Compositio Mathematica

Everett W. Howe

On the group orders of elliptic curves over finite fields

Compositio Mathematica, tome 85, nº 2 (1993), p. 229-247
<http://www.numdam.org/item?id=CM_1993__85_2_229_0>

Compositio Mathematica **85**: 229–247, 1993.

On the group orders of elliptic curves over finite fields

EVERETT W. HOWE
Department of Mathematics, University of California, Berkeley, CA 94720, U.S.A.

Received 4 June 1991; accepted 28 November 1991

Abstract. Given a prime power q, for every pair of positive integers m and n with $m \mid \gcd(n, q-1)$ we construct a modular curve over $\mathbf{F}_q$ that parametrizes elliptic curves over $\mathbf{F}_q$ along with $\mathbf{F}_q$-defined points P and Q of order m and n, respectively, with P and $(n/m)Q$ having a given Weil pairing. Using these curves, we estimate the number of elliptic curves over $\mathbf{F}_q$ that have a given integer N dividing the number of their $\mathbf{F}_q$-defined points.

1. Introduction

Given a prime power q and a positive integer N, it is natural to wonder how likely it is for a randomly chosen elliptic curve over $\mathbf{F}_q$ to have N dividing the number of its $\mathbf{F}_q$-defined points. The purpose of this paper is to make sense of this question and to provide an estimate for its answer.

Since $\mathbf{F}_q$-isomorphic curves have the same number of $\mathbf{F}_q$-defined points, we will only be interested in $\mathbf{F}_q$-isomorphism classes of elliptic curves over $\mathbf{F}_q$. In particular, we will look at the set

$$V(\mathbf{F}_q;\, N) = \{E/\mathbf{F}_q \colon N \mid \#E(\mathbf{F}_q)\}/\cong_{\mathbf{F}_q};$$

we want to know how large this set is, compared to the set of all $\mathbf{F}_q$-isomorphism classes of elliptic curves over $\mathbf{F}_q$. However, it will be easiest to estimate not the usual cardinality of $V(\mathbf{F}_q; N)$ but rather the *weighted cardinality* of $V(\mathbf{F}_q; N)$, where the *weighted cardinality* of a set S of $\mathbf{F}_q$-isomorphism classes of elliptic curves over $\mathbf{F}_q$ is defined to be

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

where $[E]$ denotes the $\mathbf{F}_q$-isomorphism class of the elliptic curve E. Often, formulas for weighted cardinalities of such sets S work out better than formulas for the usual cardinalities; for instance, we will see in Corollary 2.2 that

$$\#'\{E \colon E \text{ is an elliptic curve over } \mathbf{F}_q\}/\cong_{\mathbf{F}_q} = q, \tag{1}$$

whereas the corresponding formula for the ordinary cardinality depends on the value of q mod 12. In any case, since $\mathrm{Aut}_{\mathbf{F}_q}(E)=\{\pm 1\}$ except possibly when $j(E)$ is 0 or 1728 (see [9], § III.10), the weighted cardinality of such a set S is generally about half of its usual cardinality.

In view of (1), we will interpret the ratio $\#'V(\mathbf{F}_q; N)/q$ as the probability that a random elliptic curve over $\mathbf{F}_q$ has N dividing the number of its $\mathbf{F}_q$-defined points. The following theorem gives an estimate of this ratio.

THEOREM 1.1. *There is a constant* $C \leqslant 1/12+5\sqrt{2}/6 \approx 1.262$ *such that the following statement is true: Given a prime power q, let r be the multiplicative arithmetic function such that for all primes l and positive integers a*

$$r(l^a)=\begin{cases}\dfrac{1}{l^{a-1}(l-1)} & \text{if } q \not\equiv 1 \bmod l^c;\\[2ex] \dfrac{l^{b+1}+l^b-1}{l^{a+b-1}(l^2-1)} & \text{if } q \equiv 1 \bmod l^c,\end{cases}$$

where $b=\lfloor a/2\rfloor$, the greatest integer less than or equal to $a/2$, and $c=\lceil a/2\rceil$, the least integer greater than or equal to $a/2$. Then for all positive integers N we have

$$\left|\frac{\#'V(\mathbf{F}_q; N)}{q}-r(N)\right| \leqslant \frac{CN\rho(N)2^{\nu(N)}}{\sqrt{q}}, \tag{2}$$

where $\rho(N)=\Pi_{p|N}((p+1)/(p-1))$ and $\nu(N)$ denotes the number of prime divisors of N.

It is interesting to note that $r(N)$ is greater than $1/N$ and for many values of N is not much less than $1/\varphi(N)$. Thus, loosely speaking, when q is large with respect to N it is more likely that a random elliptic curve over $\mathbf{F}_q$ has N dividing its number of points than it is that a random integer is divisible by N.

H. W. Lenstra, Jr. has proven the inequality (2) in the special case when N and q are distinct primes with $q>3$ (see [6], Proposition 1.14, p. 660). Lenstra's proof depends on properties of modular curves over $\mathbf{F}_p$; in particular, he uses the modular curves $X(l)$ and $X_1(l)$, for primes $l \neq p$. My extension of Lenstra's proposition is obtained by extending his proof, and accordingly my proof will require the study of modular curves which I will denote $X_q(m, n)$.

In Section 2, I briefly prove some results about forms that will be needed in Sections 3 and 4. In Section 3, I define the curves $X_q(m, n)$ as quotients of more familiar modular curves, give a modular interpretation of their $\mathbf{F}_q$-defined points, and use Weil's estimate to approximate the number of their $\mathbf{F}_q$-defined points. Finally, in Section 4, I use the interpretation and bounds of Section 3 for a number of curves to prove Theorem 1.1.

NOTATION. Throughout this paper, if C is a curve over a field K, and if L is an extension field of K, we will denote by C_L the L-scheme $C \times_{\mathrm{Spec}(K)} \mathrm{Spec}(L)$. Similarly, if P is a K-defined point on such a curve C, we will denote by P_L the point on C_L obtained from P by base extension. If E is an elliptic curve over K with zero point O, then the curve E_L has a unique structure of an elliptic curve over L with zero point O_L; when we mention the curve E_L, we will be referring to it as an elliptic curve, unless we explicitly state otherwise. The letters p and l are reserved for prime numbers. For real numbers x, we will denote by $\lfloor x \rfloor$ the greatest integer less than or equal to x and by $\lceil x \rceil$ the least integer greater than or equal to x. Also, we will make use of five arithmetic functions: the Möbius function μ; the function ν such that $\nu(n)$ is the number of prime divisors of n; the Euler totient function φ, defined by $\varphi(n) = n\prod_{p/n}(1 - 1/p)$; the function ψ defined by $\psi(n) = n\prod_{p|n}(1 + 1/p)$; and the function ρ defined by $\rho(n) = \prod_{p|n}((p+1)/(p-1))$.

2. Forms

DEFINITION. Let E be an elliptic curve over a field K, and let L be an extension field of K. An elliptic curve E' over K is called an *L/K-form of E* (or simply a *form of* E, if L and K are clear from context) if E_L and E'_L are isomorphic over L. We denote by $\mathbf{E}(L/K; E)$ or simply $\mathbf{E}(E)$ the set of forms of E, up to K-isomorphism:

$$\mathbf{E}(L/K;\, E) = \{E'/K \colon E'_L \cong E_L\}/\cong_K;$$

and we denote by $[E']_K$ or simply $[E']$ the K-isomorphism class of E'. Suppose we are also given points $P, Q \in E(K)$. A triple (E', P', Q'), where E' is an elliptic curve over K and P' and Q' are points of $E'(K)$, is called an *L/K-form of* (E, P, Q) if there is an L-isomorphism from E_L to E'_L that takes P_L to P'_L and Q_L to Q'_L. We denote by $\mathbf{E}(E, P, Q) = \mathbf{E}(L/K; E, P, Q)$ the set of L/K-forms of (E, P, Q), up to K-isomorphism, and we denote by $[E', P', Q']_K$ the K-isomorphism class of the triple (E', P', Q').

Suppose L is a finite or infinite Galois extension of K with topological Galois group G, and suppose E is an elliptic curve over K. Let A be the finite group $\mathrm{Aut}_L(E_L)$ of all L-automorphisms of E_L, and let B be the group of all commutative diagrams

$$\begin{array}{ccc} E_L & \xrightarrow{\ \alpha\ } & E_L \\ \downarrow & & \downarrow \\ \mathrm{Spec}(L) & \xrightarrow{\ \bar\sigma\ } & \mathrm{Spec}(L) \end{array}$$

where α is an automorphism of E_L as a K-scheme that fixes the zero point of E_L, and where for any element σ of G we denote by $\bar{\sigma}$ the scheme automorphism of $\mathrm{Spec}(L)$ obtained from the field automorphism σ^{-1} of L. There is clearly an exact sequence of groups

$$1 \longrightarrow A \longrightarrow B \xrightarrow{\pi} G \longrightarrow 1 \tag{3}$$

where π is the projection map taking an element $(\alpha, \bar{\sigma})$ of B to the element σ of G. The sequence (3) has a canonical splitting $G \to B$ defined by sending $\sigma \in G$ to the element $(1 \times \bar{\sigma}, \bar{\sigma})$ of B, where $1 \times \bar{\sigma}$ is the K-scheme automorphism of $E_L = E \times_{\mathrm{Spec}(K)} \mathrm{Spec}(L)$ obtained by fixing E and applying $\bar{\sigma}$ to $\mathrm{Spec}(L)$. As a set, B is the product of A and G; if we give A the discrete topology and B the product topology, the sequence (3) is even an exact sequence of topological groups.

From [8] (see in particular Section III.1.3), we know that $\mathbf{E}(L/K; E)$ is isomorphic (as a set with a distinguished element) to the cohomology set $H^1(G, A)$, where the cohomology is in the sense of Section I.5 of [8] (see also [9], Sections X.2 and X.5). A cocycle, in this sense, corresponds to a continuous homomorphism $s\colon G \to B$ splitting the exact sequence (3); such a section gives an action of G on E_L, and this defines by Galois descent an elliptic curve $E(s)/K$ and an isomorphism $f_s\colon E_L - E(s)_L$, unique up to $\mathrm{Aut}_K(E(s))$–see [10] or Number V.20 of [7] for the case of finite extensions L/K, and compare problem II.4.7 (p. 106) of [3]. The group A acts on the set S of sections by conjugation, and two cocycles are cohomologous if and only if their associated sections lie in the same A-orbit of S. Also, the stabilizer of a section s is isomorphic to the group of K-automorphisms of the associated form $E(s)$. Thus the orbit-decomposition formula ([5], p. 23) gives

$$\sum_{[E'] \in \mathbf{E}(E)} \frac{\# A}{\# \mathrm{Aut}_K(E')} = \# S. \tag{4}$$

PROPOSITION 2.1. *Let E be an elliptic curve over a finite field $\mathbf{F}_q$. Then*

$$\sum_{[E']_{\mathbf{F}_q} \in \mathbf{E}(\bar{\mathbf{F}}_q/\mathbf{F}_q; E)} \frac{1}{\# \mathrm{Aut}_{\mathbf{F}_q}(E')} = 1. \tag{5}$$

Proof. In the discussion above, take $K = \mathbf{F}_q$ and $L = \bar{\mathbf{F}}_q$. Since $\mathrm{Gal}(\bar{\mathbf{F}}_q/\mathbf{F}_q) \cong \hat{\mathbf{Z}}$, the exact sequence (3) becomes

$$1 \longrightarrow A \longrightarrow B \xrightarrow{\pi} \hat{\mathbf{Z}} \longrightarrow 1.$$

Since $\hat{\mathbf{Z}}$ is freely generated as a profinite group by 1, a section $s\colon \hat{\mathbf{Z}} \to B$ is determined by $s(1)$, and every element of $\pi^{-1}(1)$ gives rise to a section. Thus, $\# S = \# \pi^{-1}(1) = \# A$, and dividing equation (4) by the finite number $\# A$ yields (5). $\square$

COROLLARY 2.2. *For every prime power q,*

$$\#'\{E\colon E \text{ is an elliptic curve over } \mathbf{F}_q\}/\cong_{\mathbf{F}_q} = q.$$

Proof. Let T be the set of elliptic curves over $\mathbf{F}_q$ up to $\bar{\mathbf{F}}_q$-isomorphism and let U be the set of elliptic curves over $\mathbf{F}_q$ up to $\mathbf{F}_q$-isomorphism. We know that the j-invariant provides a bijection between T and $\mathbf{F}_q$, so $\# T = q$. Also, $U = \bigcup_{[E]_{\bar{\mathbf{F}}_q} \in T} \mathbf{E}(E)$, so that

$$\#' U = \sum_{[E']_{\bar{\mathbf{F}}_q} \in T} \; \sum_{[E]_{\mathbf{F}_q} \in \mathbf{E}(E')} \frac{1}{\# \operatorname{Aut}_{\mathbf{F}_q}(E)} = \# T = q$$

as claimed. $\square$

There is a result analogous to Proposition 2.1 for the forms of a triple (E, P, Q).

PROPOSITION 2.3. *Let E be an elliptic curve over a finite field $\mathbf{F}_q$, and let $P, Q \in E(\mathbf{F}_q)$. Then*

$$\sum_{[E',P',Q']_{\mathbf{F}_q} \in \mathbf{E}(\bar{\mathbf{F}}_q/\mathbf{F}_q; E,P,Q)} \frac{1}{\# \operatorname{Aut}_{\mathbf{F}_q}(E', P', Q')} = 1,$$

where $\operatorname{Aut}_{\mathbf{F}_q}(E', P', Q')$ denotes the subgroup of $\operatorname{Aut}_{\mathbf{F}_q}(E')$ consisting of those automorphisms that fix P' and Q'.

Proof. This result follows from making the obvious changes in the proof of Proposition 2.1 and the discussion preceding it. $\square$

NOTATION. Suppose L is a Galois extension of a field K, E is an elliptic curve over K, and F is an L/K-form of E. Given an isomorphism $f\colon E_L \to F_L$ and an element σ of $\operatorname{Gal}(L/K)$, let f^σ be the isomorphism $(1 \times \bar{\sigma}) \circ f \circ (1 \times \bar{\sigma})^{-1}\colon E_L \to F_L$ (here one of the $1 \times \bar{\sigma}$'s is a K-scheme automorphism of E_L, and the other is a K-scheme automorphism of F_L). If f is defined locally by polynomials with coefficients in L, then f^σ is defined by the same polynomials with σ applied to the coefficients.

PROPOSITION 2.4. *Let E be an elliptic curve over a finite field $\mathbf{F}_q$, and let α be an automorphism of $E_{\bar{\mathbf{F}}_q}$. Then there is an $\bar{\mathbf{F}}_q/\mathbf{F}_q$-form F of E and an isomorphism $f\colon E_{\bar{\mathbf{F}}_q} \to F_{\bar{\mathbf{F}}_q}$ such that $\alpha = f^{-1} \circ f^\sigma$, where σ is the qth power automorphism of $\bar{\mathbf{F}}_q$.*

Proof. With notation as above, let $s: G \to B$ be the section defined by sending σ to $(\alpha \circ (1 \times \bar{\sigma}), \bar{\sigma})$ and let $F = E(s)$ and $f = f_s$. It is not difficult to check that $\alpha = f^{-1} \circ f^{\sigma}$. □

3. Modular curves over finite fields

As indicated in the Introduction, in Section 4 we will need to use bounds obtained from modular curves other than the 'standard' modular curves $X(l)$ and $X_1(l)$. In this section we define the curves we will need, and prove some basic results about them.

First, we recall some facts about Frobenius morphisms of schemes and elliptic curves (see the discussion in [4], Chapter 12). For any scheme S over $\mathbf{F}_p$, we define the (p^rth *power*) *absolute Frobenius* morphism $F_{p^r,\mathrm{abs}}: S \to S$ to be the morphism corresponding to the endomorphism $x \mapsto x^{p^r}$ of affine rings. If S is a scheme over a field K of characteristic $p > 0$, we denote by $S^{(p^r)}$ the scheme over K defined by the cartesian diagram

$$\begin{array}{ccc} S^{(p^r)} & \longrightarrow & S \\ \downarrow & & \downarrow \\ \mathrm{Spec}(K) & \xrightarrow{F_{p^r,\mathrm{abs}}} & \mathrm{Spec}(K) \end{array}$$

so that if S is defined locally by polynomials $f_i \in K[x_1, \ldots, x_n]$ then $S^{(p^r)}$ is defined locally by the polynomials $f_i^{(p^r)}$ obtained from the f_i by raising all the coefficients to the p^rth power.

In view of the cartesian property of the above diagram, the p^rth power absolute Frobenius on S factors through $S^{(p^r)}$; that is, there is a morphism $F_{p^r} = F_{p^r,S/K}: S \to S^{(p^r)}$ of K-schemes, called the (p^rth *power relative-to-K*) *Frobenius*, such that F_{p^r} composed with the map from $S^{(p^r)}$ to S is the morphism $F_{p^r,\mathrm{abs}}$ on S. If S is affine and defined by polynomials f_i as above, then F_{p^r} takes a point $P = (a_1, \ldots, a_n)$ on S to the point $P^{(p^r)} = (a_1^{p^r}, \ldots, a_n^{p^r})$ on $S^{(p^r)}$. In the special case where S is an elliptic curve E over K, there is a natural elliptic curve structure on $E^{(p^r)}$, and the Frobenius F_{p^r} is actually an isogeny. The dual isogeny of F_{p^r} (see [9], Section III.6) is the *Verschiebung* $V_{p^r}: E^{(p^r)} \to E$, and the composed map $V_{p^r} \circ F_{p^r}: E \to E$ is the multiplication-by-p^r map on E.

We also recall that an elliptic curve E over a field K of characteristic $p > 0$ is called *supersingular* if E has no $\bar{K}$-defined points of order p (see [9], Section V.3). This is equivalent to the condition that for some $r > 0$ the only $\bar{K}$-valued point in the kernel of the Verschiebung V_{p^r} is the zero point (which implies the same statement for *all* $r > 0$).

The following notation will be useful in this section and the next.

NOTATION. Suppose p is a prime number and m and n are positive integers with $m \mid n$ and m coprime to p, and write $n = n'p^r$ with n' coprime to p. If K is a field of characteristic p containing a primitive mth root of unity ζ_m and L is an extension field of K, we denote by $Z(L/K; \zeta_m, m, n)$ the set of L-isomorphism classes

$$Z(L/K; \zeta_m, m, n) = \{(E, P, Q, R): E \text{ is an elliptic curve over } K,\ P, Q \in E(K) \text{ with } \operatorname{ord} P = m \text{ and } \operatorname{ord} Q = n' \text{ and } e_m(P, (n'/m)Q) = \zeta_m, \text{ and } R \in E^{(p^r)}(K) \text{ such that } R_{\bar{K}} \text{ generates the kernel of the Verschiebung } V_{p^r}: E_{\bar{K}}^{(p^r)} \to E_{\bar{K}}\}/\cong_L$$

where $\operatorname{ord} P$ is the order of P in the group $E(K)$ and e_m is the Weil pairing on $E[m]$ (see [9], Section III.8), and where two such quadruples (E, P, Q, R) and (E', P', Q', R') are said to be L-isomorphic if there is a L-isomorphism $f: E_L \to E'_L$ such that f takes P_L to P'_L and Q_L to Q'_L and such that $f^{(p^r)}$ takes R_L to R'_L. Denote by $[E, P, Q, R]_L$ the L-isomorphism class of the quadruple (E, P, Q, R).

Also, we denote by $Y(L/K; \zeta_m, m, n)$ the set of L-isomorphism classes

$$Y(L/K; \zeta_m, m, n) = \{(E, P, Q): E \text{ is an elliptic curve over } K,\ P, Q \in E(K) \text{ with } \operatorname{ord} P = m \text{ and } \operatorname{ord} Q = n \text{ and } e_m(P, (n/m)Q) = \zeta_m\}/\cong_L$$

where two such triples (E, P, Q) and (E', P', Q') are said to be L-isomorphic if there is an L-isomorphism $f: E_L \to E'_L$ that takes P_L to P'_L and Q_L to Q'_L. Denote by $[E, P, Q]_L$ the L-isomorphism class of the triple (E, P, Q).

PROPOSITION 3.1. *Let $q = p^e$ be a prime power, suppose m and n are positive integers such that $m \mid \gcd(n, q-1)$, write $n = n'p^r$ with n' coprime to p, and pick a primitive mth root of unity $\zeta_m \in \mathbf{F}_q$. There exists a proper nonsingular irreducible curve $\bar{X}(m, n)$ over $\bar{\mathbf{F}}_q$ provided with a map $J: \bar{X}(m, n) \to \mathbf{P}^1_{\bar{\mathbf{F}}_q} \supset \mathbf{A}^1_{\bar{\mathbf{F}}_q} = \operatorname{Spec}(\bar{\mathbf{F}}_q[j])$ with the following properties:*

1. *There is a natural bijection between the set of finite points of $\bar{X}(m, n)$ (that is, the points in $J^{-1}(\mathbf{A}^1)$) and the set $Z(\bar{\mathbf{F}}_q/\bar{\mathbf{F}}_q; \zeta_m, m, n)$.*
2. *The bijection given in 1 has the property that if $x \in \bar{X}(m, n)$ corresponds to $[E, P, Q, R]_{\bar{\mathbf{F}}_q}$ then $J(x) = j(E)$, the j-invariant of E.*
3. *$\bar{X}(m, n)$ can be defined naturally over $\mathbf{F}_q$; that is, there is a proper nonsingular irreducible curve $X_q(m, n)$ over $\mathbf{F}_q$ and an isomorphism*

$$\bar{X}(m, n) \cong X_q(m, n) \times_{\operatorname{Spec}(\mathbf{F}_q)} \operatorname{Spec}(\bar{\mathbf{F}}_q) \tag{6}$$

such that the qth *power relative-to-*$\bar{\mathbf{F}}_q$ *Frobenius map* $F\colon \bar{X}(m,n)\to\bar{X}(m,n)$ *obtained from the isomorphism* (6) *and the canonical identification*

$$(X_q(m,n)\times_{\mathrm{Spec}(\mathbf{F}_q)}\mathrm{Spec}(\bar{\mathbf{F}}_q)) = (X_q(m,n)\times_{\mathrm{Spec}(\mathbf{F}_q)}\mathrm{Spec}(\bar{\mathbf{F}}_q))^{(q)}$$

has the property that if the point $x\in\bar{X}(m,n)$ *corresponds to* $[E,P,Q,R]_{\bar{\mathbf{F}}_q}$, *then* $F(x)$ *corresponds to* $[E^{(q)},P^{(q)},Q^{(q)},R^{(q)}]_{\bar{\mathbf{F}}_q}$.

Proof. We will rely heavily on results from [4].

First consider the case where $n'>2$.

Pick a primitive n'th root of unity $\zeta_{n'}\in\bar{\mathbf{F}}_q$ such that $\zeta_m=\zeta_{n'}^{n'/m}$, let $\bar{X}(n',n)$ be the $\bar{\mathbf{F}}_q$-scheme denoted in [4] by $\bar{\mathscr{M}}([\Gamma(n')]^{\mathrm{can}},[\mathrm{Ig}(p^r)])$ (in [4], see Sections 4.3 and 8.6 for the definition of $\bar{\mathscr{M}}(\cdot)$, Sections 3.1 and 9.1 for the definition of $[\Gamma(n')]^{\mathrm{can}}$, and Section 12.3 for the definition of $[\mathrm{Ig}(p^r)]$), and let $J'\colon\bar{X}(n',n)\to\mathbf{P}^1_{\bar{\mathbf{F}}_q}\supset\mathbf{A}^1_{\bar{\mathbf{F}}_q}=\mathrm{Spec}(\bar{\mathbf{F}}_q[j])$ be the natural map from $\bar{X}(n',n)$ to the "j-line" $\mathbf{P}^1_{\bar{\mathbf{F}}_q}$ defined in Section 8.2 of [4]. By their very definitions, $\bar{X}(n',n)$ and J' satisfy statements 1 and 2 of the proposition (with m replaced by n' and J replaced by J'), and from Corollary 12.7.2 (p. 368) of [4], whose hypotheses are satisfied when $n'>2$, we see that $\bar{X}(n',n)$ is a proper nonsingular irreducible curve. From Chapter 7 of [4], we know the group

$$G=(\mathrm{SL}_2(\mathbf{Z}/n'\mathbf{Z})\times(\mathbf{Z}/p^r\mathbf{Z})^*)/\pm 1$$

(where the group $\{\pm 1\}$ is embedded diagonally in the product) acts on the covering $\bar{X}(n',n)$ of $\mathbf{P}^1$; the action is such that an element

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

of G takes the point corresponding to the class $[E,P,Q,R]_{\bar{\mathbf{F}}_q}\in Z(\bar{\mathbf{F}}_q/\bar{\mathbf{F}}_q;n',n)$ to the point corresponding to the class $[E,aP+cQ,bP+dQ,uR]_{\bar{\mathbf{F}}_q}$. In fact, from Corollaries 10.13.12 (p. 336) and 12.9.4 (p. 381) of [4] we see that the degree of $\bar{X}(n',n)$ over $\mathbf{P}^1$ is equal to $\# G$; since G acts faithfully on $\bar{X}(n',n)$, this shows that $\bar{X}(n',n)$ is a Galois covering of $\mathbf{P}^1$ with group G.

Define a subgroup H of G by

$$H=\left\{\pm\left(\begin{pmatrix} 1 & 0\\ a & 1\end{pmatrix}, 1\right)\in G\colon a\equiv 0 \bmod m\right\}$$

and define $\bar{X}(m,n)$ to be the quotient of $\bar{X}(n',n)$ by the group H. Let $J\colon\bar{X}(m,n)\to\mathbf{P}^1$ be the map induced from J'.

Now, a finite point on $\bar{X}(m,n)$ corresponds to an H-orbit of the finite points on $\bar{X}(n', n)$; thus, the finite points on $\bar{X}(m, n)$ correspond to the $\bar{\mathbf{F}}_q$-isomorphism classes of sets of the form

$$\{(E, P + aQ, Q, R): a \equiv 0 \bmod m\},$$

where $[E, P, Q, R]_{\bar{\mathbf{F}}_q} \in Z(\bar{\mathbf{F}}_q/\bar{\mathbf{F}}_q; n', n)$ and where two such sets $\{(E, P+aQ, Q, R)\}$ and $\{(E', P'+aQ', Q', R')\}$ are $\bar{\mathbf{F}}_q$-isomorphic if there is an isomorphism $f: E \to E'$ such that f maps Q to Q' and the set $\{P+aQ\}$ to $\{P'+aQ'\}$ and such that $f^{(p^r)}$ maps R to R'. But there is a natural bijection between the set of all such $\bar{\mathbf{F}}_q$-isomorphism classes and the set $Z(\bar{\mathbf{F}}_q/\bar{\mathbf{F}}_q; m, n)$ given by sending the class of $\{(E, P+aQ, Q, R)\}$ to the class $[E, \frac{n'}{m}P, Q, R]_{\bar{\mathbf{F}}_q}$. Thus, $\bar{X}(m, n)$ satisfies the property given in statement 1 of the proposition.

That J satisfies the property given in statement 2 is a consequence of the fact that J' satisfies the corresponding property and of the construction just given.

Finally, that $\bar{X}(m, n)$ may be defined over $\mathbf{F}_q$ in the manner described in statement 3 follows from general principles given in [4] (see in particular the discussion in Section 12.10) and from the fact that the correspondence in statement 1 refers only to structures (in particular, the element ζ_m) that are defined over $\mathbf{F}_q$.

This completes the proof for the case where $n' > 2$. Now suppose $n' \leqslant 2$. The problem with proceeding exactly as before is that the results in [4] that we used in the case $n' > 2$ (in particular, Corollaries 12.7.2, 10.13.12 and 12.9.4) do not apply when $n' \leqslant 2$, because, in the language of [4], $[\Gamma(n')]^{\mathrm{can}}$ is not representable when $n' \leqslant 2$. Thus, we have to make some very minor modifications to our previous argument, although the general idea is exactly the same.

If $n' = 2$ let $f = 2$; if $n' = 1$ and $p \neq 3$ let $f = 3$; if $n' = 1$ and $p = 3$ let $f = 4$. Consider the curve $\bar{X}(fn', fn)$, which, as before, is a Galois covering of $\mathbf{P}^1$ with Galois group

$$G = (\mathrm{SL}_2(\mathbf{Z}/fn'\mathbf{Z}) \times (\mathbf{Z}/p^r\mathbf{Z})^*)/\pm 1,$$

and which has an interpretation as in statement 1. Now let H be the subgroup

$$H = \left\{ \pm\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, 1\right) \in G: a \equiv d \equiv 1 \bmod n',\ b \equiv 0 \bmod n', \text{ and } c \equiv 0 \bmod m \right\},$$

and let $\bar{X}(m, n)$ be the quotient of $\bar{X}(fn', fn)$ by H. The proof follows exactly as before.

Thus, the proposition is valid for all values of n'. □

There are two special kinds of points on the curves $\bar{X}(m, n)$ that we will need to keep track of.

DEFINITION. Let q, m, n, $\bar{X}(m,n)$, and J be as in Proposition 3.1. A point $x \in \bar{X}(m,n)$ is a *cusp* if x is an element of $J^{-1}(\infty)$. A point of $\bar{X}(m,n)$ which is not a cusp is called a *finite point*. A finite point of $\bar{X}(m,n)$ is a *supersingular point* if it corresponds to an equivalence class $[E,P,Q,R]_{\bar{\mathbf{F}}_q}$ with a supersingular E.

NOTATION. We denote by $g_q(m,n)$ the genus of $\bar{X}(m,n)$, by $c_q(m,n)$ the number of cusps of $\bar{X}(m,n)$, and by $s_q(m,n)$ the number of supersingular points of $\bar{X}(m,n)$.

PROPOSITION 3.2. *For all $q = p^e$, m, and $n = n'p^r$ as in Proposition* 3.1 *we have*

$$g_q(m,n) \leqslant \frac{1}{24} m\varphi(n)\psi(n) \tag{7}$$

$$c_q(m,n) \leqslant \varphi(n)\psi(n) \tag{8}$$

and when $p \mid n$ (that is, when $r > 0$) we have

$$s_q(m,n) \leqslant \frac{1}{3} m\varphi(n)\psi(n). \tag{9}$$

Proof. As in the preceding proof, we first assume that $n' > 2$.

Let the groups G and H be as in the proof of Proposition 3.1, so that $\bar{X}(m,n)$ is the quotient of $\bar{X}(n',n)$ by H. From Corollary 10.13.12 (p. 336) and Corollary 12.9.4 (p. 381) of [4] we find that

$$g_q(n',n) = \begin{cases} 1 + \dfrac{1}{24}(n-6)\varphi(n)\psi(n) & \text{if } n' = n; \\[2ex] 1 + \dfrac{1}{48}(n-12)\varphi(n)\psi(n') & \text{if } n' < n \end{cases} \tag{10}$$

$$c_q(n',n) = \frac{1}{2}\varphi(n)\psi(n')$$

$$s_q(n',n) = \frac{p-1}{24} n'\varphi(n')\psi(n'). \tag{11}$$

Since $\# H = n'/m$, the Riemann-Hurwitz formula ([9], Theorem 5.9, p. 41) gives us the estimate

$$g_q(m,n) \leqslant \begin{cases} 1 + \dfrac{1}{24}\dfrac{m}{n}(n-6)\varphi(n)\psi(n) & \text{if } n' = n; \\[2ex] 1 + \dfrac{1}{48}\dfrac{m}{n'}(n-12)\varphi(n)\psi(n') & \text{if } n' < n, \end{cases}$$

which leads to (7).

We also have the trivial bound

$$c_q(m, n) \leqslant c_q(n', n) = \frac{1}{2}\, \varphi(n)\psi(n') \leqslant \frac{1}{2}\varphi(n)\psi(n),$$

which certainly implies (8).

To get a good bound for $s_q(m, n)$, we need to determine necessary conditions for an element of H to fix a finite point of $\bar{X}(n', n)$. So suppose x is a finite point of $\bar{X}(n', n)$, corresponding to the class $[E, P, Q, R]_{\bar{\mathbf{F}}_q}$; for a non-trivial element of H to fix x, we must have $[E, P, Q, R]_{\bar{\mathbf{F}}_q} = [E, P+aQ, Q, R]_{\bar{\mathbf{F}}_q}$ for some a with $a \equiv 0$ mod m and $a \not\equiv 0$ mod n', so there must be an automorphism α of E that fixes Q and sends P to $P+aQ$. Thus $\alpha \neq \pm 1$, and from Corollary 2.7.1 (p. 85) of [4] we see that α satisfies $\alpha^2 - t\alpha + 1 = 0$ for some integer t with $|t| \leqslant 1$. In particular, this means that $(2-t)Q = 0$, which is impossible if $n' > 3$. Thus, if $n' > 3$ no non-trivial element of H fixes any finite point of $\bar{X}(n', n)$, so every finite point of $\bar{X}(m, n)$ has $\# H$ points of $\bar{X}(n', n)$ lying over it; this gives us

$$s_q(m, n) = \frac{m}{n'}\, s_q(n', n) = \frac{p-1}{24}\, m\varphi(n')\psi(n').$$

When $n' = 3$, we at least have the bound

$$s_q(m, n) \leqslant s_q(n', n) \leqslant \frac{p-1}{8}\, m\varphi(n')\psi(n'),$$

so that in any case if $p \mid n$ we have

$$s_q(m, n) \leqslant \frac{1}{24}\, m\varphi(n)\psi(n).$$

This gives us (9).

Thus, when $n' > 2$, the inequalities of the proposition hold.

When $n' \leqslant 2$, let f, G, and H be as in the case $n' \leqslant 2$ of the proof of Proposition 3.1, so that $\bar{X}(m, n)$ is the quotient of $\bar{X}(fn', fn)$ by H. Once again, one can check that equation (10) and the Riemann-Hurwitz formula lead to (7).

To prove (8), we note that it is possible to define $\bar{X}(m, n')$ as the quotient of $\bar{X}(fn', fn)$ by the subgroup of G generated by H and the image of $(\mathbf{Z}/p^r\mathbf{Z})^*$ in G; this gives us a map from $\bar{X}(m, n)$ to $\bar{X}(m, n')$ consistent with the maps from these curves to $\mathbf{P}^1$ and of degree at most $\varphi(p^r)$, so that $c_q(m, n) \leqslant \varphi(p^r)c_q(m, n')$. From this inequality we see that it suffices to prove (8) when $n = n'$, that is, when $r = 0$. But from statement 1 of Theorem 10.9.1 (p. 301) of [4] we can calculate that $c_q(2, 2) = 3$, $c_q(1, 2) = 2$, and $c_q(1, 1) = 1$, so inequality (8) *does* hold when $r = 0$.

Finally, suppose $p \mid n$. Using the trivial bound $s_q(m, n) \leqslant s_q(fn', fn)$ and equation (11), we see that

$$s_q(m, n) \leqslant \frac{p-1}{24} fn'\varphi(fn')\psi(fn');$$

it is easy to check that this inequality implies (9), except when $n = p = 3$. But in this case we notice that $G = H$, so that $\bar{X}(1, 3) = \mathbf{P}^1$ has exactly one supersingular point (corresponding to the elliptic curve with j-invariant 0), and we can verify (9) directly.

Thus, inequalities (7), (8), and (9) hold in every case. $\square$

REMARK. From equation (10) we see that 1/24 is the smallest possible constant in inequality (7). The facts that $c_q(1, 1) = 1$ and $s_2(1, 2) = 1$ show that equality is sometimes obtained in inequalities (8) and (9).

We now focus on the curves $X_q(m, n)$. In particular, we may ask whether there is a modular interpretation for the $\mathbf{F}_q$-defined points of $X_q(m, n)$. The answer is "yes".

PROPOSITION 3.3. *Let q, m, $n = n'p^r$, ζ_m, and $X_q(m, n)$ be as in Proposition* 3.1. *There is a bijection between the set of finite points of $X_q(m, n)(\mathbf{F}_q)$ (that is, the finite points of $X_q(m, n)$ that are defined over $\mathbf{F}_q$) and the set $Z(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$.*

Proof. Let $F: \bar{X}(m, n) \to \bar{X}(m, n)$ be the qth power relative-to-$\bar{\mathbf{F}}_q$ Frobenius map, as in statement 3 of Proposition 3.1. Then there is a bijection between $X_q(m, n)(\mathbf{F}_q)$ and the set of points of $\bar{X}(m, n)$ fixed by F, given by $x \mapsto x_{\bar{\mathbf{F}}_q}$. Again by statement 3 of Proposition 3.1, we know that the finite points of this last set correspond to the elements of the set

$$S = \{[E, P, Q, R]_{\bar{\mathbf{F}}_q} \in Z(\bar{\mathbf{F}}_q/\bar{\mathbf{F}}_q; \zeta_m, m, n): [E, P, Q, R]_{\bar{\mathbf{F}}_q} = [E^{(q)}, P^{(q)}, Q^{(q)}, R^{(q)}]_{\bar{\mathbf{F}}_q}\}.$$

Thus, we need only show that there is a bijection between the sets S and $Z(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$.

There is clearly an injective map from $Z(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$ to S defined by sending $[E, P, Q, R]_{\bar{\mathbf{F}}_q}$ to $[E_{\bar{\mathbf{F}}_q}, P_{\bar{\mathbf{F}}_q}, Q_{\bar{\mathbf{F}}_q}, R_{\bar{\mathbf{F}}_q}]_{\bar{\mathbf{F}}_q}$. We need only show that this map is surjective.

Suppose $[E, P, Q, R]_{\bar{\mathbf{F}}_q}$ is an element of S, and let $f: E \to E^{(q)}$ be an isomorphism that takes the quadruple (E, P, Q, R) to the quadruple $(E^{(q)}, P^{(q)}, Q^{(q)}, R^{(q)})$. Since $E \cong_{\bar{\mathbf{F}}_q} E^{(q)}$, we have $j(E) = j(E^{(q)}) = (j(E))^q$, so $j(E) \in \mathbf{F}_q$. Let E' be any elliptic curve over $\mathbf{F}_q$ with $j(E') = j(E)$; since elliptic curves over $\bar{\mathbf{F}}_q$ are classified up to $\bar{\mathbf{F}}_q$-isomorphism by their j-invariants, there is an isomorphism $g: E \to E'_{\bar{\mathbf{F}}_q}$. By Proposition 2.4, there is a form F of E' and an isomorphism $h: E'_{\bar{\mathbf{F}}_q} \to F_{\bar{\mathbf{F}}_q}$ such that

$$g \circ f^{-1} \circ (g^{(q)})^{-1} = h^{-1} \circ h^{(q)},$$

and by replacing E' with F and g with $h \circ g$, we may assume that $g^{(q)} \circ f \circ g^{-1}$ is the identity on $E'_{\bar{\mathbf{F}}_q}$.

Now consider the point $g(P) \in E'_{\bar{\mathbf{F}}_q}(\bar{\mathbf{F}}_q)$. We have

$$g(P) = (g^{(q)} \circ f \circ g^{-1})(g(P)) = g^{(q)}(f(P)) = g^{(q)}(P^{(q)}) = (g(P))^{(q)},$$

so $g(P)$ is an $\mathbf{F}_q$-defined point of $E'_{\bar{\mathbf{F}}_q}$; that is, there is a point $P' \in E'(\mathbf{F}_q)$ such that $g(P) = P'_{\bar{\mathbf{F}}_q}$. Similarly, we see that $g(Q)$ and $g^{(p^r)}(R)$ come from points $Q' \in E'(\mathbf{F}_q)$ and $R' \in E'^{(p^r)}(\mathbf{F}_q)$, so that $[E', P', Q', R']_{\bar{\mathbf{F}}_q}$ is an element of $Z(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$ that maps to the element $[E, P, Q, R]_{\bar{\mathbf{F}}_q}$ of S. Thus, the natural map from $Z(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$ to S is bijective, and the proposition is proven. □

REMARK. More generally, if K is any field containing $\mathbf{F}_q$ and $\bar{K}$ is the algebraic closure of K, we know from Lemma 8.1.3.1 (p. 225) of [4] that there is a bijection between the set of finite $\bar{K}$-valued points of $X_q(m, n)$ and $Z(\bar{K}/\bar{K}; \zeta_m, m, n)$, and we may ask whether the finite K-valued points of $X_q(m, n)$ correspond to the elements of $Z(\bar{K}/K; \zeta_m, m, n)$. The proof of Proposition 3.2 (p. 274) of [2] provides an answer: The obstruction to a K-valued point giving rise to a quadruple (E, P, Q, R) defined over K lies in a certain H^2, and it is shown in the proof of Proposition 3.2 of [2] that this obstruction is zero. In the special case $K = \mathbf{F}_q$ we consider above, the argument simplifies, because in this case the whole H^2 where the obstruction lives is trivial. One can use this argument to provide a more conceptual proof of Proposition 3.3. The interested reader should consult [2].

COROLLARY 3.4. *There is a constant $C' \leqslant 1/12 + 5\sqrt{2}/6 \approx 1.262$ such that for all q, m, and $n = n'p^r$ as in Proposition 3.1 the following statements are true:*

1. *If $n' = n$, then there is a bijection between the set $Y(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$ and the set of finite points of $X_q(m, n)(\mathbf{F}_q)$.*
2. *If $n' < n$, then there is a bijection between the set $Y(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$ and the set of finite non-supersingular points of $X_q(m, n)(\mathbf{F}_q)$.*
3. *We have the estimate*

$$|\# Y(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n) - q| \leqslant C' m\varphi(n)\psi(n)\sqrt{q}. \tag{12}$$

Proof. If $n' = n$ then there is a bijection between the sets $Y(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$ and $Z(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$, given by mapping $[E, P, Q]_{\bar{\mathbf{F}}_q}$ to $[E, P, Q, O]_{\bar{\mathbf{F}}_q}$, where O is the zero element of $E = E^{(1)}$ (which generates the kernel of the Verschiebung V_1, the identity map). Thus, statement 1 follows immediately from Proposition 3.3.

If $n' < n$, let

$$\begin{aligned} &Z'(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n) \\ &\quad = \{[E, P, Q, R]_{\bar{\mathbf{F}}_q} \in Z(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n) : E \text{ is not supersingular}\}. \end{aligned}$$

Let M be the map from $Y(\bar{\mathbf{F}}_q/\mathbf{F}_q;\ \zeta_m,\ m,\ n)$ to $Z(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$ that sends $[E, P, Q]_{\bar{\mathbf{F}}_q}$ to $[E, P, p^r Q, (n'Q)^{(p^r)}]_{\bar{\mathbf{F}}_q}$. The image of M lies in $Z'(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$, because if $Q \in E(\mathbf{F}_q)$ has order n then $n'Q$ has order $p^r \neq 1$, so that E is not supersingular. Choose integers a and b such that $ap^r + bn' = 1$; then the inverse of M is the map from $Z'(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$ to $Y(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$ that sends $[E, P, Q, R]_{\bar{\mathbf{F}}_q}$ to $[E, P, (aQ + bR')]_{\bar{\mathbf{F}}_q}$, where R' is the element of $E(\mathbf{F}_q)$ such that $(R')^{(p^r)} = R$ – this element exists and is unique because $\mathbf{F}_q$ is perfect. Thus M is a bijection between $Y(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$ and $Z'(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$, so that statement 2 follows from Proposition 3.3.

To prove statement 3 we will need to use the Weil conjectures for curves (see [11] or [1]); in particular, we will need the inequality ([11], Corollaire 3, p. 70)

$$|\# X_q(m,\ n)(\mathbf{F}_q) - 1 - q| \leqslant 2g_q(m,\ n)\sqrt{q}. \tag{13}$$

First suppose that $n' = n$. Then statement 1, combined with the inequalities (7), (8), and (13), gives us

$$|\# Y(\bar{\mathbf{F}}_q/\mathbf{F}_q;\ \zeta_m,\ m,\ n) - q| \leqslant 1 + \varphi(n)\psi(n) + \frac{1}{12} m\varphi(n)\psi(n)\sqrt{q}.$$

On the other hand, if $n' < n$, then statement 2, combined with the inequalities (7), (8), (9), and (13), gives us

$$\begin{aligned} &|\# Y(\bar{\mathbf{F}}_q/\mathbf{F}_q;\ \zeta_m,\ m,\ n) - q| \\ &\leqslant 1 + \varphi(n)\psi(n) + \frac{1}{3} m\varphi(n)\psi(n) + \frac{1}{12} m\varphi(n)\psi(n)\sqrt{q}. \end{aligned}$$

Thus, statement 3 will hold if we choose C' so that for all q, m, and n we have

$$C' \geqslant \frac{1}{m\varphi(n)\psi(n)\sqrt{q}} + \frac{1}{m\sqrt{q}} + \frac{1}{3\sqrt{q}} + \frac{1}{12}.$$

However, since $\# Y(\bar{\mathbf{F}}_q/\mathbf{F}_q; 1, 1, 1) = q$ (as we noted in the proof of Corollary 2.2, where the set was called T), we need only have the above inequality when $n > 1$. Thus, $C' = 1/12 + 5\sqrt{2}/6$ will do. □

With inequality (12) in hand, we can proceed to the calculations of Section 4.

4. Proof of the theorem

Fix a prime power $q = p^e$, and let ζ_{q-1} be a primitive $(q-1)$th root of unity in $\mathbf{F}_q$. For each m dividing $q - 1$, let ζ_m be the primitive mth root of unity $\zeta_{q-1}^{(q-1)/m}$.

Recall that for every pair (m, n) of positive integers with m dividing $\gcd(n, q-1)$ we have sets $Y(\mathbf{F}_q/\mathbf{F}_q; \zeta_m, m, n)$ and $Y(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$. For each pair (m, n) with $m \mid n$ we also define a set

$$W(\mathbf{F}_q;\, m,\, n) = \{E/\mathbf{F}_q\colon E[n](\mathbf{F}_q) \cong (\mathbf{Z}/m\mathbf{Z}) \times (\mathbf{Z}/n\mathbf{Z})\}/\cong_{\bar{\mathbf{F}}_q}.$$

Note that $W(\mathbf{F}_q; m, n)$ is empty unless m divides $q-1$; see Corollary 8.1.1 (p. 98) of [9]. Also, for every positive integer N, we have the set $V(\mathbf{F}_q; N)$. Our goal is to estimate the weighted cardinality of $V(\mathbf{F}_q; N)$.

For all the appropriate values of m, n, and N, let $v(N) = \#'V(\mathbf{F}_q; N)$ and $w(m, n) = \#'W(\mathbf{F}_q; m, n)$ and $y(m, n) = \# Y(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$ (note that $y(m, n)$ is a non-weighted cardinality). Corollary 3.4 gives us an estimate for $y(m, n)$ for all pairs (m, n) with m dividing $\gcd(n, q-1)$. To get from these estimates to an estimate for $v(N)$, we need to make explicit the relationships among the sets mentioned above.

NOTATION. Let t and u denote the multiplicative arithmetic functions defined on prime powers l^a by $t(l^a) = l^{\lfloor a/2 \rfloor}$ and $u(l^a) = l^{\lceil a/2 \rceil}$; thus, for every positive integer N we have $N/t(N)^2 = u(N)^2/N$, and this number is a squarefree integer. Also, given a positive integer n and a prime number l, we will denote by $n_{(l)}$ the largest power of l dividing n. Thus, for example, $t(24) = 2$ and $u(24) = 12$ and $24_{(2)} = 8$.

LEMMA 4.1. *Let N be any positive integer. Then*

$$V(\mathbf{F}_q;\, N) = \coprod_{d \mid \gcd(u(N), q-1)} W\left(\mathbf{F}_q;\, d,\, \frac{N}{\gcd(d,\, t(N))}\right), \tag{14}$$

and

$$v(N) = \sum_{d \mid \gcd(u(N), q-1)} w\left(d,\, \frac{N}{\gcd(d,\, t(N))}\right). \tag{15}$$

Proof. Since (15) follows from (14), it suffices to prove (14). Also, (14) is equivalent to

$$V(\mathbf{F}_q;\, N) = \coprod_{d \mid u(N)} W\left(\mathbf{F}_q;\, d,\, \frac{N}{\gcd(d,\, t(N))}\right), \tag{16}$$

because the additional sets we get in (16) are all empty.

It is easy to see that $W(\mathbf{F}_q; d, N/\gcd(d, t(N))) \subset V(\mathbf{F}_q; N)$ for each divisor d of $u(N)$. On the other hand, suppose we are given an elliptic curve E over $\mathbf{F}_q$ with $[E]_{\mathbf{F}_q} \in V(\mathbf{F}_q; N)$. It is not hard to show that if $d \mid u(N)$ then $[E]_{\mathbf{F}_q}$ is an element of $W(\mathbf{F}_q; d, N/\gcd(d, t(N)))$ if and only if d is the largest divisor of $u(N)$ for which

$\# E[d](\mathbf{F}_q) = d^2$; this is easy to check when N is a prime power, and it suffices to check only this case because for all pairs (m, n) with $m \mid n$ we have

$$W(\mathbf{F}_q;\, m,\, n) = \bigcap_{\text{primes } l} W(\mathbf{F}_q;\, m_{(l)},\, n_{(l)}).$$

Thus, for every element $[E]_{\mathbf{F}_q}$ of $V(\mathbf{F}_q; N)$ there is a unique divisor d of $u(N)$ with $[E]_{\mathbf{F}_q} \in W(\mathbf{F}_q; d, N/\gcd(d, t(N)))$, and we are done. $\square$

LEMMA 4.2. *For every pair* (m, n) *of positive integers with* m *dividing* $\gcd(n, q-1)$, *we have*

$$y(m,\, n) = m\varphi(n)\psi(n) \sum_{d:m|d|\gcd(n,q-1)} \frac{w(d,\, n)}{\psi(n/d)}. \tag{17}$$

Proof. Consider the map from $Y(\mathbf{F}_q/\mathbf{F}_q; \zeta_m, m, n)$ to $\coprod_{d:m|d|\gcd(n,q-1)} W(\mathbf{F}_q; d, n)$ that takes $[E, P, Q]_{\mathbf{F}_q}$ to $[E]_{\mathbf{F}_q}$. This map is clearly surjective.

Consider an elliptic curve E over $\mathbf{F}_q$ with $[E]_{\mathbf{F}_q} \in W(\mathbf{F}_q; d, n)$ for some d with $m|d|\gcd(n, q-1)$. It is not difficult to check that there are exactly $m\varphi(n)\psi(n)/\psi(n/d)$ ways of choosing a pair (P, Q) of points of $E(\mathbf{F}_q)$ with $\operatorname{ord} P = m$, $\operatorname{ord} Q = n$, and $e_m(P, (n/m)Q) = \zeta_m$. Two such pairs (P, Q) and (P', Q') satisfy $(E, P, Q) \cong_{\mathbf{F}_q} (E, P', Q')$ if and only if (P', Q') lies in the $\operatorname{Aut}_{\mathbf{F}_q}(E)$-orbit of (P, Q), and the size of this orbit is the index $[\operatorname{Aut}_{\mathbf{F}_q}(E) : \operatorname{Aut}_{\mathbf{F}_q}(E, P, Q)] = \# \operatorname{Aut}_{\mathbf{F}_q}(E) / \# \operatorname{Aut}_{\mathbf{F}_q}(E, P, Q)$. Summing over the various $\operatorname{Aut}_{\mathbf{F}_q}(E)$-orbits of such pairs, we obtain

$$\sum_{(P,Q)} \frac{\# \operatorname{Aut}_{\mathbf{F}_q}(E)}{\# \operatorname{Aut}_{\mathbf{F}_q}(E,\, P,\, Q)} = \frac{m\varphi(n)\psi(n)}{\psi(n/d)}.$$

Dividing by $\# \operatorname{Aut}_{\mathbf{F}_q}(E)$ and summing over $\mathbf{F}_q$-isomorphism classes of E we obtain

$$\sum_{[E,P,Q]_{\mathbf{F}_q} \in Y(\mathbf{F}_q/\mathbf{F}_q;\zeta_m,m,n)} \frac{1}{\# \operatorname{Aut}_{\mathbf{F}_q}(E,\, P,\, Q)} = \sum_{d:m|d|\gcd(n,q-1)} \frac{m\varphi(n)\psi(n)}{\psi(n/d)} \,\#' W(\mathbf{F}_q;\, d,\, n).$$

But the sum on the left-hand side is

$$\sum_{[E',P',Q']_{\bar{\mathbf{F}}_q} \in Y(\bar{\mathbf{F}}_q/\mathbf{F}_q;\zeta_m,m,n)} \; \sum_{[E,P,Q]_{\mathbf{F}_q} \in \mathbf{E}(E',P',Q')} \frac{1}{\# \operatorname{Aut}_{\mathbf{F}_q}(E,\, P,\, Q)}$$

and by Proposition 2.3 this double sum is the cardinality of $Y(\bar{\mathbf{F}}_q/\mathbf{F}_q; \zeta_m, m, n)$. This gives us (17). $\square$

LEMMA 4.3. *For every pair* (m, n) of positive integers with m dividing $\gcd(n, q-1)$, *we have*

$$w(m, n) = \frac{\psi(n/m)}{m\varphi(n)\psi(n)} \sum_{j|(\gcd(n,q-1)/m)} \frac{\mu(j)}{j} y(mj, n). \tag{18}$$

Proof. We calculate:

$$\begin{aligned}\frac{w(m, n)}{\psi(n/m)} &= \sum_{d:m|d|\gcd(n,q-1)} \frac{w(d, n)}{\psi(n/d)} \sum_{j|(d/m)} \mu(j)\\ &= \sum_{j|\gcd(n,q-1)/m} \mu(j) \sum_{d:mj|d|\gcd(n,q-1)} \frac{w(d, n)}{\psi(n/d)} = \sum_{j|(\gcd(n,q-1)/m)} \mu(j) \frac{y(mj, n)}{mj\varphi(n)\psi(n)}\end{aligned}$$

where the last equality follows from (17). Multiplying by $\psi(n/m)$ we get (18). □

Now we use the approximation that Corollary 3.4 gives us for $y(m, n)$ to define approximations for $w(m, n)$ and $v(N)$; namely, for all pairs (m, n) of positive integers with m dividing $\gcd(n, q-1)$, we define

$$\hat{w}(m, n) = \frac{q\psi(n/m)}{m\varphi(n)\psi(n)} \sum_{j|(\gcd(n,q-1)/m)} \frac{\mu(j)}{j} = \frac{q\psi(n/m)}{m\varphi(n)\psi(n)} \prod_{l|(\gcd(n,q-1)/m)} \left(1 - \frac{1}{l}\right)$$

and for all positive integers N we define

$$\hat{v}(N) = \sum_{d|\gcd(u(N),q-1)} \hat{w}\left(d, \frac{N}{\gcd(d, t(N))}\right).$$

We see from Lemma 4.3 and Corollary 3.4 that

$$\begin{aligned}|w(m, n) - \hat{w}(m, n)| &\leqslant \frac{\psi(n/m)}{m\varphi(n)\psi(n)} \sum_{j|(\gcd(n,q-1)/m)} \frac{|\mu(j)|}{j} C' mj\varphi(n)\psi(n)\sqrt{q}\\ &\leqslant C'\psi(n/m)\sqrt{q} \sum_{j|(\gcd(n,q-1)/m)} |\mu(j)| \leqslant C'\psi(n/m)2^{\nu(n)}\sqrt{q},\end{aligned}$$

where $\nu(n)$ denotes the number of prime divisors of n. From this error estimate and from Lemma 4.1, we find that

$$\begin{aligned}|v(N) - \hat{v}(N)| &\leqslant \sum_{d|\gcd(u(N),q-1)} C'\psi(N/d)2^{\nu(N)}\sqrt{q} \leqslant C'\psi(N)2^{\nu(N)}\sqrt{q} \sum_{d|N} 1/d\\ &< C'\psi(N)2^{\nu(N)}\sqrt{q} \prod_{l|N} \frac{1}{1-1/l} = C'N\rho(N)2^{\nu(N)}\sqrt{q}.\end{aligned} \tag{19}$$

To calculate $\hat{w}(m, n)$ and $\hat{v}(N)$, we note that the definition of $\hat{w}(m, n)$ shows that the ratio $\hat{w}(m, n)/q$ is multiplicative; that is,

$$\frac{\hat{w}(m, n)}{q} = \prod_l \frac{\hat{w}(m_{(l)}, n_{(l)})}{q}.$$

This equality, together with the definition of $\hat{v}(N)$, shows that $\hat{v}(N)/q$ is a multiplicative function of N. A straightforward (if tedious) verification shows that for prime powers l^a we have

$$\frac{\hat{v}(l^a)}{q} = \begin{cases} \dfrac{1}{l^{a-1}(l-1)} & \text{if } q \not\equiv 1 \bmod l^c; \\ \dfrac{l^{b+1}+l^b-1}{l^{a+b-1}(l^2-1)} & \text{if } q \equiv 1 \bmod l^c, \end{cases} \tag{20}$$

where $b = \lfloor a/2 \rfloor$ and $c = \lceil a/2 \rceil$.

Inequality (19) and equation (20) shows that Theorem 1.1 will be true if we take C to be C' and $r(N)$ to be the ratio $\hat{v}(N)/q$. □

Acknowledgements

The author was supported by a United States Department of Education National Need Fellowship. The author would like to thank Hendrik Lenstra for suggesting the proof of Proposition 2.1, and Bas Edixhoven and Hendrik Lenstra for providing helpful comments and advice.

References

[1] Enrico Bombieri: Counting points on curves over finite fields (d'après S. A. Stepanov), *Séminaire Bourbaki* 430 (1972/73), pp. 234–241 in Lecture Notes in Mathematics 383, Springer-Verlag, New York, 1974.

[2] P. Deligne and M. Rapoport: Les schémas de modules des courbes elliptiques, pp. 143–316 in *Modular Functions of One Variable II*, Lecture Notes in Mathematics 349, Springer-Verlag, New York, 1973.

[3] Robin Hartshorne: *Algebraic Geometry*, Graduate Texts in Mathematics 52, Springer-Verlag, New York, 1977.

[4] Nicholas M. Katz and Barry Mazur: *Arithmetic Moduli of Elliptic Curves*, Annals of Mathematics Studies 108, Princeton University Press, Princeton, New Jersey, 1985.

[5] Serge Lang: *Algebra*, Addison-Wesley Publishing Company, Menlo Park, California, 1984.

[6] H. W. Lenstra, Jr.: Factoring integers with elliptic curves, *Ann. of Math.* 126 (1987) 649–673.

[7] Jean-Pierre Serre: *Algebraic Groups and Class Fields*, Graduate Texts in Mathematics 117, Springer-Verlag, New York, 1988.

[8] Jean-Pierre Serre: *Cohomologie Galoisienne*, Lecture Notes in Mathematics 5, Springer-Verlag, New York, 1964.

[9] Joseph H. Silverman: *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer-Verlag, New York, 1986.

[10] André Weil: The field of definition of a variety, *Amer. J. of Math.* 78 (1956) 509–524.

[11] André Weil: *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*, Hermann, Paris, 1948.