Solutions: Isogeny-based crypto

PQCrypto Summer School 2017

July 3, 2017

1. Define
$$E/\mathbb{Q} : y^2 = x^3 + 1.$$

   (a) The line passing through $(-1, 0)$ and $(0, 1)$ is defined by $L : y = x+1$. To find the third point of intersection between L and E we plug L into E:
$$(x+1)^2 = x^3 + 1 \Leftrightarrow 0 = x^3 - x^2 - 2x = x(x+1)(x-2).$$
   So the third point in $L \cap E$ has x coordinate 2 and y coordinate $2 + 1 = 3$. Therefore
$$(-1, 0) + (0, 1) = -(2, 3) = (2, -3).$$

   (b) To compute the tangent line at the point $(0, 1)$ we need to compute the gradient of E at this point, so we first differentiate E with respect to y, giving
$$2y\frac{dy}{dx} = 3x^2.$$
   Therefore, at $(0, 1)$ the tangent to E has gradient $\frac{dy}{dx} = 0$, so the equation of the line is given by
$$L : x = 0.$$
   By plugging L into E we now see that the unique second intersection point of L with E is $(0, -1)$, hence
$$2(0, 1) = (0, -1).$$

   (c) Clearly $(0, 1) \neq \infty$ and by (b), we have that $2(0, 1) = (0, -1) \neq \infty$ so $n > 2$. Now
$$3(0, 1) = 2(0, 1) + (0, 1) = (0, 1) + (0, -1) = \infty,$$
   hence $n = 3$.

2. Define

$$E/\mathbb{F}_{17} : y^2 = x^3 + 1$$

and

$$E'/\mathbb{F}_{17} : y^2 = x^3 - 10.$$

(This was a typo in the problem sheet).

(a) Define

$$f : (x, y) \mapsto ((x^3 + 4)/x^2, (x^3 y - 8y)/x^3).$$

We want to show that $f : E \to E'$, or equivalently, that if

$$x' = (x^3 + 4)/x^2, \tag{1}$$

$$y' = (x^3 y - 8y)/x^3, \tag{2}$$

and

$$y^2 \equiv x^3 + 1 \bmod 17, \tag{3}$$

then

$$(y')^2 \equiv (x')^3 - 10 \bmod 17.$$

So assume (1), (2), and (3). Then

$$\begin{aligned}
(y')^2 + 10 &= (y^2(x^3 - 8)^2 + 10x^6)/x^6 && \text{by (2)} \\
&\equiv ((x^3 + 1)(x^3 - 8)^2 + 10x^6)/x^6 \bmod 17 && \text{by (3)} \\
&\equiv (x^9 + 12x^6 + 48x^3 + 64)/x^6 \bmod 17 \\
&\equiv (x')^3 \bmod 17 && \text{by (1)}.
\end{aligned}$$

(b) We claim that the points in the preimage of $(3, 0)$ are

$$\{(0, -1), (2, 3), (2, -3).\}$$

Any point (x, y) in the preimage of $(3, 0)$ under f must satisfy

$$x^3 y - 8y \equiv 0 \bmod 17,$$

so either $y \equiv 0 \bmod 17$ or $x^3 \equiv 8 \bmod 17$. There is a unique point in $E(\mathbb{F}_{17})$ with $y \equiv 0$ given by $P_1 = (-1, 0)$, and there are exactly 2 points in $E(\mathbb{F}_{17})$ with $x^3 \equiv 8$ given by $P_2 = (2, 3)$ and $P_3 = (2, -3)$. Hence the preimage of $(3, 0)$ under f is given by

$$\{P_i \in \{P_1, P_2, P_3\} : f(P_i) = (3, 0)\}.$$

Now

$$\begin{aligned}
f(P_1) &= (((-1)^3 + 4)/(-1)^2, 0) && = (3, 0) \\
f(P_2) &= ((2^3 + 4)/2^2, (2^3 \cdot 3 - 8 \cdot 3)/2^3) && = (3, 0) \\
f(P_3) &= ((2^3 + 4)/2^2, (2^3 \cdot (-3) - 8 \cdot (-3))/2^3) && = (3, 0),
\end{aligned}$$

and hence our claim holds.

(c) In the slides we saw that for an elliptic curve defined by $E : y^2 = x^3 + ax + b$, the j-invariant is given by

$$j(E) = 1728 \frac{4a^3}{4a^3 + 27b^2}.$$

For both E and E' we have $a = 0$, and hence

$$j(E) = j(E') = 0.$$

(d) To see that E and E' are isomorphic over $\mathbb{F}_{17^2}$, we first observe that $\left(\frac{-10}{17}\right) = -1$ and hence $\mathbb{F}_{17^2} \cong \mathbb{F}_{17}(\sqrt{-10})$. We then claim that the map

$$f : (x, y) \to (-3x, \sqrt{-10}y),$$

defined over $\mathbb{F}_{17}(\sqrt{-10})$, is an isomorphism $E' \to E$. To see this, we divide the equation for E' by -10:

$$E' : \frac{y^2}{-10} = \frac{x^3}{-10} + 1,$$

and then apply f:

$$f(E') : \frac{-10y^2}{-10} = \frac{(-3x)^3}{-10} + 1,$$

which is the equation for E. So f defines a map $E' \to E$. Similarly,

$$g : (x, y) \mapsto ((-3)^{-1}x, (\sqrt{-10}^{-1}y)$$

defines a map $E \to E'$, and $f \circ g = g \circ f = \text{id}$, so E and E' are isomorphic over $\mathbb{F}_{17^2}$.
It remains to show that E and E' are not isomorphic over $\mathbb{F}_{17}$. Given the material from the lecture, the only viable way to check is by brute force: write every invertible rational map over $\mathbb{F}_{17}$ and check that none of them work (using a computer)!
Here is a nicer way; the following is Theorem III.3.1(b) in 'Rational Points on Elliptic Curves' by Silverman and Tate:

Theorem. *Let k be a field and E, E' elliptic curves over k. Every isomorphism from E to E' defined over $\overline{k}$ restricts to an affine isomorphism of the form*

$$\phi(x, y) = (u^2x + r, u^3y + su^2x + t)$$

where $u, r, s, t \in \overline{k}$. The isomorphism is defined over k if and only if $u, r, s, t \in k$.

Observe further that as our elliptic curves are all of the form $y^2 = x^3 + ax + b$, we must always have that $s = t = 0$. We proceed by attempting to compute u and r in our case. Any $\mathbb{F}_{17}$-isomorphism from E to E' must also define an isomorphism of groups

$$E(\mathbb{F}_{17}) \to E'(\mathbb{F}_{17}),$$

so that in particular, a point of order n will be sent to a point of order n. We compute that the set of $E(\mathbb{F}_{17})$-points of order 2 is given by

$$E^{(2)} := \{(16, 0)\},$$

the set of $E(\mathbb{F}_{17})$-points of order 3 is given by

$$E^{(3)} := \{(0, 1), (0, 16)\},$$

the set of $E'(\mathbb{F}_{17})$-points of order 2 is given by

$$(E')^{(2)} := \{(3, 0)\},$$

and the set of $E'(\mathbb{F}_{17})$-points of order 3 is given by

$$(E')^{(3)} := \{(5, 8), (5, 9)\}.$$

Suppose that we have an isomorphism $E \to E'$ defined by

$$\phi : (x, y) \mapsto (u^2x + r, u^3y).$$

Then as $\phi : E^{(3)} \to (E')^{(3)}$, we conclude that $r = 5$ and $u = \pm 2$. But then

$$\phi : (16, 0) \mapsto (-4 + 5, 0),$$

so ϕ does not map $E^{(2)} \to (E')^{(2)}$, which is a contradiction.

3. As ℓ is a prime, every size ℓ subgroup of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ is isomorphic to the cyclic group $\mathbb{Z}/\ell\mathbb{Z}$. Furthermore, every element of

$$\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$$

except for $(0, 0)$ generates a cyclic group of order ℓ, and each non-zero element of such a cyclic group $G \cong \mathbb{Z}/\ell\mathbb{Z}$ generates G. Hence, the number of distinct size ℓ subgroups of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$ is given by

$$\frac{\#(\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}) - 1}{\#(\mathbb{Z}/\ell\mathbb{Z})^\times} = \frac{\ell^2 - 1}{\ell - 1} = \ell + 1.$$

From the lectures we know that for an elliptic curve $E/\mathbb{F}_q$ and a prime ℓ such that $\ell \neq p$, the ℓ-torsion of E is

$$E[\ell] \cong \mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}.$$

We also know that for every size ℓ subgroup $G \subset E[\ell]$, there exists an elliptic curve E' and a separable isogeny $\varphi : E \to E'$ with $\ker(\varphi) = G$, giving us $\ell + 1$ degree ℓ isogenies from E from the $\ell + 1$ size ℓ subgroups of $\mathbb{Z}/\ell\mathbb{Z} \times \mathbb{Z}/\ell\mathbb{Z}$.

4. For a point P on en elliptic curve, write φ_P for the isogeny with kernel $\langle P \rangle$. It suffices to show that

$$(E/\langle A \rangle)/\langle \varphi_A(B) \rangle = (E/\langle B \rangle)/\langle \varphi_B(A) \rangle = E/\langle A, B \rangle,$$

as we then get a commutative diagram

$$\begin{array}{ccc} E & \xrightarrow{\varphi_B} & E/\langle B \rangle \\ {\scriptstyle \varphi_A}\downarrow & & \downarrow{\scriptstyle \varphi_{\varphi_B(A)}} \\ E/\langle A \rangle & \xrightarrow[\varphi_{\varphi_A(B)}]{} & E/\langle A, B \rangle. \end{array}$$

Observe that A and B have coprime orders, so that $B \notin \langle A \rangle$ and $A \notin \langle B \rangle$. In particular, the image $B + \langle A \rangle$ of B under φ_A is a point of $E/\langle A \rangle$ of the same order as B. Define Λ by

$$E/\Lambda = (E/\langle A \rangle)/\langle \phi_A(B) \rangle = (E/\langle A \rangle)/\langle B + \langle A \rangle \rangle.$$

Then clearly

$$\Lambda \subseteq \langle A, B \rangle,$$

and as $B + \langle A \rangle$ has the same order as B, the cardinalities are the same, hence

$$\Lambda = \langle A, B \rangle.$$