MATH 1025: Introduction to Cryptography

Homework 4

elliptic pursuit

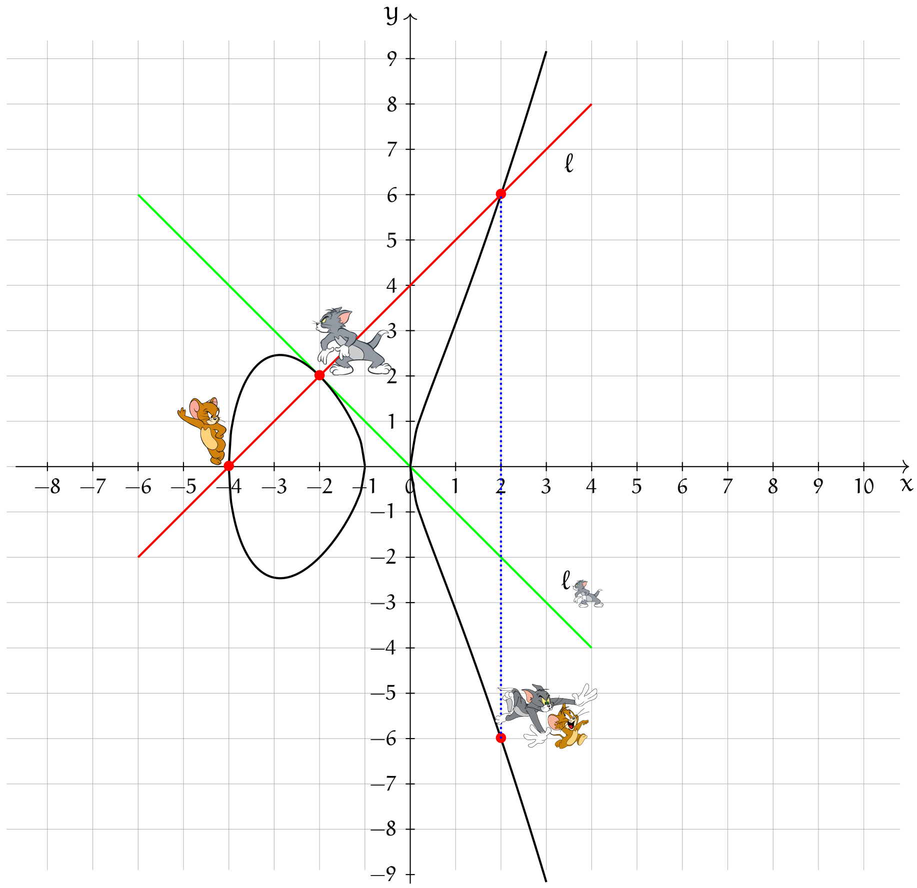
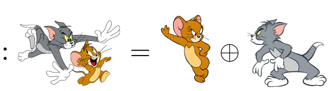


Figure 1: Addition of points on elliptic curve E : 

Problem 1. We will work with the elliptic curve $E := \{(X, Y) \mid Y^2 = X(X+1)(X+4)\}$ defined over $\mathbb{R}$.

(a) [3 **pts**] Explain why the discriminant of the polynomial $f(X) = X(X+1)(X+4)$ is not zero.[1]

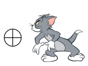
[1] **Hint:** no calculations are necessary, see the definition

(b) [2 **pts**] Check that the points  $= (-4, 0)$ and  $= (-2, 2)$ are on E.

(c) Find the coordinates of the point  $=$  $\oplus$ .

Step 1. [2 **pts**] Find equation of the line ℓ through the points  and  in the form $Y = mX + b$.

Step 2. [5 **pts**] Plug the equation obtained on the previous step into the equation of E and find the third point of intersection of ℓ and E.[2]

Step 3. [3 **pts**] Find the coordinates of the point  $=$  $\oplus$  as reflection of the third point of intersection of ℓ and E with respect to the x-axis.

Step 4. [5 **pts**] What are the coordinates of the point  $\ominus$ ?

[2] **Hint:** you will get a polynomial of degree 3 in X (the restriction of the defining equation of E to ℓ), two roots of which are the x-coordinates of points  and .

(d) Find the coordinates of the point $2 \cdot$ .

Step 1. [2 **pts**] Find equation of the line ℓ tangent to E at the point  in the form $Y = mX + b$.

Step 2. [5 **pts**] Plug the equation obtained on the previous step into the equation of E and find the second point of intersection of ℓ and E.[3]

Step 3. [3 **pts**] Find the coordinates of the point $2 \cdot$  as reflection of the second point of intersection of ℓ and E with respect to the x-axis.

(e) [5 **pts**] What is the point $2 \cdot$ ?

[3] **Hint:** you will get a polynomial of degree 3 in X (the restriction of the defining equation of E to ℓ) with  a zero of multiplicity two.

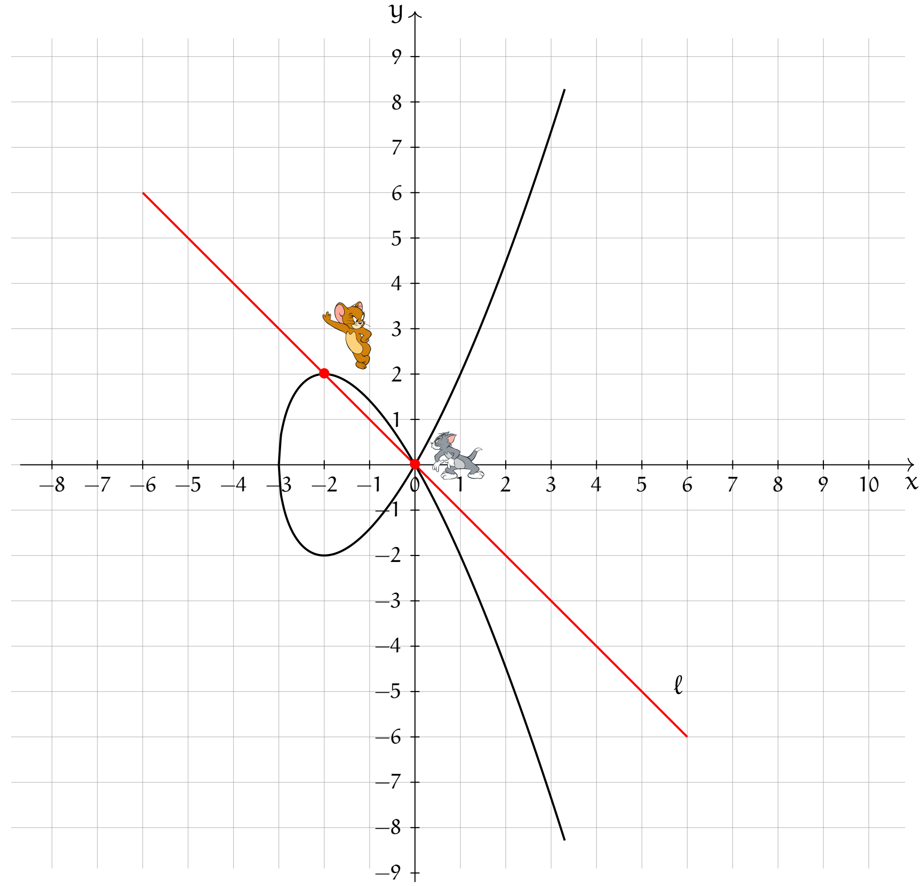


Figure 2: Addition of points on a singular elliptic curve

Problem 2. We will work with the elliptic curve $E : Y^2 = X^2(X+3)$ defined over $\mathbb{R}$.

(a) [3 **pts**] Explain why the discriminant of the polynomial $f(X) = X^2(X+3)$ is zero.[4]

(b) [2 **pts**] Check that the points  $= (-2, 2)$ and  $= (0, 0)$ are on E.

[4]**Hint:** no calculations are necessary, see the definition

(c) Next we will show that $\oplus$ does not provide a group structure on E.

Step 1. [2 **pts**] Find equation of the line ℓ through the points  and  in the form $Y = mX + b$.

Step 2. [3 **pts**] Plug $Y = mX + b$ into the equation of E and find the third point of intersection of ℓ and E.[5] Then find coordinates of the point  $\oplus$ .

Step 3. [5 **pts**] Choose any other point P on E and find the point $P \oplus$ . Conclude that operation $\oplus$ does not give rise to a group structure on E.

Problem 3. Consider the elliptic curve $E : Y^2 = X^3 + 2X + 3$ over $\mathbb{F}_7$.

(a) [5 **pts**] Check that the discriminant is nonzero (use the formula) and list the set of points $E(\mathbb{F}_7)$.

[5] **Hint:** nobody said it must be different from the first two.

(b) [10 **pts**] Make an addition table for the group $E(\mathbb{F}_7)$.

(c) [5 **pts**] Which abelian group did you get in (b)?

(d) [5 **pts**] What is the order of the point $P = (3, 1)$?

Problem 4. [10 **pts**] Let E be the elliptic curve

$$E : y^2 = x^3 + x + 1$$

and let $P = (4, 2)$ and $Q = (0, 1)$ be points on E modulo 5. Solve the elliptic curve discrete logarithm problem for P and Q, that is, find a positive integer n such that $Q = nP$.

Collision Algorithm

Problem 5. Consider the elliptic curve $E : Y^2 = X^3 - 7X + 13$ over $\mathbb{F}_{137}$.

(a) [2 **pts**] Check that the discriminant of E is not zero (use the formula).

(b) [3 **pts**] Use Hasse's theorem to find an estimate of the number of points on E.

(c) [5 **pts**] Let $P = (4, 7)$, $Q = (38, 97)$ and check that both points lie on E.

(d) [5 **pts**] The order of P is $N = 138$ (it is a generator). Our next goal is to solve the DLP, for P and Q, that is, find a positive integer s such that $Q = sP$. We will use the collision algorithm. Using part (b) of the theorem on page 3 of 'Lectures $17 - 19$' notes (with $1 \leq n = m \leq N = 138$), choose n so that you are happy with the lower bound on the probability of collision (**find the value of this lower bound**).

(e) [10 **pts**] Create two sets of numbers $A = \{a_1, a_2, \ldots, a_n\}$ and $B = \{b_1, b_2, \ldots, b_n\}$ with $1 \leq a_i, b_j \leq 137$. Use programs (`http://tsvboris.pythonanywhere.com/IntrotoCryptography`) to find the lists

$$L_1 = \{a_1 P, a_2 P, \ldots, a_n P\}$$
$$L_2 = \{b_1 P + Q, b_2 P + Q, \ldots, b_n P + Q\}$$

(f) [10 **pts**] The intersection of the two lists is nonempty with probability that you computed in (d) (if it is empty, restart from (d) or (e), in case the probability was high, but you got 'very lucky' to beat the odds). Pick any point $Z \in L_1 \cap L_2$ and, using that $Z = a_i P = b_j P + Q$, find $s \equiv a_i - b_j \bmod N$.