THE UNIVERSITY OF SYDNEY
MATH3925 PUBLIC KEY CRYPTOGRAPHY

Semester 2 **Exercises for Week 11** 2004

Let E be an elliptic curve of the form

$$E : y^2 = x^3 + ax + b.$$

1. The multiplication-by-n maps $[n]$ on an elliptic curve E with equation as above is defined by simple recursive formulas for the coordinates. The maps $[n] : E \to E$ take the form

$$P = (x, y) \longmapsto nP = \left(\frac{\phi_n(x)}{\psi_n(x, y)^2}, \frac{\omega_n(x, y)}{\psi_n(x, y)^3}\right).$$

For polynomials $\phi_n(x)$, $\psi_n(x, y)$, and $\omega_n(x, y)$. This means that the n-th multiple of a point on E is given by the evaluation of the polynomial expressions for the image coordiantes at the point coordinates.

The polynomials $\psi_n(x, y)$ are of crucial importance since they are zero precisely on the points of $E[n] = \ker([n])$. They can be defined by the recursions:

$$\begin{aligned}
&\psi_0 = 0 \quad \psi_1 = 1 \quad \psi_2 = 2y \\
&\psi_3 = 3x^4 + 6ax^2 + 12bx - a^2 \\
&\psi_4 = \psi_2 \cdot (2x^6 + 10ax^4 + 40bx^3 - 10a^2x^2 - 8abx - (2a^3 - 16b^2)) \\
&\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad (m \geq 2), \\
&\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)/\psi_2 \quad (m > 2).
\end{aligned}$$

Moreover the polynomials ϕ_n are determined by $\phi_0 = 1$ and

$$\phi_n = x\psi_n^2 - \psi_{n+1}\psi_{n-1}$$

for all $n \geq 1$.

a. Use the relation $y^2 = x^3 + ax + b$ to show that $\psi_n(x, y)^2$ can be expressed as a polynomial in x.

b. Show that this multiplication by 2 determines the addition law in the case $P_1 = P_2$ not covered by the addition formula, and compute $2P_1$ and $2P_2$. How can the group law be extended to the case $x_1 = x_2$ but $y_1 \neq y_2$?

c. Let E be the elliptic curve $y^2 = x^3 + x + 3$ over $\mathbb{F}_{61}$, having 55 elements. Use the above recursion to construct the polynomial $\psi_5(x)$. Find two roots x_1 and x_2 of this polynomial and verify that they determine 5-torsion points $(x_1, \pm y_1)$ and $(x_2, \pm y_2)$.

2. Let $E/\mathbb{F}_q$ be an elliptic curve and $P \in E(\mathbb{F}_q)$ be a point of prime order n. The n-torsion group $E[n]$ is defined to be

$$E[n] = \{Q \in E(\overline{\mathbb{F}}_q) \,:\, nQ = O\}.$$

Assume the structure theorem for the n-torsion group $E[n]$, which states that if $(n,p) = 1$ then

$$E[n] \cong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z},$$

and if $n = p$ then $E[n] \cong \mathbb{Z}/n\mathbb{Z}$ or $E[n] \cong \{O\}$.

a. Show that there exists a finite extension $\mathbb{F}_{q^r}$, and a point $Q \in E(\mathbb{F}_{q^r})$ such that $E[n] = \langle P, Q\rangle$.

b. For the elliptic curve $E/\mathbb{F}_{61}$ of the previous exercise with 5-torsion point $P = (x_1, y_1) \in E(\mathbb{F}_{61})$, find an extension $\mathbb{F}_{61^r}$ and a point $Q \in E(\mathbb{F}_{61^r})$ generating the 5-torsion subgroup.

3. In this exercise we investigate the conditions under which an elliptic curve can have a very large n-torsion subgroup $E[n]$ contained in the set of points $E(\mathbb{F}_{p^2})$.

a. Recall that the Frobenius endomorphism π, defined by $\pi(x,y) = (x^p, y^p)$, is a homomorphism of $E(\overline{\mathbb{F}}_p)$ to itself. For each r show that

$$E(\mathbb{F}_{p^r}) = \ker(\pi^r - 1).$$

b. Make use of the fact that $|E(\mathbb{F}_{p^r})|$ equals $p^r - t_r + 1$ where $\pi^{2r} - t_r\pi^r + p^r = 0$. If $|E(\mathbb{F}_p)| = p - t + 1$, then show that $|E(\mathbb{F}_{p^2})| = p^2 - (t^2 - 2p) + 1$.

c. Suppose that n is a prime greater than $4\sqrt{p}$. Show that if n divides $|E(\mathbb{F}_p)|$ and n^2 divides $|E(\mathbb{F}_{p^2})|$ then $t = 0$.

d. Show that if $t = 0$ then $|E(\mathbb{F}_{p^2})| = (p+1)^2$, and prove moreover that

$$E(\mathbb{F}_{p^2}) = E[p+1] \cong \mathbb{Z}/(p+1)\mathbb{Z} \times \mathbb{Z}/(p+1)\mathbb{Z}.$$

Hint: Show that $\pi^2 = p$ and recall that $\ker(\pi^r - 1) = E(\mathbb{F}_{p^r})$.

An elliptic curve over a field of characteristic p such that $t \equiv 0 \bmod p$ is called *supersingular*. The complement of these curves are *ordinary* elliptic curves.