## Week 7: Elliptic Curves

Jay Daigle

Occidental College

October 19, 2017

Jay Daigle (Occidental College)

Week 7: Elliptic Curves

Jay Daigle (Occidental College)

Week 7: Elliptic Curves

October 19, 2017 2 / 9

It is possible to write endlessly on elliptic curves.

-

< 1 →

э

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

Serge Lang

э

Jay Daigle (Occidental College)

Week 7: Elliptic Curves

October 19, 2017 3 / 9



\*ロト \*部ト \*注ト \*注ト



An example of the infinite dihedral group. We can accomplish any symmetry by combining a translation of some number of units with a possible  $180^{\circ}$  rotation.

Jay Daigle (Occidental College)

Week 7: Elliptic Curves

October 19, 2017 3 / 9

글 🕨 🖌 글

A D

Jay Daigle (Occidental College)

Week 7: Elliptic Curves

October 19, 2017 4 / 9

◆□ > ◆□ > ◆臣 > ◆臣 > ─ 臣

• A smooth projective genus 1 curve with a rational point

-∢ ≣ →

- ∢ 同 ▶ - ∢ 三

э

• A smooth projective genus 1 curve with a rational point

• 
$$y^2 = x^3 + ax + b$$

-∢ ≣ →

- ∢ 同 ▶ - ∢ 三

э

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



(日)

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



(日)

- 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?



3

Jay Daigle (Occidental College)









Jay Daigle (Occidental College)



<ロ> <同> <同> < 同> < 同>



Week 7: Elliptic Curves

October 19, 2017 6 / 9

- 2

<ロ> <同> <同> < 同> < 同>





<ロ> <同> <同> < 同> < 同>



æ



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

Jay Daigle (Occidental College)

Week 7: Elliptic Curves

э

< 同 ▶

글 🕨 🖌 글



・ロト ・四ト ・ヨト ・ヨト



<ロ> <同> <同> < 同> < 同>