Summer School on Elliptic and Hyperelliptic Curve Cryptography
Exercises for lectures on Wednesday, 17.09.2008

Maps on elliptic curves

[MEC1] Why is $[m]$ a morphism?
Can you represent it as a rational map?

[MEC2] Suppose E is defined over $\mathbb{F}_q$, and let π_E be the q-power Frobenius map on E (defined by $(x, y) \mapsto (x^q, y^q)$ and $P_\infty \mapsto P_\infty$). Show that $[m]$ and π_E commute – that is, that $[m]\pi_E = \pi_E[m]$.

Some extra information:

If E is an elliptic curve over k defined by

$$E : y^2 = f(x) = (x^2 + b_1x + b_0)(x - a),$$

then the point $(a, 0)$ has order 2 in $E(k)$, and generates a subgroup $S = \langle(a, 0)\rangle = \{(a, 0), 0_E\}$. The quotient isogeny $\phi : E \to F = E/S$ is defined by

$$F = E/S : y^2 = x^3 + -(4a + 2b_1)x^2 + (b_1^2 - 4b_0)x$$

and

$$\phi(x, y) = \left(\frac{x^3 - (a - b_1)x^2 - (b_1a - b_0)x - b_0a}{x - a}, \frac{(x^2 - 2ax - (b_1a + b_0))y}{(x - a)^2}\right).$$

[MEC3] (If you like abstract stuff)
If E and F are elliptic curves over k, then we write $E \sim F$ if there exists an isogeny $E \to F$. Why does $\sim$ define an equivalence relation on the set of all elliptic curves over k?

[MEC3] (If you like drawing)
Consider the curve $E : y^2 = (x - 4)(x - 1)(x + 1)$ over $\mathbb{Q}$. $E(\mathbb{Q})$ has Mordell-Weil rank 1, and torsion subgroup $(\mathbb{Z}/2\mathbb{Z})^2$, generated by any two of the points $P_1 = (1, 0)$, $P_2 = (-1, 0)$, and $P_3 = (4, 0)$. The free part of $E(\mathbb{Q})$ is generated by the point $Q = (0, 2)$.

a) Plot the curve E.
b) Plot some of the rational points of E: a few multiples of Q, and a few linear combinations of Q and the P_i.
c) Compute the quotient $\phi : E \to F = E/\langle P_i\rangle$ for one of the P_i.
d) Plot the curve F.
e) Plot the images of the points you calculated in step 2 under the isogeny you calculated in step 3.

[MEC3] Let E be defined over $\mathbb{F}_q$. Show that the q-th power Frobenius is in fact an endomorphism, i.e. show that $\pi(x, y) \in E$ and that $\pi(P + Q) = \pi(P) + \pi(Q)$.

Fast arithmetic on elliptic curves

[FEC1] Explain a 3**M** algorithm for clock addition; a 2**M** algorithm for clock doubling; and a 3**S** algorithm for clock doubling.

[FEC2] Explain a $9\mathbf{M} + 1\mathbf{S} + 1\mathbf{D}$ algorithm for addition on the Edwards curve $x^2 + y^2 = 1 + dx^2y^2$, using $(X : Y : Z)$ to represent the point $(Z/X, Z/Y)$. Don't worry about completeness; your algorithm is permitted to ignore a few exceptional points.

[FEC3] Find an explicit birational equivalence between the Edwards curve $x^2+y^2 = 1+dx^2y^2$ and the (twisted) Jacobi quartic $u^2 = dx^4 - (1 + d)x^2 + 1$.
Use the birational equivalence to figure out an addition law for the Jacobi quartic with neutral element $(0, 1)$.
Is your addition law complete?

[FEC4] Let P be a point on an elliptic curve E defined over $\mathbb{F}_p$, with $p > 3$. Show that we can compute the x-coordinate of $P+Q$ provided we know the $+x$-coordinates of P, Q, and $P - Q$.

Point counting

[PC1] Let q be a prime power and let $f(x) \in \mathbb{F}_q[x]$.

a) Show that $\gcd(x^q-x, f(x))$ is non-trivial if and only if f has at least one $\mathbb{F}_q$-rational root.

b) Show that $\gcd(x^q - x, f(x))$ equals

$$\prod_{\substack{a\in\mathbb{F}_q \\ f(a)=0}} (x - a).$$

[PC2] Let $E : Y^2 = X^3 + 2X + 1$ over $\mathbb{F}_5$.

a) Check whether E is an elliptic curve.

b) The point $P = (3, 2)$ is on E. Compute in affine coordinates $[5]P$.

c) State all points on E over $\mathbb{F}_5$.

[PC3] Let $q = p^r$ with $p > 3$. Let (x, y) be a point on $Y^2 = X^3 + AX + B$. Show that y^p can be expressed as $h(x)y$ with some polynomial $h(x) \in \mathbb{F}_q[x]$ using the curve equation.