247 (1993)
- [17] Katz, N., Mazur, B.: *Arithmetic moduli of elliptic curves.* Princeton University Press (1985)
- [18] Katz, N., Sarnak, P.: *Random Matrices, Frobenius Eigenvalues, and Monodromy.* *Colloquium publications* 45, Am. Math. Soc. (1998)
- [19] Kedlaya, K., Sutherland A.V.: Hyperelliptic curves, L -polynomials, and random matrices. In: Lachaud, G., Ritzenthaler, C., Tsfasman, M. (eds.) *Proceedings of AGCT-11, Contemporary Mathematics* 487, pp. 119-162. American Mathematical Society (2009)
- [20] Lenstra H.W.: Factoring integers with elliptic curves. *Annals of Math.* 126(2), 649-673 (1987)
- [21] Rosser, J.B., Schoenfeld, L.: Approximate formulas for some functions of prime numbers. *Illinois Journal of Math.* 6(1), 64-94 (1962)
- [22] Silverman, J.: *The arithmetic of elliptic curves.* *Graduate Texts in Mathematics* 106. Springer (1985)

- [23] Vlăduț, S.: Cyclicity statistics for elliptic curves over finite fields. *Finite Fields Appl.* 5, 13-25 (1999)
- [24] Yoshida, H.: On an analogue of the Sato conjecture. *Inventiones Math.* 19, 261-277 (1973)