

Week 7: Elliptic Curves

Jay Daigle

Occidental College

October 19, 2017

It is possible to write endlessly on elliptic curves.

It is possible to write endlessly on elliptic curves. (This is not a threat.)

Serge Lang





An example of the infinite dihedral group. We can accomplish any symmetry by combining a translation of some number of units with a possible 180° rotation.

An *elliptic curve* is:

An *elliptic curve* is:

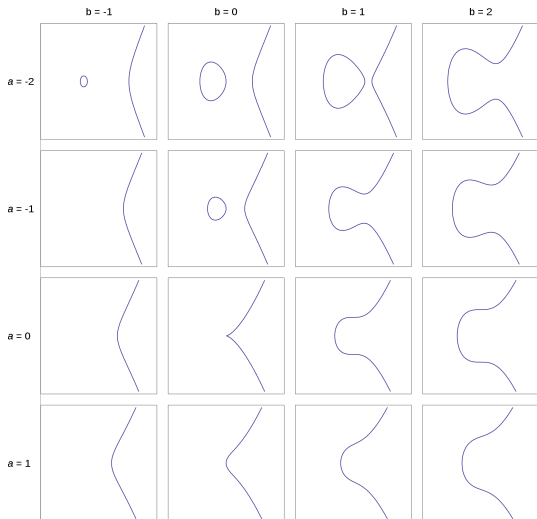
- A smooth projective genus 1 curve with a rational point

An *elliptic curve* is:

- A smooth projective genus 1 curve with a rational point
- $y^2 = x^3 + ax + b$

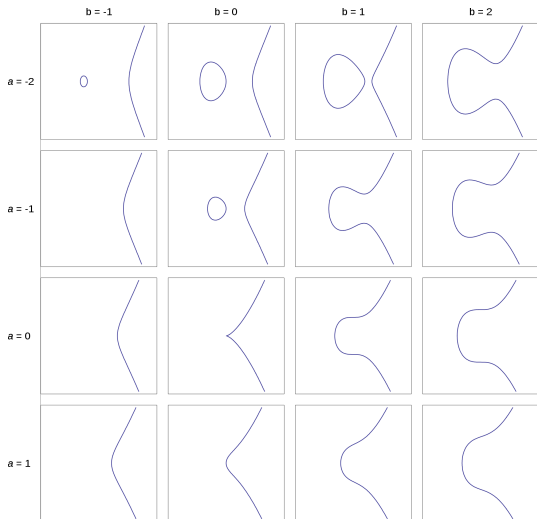
An *elliptic curve* is:

- A smooth projective genus 1 curve with a rational point
- $y^2 = x^3 + ax + b$
- *NOT* an ellipse!



An *elliptic curve* is:

- A smooth projective genus 1 curve with a rational point
- $y^2 = x^3 + ax + b$
- *NOT* an ellipse!

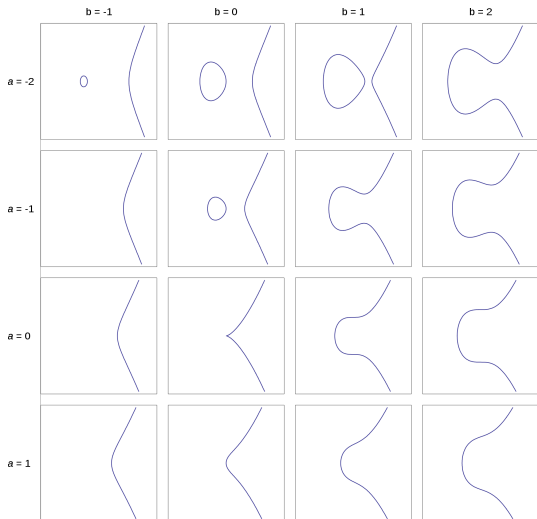


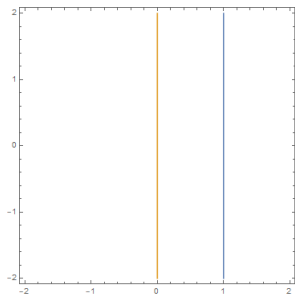
An *elliptic curve* is:

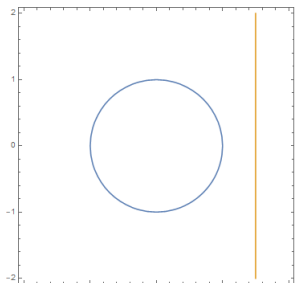
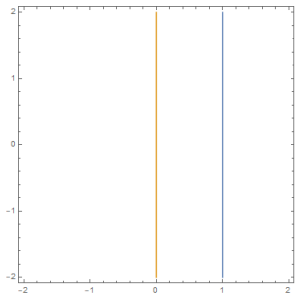
- A smooth projective genus 1 curve with a rational point
- $y^2 = x^3 + ax + b$
- *NOT* an ellipse!

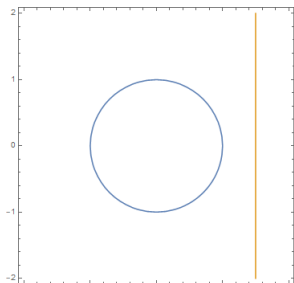
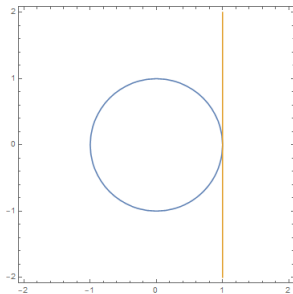
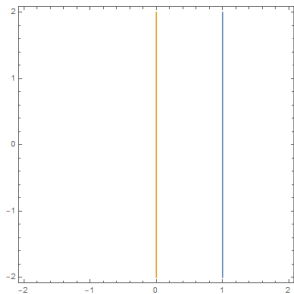
Key Question

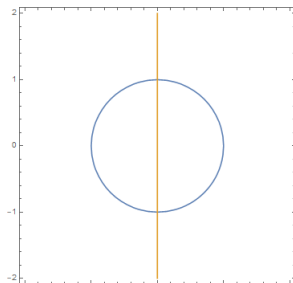
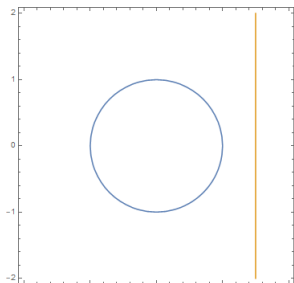
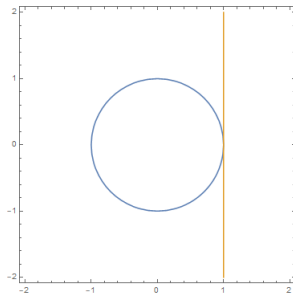
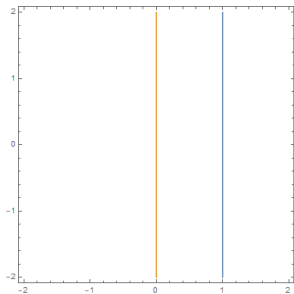
How many rational points are there?

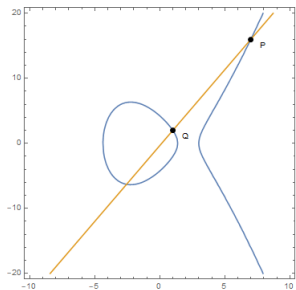


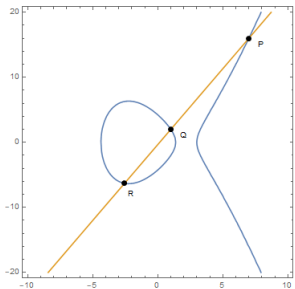
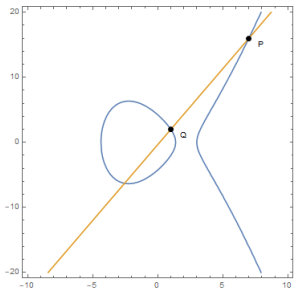


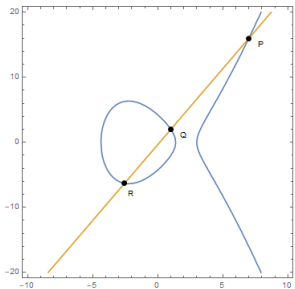
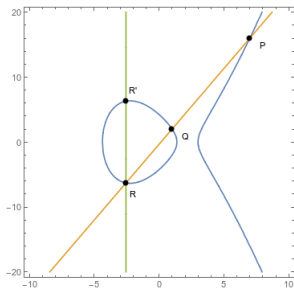
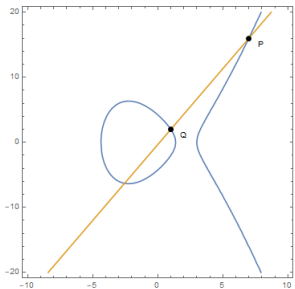












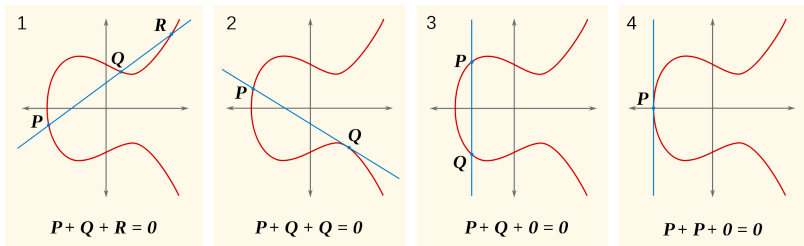


Figure: The group law on elliptic curves
Emmanuel Boutet / CC-BY-SA-3.0

