An Introduction to Supersingular Elliptic Curves and Supersingular Primes

Anh Huynh

Abstract

In this article, we introduce supersingular elliptic curves over a finite field and relevant concepts, such as formal group of an elliptic curve, Frobenius maps, etc. The definition of a supersingular curve is given as any one of the five equivalences by Deuring. The exposition follows Silverman's "Arithmetic of Elliptic Curves." Then we define supersingular primes of an elliptic curve and explain Elkies's result that there are infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. We further define supersingular primes as by Ogg and discuss the Monstrous Moonshine conjecture.

1 Supersingular Curves.

1.1 Endomorphism ring of an elliptic curve.

We have often seen elliptic curves over $\mathbb{C}$, where it has many connections with modular forms and modular curves. It is also possible and useful to consider the elliptic curves over other fields, for instance, finite fields. One of the difference we find, then, is that the number of symmetries of the curves are drastically improved. To make that precise, let us first consider the following natural relation between elliptic curves.

Definition 1. *Let E_1, E_2 be elliptic curves. An isogeny from E_1 to E_2 is a morphism*

$$\phi: E_1 \to E_2$$

such that $\phi(O) = O$.

Then we can look at the set of isogenies from an elliptic curve to itself, and this is what is meant by the symmetries of the curves.

Definition 2. *Let E be an elliptic curve. Let $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ be the ring of isogenies with pointwise addition*

$$(\phi + \psi)(P) = \phi(P) + \psi(P)$$

and multiplication given by composition

$$(\phi\psi)(P) = \phi(\psi(P)).$$

Then $\mathrm{End}(E)$ *is called the endomorphism ring of* E.

1.2 Classification of the endomorphism rings.

The first question we can ask is what kind of ring can this endomorphism ring be. The following objects are needed in the formulation of the answer.

Definition 3. *(Order of an algebra) Let* $\mathcal{K}$ *be an algebra finitely generated over* $\mathbb{Q}$. *An order* $\mathcal{R}$ *of* $\mathcal{K}$ *is a subring of* $\mathcal{K}$ *which is finitely generated as* $\mathbb{Z}$*-module and which satisfies* $\mathcal{R} \otimes \mathbb{Q} = \mathcal{K}$.

Example 4. Let $\mathcal{K}$ be the quadratic imaginary field $\mathbb{Q}\big(\sqrt{-D}\big)$ for some positive D, $\mathcal{O}$ its ring of integers. Then for each integer $f > 0$, the ring $\mathbb{Z} + f\mathcal{O}$ is an order of $\mathcal{K}$.

Definition 5. *A (definite) quaternion algebra over* $\mathbb{Q}$ *is an algebra of the form*

$$\mathcal{K} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

with the multiplication rules $\alpha^2, \beta^2 \in \mathbb{Q}, \alpha^2 < 0, \beta^2 < 0, \beta\alpha = -\alpha\beta$.

Then we have the following theorem.

Theorem 6. *(Classification of endomorphism ring) The endomorphism ring of an elliptic curve is either* $\mathbb{Z}$ *(rank 1), an order in a quadratic imaginary field* $\mathbb{Q}\big(\sqrt{-D}\big)$ *(rank 2), or an order in a quaternion algebra (rank 4).*

(See Silvermans's "Arithmetic of the Elliptic Curves" , Chapter III, Section 9 for a proof.)

If $\mathrm{char}(K) = 0$, then $\mathrm{End}(E) \otimes \mathbb{Q}$ cannot be a quaternion algebra (see remark to Theorem 12). For example, in class all we have seen so far are elliptic curves over $\mathbb{C}$, so they only have endomorphism ring as $\mathbb{Z}$ or an order in a quadratic imaginary field.

Example 7. The curve $\mathbb{C}/\mathbb{Z}[i]$ has endomorphism ring $\mathbb{Z}[i]$. The curve $\mathbb{C}/\mathbb{Z}[\sqrt{-2}]$ has endomorphism ring $\mathbb{Z}$.

If K is a finite field, however, then $\mathrm{End}(E)$ is always larger than $\mathbb{Z}$. In fact, the particular class of elliptic curves that have endomorphism ring as an order in a quarternion algebra (the maximum possible) are called supersingular elliptic curves, the main object of this exposition.

1.3 Definition of a supersingular curve.

As alluded to before, a supersingular elliptic curve is one that has the maximum number of symmetries: $\mathrm{End}(E)$ is an order in the quaternion algebra. In his 1941 paper, Deuring proved the equivalence of this and four other conditions, therefore each of which can then be considered as a definition for a supersingular curve. The main goal of this section is to state the theorem. We will need the following objects.

Definition 8. *Let R be a ring. A (one-parameter commutative) formal group $\mathcal{F}$ defined over R is a power series $F(X,Y) \in R[[X,Y]]$ satisfying:*

a) $F(X,Y) = X + Y +$ *(terms of degree* ≥ 2*).*
b) $F(X,F(Y,Z)) = F(F(X,Y),Z)$.
c) $F(X,Y) = F(Y,X)$
d) There is a unique power series $i(T) \in R[[T]]$ *such that* $F(T,i(T)) = 0$.
e) $F(X,0) = X, F(0,Y) = Y$.

In particular, for an elliptic curve E given by a Weierstrass equation with coefficients in R,

$$E\colon y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

the formal group associated to E, denoted by $\hat{E}$, is given by the power series

$$F(z_1,z_2) = z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) - (2a_3z_1^3z_2 - (a_1a_2 - 3a_3)z_1^2z_2^2 + 2a_3z_1z_2^3) + \ldots \in \mathbb{Z}[a_1,\ldots,a_6][[z_1,z_2]].$$

Definition 9. *Let R be a ring of characteristic $p > 0$. Let $\mathcal{F}, \mathcal{G}/R$ be formal groups and $f\colon \mathcal{F} \to \mathcal{G}$ a homomorphism defined over R. The height of f, denoted by* $\mathrm{ht}(f)$*, is the largest integer h such that $f(T) = g\big(T^{p^h}\big)$ for some power series $g(T) \in R[[T]]$. If $f = 0$ then* $\mathrm{ht}(f) = \infty$*. The height of $\mathcal{F}$, denoted* $\mathrm{ht}(\mathcal{F})$*, is the height of the multiplication map $[p]\colon \mathcal{F} \to \mathcal{F}$.*

Example 10. If $m \geq 1$ is prime to p, then $\mathrm{ht}([m]) = 0$, because $[m]T = mT + \ldots$.

Definition 11. *(Frobenius map) Let K be a field of positive charateristic p, and let $q = p^r$. Let $f^{(q)}$ be the polynomial obtained from f by raising each coefficient of f to the q-th power. Then for each curve C/K we can define a new curve $C^{(q)}/K$ by describing its homogeneous ideal as*

$$I\big(C^{(q)}\big) = \textit{ideal generated by } \big\{f^{(q)}\colon f \in I(C)\big\}.$$

The q-th power Frobenius morphism is the natural map from C to $C^{(q)}$ given by

$$\phi\colon C \to C^{(q)}$$

$$\phi([x_0,\ldots,x_n]) = [x_0^q,\ldots,x_n^q].$$

Definition 12. *Let $\phi\colon C_1 \to C_2$ be a map of curves defined over K. If ϕ is constant, we define the degree of ϕ to be 0; otherwise we say that ϕ is finite and define its degree by*

$$\deg \phi = [K(C_1)\colon \phi^* K(C_2)].$$

We say that ϕ is separable, inseparable, purely inseparable if the extension $K(C_1)/\phi^* K(C_2)$ has the corresponding property.

In particular, the Frobenius map is inseparable. Now we can state Deuring's theorem.

Theorem 13. *(Deuring) Let K be a perfect field of characteristic p and E/K an elliptic curve. For each integer $r \geq 1$, let*

$$\phi_r\colon E \to E^{(p^r)} \text{ and } \hat{\phi_r}\colon E^{(p^r)} \to E$$

be the p^r-th power Frobenius map and its dual.

a) The following are equivalent.
- *i. $E[p^r] = 0$ for one (all) $r \geq 1$.*
- *ii. $\hat{\phi_r}$ is (purely) inseparable for one (all) $r \geq 1$.*
- *iii. The map $[p]\colon E \to E$ is purely inseparable and $j(E) \in \mathbb{F}_{p^2}$.*
- *iv. $\mathrm{End}(E)$ is an order in a quaternion algebra.*
- *v. The formal group $\hat{E}/K$ associated to E has height 2.*

b) If the equivalent conditions in (a) do not hold, then

$$E[p^r] = \mathbb{Z}/p^r\mathbb{Z} \text{ for all } r \geq 1,$$

and the formal group $\hat{E}/K$ has height 1. Further, if $j(E) \in \bar{\mathbb{F}}_p$, then $\mathrm{End}(E)$ is an order in a quadratic imaginary field.
(See Silverman's "Arithmetic of Elliptic Curves" Chapter V, Section 3 for a proof.)

Remark 14.
1. There are further definitions, for instance in terms of sheaf cohomology and residues of differentials.
2. Note that a supersingular curve is not singular. By definition it is an elliptic curve, hence smooth.
3. Item (ii) explains what we claimed above that $\mathrm{End}(E)$ cannot be an order in a quaternion algebra if the curve over a $\mathbb{C}$: for a field to possess a non-trivial purely inseparable extension, it cannot be perfect.

An example of a supersingular elliptic curve is the curve $X_1(11)$, reduced modulo the prime 19. (See Section 2.1).

2 Supersingular Primes.

Closely related to the concept of a supersingular elliptic curve is that of a supersingular prime. There are two different definitions, each refer to a different thing.

2.1 Supersingular Primes for an elliptic curve over $\mathbb{Q}$.

Definition 15. *(Supersingular primes for an elliptic curve) If E is an elliptic curve defined over the rational numbers, then a prime p is supersingular for E if the reduction of E modulo p is a supersingular elliptic curve over the residue field $\mathbb{F}_p$.*

In his 1987 paper, Elkies shows that there are infinitely many such primes for each elliptic curve over $\mathbb{Q}$. The idea is as follow. The reduction E_p of an elliptic curve E at a good prime p is supersingular if and only if it has complex multiplication by some order $O_D = \mathbb{Z}\big[\frac{1}{2}\big(D+\sqrt{-D}\big)\big]$ $(D \equiv 0 \text{ or } 3 \bmod 4)$, such that p is ramified or inert in $\mathbb{Q}\big(\sqrt{-D}\big)$.

Note that for each D, however, there are only finitely many isomorphism classes of elliptic curves over $\bar{\mathbb{Q}}$ with complex multiplication by O_D. Furthermore, the j-invariants of these curves are conjugate algebraic integers. Thus, we can define $P_D(X)$ to be the monic integer polynomial with these j-invariants as roots. Then it makes sense to consider $P_D(X)$ in characteristic p. One of the important results in Deuring's 1941 paper is the following.

Lemma 16. *(Deuring's Lifting Lemma) Let A_0 be an elliptic curve in characteristic p, with an endomorphism α_0 which is not trivial. Then there exists an elliptic curve A defined over a number field, an endomorphism α of A, and a non-degenerate reduction of A at a place $\mathfrak{P}$ lying above p such that A_0 is isomorphic to $\bar{A}$, and α_0 corresponds to $\bar{\alpha}$ under the isomorphism.*

For a proof, see Chapter 13, Section 5 of Lang's "Elliptic Function." By the above lemma, roots of $P_D(X)$ in characteristic p are j-invariants of elliptic curves with endomorphism $\frac{1}{2}\big(D+\sqrt{-D}\big)$. This means, suppose J is the value of the j-invariant of E, then if J is a root of $P_D(X)$ modulo p, E_p will have complex multiplication in $O_{D'}$ where D' is a factor of D such that D/D' is a perfect square. The criterion is useful because prime factors of $P_D(J)$ are related to D (and J) in a quite definite way, so once we have chosen a nice enough p, the choice of D that satisfies the above condition is in fact very clear. Infinitude is in fact a consequence of the powerful Dirichlet's theorem that there are infinitely many primes in the progression $ax+b$ where a, b are coprime.

Example 17. Take the curve $X_1(11)$, whose j-invariant is $-2^{12}/11$, and let $D = 163$. Then

$$P_{163}(J) = J - j\Big(\tfrac{1+\sqrt{-163}}{2}\Big) = 2^{12}19^2 1953065174759/11.$$

The primes 19 and 1953065174759 are quadratic non-residues of 163, hence primes of supersingular reduction of E.

Theorem 18. *(Elkies) Let S be a finite set of primes. Then E has a supersingular prime outside S.*

PROOF. We can assume without loss of generality that S contains all of E's primes of bad reduction. By Dirichlet's Theorem, there is a prime l (and always one that is big enough), such that $(-1/l) = -1$, $(p/l) = +1$ for every $p \in S$. In fact, use the progression $\big(\prod_{p\in S} p\big)x + 1$, or $2\big(\prod_{p\in S} p\big)x + 1$ if $2 \notin S$.

The only real roots of P_l and P_{4l} are $j\big(\frac{1}{2}\big(1+\sqrt{-l}\big)\big)$ and $j\big(\sqrt{-l}\big)$, respectively; all others are in complex conjugate pairs. From the q-expansion $j(z)=e^{-2\pi iz}+O(1)$ as $\mathrm{Im}(z)\to\infty$, it follows that these real roots go to $-\infty$ and ∞ as $l\to\infty$. Therefore for a fixed J, we can choose a big enough l such that $P_l(J)>0$ and $P_{4l}(J)<0$.

Then, suppose $P_l(J)P_{4l}(J)=-\frac{|N|}{D}$. Here D is a perfect square, being the (deg P_lP_{4l})-th power of J's denominator. We claim that N contains a either l itself or a prime that is a quadratic non-residue of l. Either way, we have a supersingular prime of E outside of S.

Suppose otherwise, then N is the product of primes all of which are quadratic residues of l, and thus N itself is a quadratic residue of l. Thus $P_l(J)P_{4l}(J)=-\frac{|N|}{D}$ is a quadratic non-residue of l. We reach a contradiction by the following technical fact/lemma.

Lemma 19. *Modulo l, $P_l(X)$ and $P_{4l}(X)$ factor into $(X-1728)R^2(X)$, $(X-1728)S^2(X)$ for some polynomials $R(X), S(X)$.* □

As a direct corollary, there are infinitely many supersingular primes for every elliptic curve over $\mathbb{Q}$. Then it is natural to ask how these primes are distributed (for a specific curve E). In 1976, Lang and Trotter gave a conjecture on the number of supersingular primes less than a bound x. Remember that we need the prime p to be ramified or inert in the field of complex multiplication, and this happens roughly half of the times by Dirichlet's theorem. So the trace of E_p to be distributed roughly evenly in the permitted range $\big(-2p^{1/2}, 2p^{1/2}\big)$, and therefore vanish with probability $Cp^{-1/2}$. Thus there are about $C\sum_{p<x}p^{-1/2}\sim 2Cx^{1/2}/\log x$ supersingular primes less than x. As of 2010, this conjecture is open.

2.2 Supersingular primes and the Monstrous Moonshine conjectures.

For completeness, we include the second definition.

Definition 20. *(Supersingular primes) The following are equivalent (by Ogg) and can be taken as a definition:*

a) The modular curve $X_0^+(p)=X_0(p)/wp$, where wp is the Fricke involution of $X_0(p)$, has genus zero.
b) Every supersingular elliptic curve in characteristic p can be defined over the prime subfield $\mathbb{F}_p$.
c) The order of the Monster group M is divisible by p.

In fact they are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 47, 59, and 71.

These supersingular primes are not referred to with any elliptic curves. The equivalences, although proved by Ogg (by direct computation), were not well understood until Borcherd's 1992 paper "Monstrous Moonshine and Monstrous Lie Superalgebras." Ogg's paper was the starting point of the Monstrous Moonshine conjecture about the strange relations between the Monster group M and modular functions. The conjecture states that there is a unique infinite-dimensional graded M-module whose graded dimensions are the Fourier coefficients of the q-expansion of the j-function:

$$V = \bigoplus_{m \geq -1} V_m$$

such that $\dim V_m = c_m$, where

$$j(\tau) = \sum_{m \geq -1} c_m q^m.$$

References

R. Borcherds, Monstrous Moonshine and Monstrous Lie Superalgebras, Invent. Math. **109** (1992), 405-444.

M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkorper, *Math. Zeut,* **47** (1941), 47-56.

N. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over Q, *Invent. Math.* **89** (1987), 561-568.

T. Gannon, Monstrous Moonshine: The first twenty-five years, 2004, http://arxiv.org/PS_cache/math/pdf/0402/0402345v2.pdf

S. Lang, Elliptic Functions. New York: Springer-Verlag (1986). Print.

S. Lang; H. Trotter, Frobenius distributions in GL_2-extensions. Lect. Notes in Math., vol. 504. Berlin-Heidelberg-New York: Springer 1976. Print.

A.P. Ogg, Automorphismes des Courbes Modulaires, Seminair Delange-Pisot, Poitou. Theorie des nombres, **7** (1974), 1-8

J. Silverman, Arithmetic of Elliptic Curves. New York: Springer-Verlag (1986). Print.