ACTA ARITHMETICA
106.3 (2003)

Distribution of the traces of Frobenius on elliptic curves over function fields

by

Amílcar Pacheco (Rio de Janeiro)

Introduction. Let C be a smooth irreducible projective curve defined over a finite field $\mathbb{F}_q$ of q elements of characteristic $p > 3$ and $K = \mathbb{F}_q(C)$ its function field. Let E/K be a non-constant elliptic curve and $\varphi_{\mathcal{E}} : \mathcal{E} \to C$ its minimal regular model. For each $P \in C$ define $\mathcal{E}_P = \varphi_{\mathcal{E}}^{-1}(P)$. The elliptic curve E/K has good reduction at $P \in C$ if and only if $\mathcal{E}_P$ is an elliptic curve defined over the residue field κ_P of P. This field is a finite extension of $\mathbb{F}_q$ of degree $\deg(P)$. Let $t(\mathcal{E}_P) = q^{\deg(P)} + 1 - \#\mathcal{E}_P(\kappa_P)$ be the trace of Frobenius at P. By Hasse–Weil's theorem (cf. [10, Chapter V, Theorem 2.4]), $t(\mathcal{E}_P)$ is the sum of the inverses of the zeros of the zeta function of $\mathcal{E}_P$. In particular, $|t(\mathcal{E}_P)| \le 2q^{\deg(P)}$. Let $C_0 \subset C$ be the set of points of C at which E/K has good reduction and $C_0(\mathbb{F}_{q^k})$ the subset of $\mathbb{F}_{q^k}$-rational points of C_0.

Question 1. *Let $B \ge 1$ and t be integers and suppose $|t| \le 2q^{B/2}$. How large is $\pi(B,t) = \#\{P \in C_0 \mid \deg(P) \le B$ and $t(\mathcal{E}_P) = t\}$?*

A similar question was originally posed by Lang and Trotter [5] for elliptic curves over $\mathbb{Q}$ and later extended to elliptic curves over number fields [6].

For each $k \le B$ such that $|t| \le 2q^{k/2}$ we start by estimating $\pi(k,t)' = \#\{P \in C_0 \mid \deg(P) = k$ and $t(\mathcal{E}_P) = t\}$. Let $\mathcal{E}'_P = \mathcal{E}_P \times_{\kappa_P} \mathbb{F}_{q^k}$ and $\pi(k,t)'' = \#\{P \in C_0(\mathbb{F}_{q^k}) \mid t(\mathcal{E}'_P) = t\}$. The former set is contained in the latter so $\pi(k,t)' \le \pi(k,t)''$ and throughout all this paper we actually estimate $\pi(k,t)''$.

1. Preliminaries. Observe first that E/K has to be an ordinary elliptic curve, otherwise $j(E) \in \mathbb{F}_{p^2}$ (cf. [10, Chapter V, Theorem 3.1]), but this contradicts the fact that E/K is non-constant.

Let $j_{\mathcal{E}} : C \to \mathbb{P}^1$ be the j-map induced from $\varphi_{\mathcal{E}}$. We say that $P \in C_0$ is *good ordinary*, respectively *good supersingular*, if $\mathcal{E}_P$ is an ordinary,

2000 *Mathematics Subject Classification*: Primary 11G05.

This work was partially supported by CNPq research grant 300896/91-3 and Pronex #41.96.0830.00.

respectively supersingular, elliptic curve. Since the number of supersingular j-invariants in $\overline{\mathbb{F}}_q$ is finite (cf. [10, Chapter V, Theorem 4.1]), the number of good supersingular points $P \in C_0$ is also finite and bounded by an absolute constant. This does not hold for elliptic curves over $\mathbb{Q}$ (cf. [2]).

So, we will only concentrate on good ordinary $P \in C_0$. Let $C_0' = \{P \in C_0 \mid P \text{ is ordinary}\}$. Let $E/\mathbb{F}_q$ be an elliptic curve and $t(E) = q + 1 - \#E(\mathbb{F}_q)$. Then E is supersingular if and only if $p \nmid t(E)$ (cf. [10, Ex. 5.10]). Till the end of this note we assume $p \nmid t$.

2. Estimate of $\pi(k,t)''$

Notation 2.1. Let $I(t)$ be the set of the isogeny classes of elliptic curves $E/\mathbb{F}_{q^k}$ defined over $\mathbb{F}_{q^k}$ such that $\#E(\mathbb{F}_{q^k}) = q^k + 1 - t$. Let $\mathfrak{A}_{k,t}$ be the set of $\mathbb{F}_{q^k}$-isomorphism classes $[E]$ of $E \in I(t)$ and $N(t) = \#\mathfrak{A}_{k,t}$.

Definition 2.2. Let $\Delta < 0$ be an integer such that $\Delta \equiv 0$ or $1 \pmod 4$, $B(\Delta) = \{\alpha x^2 + \beta xy + \gamma y^2 \mid \alpha, \beta, \gamma \in \mathbb{Z},\ \alpha > 0 \text{ and } \beta^2 - 4\alpha\gamma = \Delta\}$ and $b(\Delta) = \{\alpha x^2 + \beta xy + \gamma y^2 \in B(\Delta) \mid \gcd(\alpha, \beta, \gamma) = 1\}$. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on $B(\Delta)$ via $\left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right) f(x,y) = f(\alpha x + \beta y, \gamma x + \delta y)$ preserving $b(\Delta)$. The sets $b(\Delta)/\mathrm{SL}_2(\mathbb{Z})$ and $B(\Delta)/\mathrm{SL}_2(\mathbb{Z})$ are finite with cardinality $h(\Delta)$ and $H(\Delta)$, respectively. The numbers $h(\Delta)$ and $H(\Delta)$ are called the *class number* and the *Kronecker class number* of Δ, respectively.

Proposition 2.3 [8, Proposition 2.2]. *Let $\Delta < 0$ be an integer such that $\Delta \equiv 0$ or $1 \pmod 4$. Then*

$$H(\Delta) = \sum_f h(\Delta/f^2), \tag{2.1}$$

where f runs through all positive divisors of Δ such that $\Delta/f^2 \in \mathbb{Z}$ and $\Delta/f^2 \equiv 0$ or $1 \pmod 4$.

Remark 2.4. Let $\mathcal{O}$ be an imaginary quadratic order with discriminant $\Delta(\mathcal{O})$ and $h_{\mathcal{O}}$ its class number. It follows from the correspondence between binary quadratic forms and complex quadratic orders that $h_{\mathcal{O}} = h(\Delta(\mathcal{O}))$, where $\Delta(\mathcal{O})$ denotes the discriminant of $\mathcal{O}$ [1, Chap. 2, Section 7, Theorem 4].

Proposition 2.5 [8, Theorem 4.5]. *Let $E \in I(t)$ and $\mathcal{O} = \mathrm{End}_{\mathbb{F}_{q^k}}(E)$. Then $\#\{[E'] \in \mathfrak{A}_{k,t} \mid \mathcal{O} = \mathrm{End}_{\mathbb{F}_q}(E')\} = h_{\mathcal{O}}$.*

Notation 2.6. Denote by $\mathcal{O}(t^2 - 4q^k)$ the imaginary quadratic order of discriminant $t^2 - 4q^k$.

Corollary 2.7 [8, Theorem 4.6]. $N(t) = H(t^2 - 4q^k)$.

Proof. By [8, Theorem 4.3], since $p \nmid t$, all imaginary quadratic orders $\mathcal{O} \supset \mathcal{O}(t^2 - 4q^k)$ occur as $\mathbb{F}_{q^k}$-endomorphism rings of elliptic curves in $I(t)$. Hence, the result follows from Propositions 2.3 and 2.5 and Remark 2.4. ∎

THEOREM 2.8. *$\pi(k,t)'' \le \deg(j_{\mathcal{E}})H(t^2 - 4q^k)$.*

Proof. Let $C_0'(\mathbb{F}_{q^k})$ be the set of $\mathbb{F}_{q^k}$-rational points of C_0' and $\mathcal{C}_{k,t} = \{P \in C_0'(\mathbb{F}_{q^k}) \mid t(\mathcal{E}_P') = t\}$, where $\mathcal{E}_P' = \mathcal{E}_P \times_{\kappa_P} \mathbb{F}_{q^k}$. Define $\psi : \mathcal{C}_{k,t} \to \mathfrak{A}_{k,t}$ by $\psi(P) = [\mathcal{E}_P']$ and let $j(\mathcal{E}_P)$ be the j-invariant of $\mathcal{E}_P$.

We claim that $\psi^{-1}([\mathcal{E}_P']) \subset j_{\mathcal{E}}^{-1}(j(\mathcal{E}_P))$. In fact, if $Q \in \psi^{-1}([\mathcal{E}_P'])$, then there exists an $\mathbb{F}_{q^k}$-isomorphism between $\mathcal{E}_Q'$ and $\mathcal{E}_P'$, in particular $j(\mathcal{E}_Q) = j(\mathcal{E}_P)$. Hence, $\#\psi^{-1}([\mathcal{E}_P']) \le \# j_{\mathcal{E}}^{-1}(j(\mathcal{E}_P)) \le \deg(j_{\mathcal{E}})$ and

$$\begin{aligned}\text{(2.2)} \qquad \pi(k,t)'' = \sum_{[E]\in\psi(\mathcal{C}_{k,t})} \#\psi^{-1}([E]) &\le \deg(j_{\mathcal{E}})\#\psi(\mathcal{C}_{k,t}) \\ &\le \deg(j_{\mathcal{E}})H(t^2 - 4q^k). \ ∎\end{aligned}$$

COROLLARY 2.9.

$$\pi(B,t) \le \Big(\sum_{\substack{k\le B \\ |t|\le 2q^k}} H(t^2 - 4q^k)\Big)\deg(j_{\mathcal{E}}).$$

REMARK 2.10. We would like to compute examples in which we could test whether the bound of Theorem 2.8 is achieved. One good sort of example comes from modular curves. However, in this case there is almost no control on $j_{\mathcal{E}}$ in contrast to the j-map J naturally associated to the modular problems. Moreover, if we observe the proof of Theorem 2.8 closely, we notice that we can replace the regular minimal model by any elliptic surface $\varphi_{\widetilde{\mathcal{E}}} : \widetilde{\mathcal{E}} \to C$ having E/K as the generic fiber, defining the notions of good ordinary (good supersingular) points in terms of the fibers of $\widetilde{\mathcal{E}} \to C$ being smooth ordinary (supersingular) elliptic curves. In this set-up it makes sense to consider the trace of Frobenius of the fibers of good ordinary points. We can also consider elliptic curves $\mathbb{E} \to C_1$ in the sense of [4, Chapter 2] defined over an affine subcurve $C_1 \subset C$ with generic fiber E/K and compute the number (still denoted by $\pi(k,t)''$) of $\mathbb{F}_{q^k}$-rational points $P \in C_1$ corresponding to good ordinary fibers $\mathbb{E}_P$ such that $t(\mathbb{E}_P') = t$. The elliptic curve comes equipped with a j-map $J : C \to \mathbb{P}^1$ and we look for conditions for $\pi(k,t)''$ to be equal to $\deg_{\mathrm{s}}(J)H(t^2 - 4q^k)$, where $\deg_{\mathrm{s}}(J)$ denotes the *separable degree* of J.

3. Affine models. Let X be a smooth irreducible projective curve over $\mathbb{F}_q$ and $Y \subset X$ an affine subcurve. Suppose there exists an elliptic curve $\mathbb{E} \to Y$ with generic fiber E/K and a map $J : X \to \mathbb{P}^1$ whose restriction to Y is given by $y \mapsto j(\mathbb{E}_y)$, where $\mathbb{E}_y$ denotes the fiber of $\mathbb{E} \to Y$ at y. Let

$Y' = \{y \in Y \mid \mathbb{E}_y \text{ is ordinary}\}$. Denote by $Y'(\mathbb{F}_{q^k})$ the subset of $\mathbb{F}_{q^k}$-rational points. Given $y \in Y'(\mathbb{F}_{q^k})$, let κ_y be its residue field and $\mathbb{E}'_y = \mathbb{E}_y \times_{\kappa_y} \mathbb{F}_{q^k}$. Let $\mathcal{Y}_{k,t} = \{y \in Y'(\mathbb{F}_{q^k}) \mid t(\mathbb{E}'_y) = t\}$ and $\pi(k,t)'' = \#\mathcal{Y}_{k,t}$. Let $\vartheta : \mathcal{Y}_{k,t} \to \mathfrak{A}_{k,t}$ be the map defined by $y \mapsto [\mathbb{E}'_y]$.

Proposition 3.1. *Suppose the following three conditions are satisfied*:

(1) $\vartheta^{-1}([\mathbb{E}'_y]) = J^{-1}(j(\mathbb{E}_y))$.

(2) ϑ *is surjective.*

(3) *For every* $y \in Y$, *the inertia degree* $f(y \mid j(\mathbb{E}_y))$ *equals* 1. *The set* $\mathcal{R} \subset Y$ *of possible ramification points of* J *is contained in* $J^{-1}(\{0, 1728\})$. *For each* $y \in \mathcal{R}$ *the ramification index* $e(y \mid 0)$ (*respectively* $e(y \mid 1728)$) *of* P *over* 0, *respectively* 1728, *equals* 3, *respectively* 2.

Then $\pi(k,t)'' = \deg_s(J) H(t^2 - 4q^k)$, *where* $\deg_s(J)$ *denotes the separable degree of* J.

Proof. In the definition of $H(\Delta)$, we count the forms $\alpha x^2 + \alpha y^2$, respectively $\alpha x^2 + \alpha xy + \alpha y^2$, in $B(\Delta)$, if they occur, with multiplicity $1/2$, respectively $1/3$. Then we need to replace $h(\Delta)$ in Proposition 2.3 by $h_w(\Delta)$, where $h_w(-3) = 1/3$, $h_w(-4) = 1/2$, and $h_w(\Delta) = h(\Delta)$ for $\Delta < -4$. The equality (2.1) does not change when reinterpreted with these multiplicities [9, Proposition 2.1]. Hence, by Propositions 2.3 and 2.5 and Remark 2.4 (cf. (2.2)),

$$\begin{aligned}\pi(k,t)'' = \sum_{[E] \in \mathfrak{A}_{k,t}} \#J^{-1}(j(E)) &= \deg_s(J) \sum_{\mathcal{O}(t^2 - 4q^k) \subset \mathcal{O}} h_w(\Delta(\mathcal{O})) \\ &= \deg_s(J) H(t^2 - 4q^k). \ \blacksquare\end{aligned}$$

4. Universal elliptic curves

4.1. *Igusa curves.* Let E be an elliptic curve defined over a field L of characteristic p. The absolute Frobenius F_{abs} induces an isogeny $F_{\mathrm{abs}} : E \to E^{(p)}$, where $E^{(p)}$ denotes the elliptic curve obtained by raising the coefficients of a Weierstrass equation of E to the pth power. For each $n \geq 1$, let $F^n_{\mathrm{abs}} : E \to E^{(p^n)}$ be the nth iterate of F_{abs}. Let V^n be the dual isogeny of the nth iterate F^n_{abs} of F_{abs}. An *Igusa structure of level* p^n in E is a generator of $\ker(V^n)$.

There exists a smooth affine curve Y_n over $\mathbb{F}_p$ parametrizing isomorphism classes of pairs (E, P), where E is an elliptic curve defined over an $\mathbb{F}_p$-scheme S and $P \in E^{(p^n)}(S)$ is an Igusa structure of level p^n. In fact, Y_n is a coarse moduli scheme for the moduli problem $[\mathrm{Ig}(p^n)] : E/S/\mathbb{F}_p \mapsto P$. The compactification X_n of Y_n obtained by adding $\phi(p^n)/2$ points at infinity (called the *cusps*) is a smooth projective irreducible curve over $\mathbb{F}_p$ called the *Igusa curve of level* p^n [4, Chapter 12], where ϕ denotes the Euler function.

An elliptic curve $E/S/\mathbb{F}_p$ is *ordinary* if each of its geometric fibers is ordinary. An *Igusa ordinary* (respectively *Igusa supersingular*) point $y \in Y_n$ is a point representing the isomorphism of a pair (E, P), where $E/S/\mathbb{F}_p$ is an ordinary elliptic curve, S an $\mathbb{F}_p$-scheme (respectively E/L is a supersingular elliptic curve, L a field of characteristic p) and $P \in E^{(p^n)}(S)$ (respectively $P \in E^{(p^n)}(L)$) is an Igusa structure of level p^n in E.

The group $(\mathbb{Z}/p^n\mathbb{Z})^*$ acts on Y_n by $a \mapsto (E, aP)$ and the group $\{\pm 1\}$ acts trivially. These actions are extended to X_n by permuting the cusps simply transitively. Let $y \in Y_n$ represent the isomorphism class of a pair (E, P). If y is Igusa supersingular, then y is fixed by $(\mathbb{Z}/p^n\mathbb{Z})^*$. If y is Igusa ordinary and $j(E) = 1728$, respectively $j(E) = 0$, then y has a stabilizer of order 2, respectively 3, in $(\mathbb{Z}/p^n\mathbb{Z})^*/\{\pm 1\}$. On all other points of Y_n, $(\mathbb{Z}/p^n\mathbb{Z})^*/\{\pm 1\}$ acts freely. We identify the quotient of X_n by $(\mathbb{Z}/p^n\mathbb{Z})^*/\{\pm 1\}$ to the projective line $\mathbb{P}^1$ and the quotient map $J_n : X_n \to \mathbb{P}^1$ is Galois of degree $\phi(p^n)/2$. Its restriction to Y_n is given by $(E, P) \mapsto j(E)$.

The curve Y_n^{ord} obtained from Y_n by removing the Igusa supersingular points is a fine moduli space for the restriction of $[\mathrm{Ig}(p^n)]$ to ordinary elliptic curves. This means that there exists a universal elliptic curve $\mathbb{E}_n \to Y_n^{\mathrm{ord}}$ such that every ordinary elliptic curve $E/S/\mathbb{F}_p$ with an Igusa structure $P \in E^{(p^n)}(S)$ of level p^n is obtained from $\mathbb{E}_n \to Y_n^{\mathrm{ord}}$ by a unique base extension. In particular, if K_n is the function field of X_n over $\mathbb{F}_p$ and E_n/K_n is the generic fiber of $\mathbb{E}_n \to Y_n^{\mathrm{ord}}$, then E_n/K_n is the unique elliptic curve defined over K_n with j-invariant $j(E_n)$ and a K_n-rational Igusa structure of level p^n.

If $E \in I(t)$ and $P \in E^{(p^n)}(\mathbb{F}_{p^k})$ is an Igusa structure of level p^n, then since E and $E^{(p^n)}$ are isogenous, we have $t \equiv p^k + 1 \pmod{p^n}$. So for the rest of this subsection, we assume $t \equiv p^k + 1 \pmod{p^n}$.

Proposition 4.1. *Conditions* (1)–(3) *of Proposition* 3.1 *are satisfied, a fortiori* $\pi(k,t)'' = (\phi(p^n)/2)H(t^2 - 4p^k)$.

Proof. In the notation of Section 3, $Y = Y_n^{\mathrm{ord}}$. Let $y \in \mathcal{Y}_{k,t}$, denote by $\mathbb{E}_{n,y}/\kappa_y$ the fiber of $\mathbb{E}_n \to Y_n^{\mathrm{ord}}$ at y and $\mathbb{E}'_{n,y} = \mathbb{E}_{n,y} \times_{\kappa_y} \mathbb{F}_{p^k}$.

(1) Let $x \in \vartheta^{-1}([\mathbb{E}'_{n,y}])$; then $\mathbb{E}'_{n,x}$ is $\mathbb{F}_{p^k}$-isomorphic to $\mathbb{E}'_{n,y}$, in particular $j(\mathbb{E}_{n,x}) = j(\mathbb{E}_{n,y})$, i.e., $x \in J_n^{-1}(j(\mathbb{E}_{n,y}))$. Let $x \in J_n^{-1}(j(\mathbb{E}_{n,y}))$, then x represents the isomorphism class of the pair $(\mathbb{E}_{n,y}, P_y)$, where $P_y \in \mathbb{E}_{n,y}^{(p^n)}(\kappa_y)$ is an Igusa structure of level p^n. By the geometric description of J_n, there is no inertia at Y_n^{ord}, hence $\kappa_x = \kappa_y$. Furthermore, $\mathbb{E}_{n,y}$ is an elliptic curve over $\kappa_y = \kappa_x$ with j-invariant equal to $j(\mathbb{E}_{n,y}) = j(\mathbb{E}_{n,x})$ having a κ_y-rational Igusa structure. It follows from the universal property of $\mathbb{E}_n \to Y_n^{\mathrm{ord}}$ that $\mathbb{E}_{n,y} = \mathbb{E}_{n,x}$, a fortiori $[\mathbb{E}'_{n,x}] = [\mathbb{E}'_{n,y}]$ and $x \in \vartheta^{-1}([\mathbb{E}'_{n,y}])$.

(2) For every $[E] \in \mathfrak{A}_{k,t}$, $\#E(\mathbb{F}_{p^k}) = \#E^{(p^n)}(\mathbb{F}_{p^k}) \equiv 0 \pmod{p^n}$. Thus, there exists an Igusa $P \in E^{(p^n)}(\mathbb{F}_{p^k})$ structure of level p^n. Let $y \in Y_n^{\mathrm{ord}}(\mathbb{F}_{p^k})$

represent the isomorphism class of the pair (E, P). But $\mathbb{E}_{n,y}$ is the unique elliptic curve over κ_y with j-invariant $j(\mathbb{E}_{n,y}) = j(E)$ having a κ_y-rational Igusa structure of level p^n. Thus, $\mathbb{E}'_{n,y} = E$. In particular, $[\mathbb{E}'_{n,y}] = [E]$ and ϑ is surjective.

Condition (3) follows from the geometric description of J_n. Consequently,

$$\pi(k,t)'' = \frac{\phi(p^n)}{2} \sum_{\mathcal{O}(t^2-4p^k)\subset\mathcal{O}} h_w(\Delta(\mathcal{O})) = \frac{\phi(p^n)}{2} H(t^2-4p^k). \ ■$$

Remark 4.2. Proposition 4.1 was implicitly used in [7, Corollary 2.13] to obtain an explicit expression for $\#X_n(\mathbb{F}_{p^k})$.

4.2. *The modular curve* $X(N)$. Let $N > 2$ be an integer not divisible by p. Let $\zeta \in \overline{\mathbb{F}}_p$ be a primitive Nth root of unity and $\mathbb{F}_q = \mathbb{F}_p(\zeta)$. Let $Y(N)$ be the affine smooth curve defined over $\mathbb{F}_q$ parametrizing isomorphism classes of triples (E, P, Q), where E is an elliptic curve defined over an $\mathbb{F}_q$-scheme S and $P, Q \in E[N](S)$ is a Drinfeld basis for $E[N](S)$ and $e_N(P,Q) = \zeta$ [4, 3.1], where e_N denotes the Nth Weil pairing (cf. [4, 2.8] and [10, III, §8]). In fact, it is a fine moduli space for the modular problem $[\Gamma(N)] : E/S/\mathbb{F}_q \mapsto (P,Q)$ such that $e_N(P,Q) = \zeta$. The compactification $X(N)$ of $Y(N)$ obtained by adding the cusps is a smooth projective irreducible curve defined over $\mathbb{F}_q$ [4, Theorem 3.7.1].

The group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts on $Y(N)$ by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(E,P,Q) \mapsto (E, aP + bQ, cP + dQ)$ and the group $\{\pm 1\}$ acts trivially. If $y \in Y(N)$ represents the isomorphism class of a triple (E,P,Q), then y has a stabilizer of order 3, respectively 2, if $j(E) = 0$, respectively $j(E) = 1728$. On all other points of $Y(N)$, $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ acts freely. The stabilizer at every cusp has order N [3, Theorem 6]. So we identify the quotient of $X(N)$ by $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm 1\}$ to the projective line $\mathbb{P}^1$. Let $\mathbb{E}(N) \to Y(N)$ be the universal elliptic curve of $Y(N)$ and $E(N)/K(N)$ its generic fiber. The quotient map $J(N) : X(N) \to \mathbb{P}^1$ is Galois of degree $(1/2)N\phi(N)\psi(N)$ and its restriction to $Y(N)$ is given by $(E,P,Q) \mapsto j(E)$, where $\psi(N) = N\prod_{l|N}(1 + 1/l)$ and l runs over the divisors of N.

Denote by $\mathcal{O}((t^2 - 4q^k)/N^2)$ the imaginary quadratic order of discriminant $(t^2 - q^k)/N^2$. Let $E \in I(t)$; we have $E[N] \subset E(\mathbb{F}_{q^k})$ if and only if $t \equiv q^k + 1 \pmod{N^2}$, $q^k \equiv 1 \pmod{N}$ and $\mathcal{O}((t^2 - 4q^k)/N^2) \subset \mathrm{End}_{\mathbb{F}_{q^k}}(E)$ [8, Proposition 3.7]. Assume till the end of this subsection that $t \equiv q^k + 1 \pmod{N^2}$ and $q^k \equiv 1 \pmod{N}$. Let $\mathfrak{A}'_{k,t} = \{[E] \in \mathfrak{A}_{k,t} \mid \mathcal{O}((t^2 - 4q^k)/N^2) \subset \mathrm{End}_{\mathbb{F}_{p^k}}(E)\}$. By [8, Theorem 4.9], $\#\mathfrak{A}'_{k,t} = H((t^2 - 4q^k)/N^2)$. Note that $H((t^2 - 4q^k)/N^2) < H(t^2 - 4q^k)$.

Proposition 4.3. *Conditions* (1) *and* (3) *of Proposition* 3.1 *are satisfied. However*, $\pi(k,t)'' = (1/2)N\phi(N)\psi(N)H((t^2 - 4q^k)/N^2)$.

Proof. In the notation of Section 3, $Y = Y(N)$. Let $y \in \mathcal{Y}_{k,t}$, denote by $\mathbb{E}(N)_y/\kappa_y$ the fiber of $\mathbb{E}(N) \to Y(N)$ at y and $\mathbb{E}(N)'_y = \mathbb{E}(N)_y \times_{\kappa_y} \mathbb{F}_{q^k}$.

(1) Let $x \in \vartheta^{-1}([\mathbb{E}(N)'_y])$; then $\mathbb{E}(N)'_x$ is $\mathbb{F}_{q^k}$-isomorphic to $\mathbb{E}(N)'_y$, in particular $j(\mathbb{E}(N)_x) = j(\mathbb{E}(N)_y)$, i.e., $x \in J(N)^{-1}(j(\mathbb{E}(N)_y))$. Let $x \in J(N)^{-1}(j(\mathbb{E}(N)_y))$; then x represents the isomorphism class of the triple $(\mathbb{E}(N)_y, P_y, Q_y)$, where P_y, Q_y is a basis for $\mathbb{E}(N)_y(\kappa_y)$ with $e_N(P, Q) = \zeta$. By the geometric description of $J(N)$, there is no inertia, hence $\kappa_x = \kappa_y$. Furthermore, $\mathbb{E}(N)_y$ is an elliptic curve over $\kappa_y = \kappa_x$ with j-invariant $j(\mathbb{E}(N)_y) = j(\mathbb{E}(N)_x)$ and a κ_y-rational basis P_y, Q_y of $\mathbb{E}(N)_y[N]$ such that $e_N(P, Q) = \zeta$. By the universal property of $\mathbb{E}(N) \to Y(N)$, $\mathbb{E}(N)_x = \mathbb{E}(N)_y$, a fortiori $[\mathbb{E}(N)'_x] = [\mathbb{E}(N)'_y]$ and $x \in \vartheta^{-1}([\mathbb{E}(N)'_y])$.

(2) For every $E \in \mathfrak{A}'_{k,t}$, by hypothesis $\mathcal{O}((t^2 - 4q^k)/N^2) \subset \mathrm{End}_{\mathbb{F}_{q^k}}(E)$, hence $E[N] \subset E(\mathbb{F}_{q^k})$, in particular there exists a basis P, Q for $E[N](\mathbb{F}_{q^k})$ such that $e_N(P, Q) = \zeta$. Let $y \in Y(N)(\mathbb{F}_{q^k})$ represent the isomorphism class of the triple (E, P, Q) satisfying $e_N(P, Q) = \zeta$. But $\mathbb{E}(N)_y$ is the unique elliptic curve defined over κ_y with κ_y-rational basis (P_y, Q_y) of $\mathbb{E}(N)_y[N]$ satisfying $e_N(P_y, Q_y) = \zeta$. Thus $\mathbb{E}(N)'_y = E$. In particular, $[\mathbb{E}(N)'_y] = [E]$ and ϑ is onto $\mathfrak{A}'_{k,t}$.

Condition (3) follows from the geometric description of $J(N)$. Therefore,

$$\begin{aligned}\pi(k,t)'' &= \frac{1}{2} N\phi(N)\psi(N) \sum_{\mathcal{O}((t^2-4q^k)/N^2)\subset\mathcal{O}} h_w(\Delta(\mathcal{O})) \\ &= \frac{1}{2} N\phi(N)\psi(N) H\biggl(\frac{t^2 - 4q^k}{N^2}\biggr). \ \blacksquare\end{aligned}$$

4.3. *The modular curve* $X_1(N)$. Let $N > 4$ be an integer not divisible by 2, 3 and p. Let $Y_1(N)$ be the smooth affine curve defined over $\mathbb{F}_p$ parametrizing isomorphism classes of pairs (E, P), where E is an elliptic curve defined over an $\mathbb{F}_p$-scheme S and $P \in E(S)$ is a point of exact order N [4, Chapter 3]. In fact, it is a fine moduli space for the moduli problem $[\Gamma_1(N)]$ defined by $(E/S/\mathbb{F}_p, P) \mapsto P$. The compactification $X_1(N)$ of $Y_1(N)$ is a smooth irreducible projective curve defined over $\mathbb{F}_p$ [4, Theorem 3.7.1].

Let $\mathbb{E}_1(N) \to Y_1(N)$ be the universal elliptic curve of $Y_1(N)$ and $E_1(N)/K_1(N)$ its generic fiber. The j-map $J(N) : X(N) \to \mathbb{P}^1$ factors through the Galois cover $X(N) \to X_1(N)$ of degree N, whose restriction to $Y(N)$ maps to $Y_1(N)$ by $(E, P, Q) \mapsto (E, P)$. It induces the j-map $J_1(N) : X_1(N) \to \mathbb{P}^1$ whose restriction to $Y_1(N)$ is given by $(E, P) \mapsto j(E)$. Since $2, 3 \nmid N$, if $y \in Y(N)$ and $y_1 \in Y_1(N)$ such that $J(N)(y) = J_1(N)(y_1)$ equals 0, respectively 1728, then the ramification index $e(y \mid y_1)$ equals 1. A fortiori, $e(y_1 \mid 0) = 3$, respectively $e(y_1 \mid 1728) = 2$. Note also that since there exists no inertia in $Y(N) \to \mathbb{A}^1$, the same holds for $Y_1(N) \to \mathbb{A}^1$, thus condition (3) of Proposition 3.1 is satisfied.

Observe that if $E \in I(t)$ has a point $P \in E(\mathbb{F}_q)$ of exact order N, then $N \mid \#E(\mathbb{F}_{p^k})$. The converse holds if N is a prime number. We assume till the end of this subsection that $N = \ell$ is a prime number different from 2, 3 and p, and $t \equiv p^k + 1 \pmod{\ell}$.

Proposition 4.4. *Conditions* (1)–(3) *of Proposition* 3.1 *are satisfied*, *a fortiori* $\pi(k,t)'' = (1/2)(\ell^2 - 1)H(t^2 - 4p^k)$.

Proof. In the notation of Section 3, $Y = Y_1(\ell)$. Let $y \in \mathcal{Y}_{k,t}$, $\mathbb{E}_1(\ell)_y/\kappa_y$ the fiber of $\mathbb{E}_1(\ell) \to Y_1(\ell)$ at y and $\mathbb{E}_1(\ell)'_y = \mathbb{E}_1(\ell)_y \times_{\kappa_y} \mathbb{F}_{p^k}$.

(1) Let $x \in \vartheta^{-1}([\mathbb{E}_1(\ell)'_y])$, then $\mathbb{E}_1(\ell)'_x$ is $\mathbb{F}_{p^k}$-isomorphic to $\mathbb{E}_1(\ell)'_y$, in particular $j(\mathbb{E}_1(\ell)_x) = j(\mathbb{E}_1(\ell)_y)$, i.e., $x \in J_1(\ell)^{-1}(j(\mathbb{E}_1(\ell)_y))$. Let $x \in J_1(\ell)^{-1}(j(\mathbb{E}_1(\ell)_y))$; then x represents the isomorphism class of the pair $(\mathbb{E}_1(\ell)_y,\ P_y)$, where $P_y \in \mathbb{E}_1(\ell)_y(\kappa_y)$ is a point of exact order ℓ. By the geometric description of $J_1(\ell)$, there is no inertia, so $\kappa_x = \kappa_y$. Furthermore, $\mathbb{E}_1(\ell)_y$ is an elliptic curve over $\kappa_y = \kappa_x$ with j-invariant $j(\mathbb{E}_1(\ell)_y) = j(\mathbb{E}_1(\ell)_x)$ and a κ_y-rational point P_y of exact order ℓ. By the universal property of $\mathbb{E}_1(\ell) \to Y_1(\ell)$, $\mathbb{E}_1(\ell)_x = \mathbb{E}_1(\ell)_y$, a fortiori $[\mathbb{E}_1(\ell)'_x] = [\mathbb{E}_1(\ell)'_y]$ and $x \in \vartheta^{-1}([\mathbb{E}_1(\ell)'_y])$.

(2) For every $E \in \mathfrak{A}_{k,t}$, by hypothesis, $\ell \mid \#E(\mathbb{F}_{p^k})$, thus there exists $P \in E(\mathbb{F}_{p^k})$ of exact order ℓ. Let $y \in Y_1(\ell)(\mathbb{F}_{p^k})$ represent the isomorphism class of the pair (E, P). But $\mathbb{E}_1(\ell)_y$ is the unique elliptic curve defined over κ_y with a κ_y-rational point P_y of exact order ℓ. Thus $\mathbb{E}_1(\ell)'_y = E$. In particular, $[\mathbb{E}_1(\ell)'_y] = [E]$ and ϑ is surjective.

Condition (3) follows from the geometric description of $J_1(\ell)$. Therefore,

$$\pi(k,t)'' = \frac{1}{2}\phi(\ell)\psi(\ell) \sum_{\mathcal{O}(t^2-4p^k)\subset \mathcal{O}} h_w(\Delta(\mathcal{O})) = \frac{1}{2}(\ell^2 - 1)H(t^2 - 4p^k). \ \blacksquare$$

References

[1] Z. Borevich and I. Shafarevich, *Number Theory*, Academic Press, 1966.

[2] N. Elkies, *The existence of infinitely many supersingular primes for every elliptic curve over* $\mathbb{Q}$, Invent. Math. 89 (1987), 561–567.

[3] J. I. Igusa, *Fibre systems of Jacobian varieties III. Fibre systems of elliptic curves*, Amer. J. Math. 81 (1959), 453–476.

[4] N. Katz and B. Mazur, *Arithmetic Moduli of Elliptic Curves*, Princeton Univ. Press, 1985.

[5] S. Lang and H. Trotter, *Frobenius Distributions in* GL_2 *Extensions*, Lecture Notes in Math. 504, Springer, 1976.

[6] V. K. Murty, *Frobenius distributions and Galois representations*, in: Proc. Sympos. Pure Math. 66, Amer. Math. Soc., 1999, 193–211.

[7] A. Pacheco, *Rational points on Igusa curves and L-functions of symmetric representations*, J. Number Theory 58 (1996), 343–360.

[8] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A 46 (1987), 183–211.

[9] R. Schoof and M. van der Vlugt, *Hecke operators and weight distributions of certain codes*, ibid. 57 (1991), 163–186.

[10] J. Silverman, *The Arithmetic of Elliptic Curves*, Grad. Texts in Math. 106, Springer, 1986.

Departamento de Matemática Pura
Universidade Federal do Rio de Janeiro (Universidade do Brasil)
Rua Guaiaquil 83
Cachambi, 20785-050 Rio de Janeiro, RJ, Brazil
E-mail: amilcar@impa.br

Received on 14.11.2001
and in revised form on 27.11.2001 (4146)