Final Worksheet for the session on 7 November 2025

In the last three sessions we have studied quadratic equations in n variables. One important result we have discussed and explored is Hasse Minkowski theorem: "If a quadratic equation has a solution in R and solutions mod p^k for all primes p and positive integers k , then it must have a solution in Q." This is often stated as local to global principle.

But the theorem breaks down for cubic equations. The famous counterexample is Selmer equation $3x^3 + 4y^3 + 5z^3 = 0$, which satisfies all conditions of Hasse Mikowski theorem but can be proved to NOT have any rational solution. The proof of no rational solution is quite complex and depends on a study of algebraic number theory and is not going to be discussed in this session.

In today's session we will discuss special kinds of cubic curves known as elliptic curves (nothing to do with ellipses). The equation that we will deal with is

$$y^2 = x^3 + Ax + B$$

where this equation represents a smooth (non-singular) curve in two dimensions). The condition for smoothness is $4A^3 + 27B^2 \neq 0$. We will only consider those equations where this condition holds.

We have seen that in the case of quadratic equations, one way to generate rational points is to intersect the quadratic curve with a rational line going through one rational point. A SIMILAR construction can be done for elliptic curves. Instead of a rational line going through one rational point we will have a chord passing through two rational points and generating new rational points.

THE MAIN POINT OF THIS SESSION IS to explore the beautiful group structure of these rational points on elliptic curves and some aspects related to this. THIS IS A VAST SUBJECT of active current research, both beautiful and complex, and we will barely scratch the surface.

Problem 1. Today we will mostly work with examples. Consider $y^2 = x^3 + 17$. First check that it is smooth.

a.) Here are a few integer points (-1,4), (-2,3), (2, 5) on the curve.

Find a few additional ones.

b.) Look at the following picture. Given two points P, Q you can join the chord and find a third point R.

If P = (-2,3), Q = (2,5), what are the coordinates of R?

Do the same for P = (-2,3) Q = (-1, 4) (You can do this without doing a lot of algebra.)

Suppose P and Q are rational, will R be rational? Will it be true for all elliptic curves?

c.) It is clear that potentially you can generate a lot, or even an infinite number of these points. Now we can ask the question, is there an algebraic structure behind this generation of rational points? Can we add two points to get a third point? The answer is yes, but in a subtle way.

FIRST, explore and decide whether we can form a group if we define the above chord operation, we can call it *, so P*Q= R becomes a group operation?

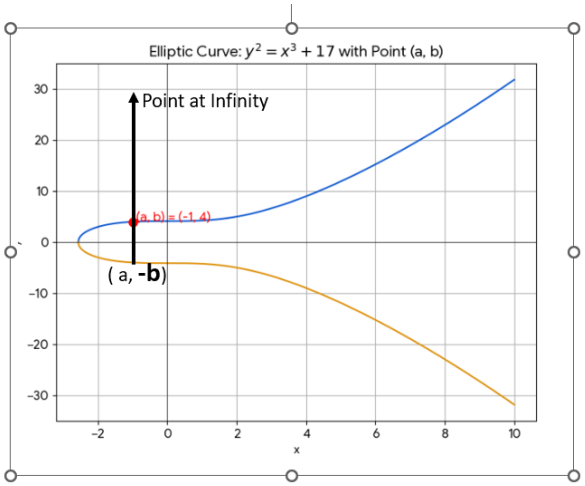
What problems will we face if we try to make this as the group law of addition of points? (Recall that for a group, you also need an identity element, and inverse element and associativity.

d.) What happens to the chord operation if we take P = Q. And also if we take P = (a, b) and Q = (a, -b)? Are these defined? What problems do we encounter?

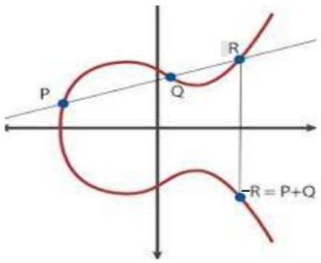
Problem 2. In Problem 1, you may noticed a few problems with defining the addition of two points P and Q to be the third point R, the point of intersection of the chord joining the first two points and the elliptic curve. Also, the chord construction seems to fail if we have a vertical chord !!! Actually, the second observation is very deep.

a.) Since we have this problem with any pair of points on vertical lines, we may as well define that points (a,b) and (a, -b) "intersect the elliptic curve at infinity" and call that point O. **Can this be the identity element of the group? Let's proceed assuming it is**.

b.) We want a chord joining any points P and Q to intersect at a third point. If we take a point (a, b) and take the point at infinity, WHAT IS THE POINT OF intersection of the chord joining P and the point at infinity with the curve? Look at the following picture.



However, if the point at infinity O is to be identified as the identity element 0, WE ALSO minimally expect that P + O = P. So, the addition would work ONLY if after joining the chord and getting a third point and then we reflect that third point against the x axis. So the law of adding two points is as shown in the picture below.



c.) Show that identifying the point at infinity O with the identity element 0 of the group makes the point P=(x,y) and Q=(x,-y) as inverse of each other. Also P + O = P for all P.

d.) Show that three collinear points P, Q, R on an elliptic curve satisfies P+Q+R = 0

e.) Calculate P + P where P is (-1, 4) for the curve $y^2 = x^3 + 17$.

f.) **What about associativity?**

Problem 3. **The Grand Result:** "The set of rational points E(Q), together with this operation , forms an **Abelian Group**. This is the central fact of elliptic curves."

Obviously the question is WHAT IS THE STRUCTURE OF THE GROUP? THIS IS still an area of active research. BUT THE FOUNDATIONAL THEOREM due to Mordell in 1922 is

Theorem (Mordell): "The group $E(\mathbb{Q})$ is **finitely generated**. This means every rational point P can be written as:

$$P = n_1P_1 + n_2P_2 + \cdots + n_rP_r + T$$

where $P_1, \ldots, P_r$ are special points of *infinite order*, T is a point of *finite order*, and n_i are integers."

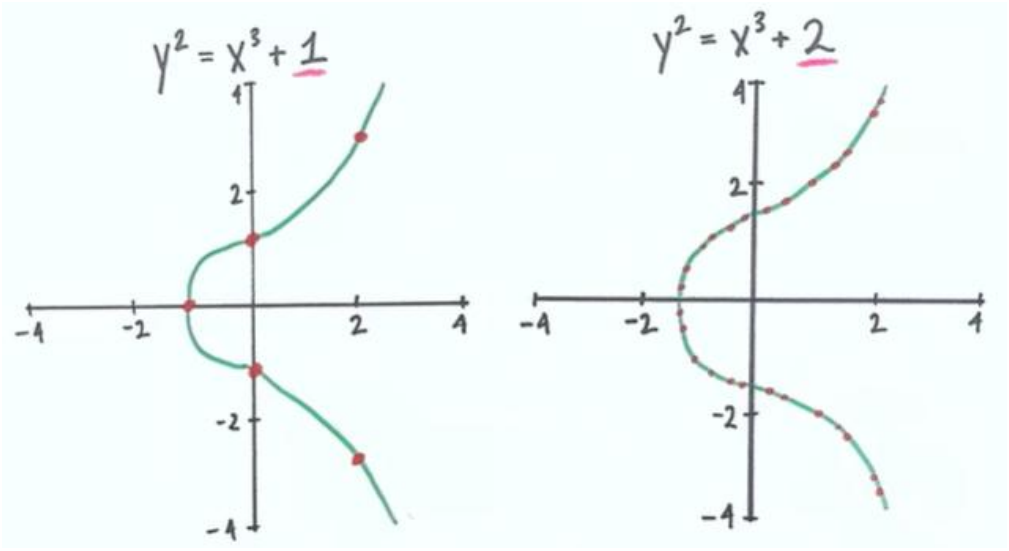
Let's explore this through simple examples: Note that the group is finitely generated but can be infinite. The Group T is called Torsion group. T is finite. E(Q) is characterised by rank r and Torsion group T.

a.) Find all **two torsion points** (First understand what that means) for the cubic curves

$y^2 = x^3 - 4x$ and $y^2 = x^3 - 1$

b.) Determining rank and the torsion group for a given elliptic curve are not trivial. The group of rational points for $y^2 = x^3 + 17$ has rank r= 2. The torsion group is trivial. See if you can identify the generators of the infinite part. The reason its torsion group is trivial is not easy to show.

c.) you can also play around with many other cubic equations. Such as



d.) There are several famous conjectures related to Ranks which we will discuss in the class. One is the rank conjecture and the other one Birch and Swinnerton-Dyer conjecture, Time permitting I will tell you what these are. If you have followed the worksheet so far, you will be able to understand the conjectures.