Lecture 3: Nagell-Lutz Theorem

In lecture we discussed the group law on the set of rational points on an elliptic curve. As always, we will suppose that C is an elliptic curve described by a cubic equation in Weierstrass form

$$y^2 = x^3 + ax^2 + bx + c.$$

where a, b, c are integers.

Remember, given two points p, q on C, we usually define $p + q$ by taking the line ℓ through p, q, computing the third point r in $\ell \cap C$, and setting $p + q = -r$. (There are also some additional cases that you should remember but that I won't outline here.) It turns out that $+$ is an associative commutative binary operation on the set of rational points.

These first exercises are intended to give you some practice with the group law. Some are taken from the book "Rational points on elliptic curves" by Silverman and Tate.

1) The elliptic curve $y^2 = x^3 - 25x$ has rational points $p = (0, 0)$ and $q = (-4, 6)$.
   a) Find $p + q$.
   b) Find $2p$.
   c) Find $2q$.

2) Consider the cubic curve $y^2 = x^3 + 17$. It contains the following five points:

$$Q_1 = (-2, 3), Q_2 = (-1, 4), Q_3 = (2, 5), Q_4 = (4, 9), Q_5 = (8, 23)$$

   a) Show that Q_2, Q_4, Q_5 can all be written as $mQ_1 + nQ_3$ for some integers m, n.
   b) Compute the points $Q_6 = -Q_1 + 2Q_3$ and $Q_7 = 3Q_1 - Q_3$.
   c) Aside from these points and their inverses, there is exactly one more rational point Q_8 with positive y-coordinate. Find it!

3) Suppose we have an elliptic curve of a somewhat general form $y^2 = x^3 + bx + c$. Let's compute a general formula for adding points. Suppose that $p = (x_1, y_1)$ and $q = (x_2, y_2)$ are rational points on the curve C with different x-coordinates and that the line ℓ connecting them has equation $y = \lambda x + \nu$.
   a) Compute λ and ν in terms of the coordinates x_1, x_2, y_1, y_2.
   b) Show that the third intersection point of $\ell \cap C$ has x-coordinate $\lambda^2 - x_1 - x_2$.
   c) Compute the coordinates of $p + q$.

4) Repeat the steps in the previous problem to give an explicit equation for $2p$ when the tangent line to p is not vertical.

1 Points of finite order

Recall that a point $p \in C$ has finite order if there is a positive integer k such that $kp = \infty$. In this case, the smallest such positive integer is called the order of p. (According to this definition, ∞ has order 1 and is the only point of order 1. We will usually neglect to mention this point in the future.)

5) Consider the cubic curve $y^2 = x^3 + 17$. Compute the order of the point $Q_1 = (-2, 3)$ and the order of the point $Q_2 = (-1, 4)$.

6) Explain why a point $p \in C$ has order 2 if and only if the tangent line to p is vertical.

7) Explain why a point $p \in C$ has order 3 if and only if the tangent line to p is triply tangent (i.e. if we substitute the equation of the line into the equation for C we obtain a polynomial with a triple root).

8) Explain why a point $p \in C$ has order 4 if and only if the tangent line to p meets C at a point with y-coordinate equal to 0 that is different from p itself.

9) Prove that if p and q are rational points with finite order then $p + q$ also has finite order. (Hint: it is easier to solve this problem using the associativity and commutativity of $+$ rather than using equations for the group law.)

The best way for understanding points of finite order is the Nagell-Lutz Theorem:

Theorem 1.1 (Nagell-Lutz)**.** *Let C be an elliptic curve with equation $y^2 = x^3 + ax^2 + bx + c$ where a, b, c are integers. Then every rational point (x, y) of finite order on C satisfies the following properties:*

1) Both x and y are integers.

2) The coordinate y is either 0 or a divisor of the discriminant

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2.$$

Furthermore, if y divides D then y^2 divides D.

This gives us a finite-time algorithm for finding all finite order points on the cubic C.

10) Using the Nagell-Lutz Theorem, find all points of finite order on the elliptic curve $y^2 = x^3 + 17$.

11) Show that the point $(0, 1)$ is not a torsion point on the curve $y^2 = x^3 - 3x + 1$. (Hint: if p is torsion, then so is every multiple kp. Do these multiples still satisfy the conclusions of Nagell-Lutz?)

12) Find all points of finite order on the elliptic curve $y^2 = x^3 + px$ where p is prime.

2 Structure of finite abelian groups

As mentioned during lecture, the set of rational points on an elliptic curve C is a finitely generated abelian group. One of the earlier exercises shows that a sum of torsion points is torsion. We conclude that the set of torsion rational points is a subgroup, and thus a finite abelian group in its own right. Let's recall the structure theorem for finite abelian groups:

Theorem 2.1. *Every finite abelian group G is isomorphic to a product of cyclic groups of prime power order:*

$$G \cong \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_k^{a_k}\mathbb{Z}$$

Furthermore, this decomposition is unique up to reordering the factors.

It turns out that for finite abelian groups, one can identify the isomorphism type by counting the number of elements of each order. (Note that this is not true for arbitrary finite groups.) This may be helpful for answering the following questions:

13) Identify explicitly the isomorphism type of the group of finite order rational points on the elliptic curve $y^2 = x^3 + 17$.

14) Identify explicitly the isomorphism type of the group of finite order rational points on the elliptic curve $y^2 = x^3 + 4x$.

15) Identify explicitly the isomorphism type of the group of finite order rational points on the elliptic curve $y^2 = x^3 + 1$.

There is a celebrated theorem of Barry Mazur that describes all possible finite abelian groups obtained from elliptic curves:

Theorem 2.2 (Mazur)**.** *Let C be an elliptic curve and let $p \in C$ be a rational point with finite order m. Then either $1 \leq m \leq 10$ or $m = 12$. Moreover, the group of rational points on C is isomorphic to one of the following groups:*

- $\mathbb{Z}/m\mathbb{Z}$ *where* $1 \leq m \leq 10$ *or* $m = 12$*, or*
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$ *where* $1 \leq n \leq 4$*.*