9. Exercise sheet
Hand in solutions until Friday, 13 January 2017, 12:00 (noon)

Exercise 9.1 (EEA, examples). (18 points)

In each run of the algorithm, use the table to document it. Think of the cross-check. State the result.

- Run the Extended Euclidean Algorithm on 42, 235. (Do NOT swap the inputs!) 3
- Compute the inverse of 42 ∈ \( \mathbb{Z}_{1009} \). 3
- Say \( L = 28 \cdot 30 \) and you choose \( e = 26 \). Is \( e \) invertible? If so determine its inverse \( d \). 3
- Say \( L = 28 \cdot 30 \) and you choose \( e = 17 \). Is \( e \) invertible? If so determine its inverse \( d \). 3
- Determine \( x \in \mathbb{Z}_{899} \) with \( x \mod 29 = 7 \) and \( x \mod 31 = 13 \). 6

Exercise 9.2 (RSA, example). (10 points)

Run RSA for \( \kappa = 40 \). Document your procedure. 10

Exercise 9.3 (Elliptic curve addition). (0+8 points)

Let \( \mathbb{F} \) be any field, \( a, b \in \mathbb{F} \) with \( 4a^3 + 27b^2 \neq 0 \). We want to derive a program for adding two points \( P, Q \) on the elliptic curve given by the equation \( y^2 = x^3 + ax + b \), ie. \( E = \{ [x, y] \in \mathbb{F}^2 \mid y^2 = x^3 + ax + b \} \cup \{ O \} \).

Say \( P = (x_P, y_P), Q = (x_Q, y_Q) \).

(i) First, we need the parameters for the line through \( P \) and \( Q \). Say, \( y = mx + c \) is its equation. Derive a formula for \( m \) first. Then express \( c \) with \( m, x_P, y_P \). +3

(ii) Next, find the coordinates for the third point \( R = (x_R, y_R) \) on the line and the curve.

To do so: plug the line equation into the curve equation. We know that \( x_P \) and \( x_Q \) must be solutions of the resulting equation. So compare it to \( (x - x_P)(x - x_Q)(x - x_R) = 0 \) and compare coefficients of \( x^2 \) to determine \( x_R \). Express \( x_R \) with \( m, x_P, x_Q \). Finally, express \( y_R \) using the line equation. +5