Elliptic Curves over Finite Fields [1]

B. Sury

1. Introduction

Jacobi was the first person to suggest (in 1835) using the group law on a cubic curve E. The chord-tangent method does give rise to a group law if a point is fixed as the zero element. This can be done over any field over which there is a rational point.

In this chapter, we study elliptic curves defined over finite fields. Our discussion will include the Weil conjectures for elliptic curves, criteria for supersingularity and a description of the possible groups arising as $E(\mathbb{F}_q)$. We shall use basic algebraic geometry of elliptic curves. Specifically, we shall need the notion and properties of isogenies of elliptic curves and of the Weil pairing. In later chapters, the theories of elliptic curves over $\mathbb{C}$, $\mathbb{R}$ and algebraic number fields will be studied. In contrast to this chapter, the basic tools to be used in the later chapters will be elliptic functions and algebraic number theory. The standard reference is Silverman's book [S].

2. Isogenies

The first important result dealing with curves over finite fields is the following beautiful fact established by Serge Lang :

Lang's theorem *Any smooth cubic curve E defined over a finite field $\mathbb{F}_q$ has a $\mathbb{F}_q$-rational point.*

Proof: We start by recalling that the Frobenius morphism ϕ_q on E over $\mathbb{F}_q$ is defined as the map $(x, y) \mapsto (x^q, y^q)$. Here, we are looking at the cubic equation for E in its Weierstrass normal form. Note that a point $P \in E(\mathbb{F}_{q^n})$ if, and only if, $\phi_q^n(P) = P$. Further, note that on fixing any point of E over $\overline{\mathbb{F}_q}$, the algebraic closure of $\mathbb{F}_q$, the chord-tangent

[1] Elliptic Curves, Modular Forms and Cryptography, *Proceedings of the Advanced Instructional Workshop on Algebraic Number Theory, HRI, Allahabad, 2000* (Eds. A. K. Bhandari, D. S. Nagaraj, B. Ramakrishnan, T. N. Venkataramana), Hindustan Book Agency, New Delhi 2003, pp. 33–47.

2000 *Mathematics subject classification.* Primary: 14G10, 14G15, 11G20.

process gives a group law on $E(\overline{\mathbb{F}_q})$. Look at $\phi : E \to E$ defined by $\phi(P) = \phi_q(P) - P$ where ϕ_q is the Frobenius map on E over $\mathbb{F}_q$. As E is complete and irreducible, the image $\phi(E)$ is either a point or the whole of E. The latter possibility evidently gives a $\mathbb{F}_q$-rational point viz., a preimage of the 'zero element' of $E(\overline{\mathbb{F}_q})$.
In the former case, write $\phi(P) = P_0$ for all P. Thus, $\phi_q(P) = P + P_0$ for all P. Hence $\phi_q^n(P) = P + nP_0$ for all P, n. On the other hand, $E(\mathbb{F}_{q^n})$ is non-empty for some n since, by definition, any point of $E(\overline{\mathbb{F}_q})$ is in $E(\mathbb{F}_{q^n})$ for some n. Now, if $Q \in E(\mathbb{F}_{q^n})$, then we get $Q = \phi_q^n(Q) = Q + nP_0$ i.e., $nP_0 = O$, the identity element of the group $E(\overline{\mathbb{F}}_q)$. But then, $\phi_q^n(P) = P$ for all n. Thus, for some n, we get $E(\overline{\mathbb{F}_q}) = E(\mathbb{F}_{q^n})$. This is a contradiction, as $E(\overline{\mathbb{F}_q})$ is infinite.

Recall from the introductory chapter [NS] that *a non-constant morphism $\phi : E_1 \to E_2$ between elliptic curves E_1 and E_2 such that $\phi(O) = O$ is called an isogeny.* Therefore, an isogeny must be surjective and must have finite kernel. In fact, we noted that: *An isogeny is a group homomorphism.*

We also recall the notion of a dual isogeny. This is characterized by the following property: *Let $\phi : E_1 \to E_2$ be an isogeny. Then, there is a unique isogeny $\hat{\phi} : E_2 \to E_1$ satisfying $\hat{\phi} \circ \phi = [\deg \phi]$. $\hat{\phi}$ is called the dual of ϕ.*

In the above statement, $[n]$ denotes the isogeny which 'adds n times'.
Remarks
(a) A more down-to-earth description of $\hat{\phi}$ is as follows:

$$\hat{\phi}(y) = [\deg_{insep}\phi]\{\sum_{z \in \phi^{-1}(y)} z - \sum_{w \in \mathrm{Ker}\phi} w\} = [\deg\phi](z)$$

for any $y \in E_2$ and any $z \in \phi^{-1}(y)$.
(b) For $K = \mathbb{C}$, an isogeny $\phi : \mathbb{C}/L \to \mathbb{C}/L'$ has degree $d = [L' : \phi(L)]$. Thus, $dL' \subseteq \phi(L) \subseteq L'$. Then, $\hat{\phi} : \mathbb{C}/L' \to \mathbb{C}/L$ is the map d/f where ϕ is 'multiplication by f'.
(c) If E is defined over $\mathbb{F}_q$ and $\pi_{q,E} : E \to E$ is the Frobenius morphism $(x, y) \mapsto (x^q, y^q)$, then $E(\mathbb{F}_q) = \mathrm{Ker}\ (1 - \phi_{q,E})$.

As we noted, an isogeny has finite kernel. What is the intersection of this kernel with the $\mathbb{F}_q$ points? Here is a rather startling fact:

Lemma *Let E_1 and E_2 be isogenous elliptic curves defined over $\mathbb{F}_q$. Then $\#E_1(\mathbb{F}_q) = \#E_2(\mathbb{F}_q)$.*
Proof: Note that any isogeny $\phi : E_1 \to E_2$ commutes with the Frobenius morphisms on E_1 and E_2. Now, ϕ is surjective. So, we

have $y \in E_2(\mathbb{F}_q) \Leftrightarrow \pi_{q,E_2}(y) = y \Leftrightarrow \pi_{q,E_2}(\phi(x)) = \phi(x) \Leftrightarrow x \in \text{Ker}\ ((1 - \pi_{q,E_2})\phi)$. Now, each $\phi^{-1}(y)$ has $\deg_{sep}\phi$ elements. Thus,

$$\#E_2(\mathbb{F}_q) = \#\text{Ker}\ ((1-\pi_{q,E_2})\phi)/\deg_{sep}\phi = \#\text{Ker}\ (\phi(1-\pi_{q,E_2}))/\deg_{sep}\phi$$
$$= \deg_{sep}(\phi(1-\pi_{q,E_1}))/\deg_{sep}\phi = \deg_{sep}(1-\pi_{q,E_1}) = \#E_1(\mathbb{F}_q).$$

We also recall the following useful facts on degrees and dual maps:
(i) $\widehat{\phi+\psi} = \hat{\phi} + \hat{\psi}$
(ii) $\widehat{[n]} = [n]$
(iii) $\deg\,[n] = n^2$
(iv) $\deg\,\hat{\phi} = \deg\,\phi$
(v) $\hat{\hat{\phi}} = \phi$
(vi) $\deg\,(-\phi) = \deg\,\phi$
(vii) $d(\phi,\psi) := \deg\,(\phi+\psi) - \deg\,\phi - \deg\,\psi$ is symmetric, bilinear on $\text{Hom}(E_1, E_2)$, where $E_{.1}, E_2$ are elliptic curve over a field
(viii) $\deg\,\phi > 0$ for any isogeny ϕ.

3. Riemann hypothesis for elliptic curves

For an elliptic curve E defined over a finite field $\mathbb{F}_q$, the most important parameter and the most obvious one that one can think of is the number of points in $E(\mathbb{F}_q)$. Let us heuristically estimate $\#E(\mathbb{F}_q)$; this will be one (corresponding to the point at infinity) more than the number of solutions (x, y) of the equation $Y^2+a_1XY+a_3Y = X^3+a_2X^2+a_4X+a_6$ with $x, y \in \mathbb{F}_q$. Each value of x yields at the most two values of y and thus $\#E(\mathbb{F}_q) \leq 1 + 2q$. Heuristically, one might expect a random quadratic equation (for y in terms of x) to have a solution with probability $1/2$. Thus, perhaps $\#E(\mathbb{F}_q) \sim q+1$. As a matter of fact, we shall prove that this is true for any E upto an error of $2\sqrt{q}$ i.e., $|\#E(\mathbb{F}_q) - q - 1| \leq 2\sqrt{q}$. This is a theorem of Hasse and, when rewritten in terms of the so-called zeta function of E, turns out to be analogous to the classical Riemann hypothesis as we shall see.

Let E be an elliptic curve defined over $\mathbb{F}_q$. Let $\pi_{q,E} : E \to E$ denote the Frobenius endomorphism.

Exercise *Prove that $\pi_{q,E}$ is a purely inseparable isogeny with* $\deg\,\pi_{q,E} = q$.

Riemann hypothesis for elliptic curves - Hasse 1934. *Let E be an elliptic curve defined over $\mathbb{F}_q$. Then,*

$$|\#E(\mathbb{F}_{q^n}) - 1 - q^n| \leq 2q^{n/2} \quad \forall n \geq 1.$$

Proof: Choose a Weierstrass equation with coefficients in $\mathbb{F}_q$. Since $Gal(\bar{\mathbb{F}}_q|\mathbb{F}_q)$ is topologically generated by $x \overset{\pi_q}{\mapsto} x^q$, a point P of $E(\bar{\mathbb{F}}_q)$ lies in $E(\mathbb{F}_q)$ iff $\pi_{q,E}(P) = P$. Thus, $P \in E(\mathbb{F}_{q^n}) \Leftrightarrow \pi^n_{q,E}(P) = P$ i.e., $E(\mathbb{F}_{q^n}) = \mathrm{Ker}(1 - \pi^n_{q,E})$. Now $1 - \pi^n_{q,E}$ is a separable morphism (since its differential is the identity). Thus $\#E(\mathbb{F}_{q^n}) = \deg(1 - \pi^n_{q,E})$.

We noted that, for any two elliptic curves E_1, E_2 over a field, the function $d : \mathrm{Hom}(E_1, E_2) \times \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$

$$(\phi, \psi) \mapsto \deg(\phi + \psi) - \deg\phi - \deg\psi$$

is a positive definite bilinear form.

By the Cauchy Schwarz inequality, we get (since $B(\phi, \phi) = 2\deg(\phi)$)

$$\begin{aligned} |\deg(1 - \pi^n_{q,E}) - \deg(1) - \deg(\pi^n_{q,E})| &\leq 2\sqrt{\deg(1)\deg(\pi^n_{q,E})} \\ \text{i.e., } |\#E(\mathbb{F}_{q^n}) - 1 - q^n| &\leq 2q^{n/2}. \end{aligned}$$

4. The Weil conjectures

In 1949, A. Weil made a series of general conjectures about varieties defined over finite fields. We shall state them in general and prove them for elliptic curves.

Let us use the notation $K_n = \mathbb{F}_{q^n}$. If V is a projective variety defined over K_1 (i.e., the zero set of a collection of homogeneous polynomials with coefficients from K_1), we want to keep account of the number $\#V(K_n)$. The natural way to do this is by means of a generating function which codifies the data. This is known as the zeta function of V and is defined as the formal power series

$$Z(V/K_1; T) = \exp\left(\sum_{n=1}^{\infty} \#V(K_n)\frac{T^n}{n}\right)$$

Note that $\#V(K_n) = \frac{1}{(n-1)!}\frac{d^n}{dT^n}\log Z(V/K_1; T)]_{T=0}$. The reason for defining the zeta function in this manner is that the series $\sum\limits_{n\geq 1} \#V(K_n)\frac{T^n}{n}$ often looks like the log of a rational function of T.

Example Let $V = \mathbb{P}^d$ considered over $\mathbb{F}_q$. Then, a point of $V(K_n)$ is the equivalence class of a $(d+1)$ - tuple $[(x_0, \ldots, x_d)]$ with $x_i \in \mathbb{F}_{q^n}$ not all zero. Here $[(x_0, \ldots, x_d)]$ and $[(y_0, \ldots, y_d)]$ are in the same class if $\exists\ t \neq 0$ in $\mathbb{F}_{q^n}$ such that $y_i = tx_i,\ \forall\ i$. Thus,

$$\#V(K_n) = \frac{q^{n(d+1)} - 1}{q^n - 1} = \sum_{i=0}^{d} q^{ni}$$

Hence,

$$\begin{aligned} \log Z(V/K_1;T) &= \sum_{n\geq 1}\sum_{i=0}^{d}\frac{q^{ni}T^n}{n} \\ &= \sum_{i=0}^{d}\log\frac{1}{1-q^iT} \\ \text{i.e.,}\quad Z(V/K_1;T) &= \prod_{i=0}^{d}\frac{1}{1-q^iT}. \end{aligned}$$

Remark
(I) One can prove that $Z(V/K_1;p^{-s}) = \sum\limits_{D\geq 0} q^{-s\deg D}$, where the sum is over $\mathbb{F}_q$-rational effective divisors. This is analogous to the Euler factor $\frac{1}{1-p^{-s}}$ of the Riemann zeta function $\zeta(s)$.

(II) We notice that in the example above, $Z(V/K_1;T)$ is in $\mathbb{Q}(T)$. Further, from the proof, we see that if $\exists\ \alpha_1,\ldots,\alpha_n \in \mathbb{C}$ with $\#V(K_n) = \alpha_1^n \pm \ldots \pm \alpha_r^n\ \forall\ n$, then the zeta function will be rational function of T. The following four conjectures are known as the Weil conjectures.

Let V be any smooth, projective variety of dimension n, defined over $K_1 = \mathbb{F}_q$. Then:

Rationality conjecture

$$Z(V/K_1;T) \in \mathbb{Q}(T)$$

Functional equation
There exists an integer χ such that

$$Z\left(V/K_1;\frac{1}{q^nT}\right) = \pm q^{n\chi/2}T^{\chi}Z(V/K_1;T)$$

Factorisation
There exists a factorisation $Z = \frac{P_1(T)P_3(T)\ldots P_{2n-1}(T)}{P_0(T)P_2(T)\ldots P_{2n-2}(T)P_{2n}(T)}$,
with $P_0 = 1-T, P_{2n} = 1-q^nT$, each $P_i(t) \in \mathbb{Z}[T]$ and

$$P_i\left(\frac{1}{q^nT}\right) = P_{2n-i}(T)\left(\frac{-1}{Tq^{n-\frac{i}{2}}}\right)^{b_i}, b_i = \deg P_i = \deg P_{2n-i}.$$

Riemann hypothesis
Each root α of $P_i(T)$ satisfies $|\alpha| = q^{-i/2}$.

The conjecture in its entirety was proved by the efforts of Weil, Dwork, M. Artin, Grothendieck, Lubkin, Deligne, Laumon. But, the first case of elliptic curves was solved by Hasse in 1934 before the conjectures were formulated in this generality by Weil in 1949. It should be pointed out that F.K. Schmidt was the first one to define the zeta function of a curve over a finite field in 1931 and he also proved some parts of the conjecture. Weil pointed out that if one had a suitable cohomology theory for abstract varieties analogous to the usual cohomology for varieties over $\mathbb{C}$, the standard properties of the cohomology theory would imply all the conjectures.
For instance, the functional equation would follow from the Poincaré duality property. Such a cohomology theory is the étale cohomology developed by M. Artin and Grothendieck.

5. Tate modules and the Weil pairing

Before proving the Weil conjectures for elliptic curves, we need to recall the Tate module and its relation to isogenies on an elliptic curve. Let E be an elliptic curve defined over $\mathbb{F}_q$. Suppose ℓ is a prime not dividing q. We know that the ℓ^n-division points of E i.e., $E[\ell^n] \stackrel{d}{=}$ Ker $[\ell^n]$ is $\simeq \mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n$. The inverse limit of the groups $E[\ell^n]$ with respect to the maps $E[\ell^{n+1}] \stackrel{[\ell]}{\to} E[\ell^n]$ is the *Tate module* $T_\ell(E) = \lim\limits_{\leftarrow} E[\ell^n]$. Since each $E[\ell^n]$ is naturally a $\mathbb{Z}/\ell^n$-module, it can be checked that $T_\ell(E)$ is a $\mathbb{Z}_\ell(= \lim\limits_{\leftarrow} \mathbb{Z}/\ell^n)$-module. It is clearly a free $\mathbb{Z}_\ell$-module of rank 2.

Evidently, any isogeny $\phi : E_1 \to E_2$ induces a $\mathbb{Z}_\ell$-module homomorphism $\phi_\ell : T_\ell(E_1) \to T_\ell(E_2)$. In particular, we have a representation : End $(E) \to M_2(\mathbb{Z}_\ell); \phi \mapsto \phi_\ell$, if $\ell \not| q$. Note that End $E \hookrightarrow$ End $T_\ell(E)$ is injective because if $\phi_\ell = 0$, then ϕ is 0 on $E[\ell^n]$ for large n i.e., $\phi = O$.

Finally, let us recall the *Weil pairing*. This is a non-degenerate, bilinear, alternating pairing

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu) \stackrel{d}{=} \lim_{\leftarrow} \mu_{\ell^n} \cong \mathbb{Z}_\ell.$$

It has the important property that $e(\phi x, y) = e(x, \hat{\phi} y)$.

Remarks For any general curves C, D, and a non-constant morphism $\phi : C \to D$, recall that $\phi^* : Div(D) \to Div(C)$ is a homomorphism defined by

$$(P) \mapsto \sum_{Q \in \phi^{-1}(P)} e_\phi(Q)(Q)$$

where $e_\phi(Q)$ is the ramification index at Q.
For $C = D$ an elliptic curve, all the $e_\phi(Q) = \deg_{insep}\phi$.
For a general C and D, $Ord_P(f \circ \phi) = e_\phi(P)Ord_{\phi(P)}(f)$ for every non constant rational function on D.

6. Weil conjectures for elliptic curves

Let us prove the Weil conjectures for elliptic curves now.

Lemma Let $\phi \in$ End (E) and $\ell \not| q$ be a prime. Then,

$$\begin{aligned} \det \phi_\ell &= \deg \phi, \\ tr\phi_\ell &= 1 + \deg\phi - \deg\,(1-\phi). \end{aligned}$$

In particular, $\det \phi_\ell, tr\phi_\ell$ are independent of ℓ, and are integers.

Proof: Let (v_1, v_2) be a $\mathbb{Z}_\ell$-basis of $T_\ell(E)$ and write $\phi_\ell = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with respect to this basis.

Now, we use the Weil pairing e which is bilinear and alternating.

$$\begin{aligned} e(v_1,v_2)^{\deg\phi} &= e((\deg\phi)v_1, v_2) \\ &= e((\hat{\phi})_\ell(\phi)_\ell v_1, v_2) = e(\phi_\ell v_1, \phi_\ell v_2) \\ &= e(av_1 + cv_2, bv_1 + dv_2) = e(v_1,v_2)^{ad-bc} \\ &= e(v_1,v_2)^{\det\,\phi_\ell}. \end{aligned}$$

Since e is non-degenerate, we get $\deg\phi = \det\,\phi_\ell$.
Finally, $tr(\phi_\ell) = 1 + \det\,\phi_\ell - \det\,(Id - \phi_\ell) = 1 + \deg\phi - \deg(1-\phi)$.

To prove the Weil conjectures for E, let us compute $\#E(K_n)$, where, as before, $K_n = \mathbb{F}_{q^n}$. Now $\#E(K_n) = \deg(1-\phi^n)$, where $\phi = \pi_{q,E}$ the Frobenius isogeny $x \mapsto x^q$.

A consequence of the above lemma is the evident fact that the characteristic polynomial of ϕ_ℓ has coefficients in $\mathbb{Z}$ when $\ell \neq$ char $\mathbb{F}_q$. Write $\det\,(Id.T - \phi_\ell) = (T-\alpha)(T-\beta); \alpha, \beta \in \mathbb{C}$.
Moreover, $\forall\ \frac{m}{n} \in \mathbb{Q}$, we get

$$\det\,\left(\frac{m}{n}Id - \phi_\ell\right) = \frac{1}{n^2}det(mId - n\phi_\ell) = \deg(m - n\phi)\frac{1}{n^2} > 0.$$

This implies $\alpha = \bar{\beta}$. Noting, by triangularising, that $\det\,(Id.T - \phi_\ell^n) = (T-\alpha^n)(T-\beta^n)$, we get:

Theorem *For all* $n \geq 1$, $\#E(K_n) = 1 - \alpha^n - \bar{\alpha}^n + q^n$ *where* $|\alpha| = q^{1/2}$. *In particular,* $Z(E/K_1;T) = \frac{1-aT+qT^2}{(1-T)(1-qT)}$, *where* $a \in \mathbb{Z}$ *and* $1 - aT + qT^2 = (1-\alpha T)(1-\bar{\alpha}T)$. *Further,* $Z\left(E/K_1; \frac{1}{qT}\right) = Z(E/K_1;T)$.

Proof: As discussed above,

$$\begin{aligned} \#E(K_n) &= \deg(1-\phi^n) \\ &= \det\,(1-\phi_l^n) = 1 - \alpha^n - \bar{\alpha}^n + q^n \end{aligned}$$

and $|\alpha| = \sqrt{q}$.

$$\begin{aligned} \log Z(E/K_1;T) &= \sum_{n\geq 1}(1 - \alpha^n - \bar{\alpha}^n + q^n)\frac{T^n}{n} \\ &= \sum \frac{T^n}{n} - \sum \frac{(\alpha T)^n}{n} - \sum \frac{(\bar{\alpha}T)^n}{n} + \sum \frac{(qT)^n}{n} \\ &= \log \frac{(1-\alpha t)(1-\bar{\alpha}T)}{(1-T)(1-qT)} \end{aligned}$$

The functional equation is obvious from the expression.
The factorisation $Z = \frac{P_1}{P_0 P_2}$ is with $P_1(T) = 1 - aT + qT^2$; so $P_1\left(\frac{1}{qT}\right) = P_1(T)(-1/T\sqrt{q})^2$.

Remark Putting $\zeta_{E/\mathbb{F}_q}(s) = Z(E/K_1; q^{-s})$, one has

$$\zeta_{E/\mathbb{F}_q}(s) = \frac{1 - aq^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})} = \zeta_{E/\mathbb{F}_q}(1-s).$$

Note that the Riemann hypothesis for $Z(E/K_1;T)$ is equivalent to the fact that the zeroes of $\zeta_{E/\mathbb{F}_q}(s)$ are on the line $Re(s) = \frac{1}{2}$.

7. Supersingularity

Supersingular curves are a special class of elliptic curves which arise naturally. One of the most useful properties they have, as we shall prove, is that their definition forces them to be defined over a small finite field and, over any field, there are only finitely many elliptic curves isogenous to a supersingular one.

Before defining supersingularity, let us recall from the introductory chapter [*NS*] that an elliptic curve E is said to have complex multiplication if $End(E) \ncong \mathbb{Z}$. Let us also recall the following result on End (E) from that chapter.

Proposition
(i) End (E) has no zero divisors.
(ii) End (E) is torsion-free.
(iii) End (E) is either $\mathbb{Z}$, or an order in an imaginary quadratic field or an order in a quaternion division algebra over $\mathbb{Q}$.

An elliptic curve E defined over a field of characteristic $p > 0$ is said to be *supersingular* if $E[p] = O$.
The following characterisation of supersingular elliptic curves is very useful and not hard to prove.

Proposition *Let K be a perfect field of characteristic $p > 0$. Then, the following statements are equivalent:*
(a) E is supersingular.
(b) $[p] : E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.
(c) $E[p^r] = \{O\}$ for some $r \geq 1$.
(d) $E[p^r] = \{O\}$ for all $r \geq 1$.
(e) $End_{\bar{K}}(E)$ is an order in a quaternion division algebra over $\mathbb{Q}$.
Proof: Let us prove the step (a) implies (b). Moreover, we show that if E_1 and E_2 are supersingular, and if $\phi : E_1 \to E_2$ is a cyclic, separable isogeny of prime degree $l \neq p$, then ϕ is defined over $\mathbb{F}_{p^2}$. Supersingularity implies that $\deg_{sep}([p])$ = Ker $[p] = E[p] = O$ i.e., $[p]$ is purely inseparable. Let ϕ_E be the Frobenius isogeny. Then, we know that $[p] = \widehat{\phi_E} \circ \phi_E$. This implies that $\widehat{\phi_E}$ is purely inseparable as well and has degree p. Therefore, by Galois theory, $\widehat{\phi_E} = \phi_E \circ \theta$ for some separable map θ. As the degree of θ has to be 1, it has to be an isomorphism. In particular, E is isomorphic to its image under the Frobenius automorphism of $\mathbb{F}_{p^2}$. Hence, $j(E) \in \mathbb{F}_{p^2}$.
The other statement about isogenies being defined over $\mathbb{F}_{p^2}$ is proved similarly as follows. By the Galois theory argument as above,

$$\phi_{E_2} \circ \phi = \psi \circ \phi_{E_1}$$

and

$$\widehat{\phi_{E_2}} \circ \psi = \alpha \circ \widehat{\phi_{E_1}}$$

for some ψ, α. Then,

$$[\ell] \circ \phi_{E_1} = \hat{\psi} \circ \psi \circ \phi_{E_1} = \hat{\psi} \circ \phi_{E_2} \circ \phi = \phi_{E_1} \circ \hat{\alpha} \circ \phi.$$

But, $[\ell]$ commutes with everything. This gives us

$$\phi_{E_1} \circ (\widehat{\phi} - \hat{\alpha}) \circ \phi = O.$$

A composition of isogenies can be zero only if one of them is zero. Therefore, since ϕ and ϕ_{E_1} are nonzero, we get $\phi = \alpha$ i.e., ϕ commutes with the action of the Frobenius morphism over $\mathbb{F}_{p^2}$. In other words, ϕ is defined over $\mathbb{F}_{p^2}$.

Remark By the above proposition, upto isomorphism there are only finitely many elliptic curves isogenous to a supersingular curve. For $p = 2, Y^2 + Y = X^3$ is the unique supersingular curve. For $p > 2$, we have the following theorem.

Theorem *Let $K = \mathbb{F}_q$ with char $K = p > 2$.*
(i) Let $f(X) \in K[X]$ be a cubic polynomial with distinct roots in $\bar{K}$ and E be the elliptic curve defined by the equation $Y^2 - f(X) = 0$. Then E is supersingular $\Leftrightarrow$ coefficient of X^{p-1} in $f(X)^{\frac{p-1}{2}}$ is 0.
(ii) Consider the Deuring polynomial $H_p(t) = \sum \begin{pmatrix} \frac{p-1}{2} \\ i \end{pmatrix} t^i$. Let $\lambda \in \bar{K}, \lambda \neq 0, 1$. Then, the elliptic curve $E : Y^2 = X(X-1)(X-\lambda)$ is supersingular $\Leftrightarrow H_p(\lambda) = 0$.

Proof: (i) Let $\chi : K^* \to \{\pm 1\}$ be the unique non-trivial character of order 2; extend χ to K by defining $\chi(0) = 0$. Then, it is easy to see that each $x \in K$ yields 0,1 or 2 points (x, y) on E accordingly as $f(x)$ is a non-square, 0 or a square i.e., $\#E(\mathbb{F}_q) = 1 + \sum\limits_{x \in K} (\chi(f(x)) + 1) = 1 + q + \sum\limits_{x \in K} \chi(f(x)) = 1 + \sum\limits_{x \in K} f(x)^{\frac{q-1}{2}} = 1 - A_q$ in K, where $A_q =$ coefficient of X^{q-1} in $f(X)^{\frac{q-1}{2}}$ since f is a cubic and $\sum\limits_{\mathbb{F}_q} x^i$ is -1 or 0 according as whether $q-1$ divides i or not. But $\#E(\mathbb{F}_q) = \deg(1 - \pi_{q,E}) = 1 - a + q = 1 - a$ i.e., $a = A_q$ in K. Thus $A_q = 0 \Leftrightarrow a = 0$ in K. As $a \in \mathbb{Z}$, this means $a \equiv 0(p)$. But $\hat{\pi}_{q,E} = [a] - \pi_{q,E}$; so $a \equiv 0(p) \Leftrightarrow \hat{\pi}_{q,E}$ purely inseparable $\Leftrightarrow E$ supersingular. We still need to show $A_q = 0 \Leftrightarrow A_p = 0$. Writing $f(X)^{\frac{p^{r+1}-1}{2}} = f(X)^{\frac{p^r-1}{2}} \left(f(X)^{\frac{p-1}{2}}\right)^{p^r}$ and equating coefficients and keeping in mind the fact that f is a cubic, one gets $A_{p^{r+1}} = A_{p^r} \cdot A_p^{p^r}$. By induction, we get $A_q = 0 \Leftrightarrow A_p = 0$. The proof of (ii) follows from (i).

Corollary *The j-invariant 0 gives supersingular curves if, and only if, $p \equiv 2$ mod 3. The j-invariant 1728 gives supersingular curves if, and only if, $p \equiv 3$ mod 4.*

Proof: $E : Y^2 = X^3 + 1$ has $j(E) = 0$ and, the coefficient of X^{p-1} in $(X^3+1)^{(p-1)/2}$ is $\binom{(p-1)/2}{(p-1)/3}$ or 0 according as $p \equiv 1 \bmod 3$ or $p \equiv 2 \bmod 3$.

This proves the first assertion since $\binom{(p-1)/2}{(p-1)/3} \not\equiv 0 \bmod p$. For the next, notice that $E : Y^2 = X^3 + X$ has $j(E) = 1728$ and, the corresponding coefficient of X^{p-1} in this case is $\binom{(p-1)/2}{(p-1)/4}$ or 0 according as $p \equiv 1 \bmod 4$ or $p \equiv 3 \bmod 4$. This proves the corollary.

As other corollaries, here are two criteria for an elliptic curve over a field of positive characteristic to be supersingular.

Corollary *Let $K = \mathbb{F}_p$. Then the elliptic curve E_λ defined by the equation $Y^2 = X(X-1)(X-\lambda)$ is supersingular if and only if $\#E_\lambda(\mathbb{F}_p) = p+1$.*
Proof: Writing $\#E_\lambda(\mathbb{F}_p) = 1 - A_p$ (where A_p is as above), E_λ is supersingular if, and only if,

$$\#E_\lambda(\mathbb{F}_p) = 1 \ \ in \ \ \mathbb{F}_p \Leftrightarrow \#E_\lambda(\mathbb{F}_p) \equiv 1(p)$$

$\Leftrightarrow \#E_\lambda(\mathbb{F}_p) = p+1$ by Hasse's theorem (Riemann hypothesis).

Corollary *E is supersingular $\Leftrightarrow$ the invariant differential w is exact.*
Proof: For $p = 2$, we can write the equation of E as $Y^2 + Y + \alpha XY = X^3$. Then, $w = \frac{dx}{1+\alpha x}$ is exact $\Leftrightarrow \alpha = 0 \Leftrightarrow E$ is $Y^2 + Y = X^3$ which is supersingular. For $p > 2$, we can write the equation of E as $Y^2 = X(X-1)(X-\lambda)$. Then $w = \frac{dx}{2y}$ is exact $\Leftrightarrow y^{p-1}\frac{dx}{y^p}$ is exact $\Leftrightarrow y^{p-1}dx$ is exact $\Leftrightarrow \{x(x-1)(x-\lambda)\}^{\frac{p-1}{2}}dx$ is exact $\Leftrightarrow$ coefficient of X^{p-1} in $\{X(X-1)(X-\lambda)\}^{\frac{p-1}{2}}$ is zero $\Leftrightarrow E$ is supersingular.

Finally, here is an interesting counting formula similar to the 'mass formula' for quadratic forms:

(Mass formula) $\frac{p-1}{24} = \sum \frac{1}{Aut(E)}$ *where the sum is over isomorphism classes of supersingular elliptic curves over a field of characteristic $p > 0$.*

8. Structure of $E(\mathbb{F}_q)$

In this final section, we discuss what possible groups can arise as groups of rational points of elliptic curves over finite fields. We prove :

Theorem *A group G of order $N = q+1-m$ is isomorphic to $E(\mathbb{F}_q)$ for some elliptic curve E over $\mathbb{F}_q$ if, and only if one of the following holds:*
(i) $(q,m) = 1, |m| \leq 2\sqrt{q}$ and $G \cong \mathbb{Z}/A \times \mathbb{Z}/B$ where $B/(A, m-2)$.
(ii) q is a square, $m = \pm 2\sqrt{q}$ and $G = (\mathbb{Z}/A)^2$ where $A = \sqrt{q} \mp 1$.

(iii) q is a square, $p \equiv 1(3), m = \pm\sqrt{q}$ and G is cyclic.
(iv) q is not a square, $p = 2$ or 3, $m = \pm\sqrt{pq}$ and G is cyclic.
(v) q is not a square, $p \not\equiv 3(4)$, $m = 0$ and G is cyclic
or q is a square, $p \not\equiv 1(4), m = 0$ and G is cyclic.
(vi) q is not a square, $p \equiv 3(4), m = 0$ and G is either cyclic or $G \cong \mathbb{Z}/M \times \mathbb{Z}/2$ where $M = \frac{q+1}{2}$.

For proving this, we shall use the following result without proof (see [TV], Theorem 2.4.30) :

Proposition *The set of isogeny classes of elliptic curves over $\mathbb{F}_q$ is in a natural bijection with the set of integers m such that $|m| \leq 2\sqrt{q}$ and one of the following holds:*
(i) $(q, m) = 1$,
(ii) q is a square and $m = \pm 2\sqrt{q}$,
(iii) q is a square, $p \not\equiv 1(3)$ and $m = \pm\sqrt{q}$,
(iv) q is not a square, $p = 2$ or 3 and $m = \pm\sqrt{pq}$
(v) q is not a square and $m = 0$ or q is a square, $p \not\equiv 1(4)$ and $m = 0$.
Moreover, $\#E(\mathbb{F}_q) = q + 1 - m$ for any curve from the isogeny class corresponding to m.

Proof of the Theorem: Firstly, let E be any elliptic curve over $\mathbb{F}_q$ and let $N = \#E(\mathbb{F}_q)$. We start with some observations which would be useful eventually even in the proof of the converse assertion that groups with properties as in (i) to (vi) of the theorem do correspond to some E over $\mathbb{F}_q$.
Now $E(\mathbb{F}_q) \subseteq E[N] \cong \mathbb{Z}/N \times \mathbb{Z}/N$ so $E(\mathbb{F}_q) \simeq \mathbb{Z}/A \times \mathbb{Z}/B$ with B/A. Let us choose a basis of $E[N] \simeq \mathbb{Z}/N \times \mathbb{Z}/N$ such that $E(\mathbb{F}_q)$ is generated by $\begin{pmatrix} A \\ 0 \end{pmatrix}$ and $\begin{pmatrix} 0 \\ B \end{pmatrix}$. Look at the Frobenius ϕ_q on $E[N]$; write the corresponding matrix in End $(E[N])$ as $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $a, b, c, d \in \mathbb{Z}/N$. Now, write $\#E(\mathbb{F}_q) = q + 1 - m$; then $m \equiv a + d \bmod N$. Also ϕ_q fixes $E(\mathbb{F}_q)$; so $aA \equiv A, dB \equiv B \bmod N$ and so $a \equiv 1, d \equiv 1 \bmod B$ since B/A.
Thus, $m - 2 \equiv a + d - 2 \equiv 0 \bmod B$ i.e., $B/(m-2)$.

Before proceeding further, let us look also at the converse assertion of the theorem. Let us look at any finite abelian group G satisfying any one of the six conditions of the theorem. We would like to show that G is isomorphic to $E(\mathbb{F}_q)$ for some E. From the fact that G is as in the theorem, it is clear that the integer m satisfies one of the conditions

of the proposition and so there is indeed some elliptic curve E' over $\mathbb{F}_q$ which is determined (uniquely upto isogeny) by m. Note that G and $E'(\mathbb{F}_q)$ have the same order N. In cases (ii) to (v) of the theorem, clearly the group is determined by its order and we immediately get $G \cong E'(\mathbb{F}_q)$. If G is as in case (i) of the theorem, we argue as follows. Consider the matrix $M' = \begin{bmatrix} m-1 & -A \\ B & 1 \end{bmatrix}$. Since $trM' \equiv m, detM' \equiv q \bmod N$ and since $(q, m) = 1$, it can be shown that M' is the matrix of the Frobenius endomorphism on some elliptic curve E over $\mathbb{F}_q$. This can be proved in a manner similar to the proof of the proposition on the structure of endomorphisms of elliptic curves. The reason for choosing the matrix M' is the following. Note that

$$M' \begin{pmatrix} A \\ 0 \end{pmatrix} = \begin{pmatrix} m-1 & -A \\ B & 1 \end{pmatrix} \begin{pmatrix} A \\ 0 \end{pmatrix} \equiv \begin{pmatrix} (m-1)A \\ 0 \end{pmatrix} \equiv \begin{pmatrix} A \\ 0 \end{pmatrix} \quad mod \quad N.$$

The last congruence is due to the fact that $B/(m-2)$ as we are in case (i). Similarly,

$$M' \begin{pmatrix} 0 \\ B \end{pmatrix} \equiv \begin{pmatrix} 0 \\ B \end{pmatrix} \quad mod \quad N.$$

As G is generated by these two elements, we have the fact that $M'g \equiv g \bmod N$ i.e., $G \subseteq E(\mathbb{F}_q)$ as M' is the Frobenius corresponding to E. As both groups have the same order N, it follows that $G \cong E(\mathbb{F}_q)$.
If G is as in case (vi), we argue as follows. Given a prime $p \equiv 3 \bmod 4$ and an odd power q of p, we want to find elliptic curves E, E' over $\mathbb{F}_q$ such that $E(\mathbb{F}_q) \cong \mathbb{Z}/(q+1)$ and $E'(\mathbb{F}_q) \cong \mathbb{Z}/(\frac{q+1}{2}) \times \mathbb{Z}/2$. To do this, it suffices to prove :
(a) for any E with $E(\mathbb{F}_q)$ cyclic, there is an isogeny $\theta : E \to E'$ of degree 2 such that $E'(\mathbb{F}_q)$ is not cyclic and
(b) for any E' over $\mathbb{F}_q$ with $E'(\mathbb{F}_q) \supseteq \mathbb{Z}/2 \times \mathbb{Z}/2$, there is an isogeny $\theta : E' \to E$ such that $E(\mathbb{F}_q)$ is cyclic.
Suppose E is as in (a). Then, since $E[4] \cap E(\mathbb{F}_q)$ is also cyclic, it has a generator v, say. Then, one can write $E[2]$ as $\{0, 2v, e, f = e + 2v\}$. Thus, $E[2] \not\subseteq E(\mathbb{F}_q)$, the Frobenius of E permutes e and f. Consider the isogeny $\theta : E \to E'$ whose kernel is generated by $2v$. Therefore, the Frobenius of E' preserves $\theta(v)$ and $\theta(e) = \theta(f)$ which gives $E'[2](\mathbb{F}_q) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. In other words, $E'(\mathbb{F}_q)$ is not cyclic.
Conversely, let E' be as in (b). Since $E'(\mathbb{F}_q) \subseteq \mathbb{Z}/2 \times \mathbb{Z}/N$, we have that $E'[4](\mathbb{F}_q) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$ or $E'[4](\mathbb{F}_q) \cong \mathbb{Z}/2 \times \mathbb{Z}/4$. In the former case, any isogeny $E' \to E$ of degree 2 has the property that $E(\mathbb{F}_q)$ is cyclic. In the

latter case, let us write $E'[4](\mathbb{F}_q) =< u, v >\cong \mathbb{Z}/2 \times \mathbb{Z}/4$. Considering the isogeny $\theta : E' \to E$ of degree 2 whose kernel is generated by $u + 2v$, it follows that $E(\mathbb{F}_q)$ is cyclic. This completes the proof that in all cases that any group G as in the theorem can be realized as $E(\mathbb{F}_q)$ for some E over $\mathbb{F}_q$.

Let us now turn to the proof of the assertion that if E is any elliptic curve over $\mathbb{F}_q$, the group $E(\mathbb{F}_q)$ satisfies one of the six conditions of the theorem. We shall argue according to the case of the proposition that the corresponding m, q satisfy.
If m, q are as in case (i) of the proposition, we have already shown at the beginning of our proof that we have the properties asserted in case (i) of the theorem.
Suppose now that we are in case (ii) of the proposition. The corresponding matrix M for the Frobenius homomorphism can be shown without too much difficulty to be a scalar matrix. Let us write $q = p^{2r}$. Then, $m = \pm 2p^r$ and $E(\mathbf{F}_q)$ has order $N = (p^r \mp 1)^2$. Therefore, if A, B are the elementary divisors of $E(\mathbf{F}_q)$ where $B|A$, then $AB = N$, $M = \pm \begin{pmatrix} p^r & 0 \\ 0 & p^r \end{pmatrix}$ and $M \begin{pmatrix} A \\ 0 \end{pmatrix} \equiv \begin{pmatrix} A \\ 0 \end{pmatrix}$ and $M \begin{pmatrix} 0 \\ B \end{pmatrix} \equiv \begin{pmatrix} 0 \\ B \end{pmatrix}$ modulo $N = (p^r \mp 1)^2$. This gives us that both $A \equiv B \equiv 0 \bmod p^r \mp 1$. As $AB = N = (p^r \mp 1)^2$, this gives $A = B = p^r \mp 1$. We have case (ii) of the theorem.
If we are in case (iii) of the proposition, then $q = N + 1 - m \equiv 1 \bmod B$ as $m \equiv 2 \bmod B$. But, we have $q = m^2 \equiv 4 \bmod B$ i.e., $B = 1$ or $B = 3$. If we had $B = 3$, then we would have $m \equiv 2, 5$ or $8 \bmod 9$ and so $q \equiv 4, 7$ or $1 \bmod 9$ respectively. Thus, we would have $N = q + 1 - m \equiv 3 \bmod 9$ which contradicts the fact that $B^2|N$. Therefore, $B = 1$ and so $E(\mathbb{F}_q)$ is cyclic i.e., we have case (iii) of the theorem.
If m, q are as in case (iv) of the proposition, we have
either

$$p = 2, \;\; m \equiv 2 \bmod B, \;\; N, B \text{ odd}, \;\; 2q = m^2 \equiv 4, \;\; q \equiv 2, \;\; N \equiv 1 \bmod B$$

or

$$p = 3, \;\; (B, 3) = 1, \;\; m \equiv 2, \;\; 3q = m^2 \equiv 4, \;\; 3N \equiv 1 \bmod B.$$

In either case, it is obviously forced that $B = 1$.
In case (v) of the proposition, we have $m = 0$ and so $0 \equiv 2 \bmod B$ gives $B = 1$ or $B = 2$. If $B = 1$ we have case (v) of the theorem and if $B = 2$, then $4|N$ and we have case (vi).
This completes the proof of the theorem.

References

[*NS*] D.S. Nagaraj and B. Sury, *A Quick Introduction to Algebraic Geometry and Elliptic Curves*, this volume.

[*S*] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer-Verlag, New York 1986.

[*TV*] M. Tsfasman and S. Vladut, *Algebraic geometric codes*, Mathematics and its applications Vol. **58**, Kluwer Academic Publishing Group 1991.

Stat-Math Unit, Indian Statistical Institute, Bangalore 560 059, India.

E-mail address: sury@isibang.ac.in