Cryptography

Prof. Dr. Joachim von zur Gathen, Konstantin Ziegler

11 Assignment: Elliptic Curves

(Due: Thursday, 4 February 2010, 23^{59})

Exercise 11.1 (Doubling on elliptic curves)**.** Let $P = (x_1, y_1)$ be a point on an elliptic curve

$$E_{a,b} = \{(u, v) \in \mathbb{R}^2 \colon v^2 = u^3 + au + b\} \cup \{\mathcal{O}\}.$$

(i) (3 points) Show that $Q = (x_3, y_3) = P + P = 2P$ can be computed using the following formula if $y_1 \neq 0$:

$$\alpha = \frac{3x_1^2 + a}{2y_1}$$
$$x_3 = \alpha^2 - 2x_1$$
$$y_3 = (x_1 - x_3)\alpha - y_1$$

Hint: Take the tangent line at the point P.

(ii) (1 points) What happens if $y_1 = 0$?

(iii) (5 points) Verify that the formula for doubling a point is the limit of the formula for addition of two points $P = (x_1, y_1)$ and $Q = (x_2, y_2) = (x_1 + \epsilon_1, y_1 + \epsilon_2)$, if Q (on the curve) converges to P. In order to do this, show that in this case the $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$ of the formula for addition converges to the α from the formula of doubling above. The fact that both Q and P are on the curve, i.e. that (x_1, y_1) and $(x_1 + \epsilon_1, y_1 + \epsilon_2)$ satisfy the curve equation, has to be used, of course.

Exercise 11.2. (3 points) The polynomial

$$f(x, y) = y^2 - x^3 - ax - b$$

defines a curve in the x-y-plane via the equation $f(x, y) = 0$. Show that the curve has a well-defined tangent vector in every point on the curve, i.e. the curve is *smooth*, if and only if

$$4a^3 + 27b^2 \neq 0.$$

Hint: Consider the inequality $\left(\frac{\partial f(x,y)}{\partial x}, \frac{\partial f(x,y)}{\partial y}\right)\Big|_P \neq (0,0)$ for the tangent vector in the point $P = (u, v)$.

Exercise 11.3. Consider the example $E = \{(u,v) \in \mathbb{F}_7^2 : v^2 = u^3 + u\} \cup \{\mathcal{O}\}$ for an elliptic curve over $\mathbb{F}_7$ from the lecture (see 1).

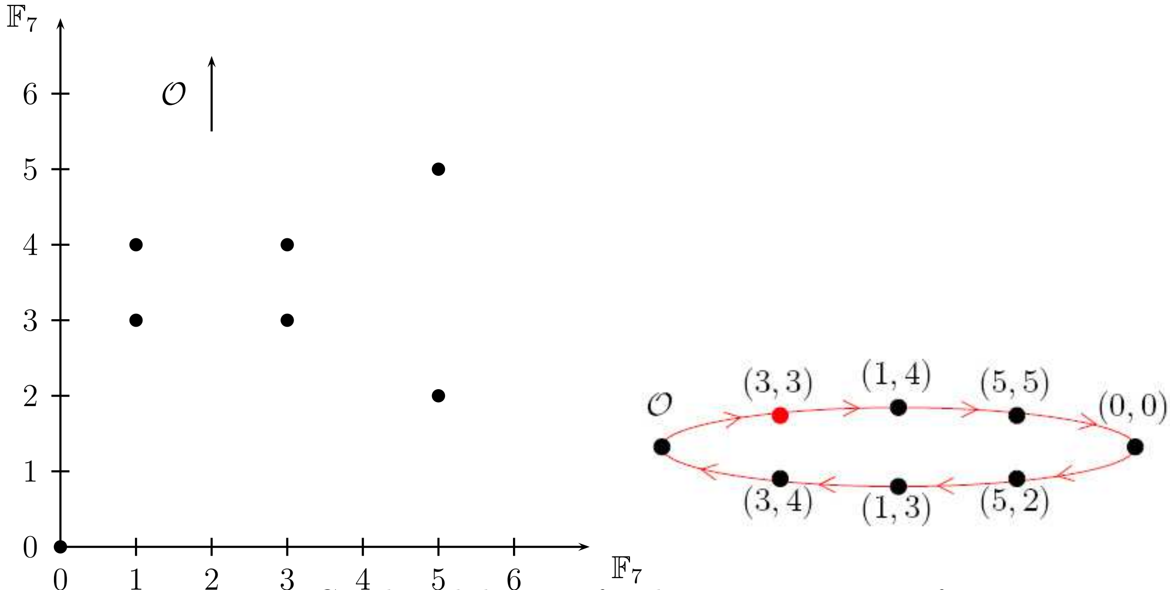

Figure 1: Graph and diagram for the group structure of E

(i) (2 points) Let $P = (5, 5)$. Determine $S = 2 \cdot P$ and $T = 5 \cdot P$ from the diagram on the right of Figure 1.

The addition of two distinct points corresponds to a secant of the graph. The doubling of a point corresponds to a tangent to the graph.

(ii) (2 points) Draw the tangent corresponding to $S = 2 \cdot P$ into the graph on the left of Figure 1.

(iii) (1 point) Determine $S + T$ from the graph on the left and check your result by doing the same computation in the diagram on the right.

Exercise 11.4. Alice and Bob heard about the cryptographic applications of elliptic curves. They want to perform a Diffie-Hellman key exchange using the elliptic curve E from the previous exercise.

(i) (1 point) List all possible generators for the cyclic group E.

ALICE and BOB publicly agree on the generator P from above. The secret key of ALICE is 3 and the secret key of BOB is 4.

(i) (3 points) Which messages are exchanged over the insecure channel and what is ALICE's and BOB's common secret key?