Elliptic pursuit

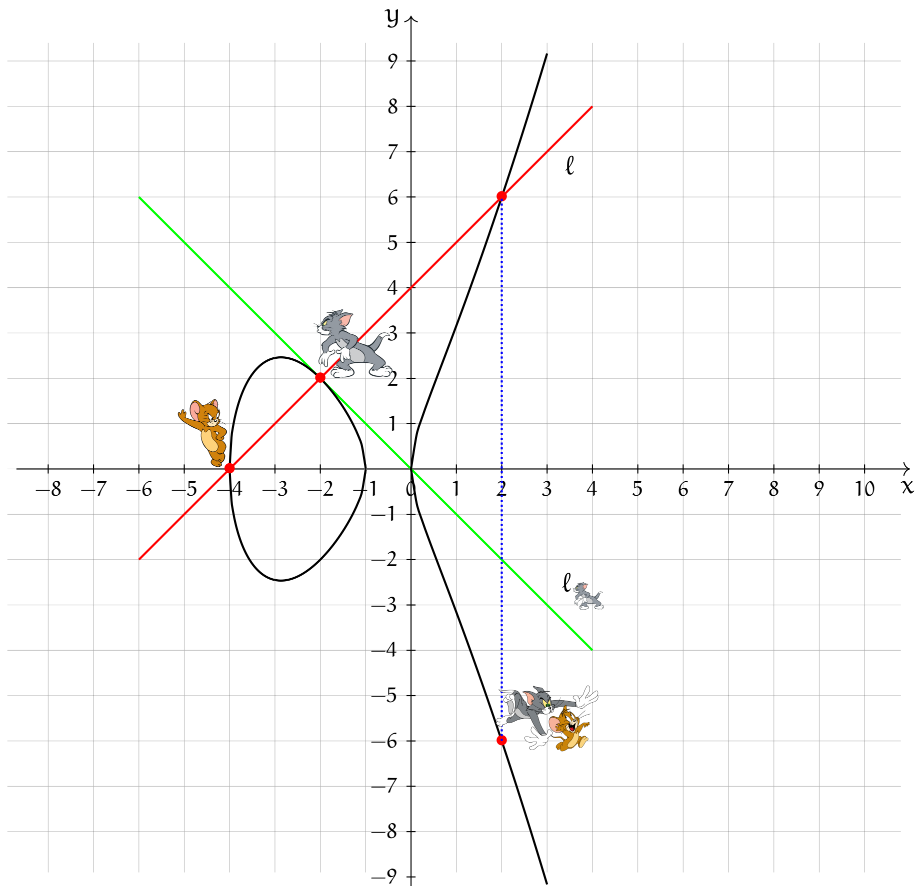

Figure 1: Addition of points on elliptic curve E :  =  $\oplus$ 

Problem 1. (25 pts) We will work with the elliptic curve $E : Y^2 = X(X+1)(X+4)$ defined over $\mathbb{R}$.

(a) Explain why the discriminant is not zero.[1]

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

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

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

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

Step 2. 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. 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. What are the coordinates of the point  $\ominus$ ?

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

Step 1. Find the equation of the line ℓ tangent to E at the point  (in the form $Y = mX + b$).

Step 2. 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]

[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  and .

[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.

Step 3. 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) What is the point $2 \cdot$ ?

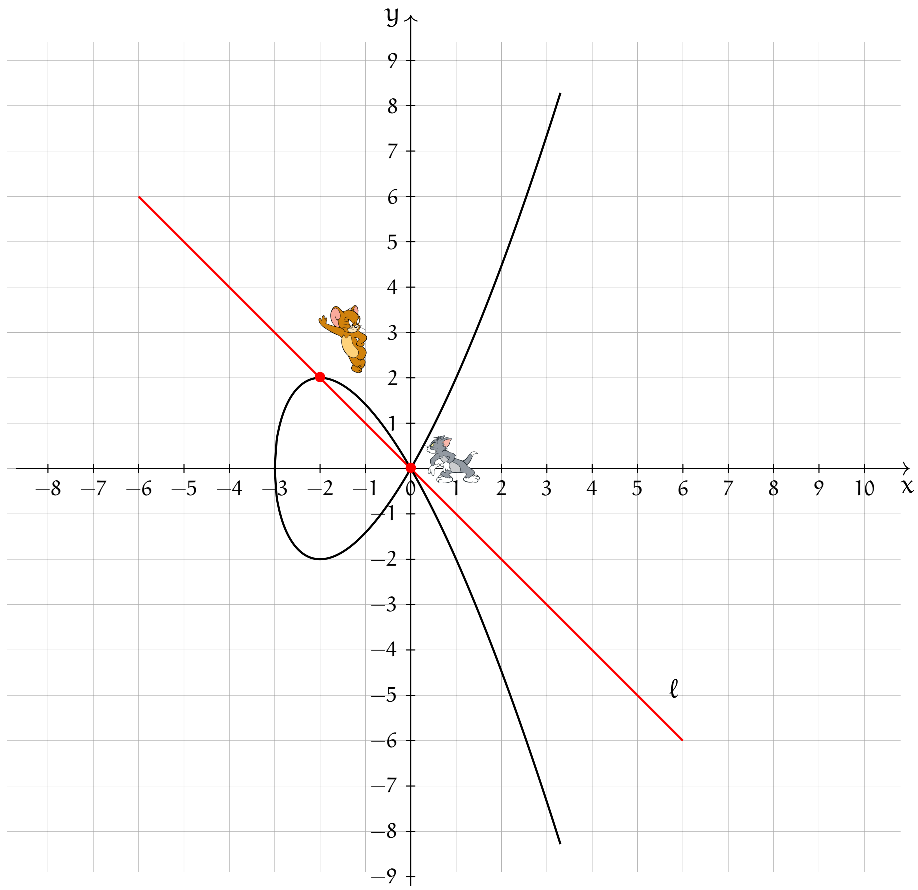

Figure 2: Addition of points on a singular elliptic curve

Problem 2. (25 pts) We will work with the elliptic curve $E : Y^2 = X^2(X+3)$ defined over $\mathbb{R}$.

(a) Explain why the discriminant is zero.[4]

(b) 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. Find equation of the line ℓ through the points  and  in the form $Y = mX + b$.

Step 2. 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. 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. (25 pts) Consider the elliptic curve $E : Y^2 = X^3 + 2X + 3$ over $\mathbb{F}_7$.

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

(b) Make an addition table for the group $E(\mathbb{F}_7)$.

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

(c) Which abelian group did you get in (b)?

(d) 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 $Q = nP$.

Elliptic Diffie-Hellman key exchange

Problem 5. (15 pts) Alice and Bob agree to use elliptic Diffie-Hellman key exchange with a prime number p, elliptic curve E, and point P being

$$p = 2671, E : y^2 = x^3 + 171x + 853, P = (1980, 431) \in E(\mathbb{F}_{2671}).$$

(a) Alice's public key is the point $Q_A = (2110, 543)$. Bob decides to use the secret multiplier $k_B = 1943$. Use the programs at http://tsvboris.pythonanywhere.com/IntrotoCryptography and find the point $Q_B \in E$, which is Bob's public key.

(b) Find the point on E which is the shared key of Alice and Bob.