Cryptography

Priv.-Doz. Dr. Adrian Spalka, Konstantin Ziegler

Assignment 11: elliptic curves
Due: Monday, 7 February 2011, 10^{00}

Disclaimer. `The solutions proposed here claim neither to be correct nor to be complete.` □

Exercise 11.1. Consider the example $E = \{(x, y) \in \mathbb{Z}_7^2 : y^2 = x^3 + x\} \cup \{\mathcal{O}\}$ for an elliptic curve over $\mathbb{Z}_7$ (see Abbildung 1).

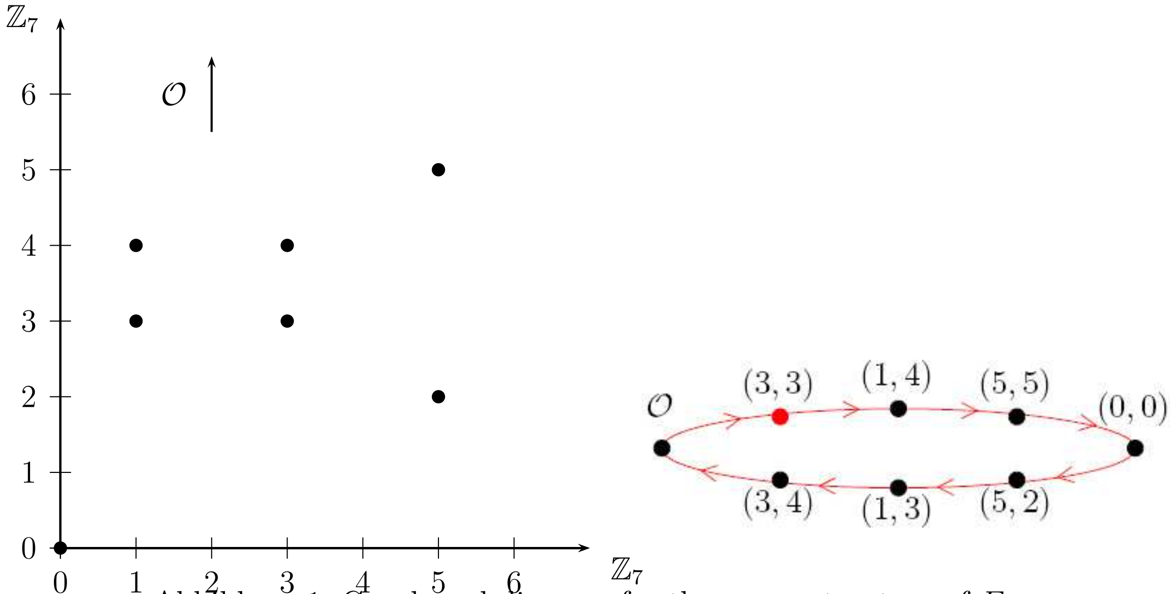


Abbildung 1: Graph and diagram for the group structure of E

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

Solution.

$$S = 2 \cdot P = (1, 3)$$
$$T = 5 \cdot P = (3, 4)$$

`Note that this comes down to just counting arrows.` P `corresponds to` 5 `arrows, hence` $2P$ `corresponds to` 10`. Analogously for` $5P$`.` □

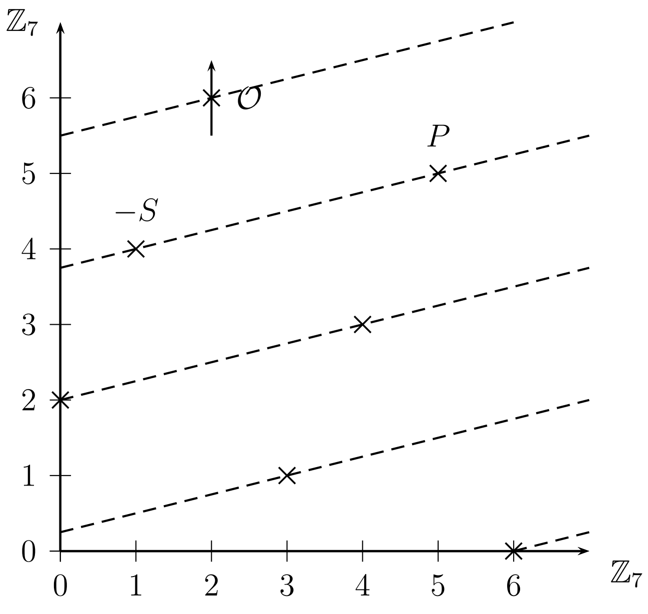
The addition of two distinct points corresponds to a secant of the graph. The doubling of a point corresponds to a tangent to the graph.

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

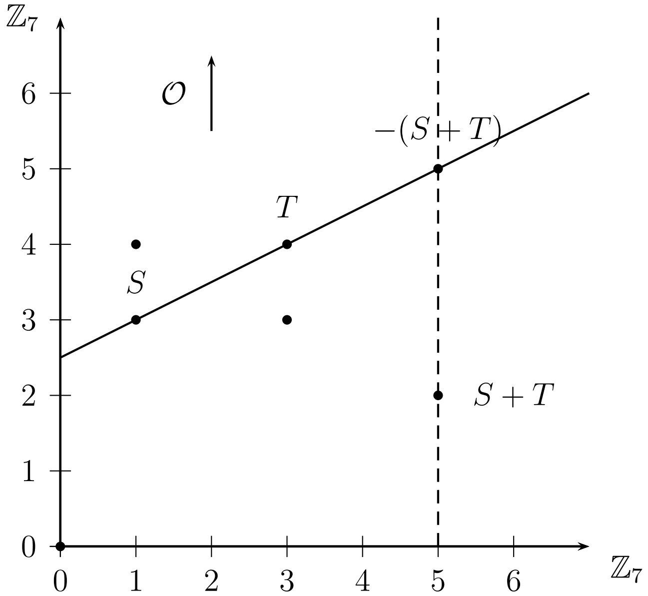
Solution. The tangent in question runs through the two poinst P and $-S$ (mind the minus sign). When drawing the tangent, you have to keep two things in mind:

- Lines ,,wrap around" when leaving the $\mathbb{Z}_7 \times \mathbb{Z}_7$-plane through one edge, entering on the opposite edge. Just as $4+5=9$,,wraps around" to 2 in $\mathbb{Z}_7$. (Some people might be reminded of some ancient computer games, like Donkey Kong or Super Mario.)
- Points in the plane are only allowed to have coordinates from $\mathbb{Z}_7 \times \mathbb{Z}_7$. There is no such thing as the point $(3, 4.5)$ in this plane. (That is also the reason, why the elliptic ,,curve" consists only of a discrete set of points.) So you may draw the line as you are used to, but please mark only the points with valid coordinates as the true solution.



To determine $S+T$ we connect the points, determine its intersection with the elliptic curve and take the mirror point. (Note, that the plane ,,wraps around",i.e. the y-value of -5 corresponds to 2 - its equal in $\mathbb{Z}_7$.) So, the sum of S and T is $(5, 2)$ or in other words $-P$. □

Exercise 11.2. 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.

Solution. The generators are all the elements in the cycle in Abbildung 1 which are at a position coprime to the group order, i.e. at position 1, 3, 5 and 7. Let us list them:

$$\{(3,3),(5,5),(5,2),(3,4)\}.$$

□

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

Solution. The information that has to travel over the insecure channel consists of the equation for the elliptic curve E, along with the size of the prime field $\mathbb{Z}_7$ and the generator P of the cyclic group, that we are working in.

Additionally for ALICE and BOB, the former has to transmit the public version of her private key:

$$3 \cdot P = (3,3)$$

and the latter transmits

$$4 \cdot P = (0,0).$$

Their common secret key is

$$3 \cdot (4P) = 4 \cdot (3P) = 12 \cdot P = (0,0).$$

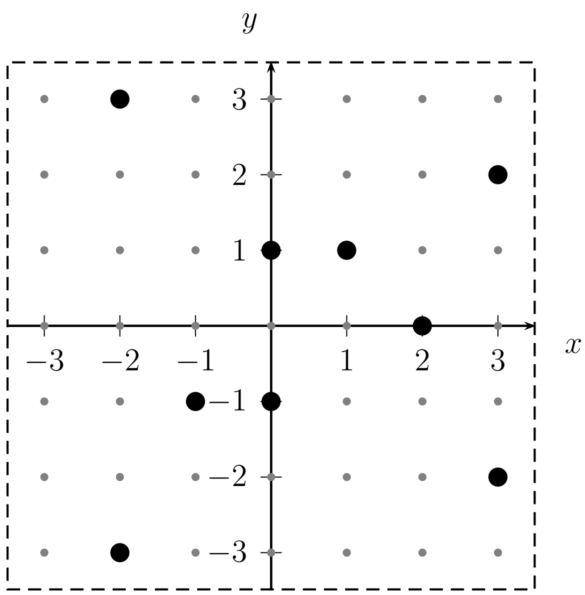
It is a coincidence, that the common key is equal to Bob's public key. (But note, that this coincidence is not very surprising, since the group is really small.)

Note, that the private key is an integer between 0 and 7, while the public key is a point (x, y) on the elliptic curve. That should *not* surprise you - the group on the public level and the group on the private level share the same structure, but might totally differ in notation. □

Exercise 11.3 (Elliptic curves)**.** Consider the elliptic curve E over $\mathbb{Z}_7$ given by

$$y^2 = x^3 - x + 1.$$

(i) In order to draw a picture of E we fix a set of representatives for $\mathbb{Z}_7$: $\{-3, -2, -1, 0, 1, 2, 3\}$. Most points of E are already drawn in the coordinate system below. Three points are missing in the picture. Draw them—without performing any explicit computation—and give a reason.



Solution. The missing points are $\mathcal{O}$, $(1, -1)$, and $(-1, 1)$. The first one because of the definition of an elliptic curve and the other two, because of the symmetry with regard to the y-coordinate. □

(ii) Add the points $P(2, 0)$ and $Q(1, 1)$ graphically.

(iii) Determine the inverse of $S(3, 2)$ graphically.

Solution. The line joining P and Q intersects E at $(-2,-3)$ and the mirror point $(-2,3)$ is therefore the required sum $P+Q$.

The inverse is the mirror image with respect to the x-axis, i.e. $-S(3,-2)$. $\square$