Week 7: Elliptic Curves

Jay Daigle

Occidental College

October 9, 2018

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:

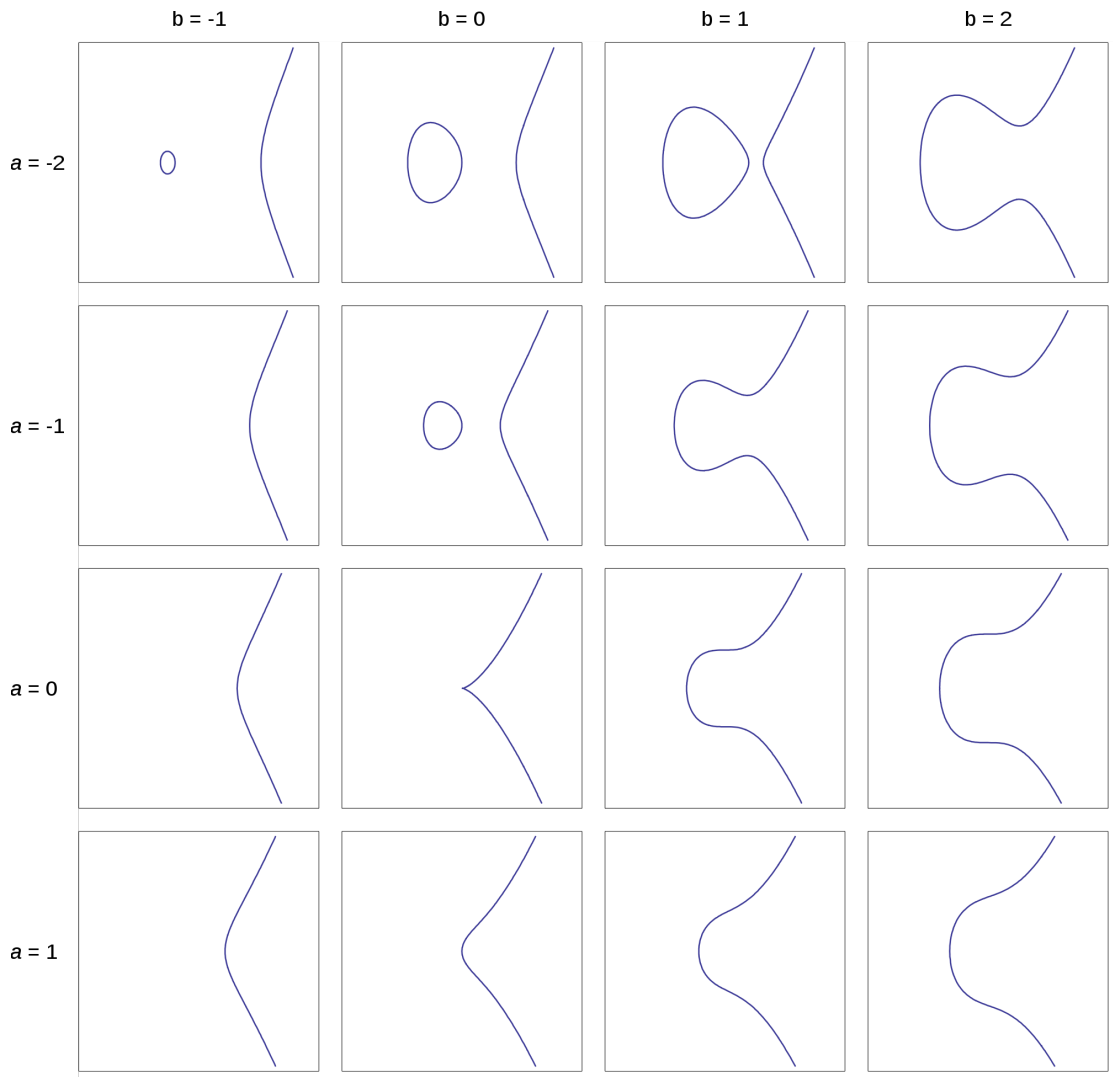
- A smooth projective genus 1 curve with a rational point

An *elliptic curve* is:

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

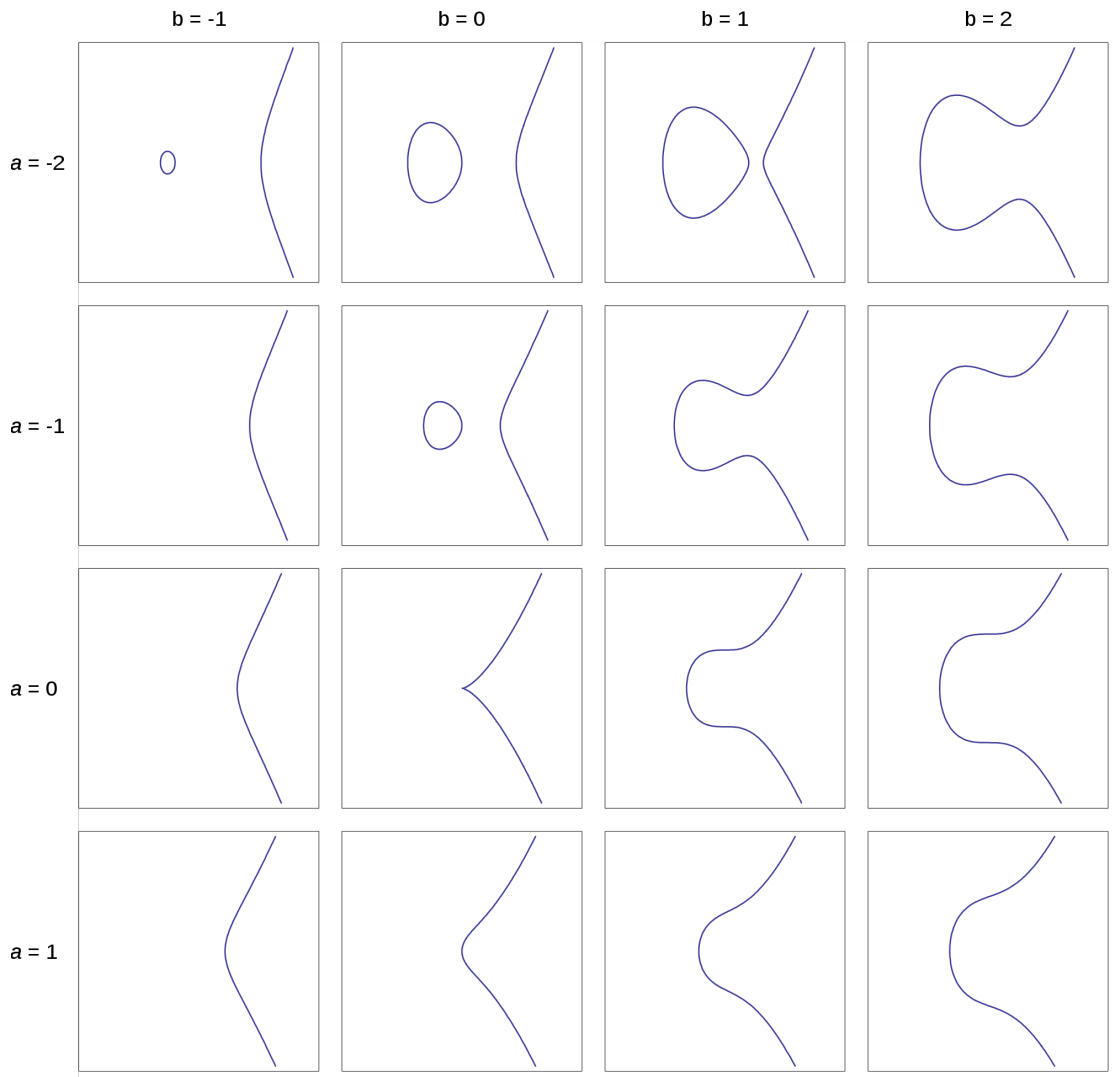
An *elliptic curve* is:

- 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!

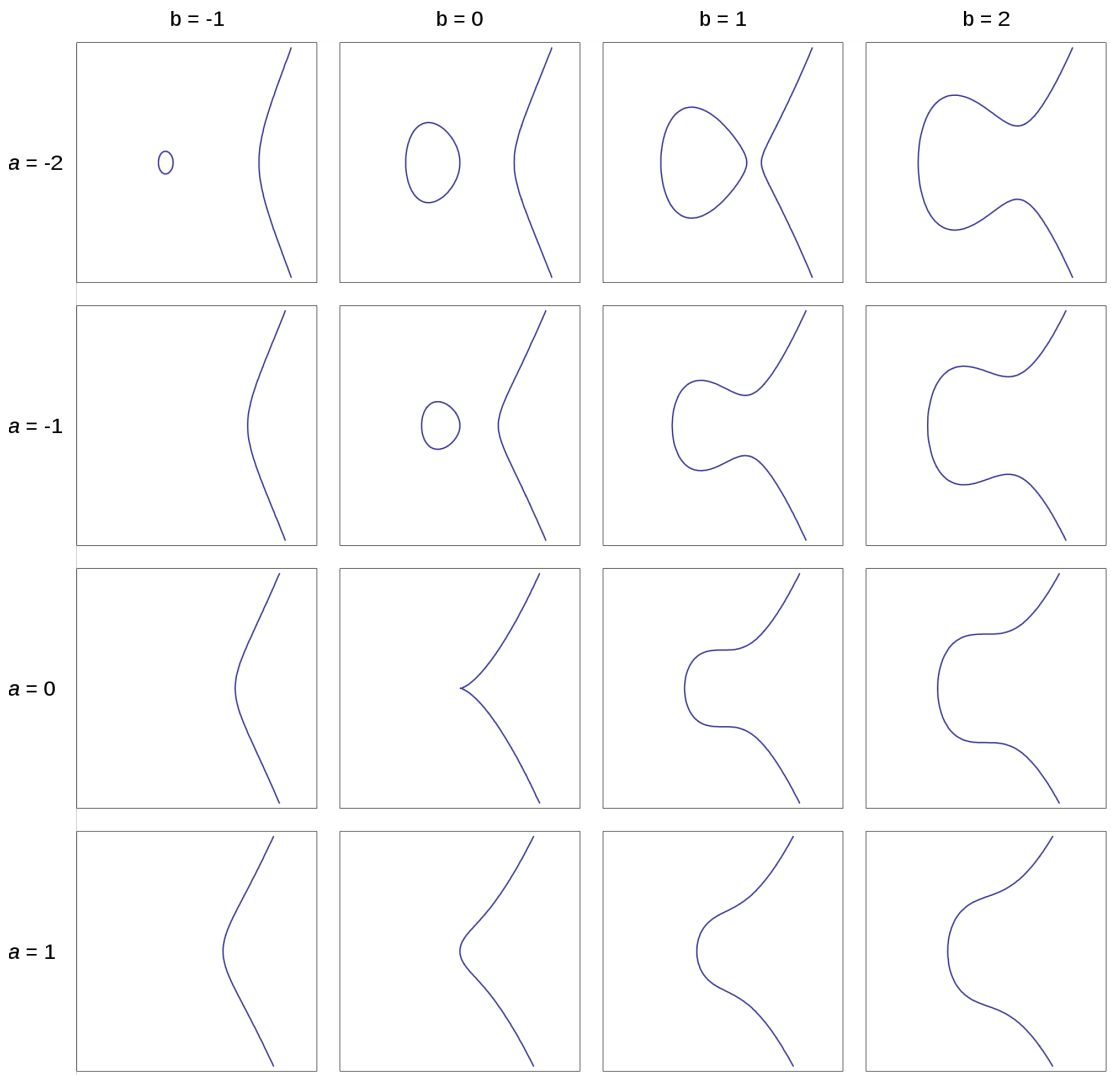


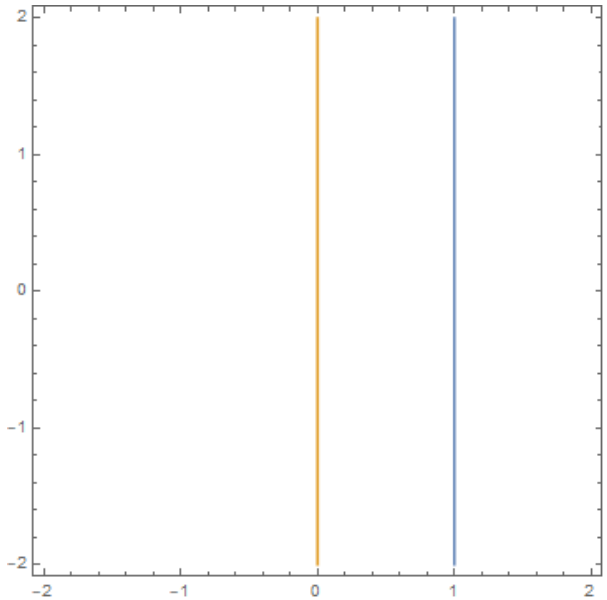
An *elliptic curve* is:

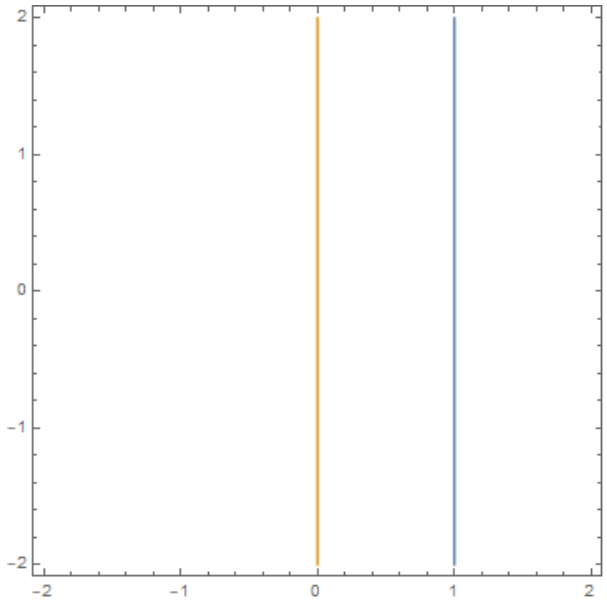
- A smooth projective genus 1 curve with a rational point
- $y^2 = x^3 + ax + b$
- *NOT* an ellipse!

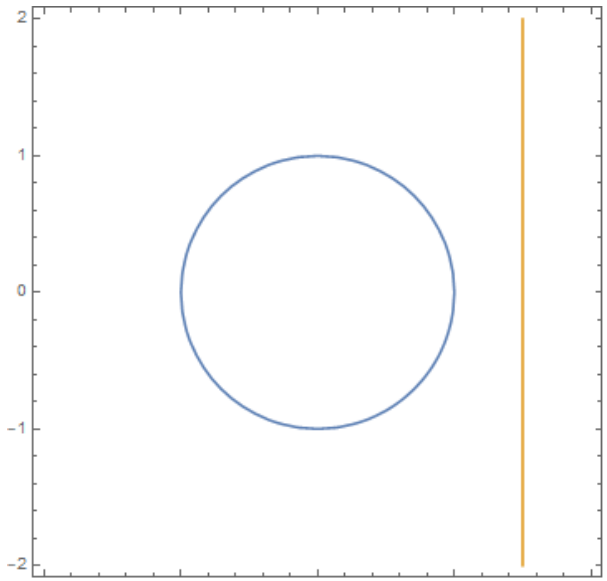
Key Question

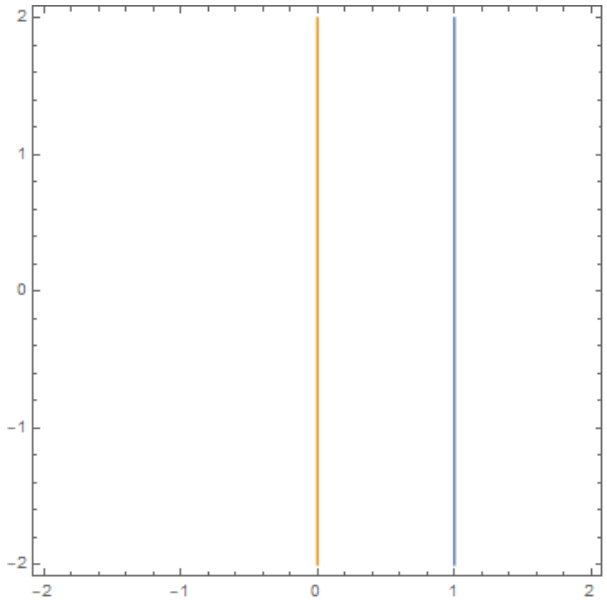
How many rational points are there?

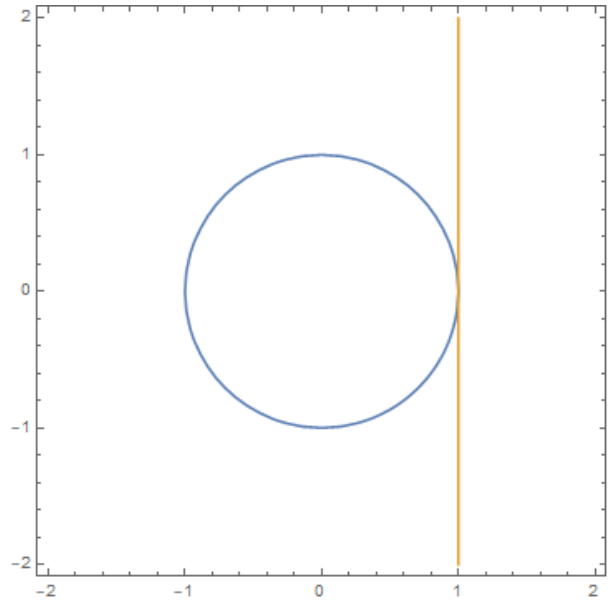


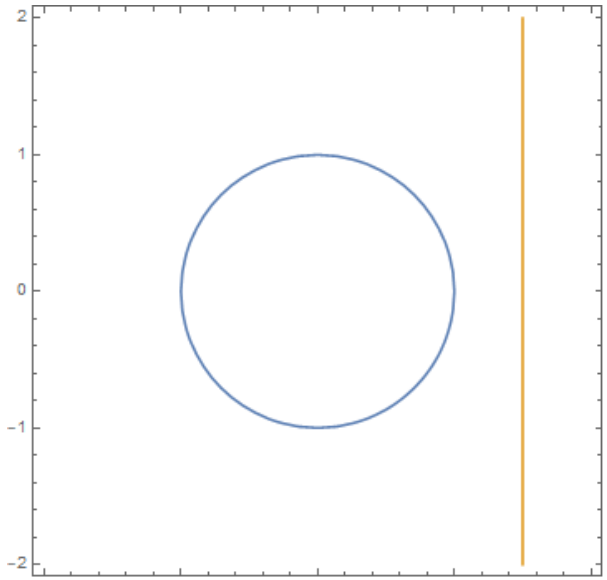

2
1
0
−1
−2
−2
−1
0
1
2

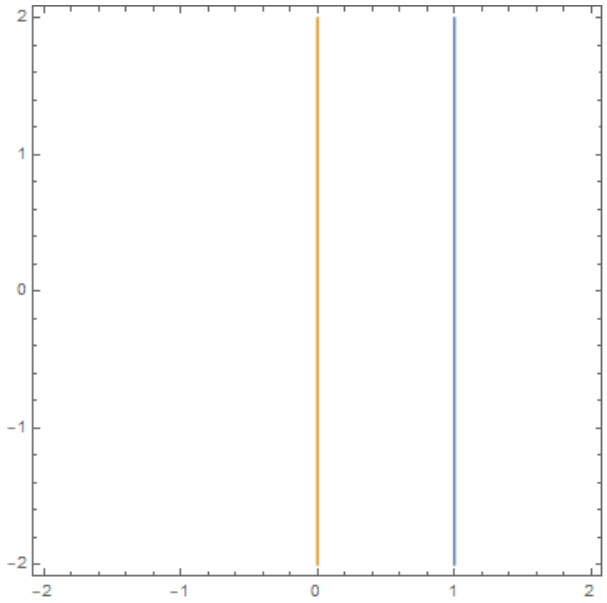

2
1
0
−1
−2
−2
−1
0
1
2

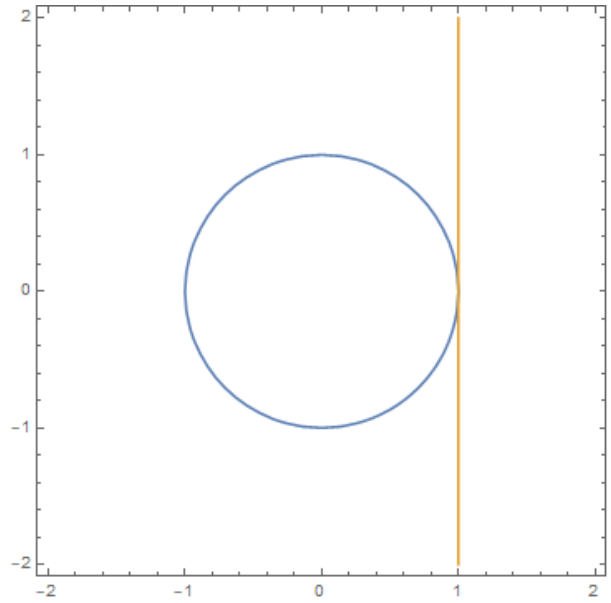

2
1
0
−1
−2

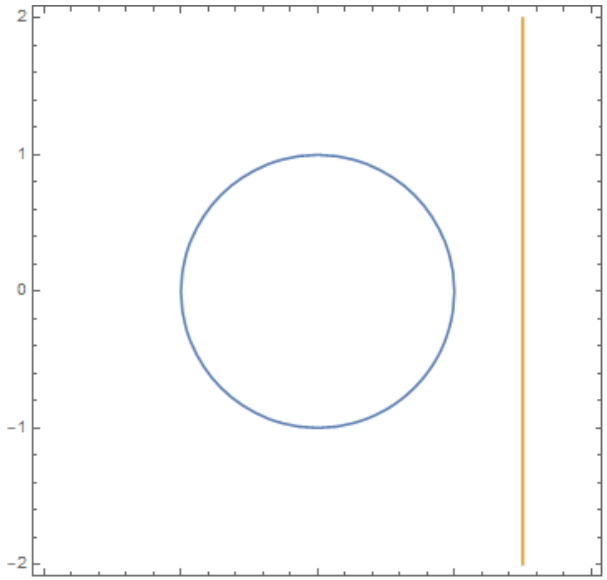

2
1
0
−1
−2
−2
−1
0
1
2

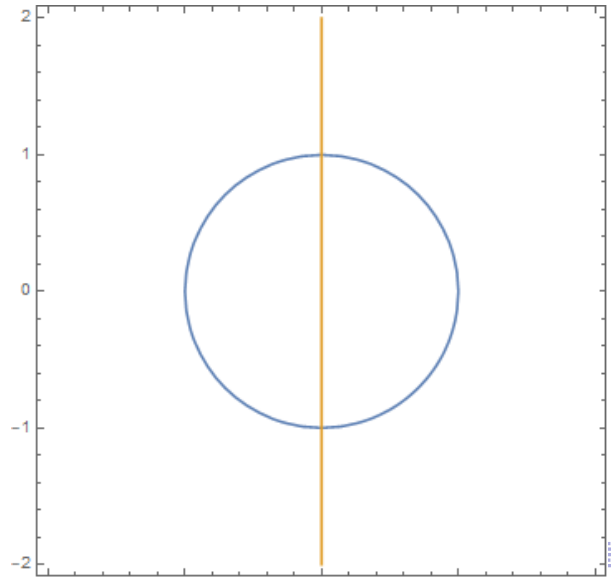

2
1
0
−1
−2
−2
−1
0
1
2

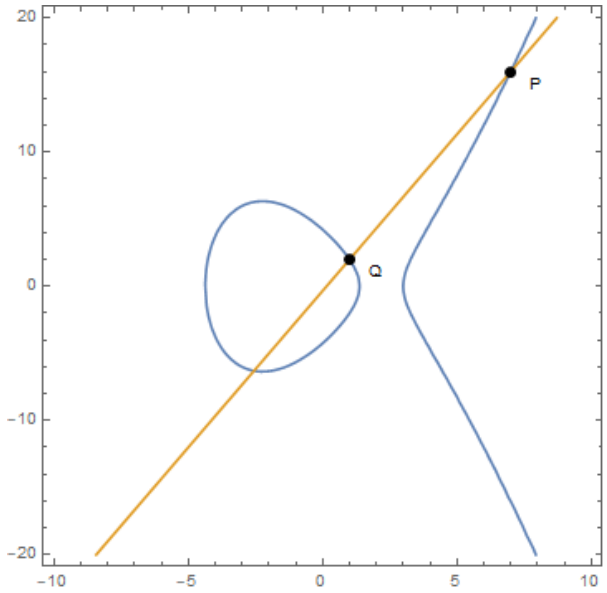

2
1
0
−1
−2

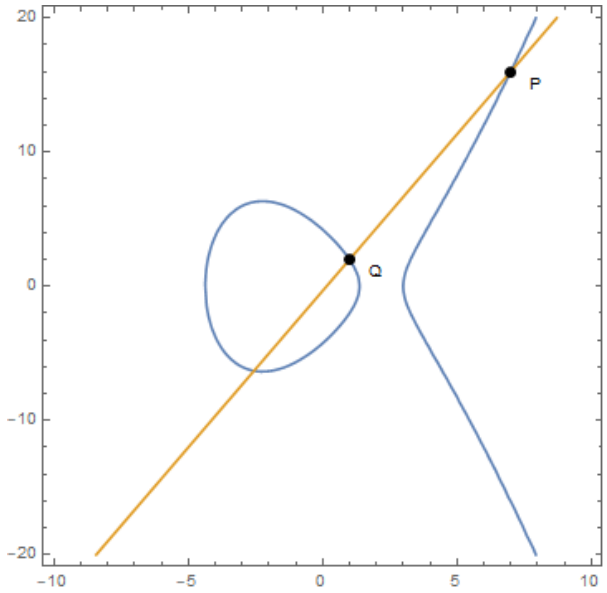

2
1
0
−1
−2
−2
−1
0
1
2

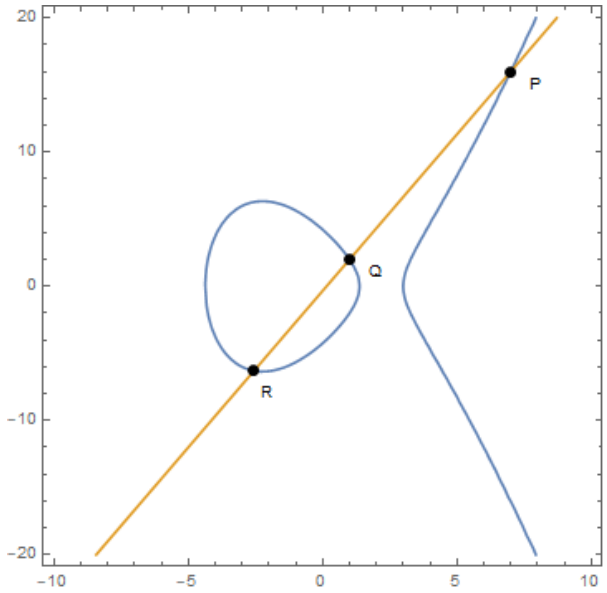

2
1
0
−1
−2
−2
−1
0
1
2

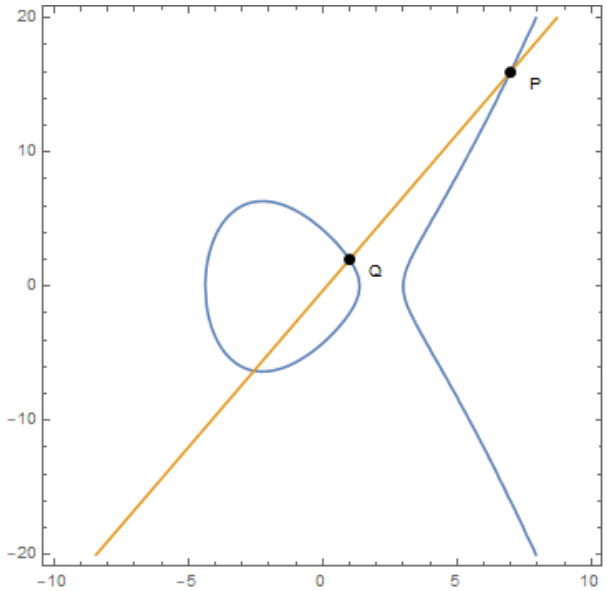

2
1
0
−1
−2

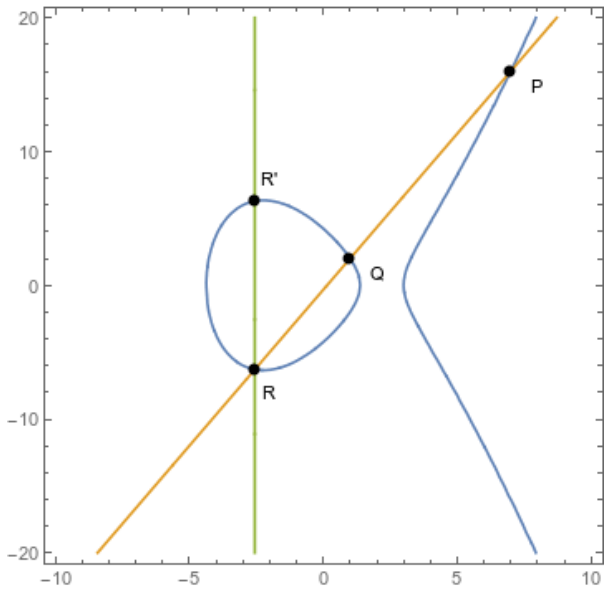

2
1
0
−1
−2

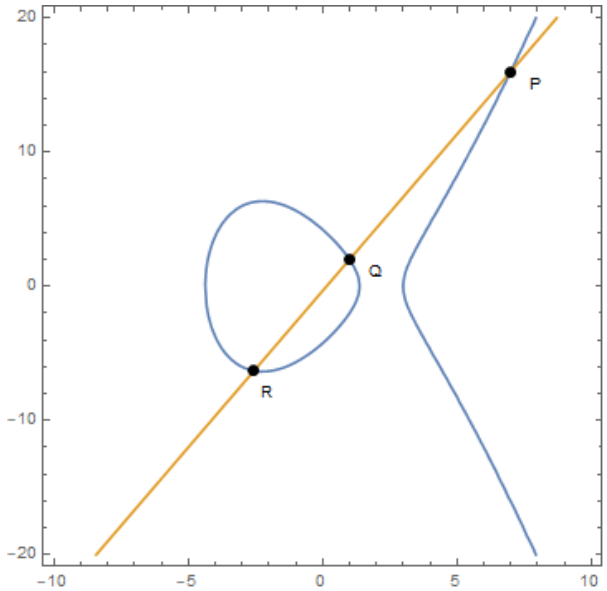

P
Q
20
10
0
−10
−20
−10
−5
0
5
10


P
Q
20
10
0
−10
−20
−10
−5
0
5
10


P
Q
R
20
10
0
−10
−20
−10
−5
0
5
10


P
Q


P
R'
Q
R


P
Q
R

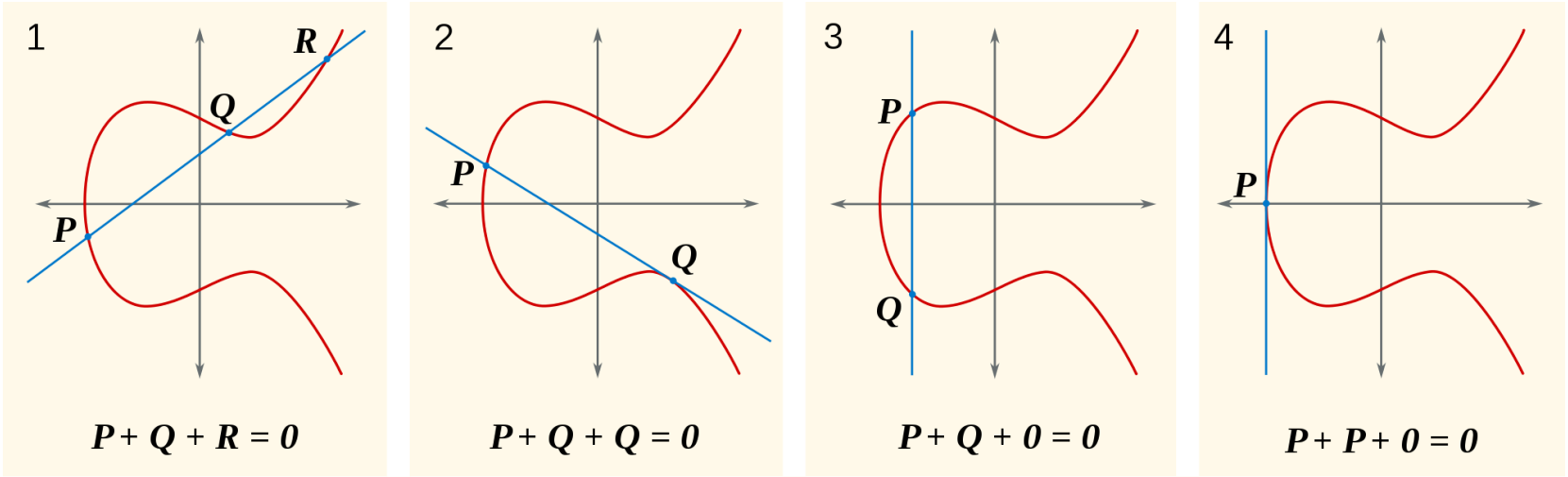
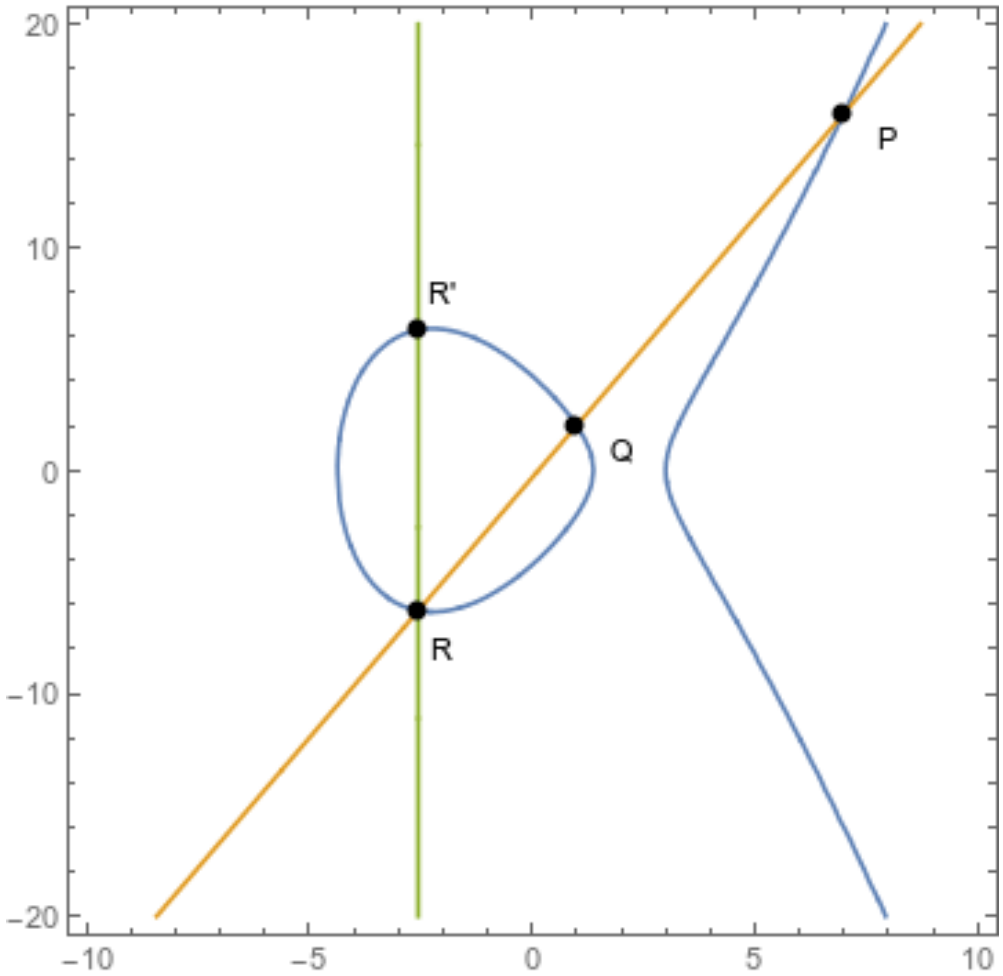
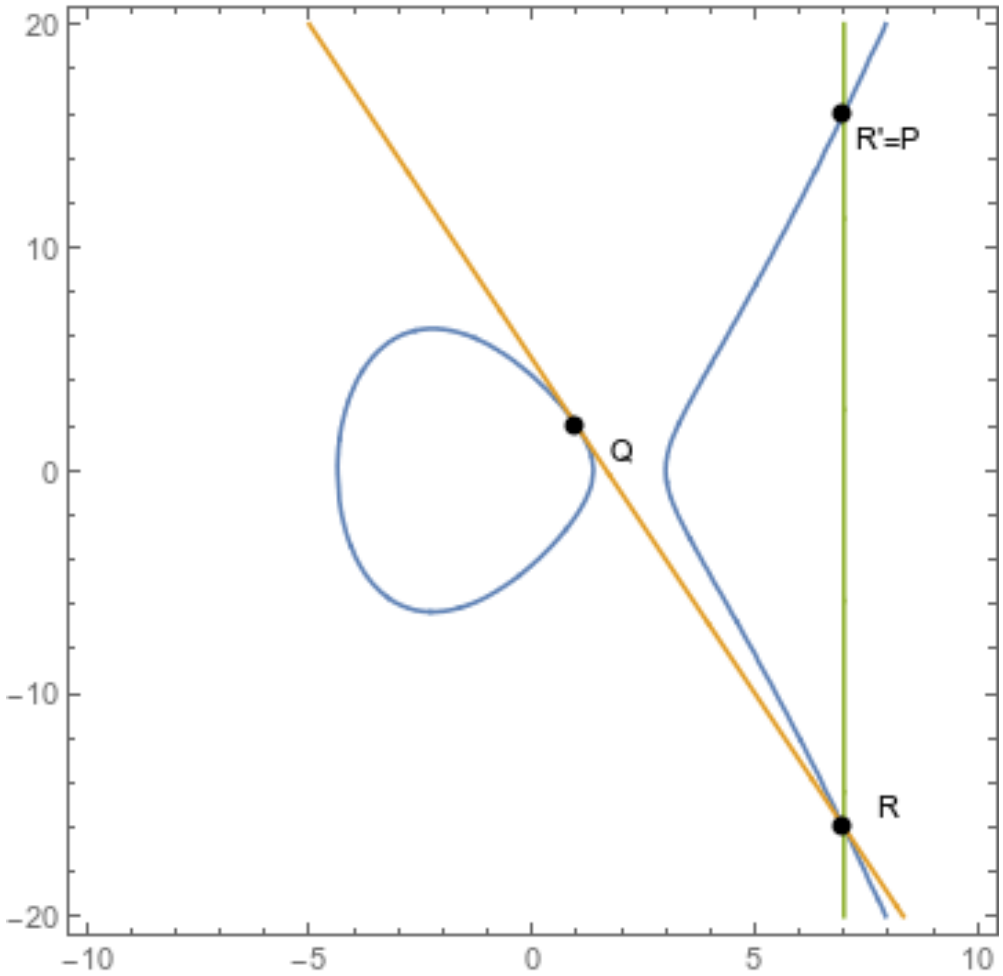


Figure: The group law on elliptic curves
Emmanuel Boutet / CC-BY-SA-3.0


20
10
0
−10
−20
−10
−5
0
5
10
P
R'
Q
R


20
10
0
−10
−20
−10
−5
0
5
10
R'=P
Q
R