

Homework 4

Due 23.04.2009

Please save your Mathematica code in a .nb file and e-mail it to me.

- 1.M Given an elliptic curve \mathcal{C} with rational coefficients, write a procedure that takes as input two points P and Q , and the elliptic curve \mathcal{C} , and computes $P \oplus Q$.

You can test your procedure on the following curve: $y^2 = x^3 + x - 1$ with the points $A = (2, 3)$, $B = (2, -3)$, and $C = (1, 1)$. Use these points to compute $2A$, $A \oplus B$, $A \oplus C$, and $B \oplus C$.

- 2 Consider the \star operation between points on an elliptic curve \mathcal{C} , as defined in class.

(a) Prove that there is no identity element for this composition, that is, there is no P_0 such that $P \star P_0 = P$ for all points P on \mathcal{C} .

(b) Prove that \star is not associative. That is, in general, $P \star (Q \star R) \neq (P \star Q) \star R$.

- 3 The Nagell-Lutz Theorem says the following:

Let $y^2 = f(x) = x^3 + ax^2 + bx + c$ be an elliptic curve with $a, b, c \in \mathbb{Z}$, and let $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$ be its discriminant. Suppose $P = (x, y) \in \mathbb{Q} \times \mathbb{Q}$ is a rational point of finite order in the abelian group associated to the elliptic curve. Then x and y are in \mathbb{Z} , and either $y = 0$, in which case P has order 2, or else y divides D .

Using the Nagell-Lutz Theorem determine all the rational points of finite order on the curve $y^2 = x^3 - x^2 + x$ and also determine the structure of the group formed by these points. (You may use your Mathematica program for exercise 1 to compute multiples of the points of finite order. This will help you determine the subgroup structure.)

4. Prove that the number of **projective** solutions to the equation

$$x^3 + y^3 + z^3 = 0,$$

where $x, y, z \in \mathbb{F}_p$ and $p \not\equiv 1 \pmod{3}$, is $p + 1$.