**Summer School on Elliptic and Hyperelliptic Curve Cryptography**

Exercises for lectures on Tuesday, 16.09.2008

## Forms of elliptic curves

**[EC1]** Consider the curve $y^2 = x^3 + x^2$ over $\mathbb{R}$.

a) How many points are there at infinity?

b) Study the curve for singularities.

c) Blow up the singularities if you found any.

**[EC2]** Let $y^2 = f(x), \deg(f) = 3$ describe an elliptic curve over $\mathbb{F}_q, q$ odd.

a) Which points have order 2?

b) Give a criterion on the coefficients of $f$ to ensure that $(0,0)$ is on the curve and that there exists a point $P$ on $E$ with $[2]P = (0,0)$.

c) Study all exceptional points of the birational equivalences to and from Edwards curves (p.19; don't look at p.20 unless you need a hint). How can the map to Edwards curves be extended if $d$ is a square, i.e. which points maps on the Weierstrass cure to which points on the blow-up at infinity on the Edwards curve.

**[EC3]** Use sage or magma to show that the addition

$$(x_3, y_3) = ((x_1y_1 + x_2y_2)/(x_1x_2 + y_1y_2), (x_1y_1 - x_2y_2)/(x_1y_2 - y_1x_2))$$

matches the usual Edwards curve addition if the denominators are non-zero.

## Fast Arithmetic in Finite Fields

**[FF1]** Prove that the prime field inversion algorithm (cf. slide 28) returns the inverse of $x \bmod p$.

*Hint: Find a loop invariant.*

**[FF2]** Show the square root computation algorithm (cf. slide 36) computes a square root of $a$.

**[FF3]** Adapt Karatsuba method to multiply two polynomials in $\mathbb{F}_2[X]$.

Test your approach to check that

$$(X^{14}+X^8+X^2)(X^{20}+X^{10}+X^4+X) = X^{34}+X^{28}+X^{24}+X^{22}+X^{15}+X^9+X^6+X^3$$

**[FF4]** Show the following:

The equation $X^2 + X = c$ has a solution in $\mathbb{F}_{2^d}$ if and only if $\mathrm{Tr}(c) = 0$. If $x$ is a solution then $x + 1$ is the other one.

If $d$ is odd, then

$$x = \sum_{i=0}^{(d-3)/2} c^{2^{2i+1}}.$$

**Elliptic curves over $\mathbb{Q}$**

**[EQ1]** 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

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

and a short computer search gives some more

$$P_6 = (43, 282), P_7 = (52, 375), P_8 = (5234, 378661).$$

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

$$P = [m]P_1 \oplus [n]P_3 \text{ with } m, n \in \mathbb{Z}.$$

**[EQ2]** Explain why there is no elliptic curve over $\mathbb{Q}$ with a point of order 17.

**[EQ3]** Find all primes of bad reduction for the curve

$$E_2 : y^2 = x^3 - 3x + 101.$$

**[EQ4]** Reduce the curve $E_2$ modulo 7 and give all points on the curve.