Summer School on Elliptic and Hyperelliptic Curve Cryptography
Exercises for lectures on Monday, 15.09.2008

Alice, Bob, and finite fields exercises

[ABF1] Let $(G, \oplus)$ be a finite commutative group of order $|G| = n$ with neutral element O.

a) Show that for all $P \in G$ one has $[n]P = O$.

b) Show that for all $P \in G$ one has $\mathrm{ord}(P)|n$.

[ABF2] 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 $\mathbb{F}_{239}$.

[ABF3] 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 $65536 = 2^{16}$).

[ABF4] Let $q = p^r$ be a power of an odd prime. Let $f \in \mathbb{F}_q[x]$ be monic of degree 5. Give a complete study of the factorization patterns and the field extensions over which f factors completely.

[ABF5] Fix a nonzero element a of $\mathbb{F}_q$. How many 7th roots does a have in $\mathbb{F}_q$? Prove that there are 7 if $q \bmod 7 = 1$ and $a^{(q-1)/7} = 1$; 0 if $q \bmod 7 = 1$ and $a^{(q-1)/7} \neq 1$; and 1 if $q \bmod 7 \neq 1$.
In the last case give a formula for the 7-th root. (Hint: Use Euclid's algorithm to compute $\gcd\{x^q - x, x^7 - a\}$. If you're bored, write down three different proofs.)

[ABF6] Let $q = p^r$. Under which conditions on n and p^r can there exist irreducible binomials $x^n - a$ for some value a?

a) For which n do there exist irreducible binomials of degree n over $\mathbb{F}_{2^r}$?

b) For which q do there exist irreducible binomials of degree 7 over $\mathbb{F}_q$?

Edwards curve exercises

[EC1] a) Assume that $x_1, y_1, x_2, y_2 \in \mathbb{R}$ satisfy $x_1^2 + y_1^2 = 1$ and $x_2^2 + y_2^2 = 1$. Define

$$(x_3, y_3) = (x_1y_2 + y_1x_2, y_1y_2 - x_1x_2).$$

Prove that $x_3^2 + y_3^2 = 1$. In other words, the clock addition law defines a binary operation on $\mathrm{Clock}(\mathbb{R})$.

b) Prove that $\mathrm{Clock}(\mathbb{R})$ is a group under clock addition. In particular, prove that the clock addition law is associative.

[EC2] Assume that A is an algorithm that quickly computes discrete logs in $\mathbb{F}_{q^2}^*$. Explain how to use A to quickly compute discrete logs in $\mathrm{Clock}(\mathbb{F}_q)$. Is it enough for A to quickly compute discrete logs in $\mathbb{F}_q^*$?

[EC3] a) Assume that $x_1, y_1, x_2, y_2 \in \mathbb{R}$ satisfy $x_1^2+y_1^2 = 1-30x_1^2y_1^2$ and $x_2^2+y_2^2 = 1-30x_1^2y_1^2$. Define

$$(x_3, y_3) = \left(\frac{x_1y_2 + y_1x_2}{1 - 30x_1x_2y_1y_2}, \frac{y_1y_2 - x_1x_2}{1 + 30x_1x_2y_1y_2}\right).$$

Prove that $x_3^2+y_3^2 = 1-30x_3^2y_3^2$. In other words, the Edwards addition law defines a binary operation on the Edwards curve $x^2 + y^2 = 1 - 30x^2y^2$.

b) Prove that the Edwards curve is a group under the Edwards addition law. In particular, prove that the Edwards addition law is associative. You are permitted, and advised, to use a computer-algebra system to help with the calculations.

Scalar-multiplication exercise

[SM1] Regarding the 2^k-ary scalar multiplication method:

a) Show that it is sufficient to precompute the odd multiples of P: $[3]P, \ldots, [2^k-1]P$

b) Given k, what is the complexity of the 2^k-ary method?

c) Is there a similar generalization of the right-to-left binary method?

[SM2] Show that the density of the NAF_w is $\frac{1}{w+1}$.
Hint: Evaluate the average number of bits eliminated at each step in the algorithm computing the NAF_w.