Week 7: Elliptic Curves

Jay Daigle

Occidental College

October 10, 2019

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

Groups

Groups

Definition

A group is a set G and a binary operation $\star : G \times G \to G$ with the properties that:

Groups

Definition

A group is a set G and a binary operation $\star : G \times G \to G$ with the properties that:

1. *Identity element: There is a $e \in G$ such that $e \star g = g \star e = g$ for all $g \in G$*

Groups

Definition

A group is a set G *and a binary operation* $\star : G \times G \to G$ *with the properties that:*

1. *Identity element: There is a* $e \in G$ *such that* $e \star g = g \star e = g$ *for all* $g \in G$
2. *Inverses: For every* $g \in G$*, there is an inverse element* g^{-1} *such that* $g \star g^{-1} = g^{-1} \star g = e$

Groups

Definition

A group is a set G and a binary operation $\star : G \times G \to G$ with the properties that:

1. *Identity element: There is a $e \in G$ such that $e \star g = g \star e = g$ for all $g \in G$*
2. *Inverses: For every $g \in G$, there is an inverse element g^{-1} such that $g \star g^{-1} = g^{-1} \star g = e$*
3. *Associative: for every $f, g, h \in G$ we have $(f \star g) \star h = f \star (g \star h)$.*

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.

Fields

Fields

Definition

A field is a set K together with two operations $+$ and $\cdot$, such that

Fields

Definition

A field is a set K together with two operations $+$ and $\cdot$, such that

1. *K is an abelian group under the operation $+$;*

Fields

Definition

A field is a set K together with two operations $+$ and $\cdot$, such that

1. *K is an abelian group under the operation $+$;*
2. *The set $K \setminus \{0\}$ of non-zero elements of K is an abelian group under $\cdot$;*
3. *and we have the distributive law $k(x+y) = kx + ky$.*

An *elliptic curve* is:

An *elliptic curve* is:

- A smooth projective genus 1 curve with a rational point

An *elliptic curve* is:

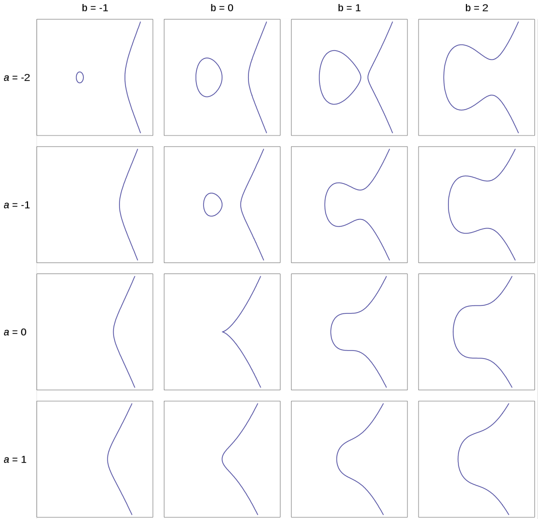
- A smooth projective genus 1 curve with a rational point
- $y^2 = x^3 + ax + b$

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!

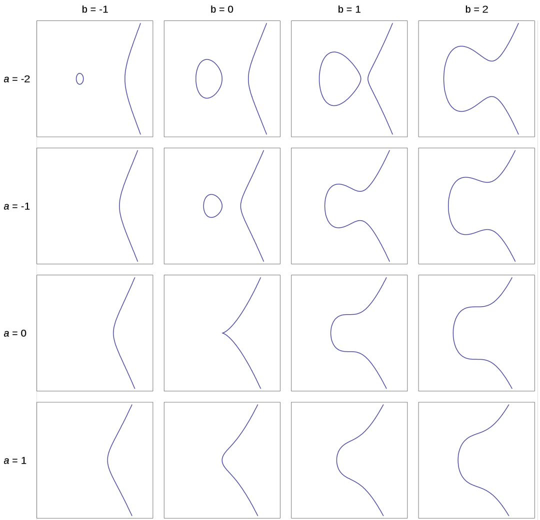


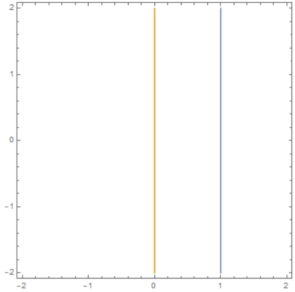
An *elliptic curve* is:

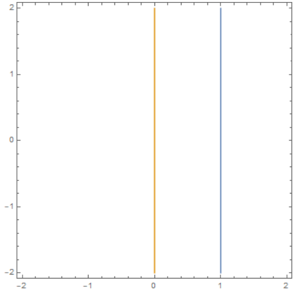
- A smooth projective genus 1 curve with a rational point
- $y^2 = x^3 + ax + b$
- *NOT* an ellipse!

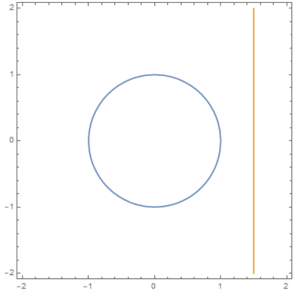
Key Question

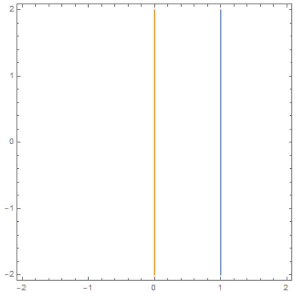
How many rational points are there?

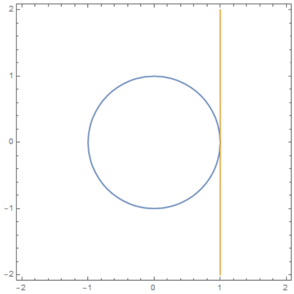


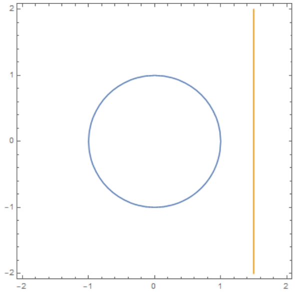

2
1
0
-1
-2
-2
-1
0
1
2

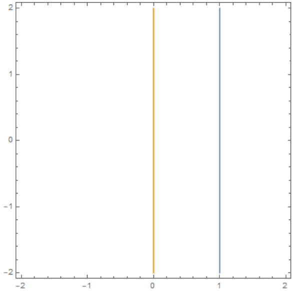

2
1
0
−1
−2
−2
−1
0
1
2

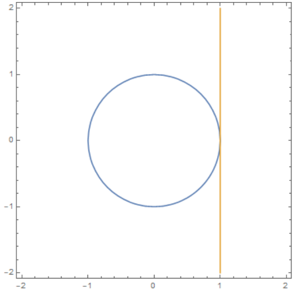

2
1
0
−1
−2
−2
−1
0
1
2

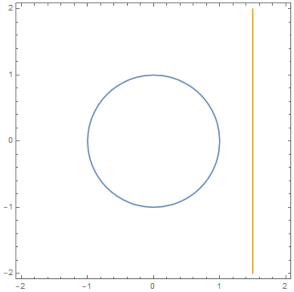

2
1
0
−1
−2
−2 −1 0 1 2

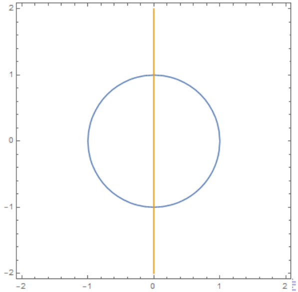

2
1
0
−1
−2
−2 −1 0 1 2

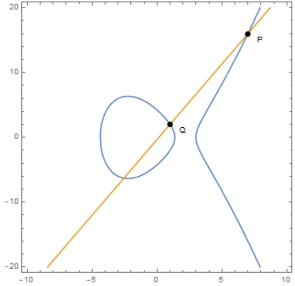

2
1
0
−1
−2
−2 −1 0 1 2

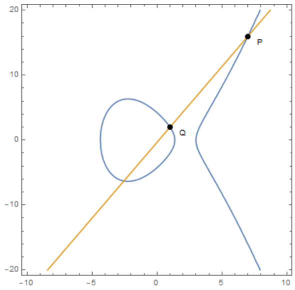

2
1
0
−1
−2
−2 −1 0 1 2

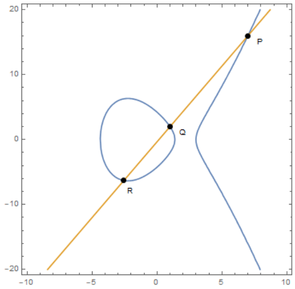

2
1
0
−1
−2
−2 −1 0 1 2

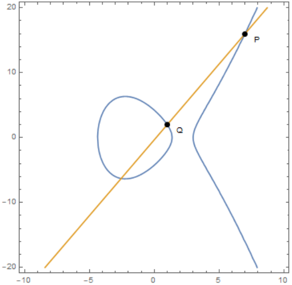

2
1
0
−1
−2
−2 −1 0 1 2

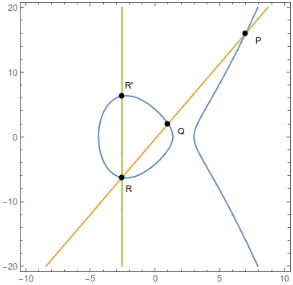

2
1
0
−1
−2
−2 −1 0 1 2

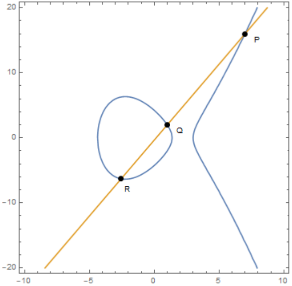

20
10
0
−10
−20
−10
−5
0
5
10
P
Q


P
Q


P
Q
R


P
Q
20
10
0
−10
−20
−10
−5
0
5
10


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


P
Q
R
20
10
0
−10
−20
−10
−5
0
5
10

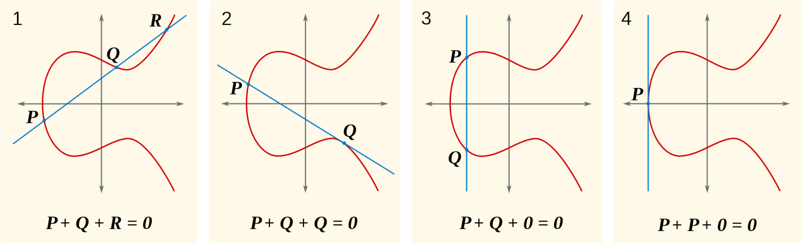
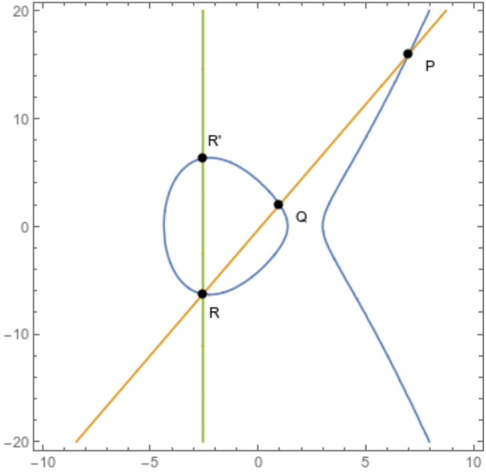
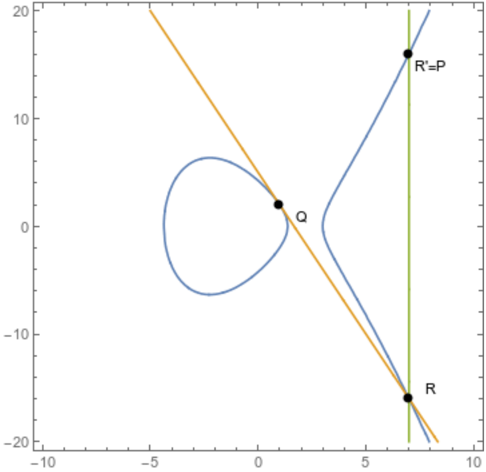


Figure: The group law on elliptic curves
Emmanuel Boutet / CC-BY-SA-3.0


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


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