1 Characterization of Supersingular Elliptic Curves

Let $E/\mathbb{Q}$ be an elliptic curve which has complex multiplication by an order $\mathcal{O}$ in a quadratic imaginary field, say k. That is, $\mathrm{End}(E) \cong \mathcal{O} \subseteq \mathcal{O}_k$ where $\mathcal{O}_k$ is the ring of integers of k. Let p be a prime and always assume that E has a good reduction at p. We denote the reduced curve by $\tilde{E}_p$, or by $\tilde{E}$ when p is clear from the context. By definition, $\tilde{E}$ is supersingular if $\mathrm{End}(\tilde{E})$ is an order in a quaternion algebra. Now, let π be the p-power Frobenius map, and if ϕ is an isogeny between elliptic curves denote the dual of ϕ by $\hat{\phi}$. Then one can show that the following are equivalent ([Sil], Theorem 3.1)

1. $\mathrm{End}(\tilde{E})$ is an order in a quaternion algebra.
2. $\tilde{E}[p^r] = 0$ for all $r \geq 1$.
3. $\hat{\pi}$ is purely inseparable.

Fixing the notation as above we will prove that

Theorem 1.1. *(Theorem 12, p.182, [Ser]) $\tilde{E}_p$ is supersingular if and only if p ramifies or remains prime in k.*

First we prove another characterization for supersingular elliptic curves.

Lemma 1.2. *Let $E/\mathbb{F}_p$ be an elliptic curve and $\#E(\mathbb{F}_p) = p + 1 - t$. Then E is supersingular if and only if $t \equiv 0 \pmod{p}$.*

Proof. First note that if ϕ is any endomorphism of E the it is a zero of the polynomial

$$\begin{aligned} f_\phi(X) &= (X - \phi)(X - \hat{\phi}) \\ &= X^2 - (\phi + \hat{\phi})X + \phi \circ \hat{\phi} \end{aligned}$$

Note that $\deg(1 - \phi) = f([1]) = [1] - (\phi + \hat{\phi}) + [\deg(\phi)]$ and so for some integer t_ϕ we can rewrite the polynomial of ϕ as

$$f_\phi(X) = X^2 - ([t_\phi])X + [\deg(\phi)]$$

where $[t_\phi] = \phi + \hat{\phi}$. In particular, for the Frobenious endomorphism we obtain

$$f_\pi(X) = X^2 - ([t_\pi])X + [p]$$

where $[t_\pi] = \pi + \hat{\pi}$. Now, using Corollary 5.5 in [Sil] gives

$$\begin{aligned} E \text{ is supersingular} &\Leftrightarrow \hat{\pi} \text{ is purely inseparable} \\ &\Leftrightarrow [t_\pi] - \pi \text{ is purely inseparable} \\ &\Leftrightarrow t_\pi \equiv 0 \pmod{p}. \end{aligned}$$

Finally, note that $[\#E(\mathbb{F}_p)] = [\deg_s(1-\pi)] = [\deg(1-\pi)] = f_\pi([1]) = [p+1-t_\pi]$, that is $t = t_\pi$ and we are done. □

Lemma 1.3. *Let ϕ be an isogeny from $E_1/\mathbb{Q}$ to $E_2/\mathbb{Q}$. Let p be a prime and suppose that E_1 and E_2 have good reduction modulo p, say $\tilde{E}_1$ and $\tilde{E}_2$. Then $\tilde{E}_1$ is supersingular if and only if $\tilde{E}_2$ is supersingular.*

Proof. We first prove that if $\tilde{E}_2$ is supersingular then $\tilde{E}_1$ is supersingular. Let $\tilde{\phi}$ be the isogeny from $\tilde{E}_1$ to $\tilde{E}_2$ obtained by reducing ϕ modulo p. Suppose that $\tilde{E}_1$ is not supersingular. Then there exists a nontrivial point of order p on $\tilde{E}_1$, say P. If $\tilde{\phi}(P) \neq O$ then $Q := \tilde{\phi}(P)$ is a nontrivial point of order p on $\tilde{E}_2$ and E_2 so is not supersingular. If $\tilde{\phi}(P) = O$ for all such points P on $\tilde{E}_1$ then $p \mid \deg_s \tilde{\phi} = \deg_s \hat{\tilde{\phi}} = \#\hat{\tilde{\phi}}^{-1}(O)$. That is, there exists $O \neq Q$ on $\tilde{E}_2$ such that $pQ = O$ and so $\tilde{E}_2$ is not supersingular. We can argue similarly as above by considering the dual isogeny $\hat{\tilde{\phi}}$ and prove the converse. □

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication $\mathcal{O} \subseteq \mathcal{O}_k$. It is possible to find an isogeny $\phi : E \to E'$ such that $\mathrm{End}(E') \cong \mathcal{O}_k$ ([Koh], [Galb]). Assuming that E and E' have good reduction at some prime p, $\tilde{E}_p$ is supersingular if and only if $\tilde{E'}_p$ is supersingular by Lemma 1.3. So we can restate Theorem 1.1 as

Theorem 1.4. *Let $E/\mathbb{Q}$ be an elliptic curve which has complex multiplication by the maximal order $\mathcal{O}_k$ in a quadratic imaginary field k. Suppose that E has a good reduction at prime p. Then $\tilde{E}_p$ is supersingular if and only if p ramifies or remains prime in k.*

Proof. Suppose first that p remains prime in k. Let $\mathrm{End}(\tilde{E}) \cong \mathcal{O}$ for some order $\mathcal{O}$ in k and let $\theta : \mathcal{O} \to \mathrm{End}(\tilde{E})$ be the corresponding isomorphism. Take $\alpha \in \mathcal{O}$ such that $\theta(\alpha) = \pi$ is the p-power Frobenius map. The characteristic polynomial of π gives $\theta(\alpha) \circ \widehat{\theta(\alpha)} = [p]$. Now, setting $\widehat{\theta(\alpha)} = \theta(\beta)$ we get $\alpha\beta = p$. That is, α is an element in $\mathcal{O}$ with norm p (note that α and β are nonunits). However, we observe that if $\mathcal{O}_k$ is the maximal order in k and p remains prime in k then $\mathcal{O}_k$ cannot contain any element of order p as otherwise if a is an element of order p with its conjugate a' then $aa' = p$

and $p\mathcal{O}_k = \mathfrak{a}\mathfrak{a}'$, contradiction. Hence, $\mathcal{O}$ must be an order in a quaternion algebra and so $\tilde{E}$ is supersingular.

Now, suppose p ramifies in $k = \mathbb{Q}(\sqrt{d})$. Then $p = \mathfrak{p}\mathfrak{p} = \langle p, \sqrt{d}\rangle^2$. If α is the element in the order $\mathcal{O} \cong \mathrm{End}(\tilde{E})$ which corresponds to π then the norm of α is p and so $\mathfrak{p} =< \alpha >$. Then $\pi + \hat{\pi} = \mathrm{trace}(\alpha) = mp$ for some integer m and by Lemma 1.2, $\tilde{E}$ is supersingular.

Next assuming that p splits in k we prove $\tilde{E}$ contains a nontrivial point of order p, that is $\tilde{E}$ is not supersingular. First note that there is a unique isomorphism $\theta : \mathcal{O}_k \to \mathrm{End}(E)$ such that for any invariant differential w on E we have $\theta(\alpha)^* w = \alpha w$ for all $\alpha \in \mathcal{O}_k$ (p.97, [Sil2]). Let $p\mathcal{O}_k = \mathfrak{p}\mathfrak{p}'$. Choose an integer m such that $\mathfrak{p}^m = \mu\mathcal{O}_k$ and $\mathfrak{p}'^m = \mu'\mathcal{O}_k$. If θ is a as above and w is a differential such that its reduction modulo p, say $\tilde{w}$, is not zero then $\widetilde{\theta(\mu')}^* \tilde{w} = \tilde{\mu'}\tilde{w} \neq 0$ as $\mu' \notin \mathfrak{p}$, and so $\widetilde{\theta(\mu')}$ is separable (Proposition 4.2, p.35, [Sil]). On the other hand, since $\mu\mu' = p^m$ we have $\theta(\mu)\theta(\mu') = [p^m]$, that is $\theta(\mu')$ has degree a power of p and so $\widetilde{\theta(\mu')}$ has degree a power of p. Finally, since $\widetilde{\theta(\mu')}$ is separable, we conclude that $p \mid \deg_s(\widetilde{\theta(\mu')})$ and $\tilde{E}$ has a nontrivial point of order p. □

References

[Galb] S. Galbraith, Constructing isogenies betweeen elliptic curves Over Finite Fields, London Math. Soc., Journal of Computational Mathematics, Vol. 2, p. 118-138 (1999).

[Koh] D. Kohel, Endomorphism rings of elliptic curves over finite fields, Berkeley PhD thesis, (1996).

[Ser] S. Lang, Elliptic Functions, Springer- Verlag, (1987).

[Sil] J. H. Silverman, The Arithmetic of Elliptic Curves, Springer-Verlag, (1986).

[Sil2] J. H. Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Springer- Verlag, (1994).