Summer School on Elliptic and Hyperelliptic Curve Cryptography
Exercises for lectures on Wednesday, 13.09.2006

Odd-elliptic-curves exercises :–)

[OEC1] Compute the 31st multiple of $(1,7)$ on the elliptic curve $y^2 = x^3 - 3x$ over $\mathbb{Z}/17$. Can you also figure out the order of $(1,7)$?

[OEC2] Montgomery gave fast recursive formulas for computing the x-coordinates of nP and $(n+1)P$ from the x-coordinate of a point P on an elliptic curve of the form $y^2 = x^3 + ax^2 + x$. What if you also want the y-coordinate of nP? Express $Y(nP)$ generically as a rational function of $a, X(P), Y(P), X(nP), X((n+1)P)$.

Even-elliptic-curves exercise

[EEC1] Show that an elliptic curve of the form $y^2 = x^3 + a_2x^2 + a_4x + a_6$ over $\mathbb{F}_{2^n}$ is singular.

[EEC2] Show that an elliptic curve of the form $y^2 + a_3y = x^3 + a_2x^2 + a_4x + a_6, a_3 \in \mathbb{F}_{2^n}^*, a_2, a_4, a_6 \in \mathbb{F}_{2^n}$ is non-singular. Show that such elliptic curves are supersingular.
Hint: use the criterion on the 2-torsion.
Show also that there is only one isomorphism class of supersingular curves over $\bar{\mathbb{F}}_2$.

[EEC3] Check how to find the correct y-value for repeated doublings, consult i.e. the Handbook of Elliptic and Hyperelliptic Curve Cryptography.

[EEC4] Let $E : y^2 + (a_3x + a_1)y = x^3 + a_2x^2 + a_4x + a_6$ be an elliptic curve over $\mathbb{F}_2$ and consider it over an extension field $\mathbb{F}_{2^n}$.

(a) Show that if $P = (x_P, y_P) \in E(\mathbb{F}_{2^n})$ then also $\mathcal{F}_2(P) = (x_P^2, y_P^2) \in E(\mathbb{F}_{2^n})$.

(b) For $E : y^2 + y = x^3 + 1$ compute $|E(\mathbb{F}_2)|, |E(\mathbb{F}_{2^2})|, |E(\mathbb{F}_{2^3})|, |E(\mathbb{F}_{2^n})|$.

(c) Show how to compute the τ-adic representation of a number on $E : y^2 + xy = x^3 + 1$, i.e. find the characteristic polynomial and show how to compute the next coefficient. How can this representation be shortened.

(d) Do the same for $E : y^2 = x^3 + x^2 - 1$ for $E/\mathbb{F}_3$ considered over $\mathbb{F}_{3^n}$.

(e) Compute all extension degrees n between 160 and 240 so that $|E_a(\mathbb{F}_{2^n})|$ is almost prime where
$$E_a : y^2 + xy = x^3 + ax^2 + 1, \; a \in \mathbb{F}_2.$$

Point-counting exercises

[PC1] Let p be prime, and let a be an integer. Give an algorithm to compute the Legrende symbol $(\frac{a}{p}) \in \{-1, 0, 1\}$.

[PC2] Let p be an odd prime that is congruent to 2 mod 3. For $b \in \mathbb{F}_p^*$, define the elliptic curve $E_b : Y^2 = X^3 + b$. Prove that E_b has exactly $p+1$ points over $\mathbb{F}_p$.

[PC3] Let $p \geq 5$ be prime, and let $E : Y^2 = X^3 + aX + b$ be an elliptic curve over $\mathbb{F}_p$. Prove that $\#E(\mathbb{F}_p)$ is even if and only if the polynomial $X^3 + aX + b \in \mathbb{F}_p[X]$ has a root in $\mathbb{F}_p$.

[PC4] Pronounce the name Schoof in a way that Reinier is happy.
Hint: Reinier also likes beer.

CM1 exercises

[CM1] Let z be an element of the upper half plane $\mathbf{H}$, and let G be the subgroup of $\mathrm{SL}_2(\mathbb{Z})$ generated by $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. The group G acts on $\mathbf{H}$ by linear fractional transformations.

(a) Let $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element of G. Prove that we have $\mathrm{Im}(Az) = \mathrm{Im}(z)/|cz+d|^2$.

(b) Prove that there exists $B \in G$ such that $\mathrm{Im}(Bz)$ is maximal.

(c) Prove that there exists $C \in G$ such that $z' = CBz$ has real part between $-\frac{1}{2}$ and $\frac{1}{2}$, where B is as in part (b).

(d) Prove that the element $z' \in \mathbf{H}$ from part (c) lies in

$$\Big\{\tau \in \mathbf{H} \mid (\mathrm{Re}(\tau) \in [-\frac{1}{2}, \frac{1}{2}),\, |\tau| > 1) \quad \text{or} \quad (|\tau| = 1 \text{ and } \mathrm{Re}(\tau) \in [-\frac{1}{2}, 0]\Big\}.$$

[CM2] Let $\Lambda \subset \mathbb{C}$ be a lattice. The elliptic curve $\mathbb{C}/\Lambda$ can be given by the Weierstraß equation $E : Y^2 = 4X^3 - g_2(\Lambda)X - g_3(\Lambda)$. Prove that we have

$$j(E) = 1728 \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27 g_3(\Lambda)^2} \in \mathbb{C}.$$