Lecture 10

Jose Capco (jcapco@risc.jku.at)

In the last lecture, we gave the rule of addition for points on an elliptic curve. However, there were no examples. We give one here

Example 1. Let $K = \mathbb{F}_5$ and $E : y^3 = x^3 + x + 1$. We check if E is an elliptic curve

$$\Delta_E = 4a^3 + 27b^2 = 4 + 2 = 1 \bmod 5$$

So E is an elliptic curve over $\mathbb{F}_5$. We can even count the points of $E = E(\mathbb{F}_5)$. The points (α, β) on E should satisfy $\alpha^3 + \alpha + 1$ is a quadratic residue modulo 5. We note that the quadratic residue mod 5 are the numbers $\{0, 1, -1\}$ mod 5 and their square roots are $\{0, \pm 1, \pm 2\}$ mod 5. Now we compute all $\alpha \in \mathbb{F}_5$ such that $f(\alpha) \in \{0, 1, -1\}$, where $f(x) = x^3 + x + 1$. We see that

$$f(\pm 2) = f(0) = 1,\ f(-1) = -1 \quad \text{and } f(\alpha) \neq 0 \forall \alpha \in K$$

So the points of E are

$$\{O, (0,1), (0,-1), (2,1), (-2,1), (2,-1), (-2,-1), (-1,2), (-1,-2)\}$$

Finally let us compute, for $P = (0, 1)$ and $Q = (2, -1)$, the point $P + Q$ for the group structure of E.
We see that $x_P \neq x_Q$ so we can compute the slope

$$\mu = \frac{y_Q - y_P}{x_Q - x_P} = \frac{-1 - 1 \bmod 5}{2 - 0 \bmod 5} = -1 \bmod 5$$

Thus

$$x_{P+Q} = \mu^2 - x_P - x_Q = 1 - 0 - 2 = -1 \bmod 5$$
$$y_{P+Q} = -y_P - \mu(x_{P+Q} - x_P) = -1 - (-1)(-1 - 0) = -2 \bmod 5$$

So $P + Q = (-1, -2)$

Recall that in the last lecture we wrote isogenies $\phi(x, y) = (R_1(x, y), R_2(x, y))$ for rational functions R_1 and R_2 and we then conclude we can write $R_1(x, y) = r_1(x)$ and $R_2(x, y) = yr_2(x)$ for rational functions r_1 and r_2. Furthermore we wrote $r_1 = p/q$ for polynomials p and q. With this convention we are able to define the *degree* of an isogeny.

Definition.

- We also define the *degree* of an isogeny ϕ to be

$$\deg \phi := \max\{\deg p, \deg q\}$$

  if $\phi \not\equiv O$ and if $\phi \equiv O$ then define $\deg(\phi) = 0$. We also say that ϕ is *separable* if $r_1'(x) \not\equiv 0$ i.e. if p' or q' is not 0 (see the exercise of the last lecture).

- We denote the set of all isogenies from E_1 to E_2 by $\mathrm{Hom}(E_1, E_2)$ and the set of all endomorphism of an elliptic curve E as $\mathrm{End}(E)$.

We may need a lot of machinery (commutative algebra) to prove the facts below, so we will take them for granted

Remark 2.

a.) The definition for degree and separability of isogeny comes from a characterization of separability and degree of the pullback of the function fields $\phi^* : K(E_2) \hookrightarrow K(E_1)$. Thus, in particular, if we have two isogenies $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_3$ then

$$\deg(\psi \circ \phi) = (\deg \psi)(\deg \phi)$$

b.) A non-constant isogeny $\phi : E_1 \to E_2$ is a surjective map.

Example 3. Consider the duplication map of the last example. We compute the degree of this map

$$R_1(x, y) = \left(\frac{3x^2 + a}{2y}\right)^2 - 2x \quad \Rightarrow \quad r_1(x) = \frac{x^4 - 2ax^2 - 8bx + a^2}{4(x^3 + ax + b)}$$

One checks that the numerator and denominator do not have common zero in E, so $\deg \phi = 4$. Furthermore, we see that $q'(x) = 4(3x^2 + a) \not\equiv 0$ (check this also for $\operatorname{char} K = 3$!) which means that ϕ is separable.

Notation. We have seen the duplication endomorphism $\phi : E(\bar{K}) \to E(\bar{K})$, this is often denoted as

$$[2] : E(\bar{K}) \to E(\bar{K})$$

and can clearly be restricted to a morphism $E \to E$. We can also talk about endomorphisms that are n-multiples of points in E (for any $n \in \mathbb{Z}$) and this is similarly denoted $[n]$.

Exercise 1. Given an elliptic curve $E : y^2 = x^3 + ax + b$ over K with $\operatorname{char} K \nmid 6$, show that $\deg[n] = n^2$

Henceforth, unless otherwise stated, $\operatorname{char} K \neq 2$. Also, starting from the Theorem below, since we treat $\operatorname{Hom}(E_1, E_2)$ as a $\mathbb{Z}$-module, when we write $m\phi$ for an isogeny ϕ and a number m, we actually mean $[m] \circ \phi$ ($[m]$ defined in the endomorphism ring of the codomain of ϕ).

Theorem 4. Let E, E_1, E_2 be elliptic curves over K then

a.) $\operatorname{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module.

b.) The endomorphism ring $\operatorname{End}(E)$ has no zero-divisors and is of characteristic 0.

c.) The map $\operatorname{End}(E) \times \operatorname{End}(E) \to \mathbb{Z}$ defined by

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

is $\mathbb{Z}$-bilinear i.e. we have the identity

$$\deg(m\phi + n\psi) = m^2 \deg \phi + n^2 \deg \psi + mn(\deg(\phi + \psi) - \deg \phi - \deg \psi)$$

for all $\phi, \psi \in \operatorname{End}(E)$ and $m, n \in \mathbb{Z}$

d.) Let $K = \mathbb{F}_p$ and $m, n \in \mathbb{Z}$ such that $(m, n) \neq (0, 0)$ then $m\phi_p + n$ is separable iff $p \nmid n$.

Partial Proof. We will only partially prove the above theorem

a.) Clearly $\operatorname{Hom}(E_1, E_2)$ is $\mathbb{Z}$-module i.e. $(\phi + \psi)(P) = \phi(P) + \psi(P)$ and $n\phi = [n] \circ \phi$ (where $[n]$ is in $\operatorname{End}(E_2)$. From the exercise we learn that $[n] \in \operatorname{End}(E_2)$ is non-constant for all non-zero $n \in \mathbb{Z}$. Consider now $[n] \circ \phi$ for some non-trivial $\phi \in \operatorname{Hom}(E_1, E_2)$ and $n \neq 0$, then if $[n] \circ \phi = [0]$ we get

$$\deg([n] \circ \phi) = \deg[n] \deg \phi = 0$$

which implies that $n = 0$ and this is a contradiction.

b.) Since End(E) is torsion-free it has characteristic zero i.e. $[n]\phi \neq 0$ for non-trivial n and ϕ. Moreover, if $\phi \circ \psi = [0]$ we get

$$\deg(\phi \circ \psi) = \deg \phi \deg \psi = 0$$

and this implies that ϕ or ψ is $[0]$.

c.) We just prove the identity assuming $\mathbb{Z}$-bilinearity. We get

$$\deg(m\phi + n\psi) - \deg(m\psi) - \deg(n\phi) = mn(\deg(\psi + \phi) - \deg \psi - \deg \phi)$$

so

$$\deg(m\phi + n\psi) = \deg(m\psi) + \deg(n\phi) + mn(\deg(\psi + \phi) - \deg \psi - \deg \phi)$$

But

$$\deg(m\phi) = \deg([m]) \deg \phi = m^2 \deg \phi$$

and similarly $\deg(n\psi) = n^2 \deg \psi$, so we obtain the result.

□

Studying endomorphism of elliptic curve has several applications, one of which is the proof of Hasse's theorem which gives a bound to the number of points in an elliptic curve over a finite field. There is a weaker statement to Hasse's theorem that we can immediately prove:

Proposition 5. Let $E : y^2 = f(x)$ be an elliptic curve over a finite field $\mathbb{F}_p$, where p is a prime number greater than 3, then

$$\#E = p + 1 + \sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right)_L$$

Proof. The solutions in $E\backslash\{O\}$ of $y^2 = f(x)$ is given by the numbers of x such that $f(x)$ is a quadratic residue mod p. The Legendre symbol evaluates to $0, 1, -1$ respectively for $1, 2, 0$ solutions to $y^2 = f(x)$. Thus

$$\#(E\backslash\{O\}) = \sum_{x=0}^{p-1} \left(\left(\frac{f(x)}{p} \right)_L + 1 \right) = p + \sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right)_L$$

the desired result follows after adding O. □

We however want to prove a more general result, namely

Hasse's Theorem. Let $E : y^2 = f(x)$ be an elliptic curve over a finite field $\mathbb{F}_p$, then $\#E$ is in the interval

$$[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$$

We will use isogenies to prove this. For this we need ...

Proposition 6. Let $\phi \neq 0$ be a non-trivial separable isogeny, then[1]

$$\deg \phi = \# \ker(\phi)$$

Proof. We assume $\phi : E_1 \to E_2$ and $E_1 : y^2 = f_1(x)$ and $E_2 : y^2 = f_2(x)$. For points in $E_1(\bar{K})\backslash\{O_1\}$, let $\phi(x, y) = (r_1(x), yr_2(x))$ with $r_1 = p/q$ for some $p, q \in K[x]$ with no non-constant common factor. Since ϕ is separable we get $r_1' \not\equiv 0$, so $pq' - p'q \not\equiv 0$.

[1] in fact, non-constant isogenies are finite maps, i.e. the preimage of a point is finite

Let S be the set of zeros of $q(pq' - p'q)$ in $\bar{K}$. We first show that we can choose an $(\alpha, \beta) \in E_2(\bar{K})\backslash\{O_2\}$ such that

1. $\alpha \neq 0$ and $\beta \neq 0$.
2. $\deg(p(x) - \alpha q(x)) = \deg \phi = \max\{\deg p, \deg q\}$
3. $\alpha \notin r_1(S)$
4. $(\alpha, \beta) \in \phi(E_1(\bar{K}))\backslash\{O_2\}$

This (α, β) exists because

- $p'q - pq'$ is not identical to 0, thus it has only finite zeros, thus $r_1(S)$ is also finite
- There are only finitely many $\alpha \in \overline{K^*}$ that $\deg \phi > \deg(p(x) - \alpha q(x))$
- We can thus arbitrarily choose an element in $\alpha \in r_1(\bar{K}) \cap \bar{K}^*$ ($\bar{K}^*$ is infinite!) such that $\deg \phi = \deg(p(x) - \alpha q(x))$ and is neither in $r_1(S)$ nor a zero of f_2
- Since $f_2(\alpha) \neq 0$, $\beta \neq 0$.

We claim that for this $(\alpha, \beta) \in \phi(E_1(\bar{K})$ we have

$$\#\phi^{-1}(\alpha, \beta) = \deg \phi$$

Suppose $\phi(\alpha_1, \beta_1) = (\alpha, \beta)$ i.e.

$$\alpha = \frac{p(\alpha_1)}{q(\alpha_1)} \qquad \beta_1 r_2(\alpha_1) = \beta$$

Since the $(\alpha, \beta) \neq O_2$, we must have $q(\alpha_1) \neq 0$ (see Exercise). Furthermore, since $\beta \neq 0$, we can write $\beta_1 = \beta / r_2(\alpha_1)$. Thus β_1 is determined by α_1 and we need only count the α_1 in the preimage. By our assumption on (α, β), we just need to show that $p - \alpha q$ does not have multiple roots.

Suppose, by contradiction, that $p - \alpha q$ has multiple roots. In other words, we assume that there is an $\alpha_0 \in \bar{K}$ such that

$$p(\alpha_0) - \alpha q(\alpha_0) = 0 \qquad p'(\alpha_0) - \alpha q'(\alpha_0) = 0$$

This yields

$$\alpha p(\alpha_0) q'(\alpha_0) = \alpha q(\alpha_0) p'(\alpha_0)$$

But this implies that $\alpha_0 \in S$ and so $\alpha = r(\alpha_0) \in r(S)$ which is a contradiction. □