Elliptic curve cryptography, winter 2009

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

1. Exercise sheet
Hand in solutions until Sunday, 1 November 2009, 23^{59}

A word on the exercises. They are important. Of course, you know that. We require that you obtain at least 20% of the credits in order to be admitted to the final exam. Just as an additional motivation, you will get a bonus for the final exam if you earn more than 60% or even more than 80% of the credits.

Exercise 1.1 (Secure email). (6 points)

(i) Send a digitally signed email with the subject "`[09ws-ecc-handin] hello`" to us at `09ws-ecc-handin@lists.bit.uni-bonn.de` from your personal account. The signature must be verifiable and correct. [It is a good idea to verify this by sending a blind carbon copy (Bcc) to oneself.] 3

With Thunderbird I recommend using `enigmail` and `gpg`. In any case make sure to register your key eg. at `http://wwwkeys.de.pgp.net/`.

Choose yourself among this and possible other solutions. In any case use a pgp key pair.

Note: Future exercise hand-ins will only be accepted via signed email. Then a bonus point will be awarded for a correct signature and a malus for a missing or invalid signature.

The deadline for this part is Monday, 2 November, 23:59:59.

(ii) Find the fingerprint of your own PGP key. Bring 10 printouts of it to the next tutorial. (Do not send me an email with it. Guess, why!) 3

Sign all your collegues' public keys and our two keys: The corresponding fingerprints of our PGP keys are

```
F753 FA1F 70C8 0B4A 0181 8B50 B6EF 9CA3 B967 0465
```

and

```
FC11 51FB 995E 58A0 186B B701 306A DAFE 965F 1E54
```

Find our keys in your key management tool, after verification give it some or full trust, sign and submit your decision to the key server. (Make sure that things *are* visible on the server! Join with your fellow students to synchronize you.)

The deadline for this last signing part is Thursday, 5 November.

Exercise 1.2 (A polynomial over $\mathbb{F}_4$). (2 points)

2 Factor the polynomial $y^2 + y + 1$ over $\mathbb{F}_4$.

Exercise 1.3 (Computing in $\mathbb{F}_{256}$). (4+5 points)

Let M be your student id. Let

$$a = M \bmod 256, b = (M \operatorname{div} 256) \bmod 256, \text{ and } c = (a + b) \bmod 256$$

Now interpret a, b and c as elements of $\mathbb{F}_{256}$. We consider this field as the set of polynomials over $\mathbb{F}_2$ of degree less than 8: $a_0 + a_1 x + a_2 x^2 + \cdots + a_7 x^7$ with $a_i \in \mathbb{F}_2 = \{0, 1\}$. Addition and multiplication are obtained from addition and multiplication of polynomials modulo $m := x^8 + x^4 + x^3 + x + 1$ (we grant that m is irreducible over $\mathbb{F}_2$), for example, $x^5 \cdot x^6 = x^7 + x^6 + x^4 + x^3$ in $\mathbb{F}_{256}$. Sometimes we identify $a_0 + a_1 x + a_2 x^2 + \cdots + a_7 x^7$ with the integer $a_0 + a_1 2 + a_2 2^2 + \cdots + a_7 2^7 \in \mathbb{N}_{<256}$ (in decimal or hexadecimal notation) or the bit vector $[a_0, a_1, a_2, \ldots, a_7]$. Compute in $\mathbb{F}_{256}$

2 (i) $a + b$ (Attention! Usually the result will not be c!),

2 (ii) $a \cdot b$, and

+5 (iii) $1/a$ (or $1/b$ in case $a = 0$).

Note: If $x = x_1 \cdot 256 + x_0$ with $0 \leq x_0 < 256$, then $x \operatorname{div} 256 = x_1$ and $x \operatorname{rem} 256 = x_0$.

Exercise 1.4 (Be smooth). (7 points)

In the lecture we have seen several examples of cubic curves. Your task is now to show that certain points are *not* smooth. Fix any field k.

2 (i) Consider the curve $y^2 - x^3 = 0$. Show that the point $(0, 0)$ is non-smooth.

3 (ii) Find all non-smooth points $(x, y) \in k^2$ of the curve $y^2 - x^2(x + 3) = 0$.

2 (iii) Show that $y - x^3 = 0$ is smooth for all points $(x, y) \in k^2$.

Exercise 1.5 (The world at infinity). (4+8 points)

In the lecture we have seen that we need to talk about points at infinity. In this exercise we will clarify this. If we have any field k, the two-dimensional *projective space* $\mathbb{P}^2_k$ over k is given by equivalence classes of triples (X, Y, Z) with $X, Y, Z \in k$ and at least one of the three non-zero. Two triples (X_1, Y_1, Z_1) and (X_2, Y_2, Z_2) are said to be equivalent if there is a nonzero $\lambda \in k$ with $(X_1, Y_1, Z_1) = (\lambda X_2, \lambda Y_2, \lambda Z_2)$. We write for the equivalence class of (X, Y, Z) usually $(X : Y : Z)$. If $(X : Y : Z)$ is a point with $Z \neq 0$, then $(X : Y : Z) = (X/Z : Y/Z : 1)$ and we have a "finite" point in $\mathbb{P}^2_k$. All the points $(X : Y : 0)$ are called the *points at infinity* in $\mathbb{P}^2_k$. We wish to look at our cubics $f(x, y)$ projectively. To do so, we define the homogenized version $F(X, Y, Z)$ of f by $F(X, Y, Z) := Z^{\deg(f)} f(X/Z, Y/Z)$. Then $F(\lambda X_2, \lambda Y_2, \lambda Z_2) = \lambda^{\deg(f)} F(X_1, Y_1, Z_1)$, i.e. if F vanishes at (X_1, Y_1, Z_1) then F vanishes at each representative of the class $(X_1 : Y_1 : Z_1)$. Thus it makes sense to say that F vanishes at $(X_1 : Y_1 : Z_1)$.

(i) Consider the curve given by $f = y^2 - x^3$, compute its homogenized version and show that it is smooth at the point at infinity. 4

(ii) Show that $h = y - x^3$ does not define an elliptic curve. (You have done most of the work in Exercise 1.4(iii)!) +4

(iii) Show that the curve given by $g = y^2 - x^2(x + 3) - \frac{1}{2}$ is an elliptic curve. +4