Summer School on Elliptic and Hyperelliptic Curve Cryptography

Exercises for lectures on Monday, 03.09.2007

1. Let $E/\mathbb{Q}$ be the elliptic curve given by $E : y^2 = x^3 + 17$. Note that the following points are in $E(\mathbb{Q})$ (or check it yourself):

   $$P_1 = (-2, 3), P_2 = (-1, 4), P_3 = (2, 5), P_4 = (4, 9), P_5 = (8, 23).$$

   Verify the following relations:

   $$P_5 = [-2]P_1, P_4 = P_1 \ominus P_3.$$

2. Let E be an elliptic curve defined over $\mathbb{F}_2$. Show that $\sigma(x_0, y_0) = (x_0^2, y_0^2)$ is a point on E if $(x_0, y_0) \in E$ and show that $\sigma(P \oplus Q) = \sigma(P) \oplus \sigma(Q)$.

3. Let f be a polynomial over a field k. Define $g = \gcd\{f, f'\}$. Prove that $\deg g = 0$ if and only if f is square-free.

4. Let $\mathrm{Char}(k) \neq 2$. We have seen that every elliptic curve is isomorphic to one of the form $y^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6$. Give a condition on f so that E is non-singular. (Hint: use the previous exercise).

5. Let $f \in k[x]$ split as $f(x) = (x - a_1)(x - a_2) \cdots (x - a_n)$ over $\bar{k}$. The *discriminant* of f is given by $\mathrm{disc}(f) = \prod_{1 \leq i < j \leq n}(a_i - a_j)^2$. The relation with elliptic curves is: $\mathrm{disc}(f) \neq 0 \Leftrightarrow f$ has only simple roots $\Leftrightarrow E : y^2 = f(x)$ is elliptic curve.

   Compute the discriminant of $f(x) = x^3 + x^2 + bx$.

6. Use the Baby-Step Giant-Step algorithm and/or Pollard's rho algorithm to compute the discrete logarithm of 15 to the base $g = 2$ in the multiplicative group of the finite field $\mathbb{F}_{239}$.

7. Use the Pohlig-Hellman algorithm to compute the discrete logarithm of 2 to the base of 3 in the multiplicative group of $\mathbb{F}_{65537}$. (Hint $65536 = 2^{16}$).

8. Consider $C : y^2 = x^5 + 4x^3 + 3x^2 + 11x + 5$ over $\mathbb{F}_{17}$. Find at least one divisor class defined over $\mathbb{F}_{17}$ where the representative has two affine points.

9. Show by direct computation that for $g = 2$ each class can be represented with at most 2 affine points, i.e. start with a degree zero divisor of arbitrary length and show how to reduce it.