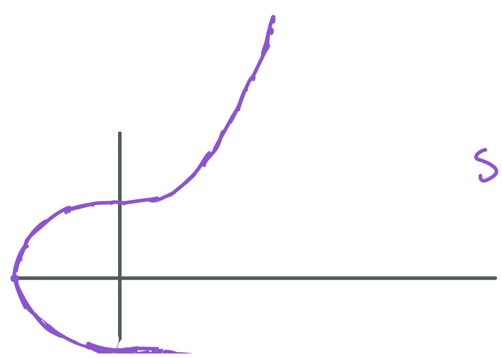
Math 4400

Week 14 - Tuesday

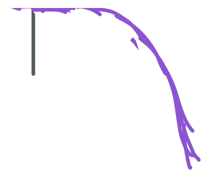
Elliptic curves

We've spent a lot of time talking about degree 2 (i.e. quadratic) equations... what about degree 3?

Example: $E: y^2 = x^3 + 8$



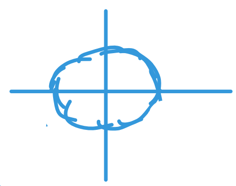
Solutions in $\mathbb{R}^2$



Amazing fact: the points on this curve* form a <u>group</u>.

Note: actually have already seen similar things:

- the real solutions to $x^2+y^2=1$

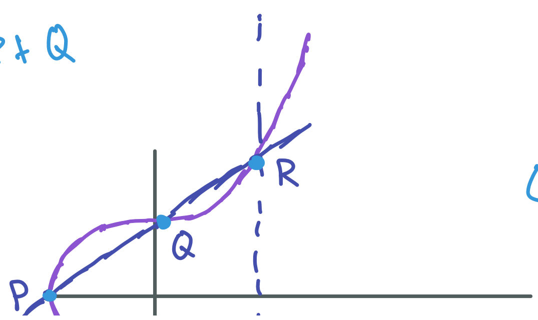


form a group if we view them as the unit circle $|z|=1$ in $\mathbb{C}$. $z \leftrightarrow x+yi$.

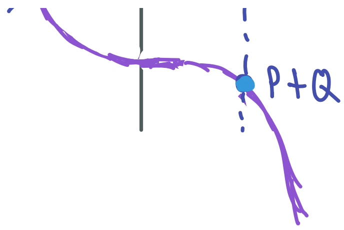
- In fact, for any D, the solutions to $x^2+Dy^2=1$ form a group (for integer solutions by working in $\mathbb{Z}[\sqrt{D}]$)

How to add 2 points:

To compute $P+Q$



Note if (x,y) is a solution so is $(x,-y)$

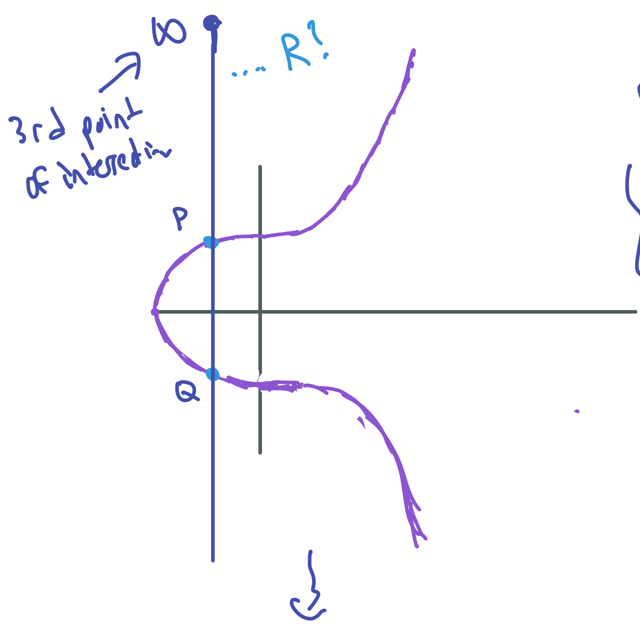


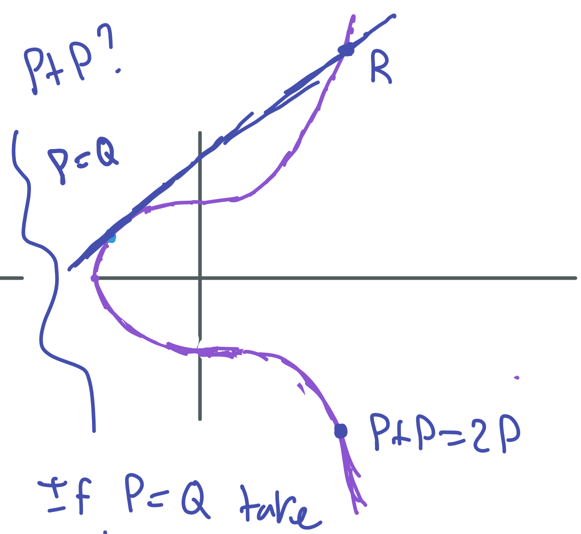
Addition law: To compute $P+Q$,

1. Draw the line through P and Q
2. Take its 3rd point of intersection with E
3. Reflect it across the x axis to get $P+Q$

This <u>almost</u> works. Two issues:

- What if P and Q have same x-coordinate?
- What if $P = Q$?





If $P=Q$ take tangent line.

Add one more point ∞ — corresponds to "vertical asymptote" of the graph.
i.e a point that lies on every vertical line

When we flip ∞ about the x-axis get ∞ back.
So $P+Q=\infty$ if P and Q are as in first picture

Fact: This really gives a commutative group law (with ∞ as the identity element).
Inverse of (x,y) is $(x,-y)$.

Fact: Works for any equation $y^2=x^3+Ax+B$ as long as x^3+Ax+B has no multiple roots.
(need to have a tangent line at every point).

Fact: Works over any field!

Fact: If A, B are integers, then there are only finitely many integer solutions. (Siegel).

Example: For $y^2=x^3+8$ here are some:
$(-2,0)$ $(1,3)$ $(1,-3)$ $(2,4)$ $(2,-4)$

Fact: If A, B are rational, then there can be infinitely many rational solutions to $y^2=x^3+Ax+B$,
BUT they can be generated from finitely many (like Pell's equation).

(Mordell–Weil theorem)

(Like integer solutions to Pell's equation!)

Fact: Fermat's Last Theorem – there are no non-trivial integer solutions to $x^n + y^n = z^n$ $n \geq 3$ – was proven in the 90s by Wiles (+Taylor) by reducing to a problem about elliptic curves

Fact: The Birch & Swinnerton Dyer conjecture – a Clay millenium problem with a \$1,000,000 prize – is about relating rational and mod p solutions to

$$y^2 = x^3 + Ax + B \quad \text{for } A, B \text{ integers}$$