Journal of Number Theory **95**, 303–312 (2002)
doi:10.1006/jnth.2001.2760

Legendre Elliptic Curves over Finite Fields

Roland Auer[1] and Jaap Top

Vakgroep Wiskunde RuG, P.O. Box 800, 9700 AV Groningen, The Netherlands
E-mail: auer@math.rug.nl, top@math.rug.nl

Communicated by K. Ribet

Received June 22, 2001; revised August 22, 2001

We show that every elliptic curve over a finite field of odd characteristic whose number of rational points is divisible by 4 is isogenous to an elliptic curve in Legendre form, with the sole exception of a minimal respectively maximal elliptic curve. We also collect some results concerning the supersingular Legendre parameters.

1. INTRODUCTION

Throughout this paper, $q > 1$ denotes a power of an odd prime number p, and k is a field. Given two elliptic curves E/k and E'/k, all morphisms from E to E' are understood to be defined over k. In particular, we simply write $\mathrm{End}(E)$ for the ring of all endomorphisms of E/k. The notation $E \simeq E'$ indicates that E is isomorphic to E', and $E \sim E'$ means that E and E' are isogenous. The endomorphism of multiplication by $m \in \mathbf{Z}$ on E is denoted by $[m]$. In case $k = \mathbf{F}_q$, it is a well known fact (see [13]) that $E \sim E'$ if and only if $|E(\mathbf{F}_q)| = |E'(\mathbf{F}_q)|$. The Frobenius endomorphism on an elliptic curve $E/\mathbf{F}_q$ will be denoted by $\phi = \phi_q$.

For $\mathrm{char}(k) \neq 2$ and $\lambda \in k \setminus \{0, 1\}$, the *Legendre elliptic curve* E_λ/k is given by the equation $y^2 = x(x-1)(x-\lambda)$. All its 2-torsion points are rational. An arbitrary elliptic curve E/k with this property has an equation of the form $y^2 = x(x-\alpha)(x-\beta)$ with $\alpha, \beta \in k^*$ (after a suitable choice of coordinates). Investigating the possible transformations (see [12, III, Sect. 1]) yields that E is *Legendre isomorphic* (i.e., isomorphic to a Legendre elliptic curve) if and only if at least one of $\pm\alpha, \pm\beta, \pm(\alpha-\beta)$ is a square in k. This is always true when $k(\sqrt{-1})$ is algebraically closed or when $k = \mathbf{F}_q$ with $q \equiv 3 \bmod 4$, but not, e.g., for $k = \mathbf{F}_{13}$, $\alpha = -2$ and $\beta = 5$. So the next question to ask is whether E is isogenous to a Legendre elliptic curve, or *Legendre isogenous*, for short. For $k = \mathbf{F}_q$, this can be answered affirmatively, with precisely one exception, which occurs when q is a square.

[1] To whom correspondence should be addressed.

0022-314X/02 $35.00

THEOREM 1.1. *Let $E/\mathbf{F}_q$ be an elliptic curve. Write $q = r^2$, such that $r \equiv 1 \bmod 4$ when q is a square. Then E is Legendre isogenous if and only if* $|E(\mathbf{F}_q)| \in 4\mathbf{Z}\setminus\{(r+1)^2\}$.

A proof of this result will be presented in the next section. In the third section we collect some results concerning the *supersingular Legendre parameters*, i.e., the values of $\lambda \in \mathbf{F}_q$ for which E_λ is supersingular. Section 4 contains some remarks on the 'average' number $|E_\lambda(\mathbf{F}_q)|$ when λ ranges over $\mathbf{F}_q\setminus\{0,1\}$, and the final section considers an analogue in characteristic 2.

Our motivation for studying this originated from the problem of finding lower bounds for the maximum number $N_q(3)$ of rational points on genus 3 curves over $\mathbf{F}_q$. For example, we have used the main result of the present paper to prove $N_{3^n}(3) \geqslant 3^n + 6\sqrt{3^n} - 23$ for every $n \geqslant 1$. We plan to present this and similar results in a forthcoming paper.

2. ISOGENIES OF LEGENDRE ELLIPTIC CURVES

In this section we assume the characteristic of k to be different from 2.

LEMMA 2.1. *Let E/k be given by $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ with $\alpha, \beta, \gamma \in k$, $\alpha \neq \beta \neq \gamma \neq \alpha$. Then $(\gamma, 0) \in [2]E(k) \Leftrightarrow \gamma - \alpha,\ \gamma - \beta \in k^{*2}$.*

Proof. This is true because the homomorphism (see [9, Theorem 1.2] and [12, X, Sect. 1])

$$(x-\alpha, x-\beta, x-\gamma) : E(k) \to k^*/k^{*2} \times k^*/k^{*2} \times k^*/k^{*2}$$

has kernel $[2]E(k)$ and sends $(\gamma, 0)$ to $(\gamma-\alpha, \gamma-\beta, (\gamma-\alpha)(\gamma-\beta))$. ∎

Given an elliptic curve E/k with Weierstrass equation $y^2 = f(x)$ and an element $\alpha \in k^*$, we denote by $E^{(\alpha)}/k$ the elliptic curve with equation $\alpha y^2 = f(x)$. Note that $E \simeq E^{(\alpha)}$ for $\alpha \in k^{*2}$. If $E/\mathbf{F}_q$ and α is non-square in $\mathbf{F}_q$, then counting points by means of the quadratic character on $\mathbf{F}_q$ yields $|E(\mathbf{F}_q)| + |E^{(\alpha)}(\mathbf{F}_q)| = 2q + 2$.

LEMMA 2.2. *Let E/k be an elliptic curve, and let $\alpha \in k^*$ be non-square. Suppose $E \simeq E^{(\alpha)}$. Then $j(E) = 1728$ and $k(\sqrt{\alpha}) = k(\sqrt{-1})$.*

Proof. This can be seen from a calculation using the explicit form of a possible isomorphism (see [12, III, Sect. 1 and Appendix A]). Alternatively, one may use the theory of twisting ([12, X, Sect. 5]): the condition $E \simeq E^{(\alpha)}$ implies that the cocycle $\sigma \mapsto [\sigma(\sqrt{\alpha})/\sqrt{\alpha}]$ is trivial in $H^1(\mathrm{Gal}(\bar{k}/k),$

$\mathrm{Aut}(E \otimes \bar{k})$), and hence of the form $\sigma \mapsto \sigma(\varphi) \circ \varphi^{-1}$ for some $\varphi \in \mathrm{Aut}(E \otimes \bar{k})$. Then φ has order 4, from which the lemma easily follows. ∎

Let us return to the Legendre elliptic curves E_λ/k with $\lambda \in k\backslash\{0,1\}$. It is well known (see [12, III, Sect. 1]) that $E_\lambda \otimes \bar{k} \simeq E_\mu \otimes \bar{k}$ if and only if $\mu \in [\lambda] := \{\lambda, 1-\lambda, 1/\lambda, 1-1/\lambda, 1/(1-\lambda), \lambda/(\lambda-1)\}$, the orbit of λ under the group generated by the two transformations $\lambda \mapsto 1/\lambda$ and $\lambda \mapsto 1-\lambda$ on $\mathbf{P}^1$.

Proposition 2.1. *Let $\lambda \in \mathbf{F}_q\backslash\{0,1,-1,2,1/2\}$. The following conditions are equivalent.*

(a) *$E_\lambda \simeq E_\mu$ over $\mathbf{F}_q$ for all $\mu \in [\lambda]$.*
(b) *$-1, \lambda, 1-\lambda \in \mathbf{F}_q^{*2}$.*
(c) *$E_\lambda[4](\mathbf{F}_q) \simeq \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$.*

If $E_\lambda^{(\alpha)}/\mathbf{F}_q$ is not Legendre isomorphic for some $\alpha \in \mathbf{F}_q^*$, then the above conditions are satisfied.

Proof. Since $-1 \notin [\lambda]$, we know that $j(E_\lambda) \neq 1728$. From Lemma 2.2 and the isomorphisms $E_\lambda^{(-1)} \simeq E_{1-\lambda}$, $E_\lambda^{(\lambda)} \simeq E_{1/\lambda}$ and $E_\lambda^{(1-\lambda)} \simeq E_{\lambda/(\lambda-1)}$ one concludes (a) ⇔ (b). The equivalence of (b) and (c) follows directly from Lemma 2.1.

If $E_\lambda^{(\alpha)}$ is not Legendre isomorphic, then α must be non-square, and none of the curves $E_\lambda^{(-1)}$, $E_\lambda^{(\lambda)}$ and $E_\lambda^{(1-\lambda)}$ is isomorphic to $E_\lambda^{(\alpha)}$ since they are all Legendre isomorphic. This implies that $-1, \lambda, 1-\lambda \in \mathbf{F}_q^{*2}$. ∎

Proposition 2.2. *Let $p' = (-1)^{(p-1)/2}p$ and suppose $E_\lambda/\mathbf{F}_q$ is supersingular. Then $\lambda \in \mathbf{F}_{p^2}$ and $E_\lambda(\mathbf{F}_{p^2}) \simeq \mathbf{Z}/(p'-1)\mathbf{Z} \times \mathbf{Z}/(p'-1)\mathbf{Z}$.*

Proof. Since E_λ is supersingular, it has j-invariant $j := j(E_\lambda) \in \mathbf{F}_{p^2}$ (cf. [12, V, Theorem 3.1]). Hence there exists an elliptic curve $E/\mathbf{F}_{p^2}$ such that $E_\lambda \otimes \bar{\mathbf{F}}_p \simeq E \otimes \bar{\mathbf{F}}_p$. Multiplication by p on E is purely inseparable of degree $p^2 = \deg \phi$ (again [12, V, Theorem 3.1]), and therefore it factors as $[p] = \psi \circ \phi$ for some automorphism ψ of E. Assuming $j \neq 0$, 1728 for a moment implies $\psi = [\pm 1]$, hence $\phi = [\pm p]$ and $E(\mathbf{F}_{p^2}) = E[1-\phi](\bar{\mathbf{F}}_p) = E[p \pm 1](\bar{\mathbf{F}}_p) \simeq (\mathbf{Z}/(p \pm 1)\mathbf{Z})^2$. As $p \pm 1$ is even, E has an equation $y^2 = x(x-\alpha)(x-\beta)$ with $\alpha, \beta \in \mathbf{F}_{p^2}^*$. From $E^{(\alpha)} \simeq E_{\beta/\alpha}$ we conclude $\beta/\alpha \in [\lambda]$ and therefore $\lambda \in \mathbf{F}_{p^2}$. For $j \in \{0,\ 1728\}$, the latter fact follows from an easy calculation.

Therefore we may consider $E_\lambda/\mathbf{F}_{p^2}$. Comparing the list in [14, p. 536] (see also [15]) with the condition $|E_\lambda(\mathbf{F}_{p^2})| \in 4\mathbf{Z}$ leaves us with the cases $|E_\lambda(\mathbf{F}_{p^2})| = (p \pm 1)^2$, so $E_\lambda^{(\alpha)}(\mathbf{F}_{p^2}) \simeq (\mathbf{Z}/(p'-1)\mathbf{Z})^2$ for suitable $\alpha \in \mathbf{F}_{p^2}^*$. Now $p' - 1 \equiv 0 \bmod 4$, which means in particular that $(0,0) \in [2]E_\lambda^{(\alpha)}(\mathbf{F}_{p^2})$. By Lemma 2.1, this implies $-\alpha \in \mathbf{F}_{p^2}^{*2}$. Hence also α is a square in $\mathbf{F}_{p^2}^*$ and thus $E_\lambda \simeq E_\lambda^{(\alpha)}$. ∎

We are now ready to complete the

Proof of Theorem 1.1. First of all, $E \sim E_\lambda$ for some $\lambda \in \mathbf{F}_q \setminus \{0,1\}$ implies $|E(\mathbf{F}_q)| = |E_\lambda(\mathbf{F}_q)| \in 4\mathbf{Z}$ since $E_\lambda(\mathbf{F}_q)$ contains the whole 2-torsion subgroup. Moreover, if q is a square and E_λ is supersingular, then $\phi = [r]$ on $E_\lambda/\mathbf{F}_q$ by Proposition 2.2, and so $|E_\lambda(\mathbf{F}_q)| \neq (r+1)^2$.

To show the opposite direction, we suppose $|E(\mathbf{F}_q)| \in 4\mathbf{Z} \setminus \{(r+1)^2\}$ for the rest of the proof. If E does not have all its 2-torsion rational, then $E(\mathbf{F}_q)$ must contain a point P of order 4. Choose $Q \in E[2](\bar{\mathbf{F}}_p) \setminus \langle [2]P \rangle$. Then $\phi_q(Q) \equiv Q \bmod [2]P$, and so $\tilde{E} = E/\langle [2]P \rangle$ does have rational 2-torsion $\tilde{E}[2](\mathbf{F}_q) = \langle P \bmod [2]P, Q \bmod [2]P \rangle \simeq \mathbf{Z}/2\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$, generated by the images of P and of Q in $E/\langle [2]P \rangle$. We therefore may assume that E is given by an equation $y^2 = x(x-\alpha)(x-\beta)$ with $\alpha, \beta \in \mathbf{F}_q^*$. Hence $E^{(\alpha)} \simeq E_\lambda$ with $\lambda := \beta/\alpha$.

Let us first assume that E is supersingular. Once more investigating the list in [14, p. 536] yields either $|E(\mathbf{F}_q)| = q+1$ with non-square q, or $|E(\mathbf{F}_q)| = (r-1)^2$ with q a square. In the first case we have $|E(\mathbf{F}_q)| = |E^{(\alpha)}(\mathbf{F}_q)|$, hence $E \sim E^{(\alpha)}$, which implies the theorem. In the second case, we must have $E \simeq E^{(\alpha)} \simeq E_\lambda$ by Proposition 2.2.

Now suppose E is ordinary. If $E_\lambda^{(\alpha)}$ is Legendre isogenous, the theorem is proven. Otherwise we may assume $E_\lambda[4](\mathbf{F}_q) \simeq \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/4\mathbf{Z}$ and $-1 \in \mathbf{F}_q^{*2}$ by Proposition 2.1. Using Rück's theorem [8], we conclude that $E_\lambda \sim E'$ where $E'/\mathbf{F}_q$ is an elliptic curve with $E'[4](\mathbf{F}_q) \simeq \mathbf{Z}/4\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Clearly, we can choose the coordinates such that E' has an equation $y^2 = x(x-\alpha')(x-\beta')$ with $\alpha', \beta' \in \mathbf{F}_q^*$ and $(0,0) \in [2]E'(\mathbf{F}_q)$. But then $-\alpha' \in \mathbf{F}_q^{*2}$ by Lemma 2.1. Thus, $E' \simeq E_{\lambda'}$ with $\lambda' = \beta'/\alpha'$, and this time $E_{\lambda'}^{(\alpha)}/\mathbf{F}_q$ is Legendre isomorphic according to Proposition 2.1. ∎

3. SUPERSINGULAR LEGENDRE PARAMETERS

From Proposition 2.2, we see that not only the supersingular j-invariants but even the supersingular Legendre parameters are in $\mathbf{F}_{p^2}$. This is well known; compare [3, pp. 94, 97]. The proof of Proposition 2.2 moreover shows that these supersingular Legendre parameters are squares in $\mathbf{F}_{p^2}^*$. One can prove an even stronger result, which also seems to be well known. See

[1, Theorem 1.9A] for a statement of the results in this section; Brock's approach is rather different from the one presented here.

PROPOSITION 3.1. *Let $\lambda \in \mathbf{F}_q \backslash \{0, 1\}$ such that E_λ is supersingular. Then $-\lambda \in \mathbf{F}_{p^2}^{*8}$.*

Proof. By Proposition 2.2, we have $\lambda \in \mathbf{F}_{p^2}$ and $E_\lambda(\mathbf{F}_{p^2}) \simeq (\mathbf{Z}/(p'-1)\mathbf{Z})^2$ with $p' := (-1)^{(p-1)/2} p \equiv 1 \bmod 4$. In particular, condition (c) of Proposition 2.1 is satisfied with $q = p^2$, hence $\lambda \in \mathbf{F}_{p^2}^{*2}$. Let us fix square roots $\sqrt{\lambda}, \sqrt{-1} =: i \in \mathbf{F}_{p^2}$. By [12, III, Example 4.5], $E = E_\lambda / \langle (0,0) \rangle$ has an equation $y^2 = x(x + (\sqrt{\lambda}+1)^2)(x + (\sqrt{\lambda}-1)^2)$, so $E_\lambda \sim E \simeq E_{\hat{\lambda}}$ with $\hat{\lambda} := \left(\frac{\sqrt{\lambda}+1}{\sqrt{\lambda}-1}\right)^2$. Because $E_{1-\hat{\lambda}}$ is supersingular, too, we can conclude $1 - \hat{\lambda} = \left(\frac{2i}{\sqrt{\lambda}-1}\right)^2 \sqrt{\lambda} \in \mathbf{F}_{p^2}^{*2}$. This shows that λ is a fourth power in $\mathbf{F}_{p^2}$. Applying this result to $1 - \hat{\lambda}$ instead of λ yields

$$\lambda, \frac{1-\hat{\lambda}}{(1+i)^4} = \frac{\sqrt{\lambda}}{(\sqrt{\lambda}-1)^2} \in \mathbf{F}_{p^2}^{*4}. \qquad (*)$$

The point $P := (\sqrt{\lambda}, i(\lambda - \sqrt{\lambda})) \in E_\lambda(\mathbf{F}_{p^2})$ has order 4, namely $[2]P = (0,0)$. As in the proof of Lemma 2.1, the group homomorphism

$$(x, x-1, x-\lambda) : E_\lambda(\mathbf{F}_{p^2}) \to \mathbf{F}_{p^2}^{*}/\mathbf{F}_{p^2}^{*2} \times \mathbf{F}_{p^2}^{*}/\mathbf{F}_{p^2}^{*2} \times \mathbf{F}_{p^2}^{*}/\mathbf{F}_{p^2}^{*2}$$

has kernel $[2]E_\lambda(\mathbf{F}_{p^2})$ and sends P to $(\sqrt{\lambda}, \sqrt{\lambda}-1, \sqrt{\lambda}-\lambda)$. Together with $(*)$ we obtain the equivalence

$$\begin{aligned} -1 \in \mathbf{F}_{p^2}^{*8} &\Leftrightarrow 16 | p^2 - 1 = (p'-1)(p'+1) \\ &\Leftrightarrow p' \equiv 1 \bmod 8 \Leftrightarrow p \in [2]E_\lambda(\mathbf{F}_{p^2}) \\ &\Leftrightarrow \sqrt{\lambda} - 1 \in \mathbf{F}_{p^2}^{*2} \Leftrightarrow \lambda \in \mathbf{F}_{p^2}^{*8}. \end{aligned}$$

Since we already knew that $\lambda \in \mathbf{F}_{p^2}^{*4}$, the desired result drops out. ∎

Recall from [2, 6] that the supersingular Legendre parameters are exactly the $m := (p-1)/2$ distinct roots of the Deuring polynomial $H_p(x) = (-1)^m \sum_{k=0}^{m} \binom{m}{k}^2 x^k \in \mathbf{F}_p[x]$. Thus, Proposition 3.1 says that $H_p(-x)$ divides $x^{(p^2-1)/8} - 1$.

Concerning the number $s_p := |\{\lambda \in \mathbf{F}_p : H_p(\lambda) = 0\}|$ of supersingular Legendre parameters in $\mathbf{F}_p$, we have the following. Write $h(-p)$ for the class number of (the ring of integers in) $\mathbf{Q}(\sqrt{-p})$.

PROPOSITION 3.2. *The number s_p of supersingular Legendre parameters in $\mathbf{F}_p$ satisfies*

(a) $s_p = 0$ *if and if* $p \equiv 1 \bmod 4$.
(b) $s_3 = 1$.
(c) *If* $p \equiv 3 \bmod 4$ *and* $p > 3$, *then* $s_p = 3h(-p)$.

In the proof, the following lemma will be used.

LEMMA 3.1. *Assume $p > 3$ and $q \equiv 3 \bmod 4$, and let $E/\mathbf{F}_q$ be an elliptic curve with j-invariant $j(E) \neq 0$. If E is Legendre isomorphic, then there are exactly 3 values of $\lambda \in \mathbf{F}_q \backslash \{0, 1\}$ such that $E \simeq E_\lambda$.*

Proof. Note that $E_\lambda^{(-1)} \simeq E_{1-\lambda}$ and $E_{1/\lambda}^{(-1)} \simeq E_{1-1/\lambda}$ and $E_{1/(1-\lambda)}^{(-1)} \simeq E_{\lambda/(\lambda-1)}$. Assume $j := j(E_\lambda) \neq 0, 1728$ for the moment. Then $[\lambda]$ has 6 elements and, using Lemma 2.2, exactly one from each pair $\{\lambda, 1-\lambda\}$, $\{1/\lambda, 1-1/\lambda\}$ and $\{1/(1-\lambda), \lambda/(\lambda-1)\}$ yields a curve isomorphic to E_λ over $\mathbf{F}_q$.

The remaining case $j = 1728$ corresponds to $\lambda \in \{-1, 2, 1/2\}$. These three values are different since we assume the characteristic to be > 3. The curves E_{-1} and E_2 are obviously isomorphic. Moreover, $E_2^{(2)} \simeq E_{1/2} \simeq E_{1/2}^{(-1)} \simeq E_2^{(-2)}$. Since $q \equiv 3 \bmod 4$, one of $2, -2$ is a square in $\mathbf{F}_q^*$, hence $E_{1/2} \simeq E_2$, and again we find 3 values of $\lambda \in \mathbf{F}_q \backslash \{0, 1\}$ giving the same curve. ∎

Proof of Proposition 3.2. (b) holds because $H_3(x) = -x - 1$. We now assume $p > 3$. Then a supersingular elliptic curve over $\mathbf{F}_p$ has $p + 1$ rational points. For $p \equiv 1 \bmod 4$ this number is not divisible by 4. Therefore, $s_p = 0$ in this case. Since $s_p > 0$ when $p \equiv 3 \bmod 4$ (this follows from $H_p(-1) = 0$ for such p, or alternatively, from the fact that H_p has odd degree when $p \equiv 3 \bmod 4$, while all irreducible factors have degree $\leqslant 2$ by Proposition 2.2), (a) follows.

To prove (c), consider a supersingular elliptic curve $E/\mathbf{F}_p$ with $3 < p \equiv 3 \bmod 4$. Since $\phi^2 = [-p]$ on $E/\mathbf{F}_p$, we have $\mathbf{Z}[\sqrt{-p}] \simeq \mathbf{Z}[\phi] \subseteq \mathrm{End}(E)$. Now $\mathrm{End}(E)$ is commutative (since all $\mathbf{F}_p$-endomorphisms by definition commute with ϕ and $\mathrm{End}(E \otimes \bar{\mathbf{F}}_p)$ has rank 4), and therefore $\mathrm{End}(E) \subset \mathbf{Z}\left[\frac{1-\sqrt{-p}}{2}\right]$. From this, one concludes that $\mathrm{End}(E) \simeq \mathbf{Z}\left[\frac{1-\sqrt{-p}}{2}\right]$, the ring of integers in $\mathbf{Q}(\sqrt{-p})$, precisely when $1 - \phi$ is divisible by 2 in $\mathrm{End}(E)$, which happens if and only if ϕ acts trivially on $E[2](\bar{\mathbf{F}}_p)$, in other words, if and only if all 2-torsion on E is $\mathbf{F}_p$-rational. In particular, a supersingular $E_\lambda/\mathbf{F}_p$ satisfies $\mathrm{End}(E_\lambda) \simeq \mathbf{Z}\left[\frac{1-\sqrt{-p}}{2}\right]$.

Conversely, if an elliptic curve $E/\mathbf{F}_p$ satisfies $\mathrm{End}(E) \simeq \mathbf{Z}\left[\frac{1-\sqrt{-p}}{2}\right]$, then E is supersingular (the trace of an element of norm p is divisible by p in the latter ring), and by the argument above, there are $\alpha, \beta \in \mathbf{F}_p^*$ such that E can be given by an equation $y^2 = x(x-\alpha)(x-\beta)$. Hence $E \simeq E_{\beta/\alpha}^{(\alpha)} \simeq E_{1-\beta/\alpha}^{(-\alpha)}$. Since $p \equiv 3 \bmod 4$, one of $\alpha, -\alpha$ is a square in $\mathbf{F}_p^*$, and we conclude that E is Legendre isomorphic. Moreover, $j(E) \neq 0$ because otherwise $p \equiv 2 \bmod 3$ by supersingularity, while to have all 2-torsion rational one would need $p \equiv 1 \bmod 3$. Hence Lemma 3.1 applies, and we find precisely 3 values of $\lambda \in \mathbf{F}_p \backslash \{0, 1\}$ for which $E \simeq E_\lambda$.

The conclusion is that the number s_p of supersingular values of $\lambda \in \mathbf{F}_p$ equals 3 times the number of $\mathbf{F}_p$-isomorphism classes of elliptic curves $E/\mathbf{F}_p$ with $\mathrm{End}(E) \simeq \mathbf{Z}\left[\frac{1-\sqrt{-p}}{2}\right]$. By Waterhouse [14, Theorem 4.5] (compare [10, p. 194] where a small correction is given), the latter number equals $h(-p)$. ∎

It is known that $h(-p) > \frac{1}{55}\log(p)$ [5, p. 232; 7, p. 321]. Hence, in particular, Proposition 3.2 implies that for $p \equiv 3 \bmod 4$, the number of $\mathbf{F}_p$-rational zeroes of H_p tends to infinity when $p \to \infty$.

4. SOME STATISTICS CONCERNING LEGENDRE ELLIPTIC CURVES

We will briefly discuss some statistical observations concerning the numbers $|E_\lambda(\mathbf{F}_q)|$. First of all, these are integers $\equiv 0 \bmod 4$, and by the Hasse inequality, they lie in the interval $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$. Moreover, if an integer $N = q+1-t$ in this interval does *not* occur as the number of points of some elliptic curve over $\mathbf{F}_q$, then $\gcd(t, q) \neq 1$ (see [14, Theorem 4.1]; in fact, this reference for given q even precisely describes the remaining at most 5 values of t with $\gcd(t, q) \neq 1$ for which an elliptic curve over $\mathbf{F}_q$ with N points exists). It follows that there are roughly $\sqrt{q}(1-1/p)$ numbers $N \equiv 0 \bmod 4$ which appear as the number of points of some elliptic curve over $\mathbf{F}_q$. By our main theorem, all but at most one of these appear as the number of points of some $E_\lambda/\mathbf{F}_q$. Since there are $q-2$ elliptic curves $E_\lambda/\mathbf{F}_q$, this implies that 'on average' there are roughly $p\sqrt{q}/(p-1)$ values of $\lambda \in \mathbf{F}_q \backslash \{0, 1\}$ such that $|E_\lambda(\mathbf{F}_q)|$ equals a given occurring N.

If the numbers $|E_\lambda(\mathbf{F}_q)|$ had an average of $q+1$ over all $\lambda \in \mathbf{F}_q\backslash\{0,1\}$, then

$$S(q) := \sum\nolimits_{\lambda\in\mathbf{F}_q\backslash\{0,1\}} |E_\lambda(\mathbf{F}_q)|$$

would equal $\bar{S}(q) := (q-2)(q+1) = q^2 - q - 2$. But this is impossible for $q \equiv 1 \bmod 4$ because then $\bar{S}(q) \equiv 2 \bmod 4$.

Proposition 4.1. $S(q) = \bar{S}(q) + 1 + (-1)^{(q-1)/2}$.

Proof. This can by shown by naively computing

$$\begin{aligned}\tilde{S}(q) &:= |\{(x,y,\lambda) \in \mathbf{F}_q^3 : y^2 = x(x-1)(x-\lambda)\}| \\ &= 2q + |\mathbf{F}_q\backslash\{0,1\} \times \mathbf{F}_q| = q^2,\end{aligned}$$

$$\begin{aligned}S_0(q) &:= |\{(x,y) \in \mathbf{F}_q^2 : y^2 = x^2(x-1)\}| \\ &= 2 + 2|\mathbf{F}_q^{*2}\backslash\{-1\}| = q - (-1)^{(q-1)/2} \text{ and}\end{aligned}$$

$$S_1(q) := |\{(x,y) \in \mathbf{F}_q^2 : y^2 = x(x-1)^2\}| = 2 + 2|\mathbf{F}_q^{*2}\backslash\{1\}| = q - 1.$$

Then $S(q) = q - 2 + \tilde{S}(q) - S_0(q) - S_1(q) = q^2 - q - 1 + (-1)^{(q-1)/2}$. ∎

An alternative method for computing $S(q)$ is by considering the rational elliptic surface $X \to \mathbf{P}^1$ corresponding to the Legendre family over the λ-line. Compare [4, p. 56] for similar calculations. The surface X has fibre $X_\lambda = E_\lambda$ over $\lambda \in \mathbf{F}_q\backslash\{0,1\}$. Over $\lambda = 1$ the fibre X_1 consists of two $\mathbf{P}^1$'s meeting in two rational points. Hence $|X_1(\mathbf{F}_q)| = 2q$. Over $\lambda = 0$ the fibre X_0 also consists of two copies of $\mathbf{P}^1$ meeting in two points; however, these points are rational precisely when -1 is a square in $\mathbf{F}_q$. This implies $|X_0(\mathbf{F}_q)| = 2q + 1 - (-1)^{(q-1)/2}$. Finally, the fibre X_∞ is of Kodaira type I_2^* and $|X_\infty(\mathbf{F}_q)| = 7q + 1$. The Lefschetz trace formula now shows that $|X(\mathbf{F}_q)| = q^2 + 10q + 1$ and hence $S(q) = |X(\mathbf{F}_q)| - |X_0(\mathbf{F}_q)| - |X_1(\mathbf{F}_q)| - |X_\infty(\mathbf{F}_q)| = q^2 - q - 1 + (-1)^{(q-1)/2}$.

5. AN ANALOGUE IN CHARACTERISTIC TWO

For the sake of completeness, we consider the situation in characteristic 2. Let $n \in \mathbf{N}$. For each $\lambda \in \mathbf{F}_{2^n}^*$, we have the elliptic curve $E_\lambda/\mathbf{F}_{2^n}$ given by the equation $y^2 + xy = x^3 + \lambda$. Since $j(E_\lambda) = 1/\lambda$, they are mutually non-isomorphic.

PROPOSITION 5.1. *An elliptic curve $E/\mathbf{F}_{2^n}$ satisfies $|E(\mathbf{F}_{2^n})| \in 4\mathbf{Z}$ if and only if $E \simeq E_\lambda$ for some $\lambda \in \mathbf{F}_{2^n}^*$.*

Proof. Recall that $E/\mathbf{F}_{2^n}$ is ordinary, i.e., $|E(\mathbf{F}_{2^n})| \in 2\mathbf{Z}$, if and only if (after a suitable choice of coordinates) it has an equation $y^2 + xy = x^3 + \beta x^2 + \lambda$ with $\beta \in \mathbf{F}_{2^n}$ and $\lambda \in \mathbf{F}_{2^n}^*$, and then $j(E) = 1/\lambda$ (see [12, Appendix A]). Thus, we may assume that E has such an equation. For $\alpha \in \mathbf{F}_{2^n}$, we denote by $E^{(\alpha)}$ the elliptic curve with equation $y^2 + xy = x^3 + (\alpha + \beta)x^2 + \lambda$. Then $E \simeq E^{(\alpha)}$ if and only if $\mathrm{Tr}(\alpha) = 0$, where Tr denotes the trace from $\mathbf{F}_{2^n}$ to $\mathbf{F}_2$. Otherwise $E^{(\alpha)}$ is a quadratic twist of E and $|E(\mathbf{F}_{2^n})| + |E^{(\alpha)}(\mathbf{F}_{2^n})| = 2^{n+1} + 2 \equiv 2 \bmod 4$. It therefore remains to verify that $|E_\lambda(\mathbf{F}_{2^n})| \in 4\mathbf{Z}$. Treating the point at infinity and $(0, \sqrt{\lambda}) \in E_\lambda(\mathbf{F}_{2^n})$ separately, and dividing the equation by x^2, we obtain $|E_\lambda(\mathbf{F}_{2^n})| = 2 + 2N$ with

$$\begin{aligned} N &= |\{x \in \mathbf{F}_{2^n}^* : \ \mathrm{Tr}(x + \lambda/x^2) = 0\}| \\ &= |\{x \in \mathbf{F}_{2^n}^* : \ \mathrm{Tr}(x) = \mathrm{Tr}(\sqrt{\lambda}/x)\}|, \end{aligned}$$

which is odd because $x \mapsto \sqrt{\lambda}/x$ is an involution on $\mathbf{F}_{2^n}^*$ with precisely one fixed point. ∎

Applying the Frobenius isogeny ϕ_2 to E_λ results in the curve E_{λ^2}. Putting $\xi = x$ and $\eta = y + \lambda$, one finds that E_{λ^2} can be given by the equation $\eta^2 + \xi\eta = \xi^3 + \lambda\xi$. For this equation, a result like the one given above can be found in a paper by Schoof and van der Vlugt [11, p. 172].

ACKNOWLEDGMENTS

It is our pleasure to thank Robert Carls, Marius van der Put, Jasper Scholten, and Bart de Smit for their interest in this work, and Brad Brock for pointing out some relevant references.

REFERENCES

1. B. W. Brock, "Superspecial Curves of Genera Two and Three," Ph.D. thesis, Princeton University, 1993.
2. M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 197–272.
3. B. Dwork, p-adic cycles, *Inst. Hautes Études Sci. Publ. Math.* **37** (1969), 27–115.
4. B. van Geemen and J. Top, Selfdual and non-selfdual 3-dimensional Galois representations, *Compositio Math.* **97** (1995), 51–70.
5. B. H. Gross and D. B. Zagier, Heegner points and derivatives of L-series, *Invent. Math.* **84** (1986), 225–320.
6. J. Igusa, Class number of a definite quaternion with prime discriminant, *Proc. Nat. Acad. Sci. USA* **44** (1958), 312–314.

7. J. Oesterlé, Nombres de classes des corps quadratiques imaginaires, *Astérisque* **121–122** (1985), 309–323.
8. H.-G. Rück, A note on elliptic curves over finite fields, *Math. Comp.* **49** (1987), 301–304.
9. E. F. Schaefer, 2-descent on the Jacobians of hyperelliptic curves, *J. Number Theory* **51** (1995), 219–232.
10. R. Schoof, Nonsingular plane cubic curves over finite fields, *J. Combin. Theory Ser. A* **46** (1987), 183–211.
11. R. Schoof and M. van der Vlugt, Hecke operators and the weight distributions of certain codes, *J. Combin. Theory Ser. A* **57** (1991), 163–186.
12. J. H. Silverman, "The Arithmetic of Elliptic Curves," Springer-Verlag, New York, 1986.
13. J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966), 134–144.
14. W. C. Waterhouse, Abelian varieties over finite fields, *Ann. Set. École Norm. Sup. (4)* **2** (1969), 521–560.
15. Hui June Zhu, Group structures of elementary supersingular abelian varieties over finite fields, *J. Number Theory* **81** (2000), 292–309.