Summer School on Elliptic and Hyperelliptic Curve Cryptography
Exercises for lectures on Monday, 11.09.2006

If you need a computer algebra system we recommend to use magma. There is an online calculator at
`http://magma.maths.usyd.edu.au/calc/`

Finite-field exercises

Exercises F1–F5 analyze several strategies for factoring a nonzero polynomial f in one variable over a finite field k. Each strategy chooses a polynomial h, computes $g = \gcd\{f, h\}$, and factors f as the product of g and f/g, which can then be factored recursively. Of course, the recursion makes progress only if $0 < \deg g < \deg f$.
Each exercise starts with the following hypotheses:
q is a prime power; $\mathbb{F}_q$ is your favorite field of size q; and $f \in \mathbb{F}_q[x]$ is a nonzero polynomial.

[FF1] Define $g = \gcd\{f, f'\}$. Prove that $\deg g = 0$ if and only if f is square-free.

[FF2] Define $g = \gcd\{f, f'\}$. Prove that if $\deg g = \deg f$ and $f = \sum_i f_i x^i$ then $f = (\sum_i f_{iq} x^i)^q$.

[FF3] Define $g = \gcd\{f, x^q - x\}$. Prove that $g = \prod_{r \in \mathbf{F}_q : f(r)=0}(x - r)$; in particular, $\deg g$ is the number of distinct roots of f in $\mathbb{F}_q$.

[FF4] 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 $q \bmod 7 \neq 1$. (Hint: Use Euclid's algorithm to compute $\gcd\{x^q - x, x^7 - a\}$. If you're bored, write down three different proofs.)

[FF5] More generally, define $g = \gcd\{f, x^{q^n} - x\}$. Prove that g is the product of the distinct irreducibles that (1) divide f and (2) have degree dividing n.

There's much more to say about polynomial factorization. For example, if $f = (x-a)(x-b)$ with $a \neq b$, then f is not factored by any of the above strategies. But choosing a random $s \in \mathbb{F}_q$ and computing $\gcd\{f, (x - s)^{(q-1)/2} - 1\}$ has a good chance of producing $x - a$ or $x - b$. Can you figure out the exact chance? I implicitly assumed that q is odd when I wrote $(q-1)/2$; can you figure out a replacement for $(x-s)^{(q-1)/2} - 1$ if q is even?

Elliptic curve exercises

[EC1] Let $\mathbb{F}_q$ be a finite field of $\mathrm{Char}(\mathbb{F}_q) > 3$ and let a curve be given by

$$E : y^2 = x^3 + Ax + B.$$

Show that E is an elliptic curve (i.e. is non-singular) if and only if $x^3 + Ax + B$ has only simple roots over the algebraic closure, i.e. if it is squarefree.
Hint: Use exercise **FF1**.

[EC2] Let $\mathrm{Char}(K) > 3$. Find the group law using the chord and tangent method for a curve of the form

$$y^2 = x^3 + Ax + B.$$

Particularly give the coordinates of $P_1 \oplus P_2$ and $[2]P_1$ in terms of the coordinates of $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$ and state the exceptional cases.
Do the same for $E' : y^2 + (a_1x + a_3)y = x^3 + a_2x^2 + a_4x + a_6$.

[EC3] Let $E/\mathbb{Q}$ be the elliptic curve given by

$$E : y^2 = x^3 + 17.$$

A brief inspection reveals some points with integer coordinates

$$P_1 = (-2, 3), P_2 = (-1, 4), P_3 = (2, 5), P_4 = (4, 9), P_5 = (8, 29),$$

and a short computer search gives some more

$$P_6 = (48, 282), P_7 = (52, 375), P_8 = (5234, 378661).$$

Verify the following relations:

$$P_5 = [-2]P_1, P_4 = P_1 \ominus P_3, P_7 = [3]P_1 \ominus P_3.$$

Remark: It is not easy to prove that every rational point $P \in E(\mathbb{Q})$ can be written in the form

$$P = [m_1]P_1 \oplus [m_2]P_2 \text{ with } m_1, m_2 \in \mathbb{Z}$$

for some P_1, P_2.

Scalar-multiplication exercise

[SM1] Compute the NAF of 31 and 33.

Generic-attacks exercises

[GA1] 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 $\mathbb{F}_{239}$.

[GA2] 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 $65536 = 2^{16}$).