Group Structure on an Elliptic Curve

Sam Mergendahl

December 4, 2015

A Couple of Definitions

- A rational cubic is a cubic polynomial with coefficents in $\mathbb{Q}$

A Couple of Definitions

- A rational cubic is a cubic polynomial with coefficents in $\mathbb{Q}$
- Any cubic with a rational point can be transformed through linear transformations into Weierstrass Normal Form

A Couple of Definitions

- A rational cubic is a cubic polynomial with coefficents in $\mathbb{Q}$
- Any cubic with a rational point can be transformed through linear transformations into Weierstrass Normal Form
  (ie) $y^2 = f(x) = x^3 + ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}$

A Couple of Definitions

- A rational cubic is a cubic polynomial with coefficents in $\mathbb{Q}$
- Any cubic with a rational point can be transformed through linear transformations into Weierstrass Normal Form
  (ie) $y^2 = f(x) = x^3 + ax^2 + bx + c$ where $a, b, c \in \mathbb{Z}$
- Let $C(\mathbb{Q}) = \{P = (x, y) \in C \mid x, y \in \mathbb{Q}\}$ be the set of points on C with rational cordinates

A Couple of Definitions (*cont.*)

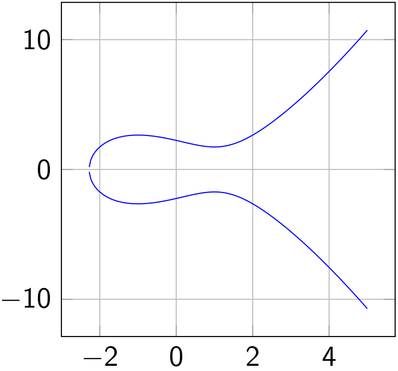
- if $f(x)$ has distinct complex roots we call it an elliptic curve

A Couple of Definitions (*cont.*)

- if $f(x)$ has distinct complex roots we call it an elliptic curve (ie) it is non-singular or its discriminant $\neq 0$

A Couple of Definitions (*cont.*)

- if $f(x)$ has distinct complex roots we call it an elliptic curve
  (ie) it is non-singular or its discriminant $\neq 0$
  (eg) $y^2 = x^3 - 3x + 5$



Intersecting Points

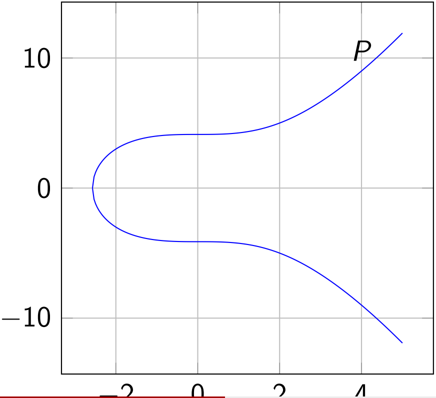
- How could we make the set of points on the elliptic curve a group?

Intersecting Points

- How could we make the set of points on the elliptic curve a group?
- Given curve C and $P, Q \in C(\mathbb{Q})$, does the rational line generated from P and Q always intersect C at 3 points?

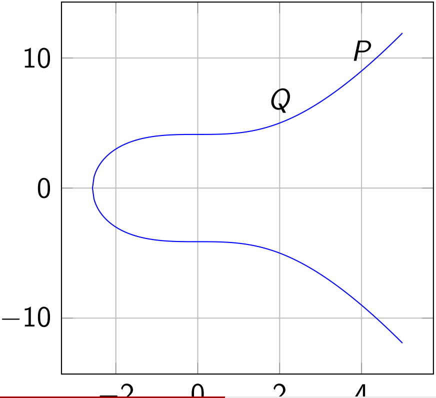
Intersecting Points

- How could we make the set of points on the elliptic curve a group?
- Given curve C and $P, Q \in C(\mathbb{Q})$, does the rational line generated from P and Q always intersect C at 3 points?
  (eg) $y^2 = x^3 + 17$ intersect with rational line generated by points $P = (4, 9)$ and $Q = (2, 5)$



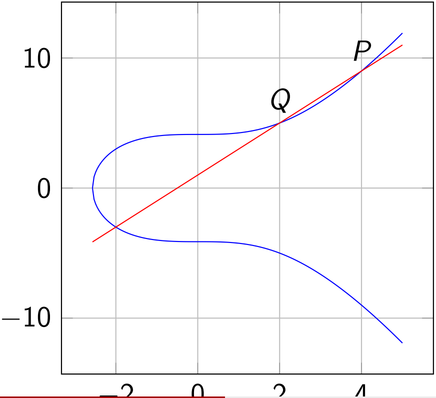
Intersecting Points

- How could we make the set of points on the elliptic curve a group?
- Given curve C and $P, Q \in C(\mathbb{Q})$, does the rational line generated from P and Q always intersect C at 3 points?
  (eg) $y^2 = x^3 + 17$ intersect with rational line generated by points $P = (4, 9)$ and $Q = (2, 5)$



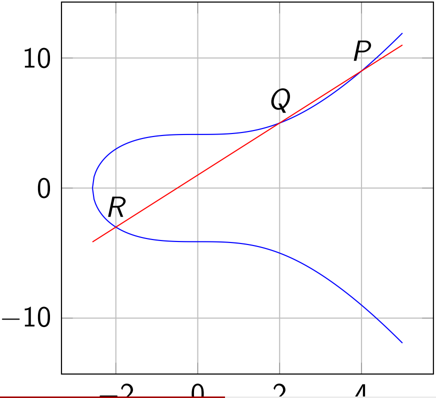
Intersecting Points

- How could we make the set of points on the elliptic curve a group?
- Given curve C and $P, Q \in C(\mathbb{Q})$, does the rational line generated from P and Q always intersect C at 3 points?
  (eg) $y^2 = x^3 + 17$ intersect with rational line generated by points $P = (4, 9)$ and $Q = (2, 5)$



Intersecting Points

- How could we make the set of points on the elliptic curve a group?
- Given curve C and $P, Q \in C(\mathbb{Q})$, does the rational line generated from P and Q always intersect C at 3 points?
  (eg) $y^2 = x^3 + 17$ intersect with rational line generated by points $P = (4, 9)$ and $Q = (2, 5)$



Intersecting Points (*cont.)*

- In general, Bezout's Theorem tells us that two curves (one of degree m and the other of degree n) will intersect at mn points

Intersecting Points (*cont.*)

- In general, Bezout's Theorem tells us that two curves (one of degree m and the other of degree n) will intersect at mn points
- Now, we need to be careful of a few things

Intersecting Points (*cont.*)

- In general, Bezout's Theorem tells us that two curves (one of degree m and the other of degree n) will intersect at mn points
- Now, we need to be careful of a few things
  - projective space

Intersecting Points (*cont.*)

- In general, Bezout's Theorem tells us that two curves (one of degree m and the other of degree n) will intersect at mn points
- Now, we need to be careful of a few things
  - projective space
  - multiplicities

Intersecting Points (*cont.*)

- In general, Bezout's Theorem tells us that two curves (one of degree m and the other of degree n) will intersect at mn points
- Now, we need to be careful of a few things
  - projective space
  - multiplicities
- If we take the tangent line from $P \in C(\mathbb{Q})$ it will intersect at exactly one other rational point

Intersecting Points (*cont.*)

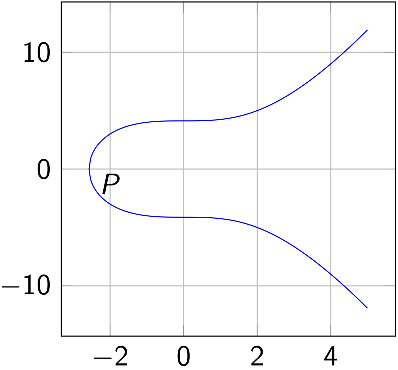
- In general, Bezout's Theorem tells us that two curves (one of degree m and the other of degree n) will intersect at mn points
- Now, we need to be careful of a few things
  - projective space
  - multiplicities
- If we take the tangent line from $P \in C(\mathbb{Q})$ it will intersect at exactly one other rational point
- Unless P is an inflection point, then it has multiplicity three and will not intersect anywhere else

Intersecting Points (*cont.*)

- Let's denote this process of connecting two rational points by a rational line to get a third rational point by *

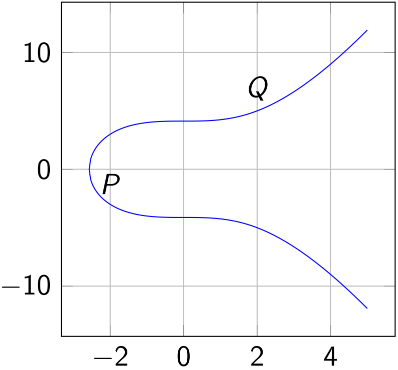
Intersecting Points (*cont.*)

- Let's denote this process of connecting two rational points by a rational line to get a third rational point by *



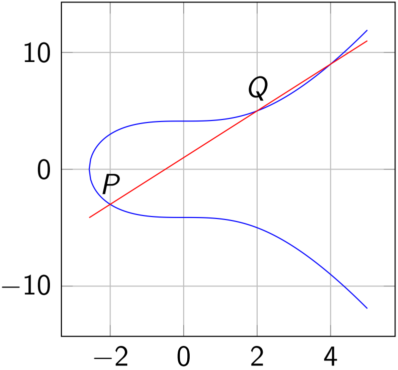
Intersecting Points (*cont.*)

- Let's denote this process of connecting two rational points by a rational line to get a third rational point by *



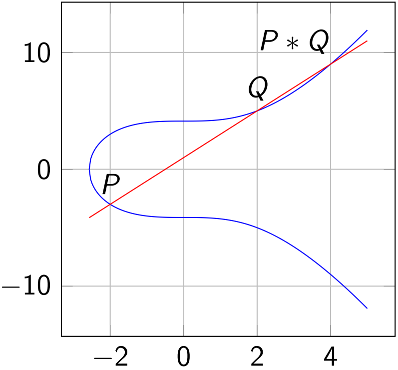
Intersecting Points (*cont.)*

- Let's denote this process of connecting two rational points by a rational line to get a third rational point by *



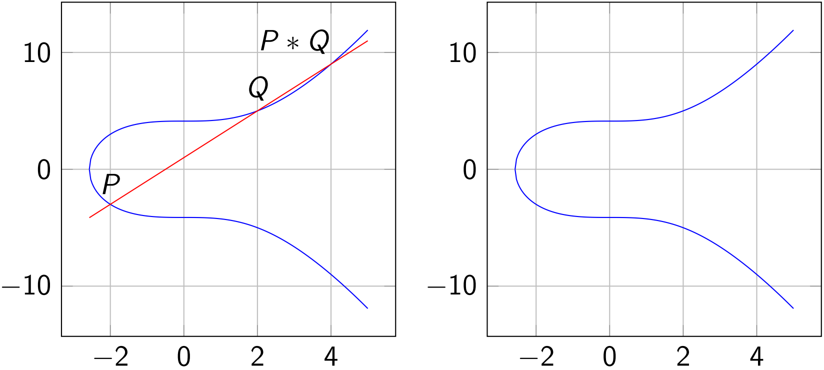
Intersecting Points (*cont.*)

- Let's denote this process of connecting two rational points by a rational line to get a third rational point by *



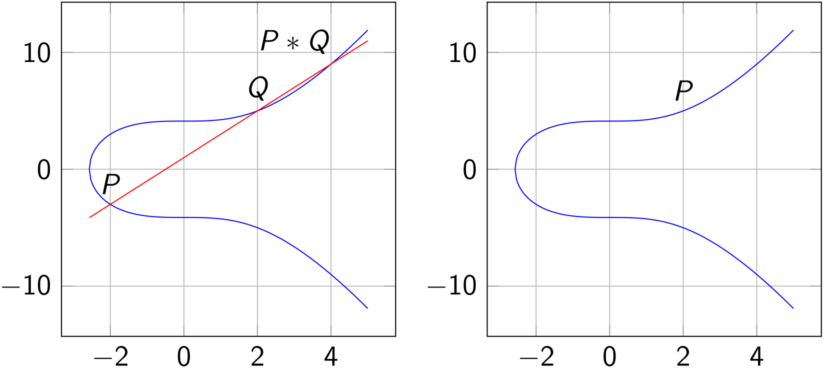
Intersecting Points (*cont.*)

- Let's denote this process of connecting two rational points by a rational line to get a third rational point by *



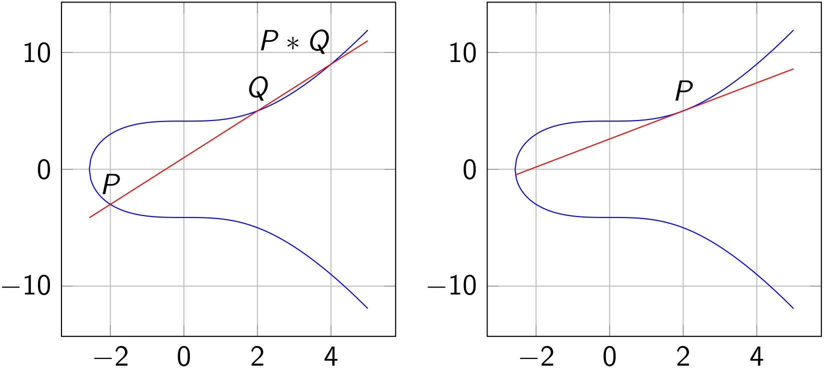
Intersecting Points (*cont.*)

- Let's denote this process of connecting two rational points by a rational line to get a third rational point by *



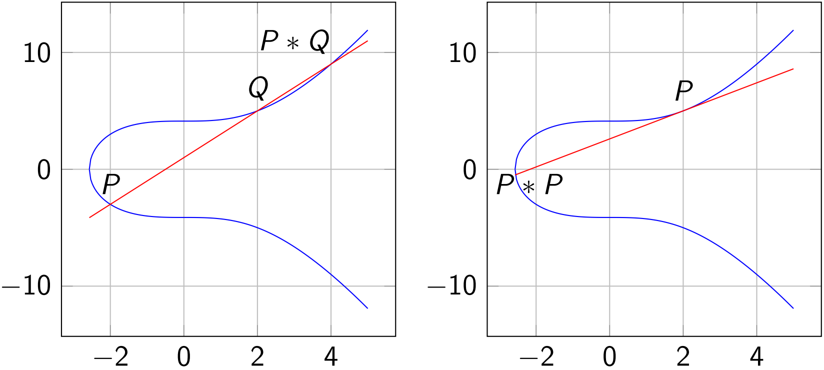
Intersecting Points (*cont.*)

- Let's denote this process of connecting two rational points by a rational line to get a third rational point by *



Intersecting Points (*cont.*)

- Let's denote this process of connecting two rational points by a rational line to get a third rational point by *



Group Law

- Is * a group law?

Group Law

- Is * a group law?
- Not quite, in particular, there is no identitiy element

Group Law

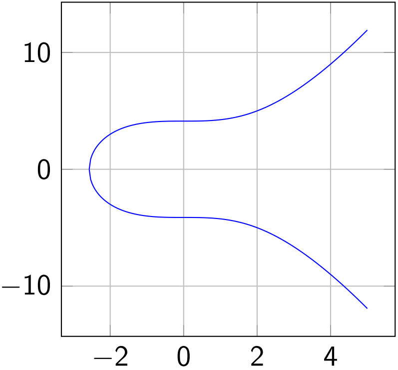
- Is * a group law?
- Not quite, in particular, there is no identitiy element
- Instead let $\mathcal{O}$ be a fixed point in $C(\mathbb{Q})$ and let $P + Q = (P * Q) * \mathcal{O}$

Group Law (*cont.*)

- (eg) if $P = (-2, 3)$, $Q = (-1, 4)$, $\mathcal{O} = (-2, -3)$, then $P + Q = (2, 5)$ on $y^2 = x^3 + 17$

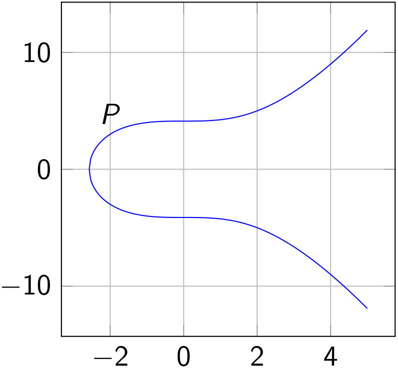
Group Law (*cont.)*

- (eg) if $P = (-2, 3)$, $Q = (-1, 4)$, $\mathcal{O} = (-2, -3)$, then $P + Q = (2, 5)$ on $y^2 = x^3 + 17$



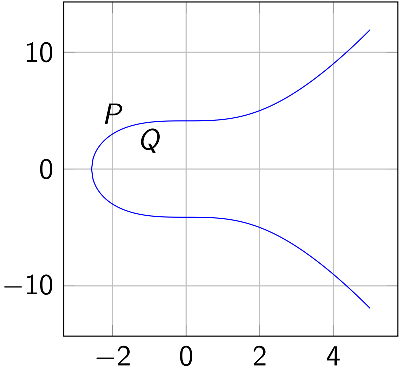
Group Law (*cont.*)

- (eg) if $P = (-2, 3)$, $Q = (-1, 4)$, $\mathcal{O} = (-2, -3)$, then $P + Q = (2, 5)$ on $y^2 = x^3 + 17$



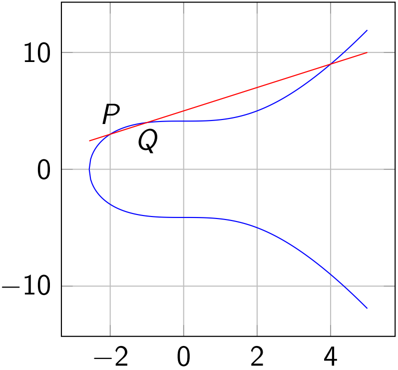
Group Law (*cont.*)

- (eg) if $P = (-2, 3)$, $Q = (-1, 4)$, $\mathcal{O} = (-2, -3)$, then $P + Q = (2, 5)$ on $y^2 = x^3 + 17$



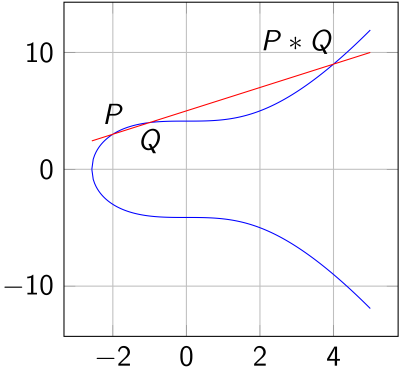
Group Law (*cont.*)

- (eg) if $P = (-2, 3)$, $Q = (-1, 4)$, $\mathcal{O} = (-2, -3)$, then $P + Q = (2, 5)$ on $y^2 = x^3 + 17$



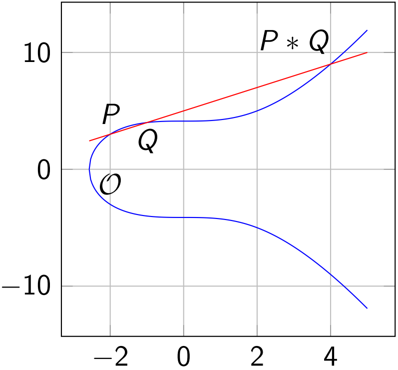
Group Law (*cont.*)

- (eg) if $P = (-2, 3)$, $Q = (-1, 4)$, $\mathcal{O} = (-2, -3)$, then $P + Q = (2, 5)$ on $y^2 = x^3 + 17$



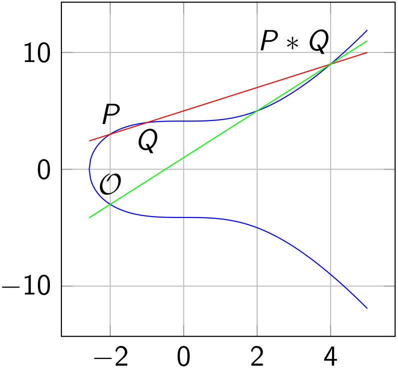
Group Law (*cont.*)

- (eg) if $P = (-2, 3)$, $Q = (-1, 4)$, $\mathcal{O} = (-2, -3)$, then $P + Q = (2, 5)$ on $y^2 = x^3 + 17$



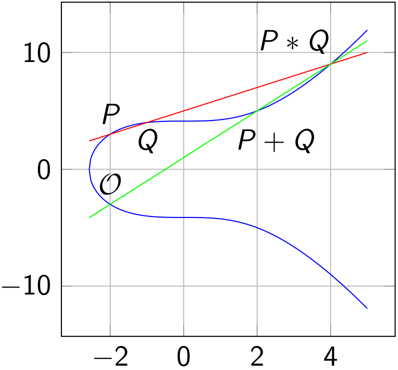
Group Law (*cont.*)

- (eg) if $P = (-2, 3)$, $Q = (-1, 4)$, $\mathcal{O} = (-2, -3)$, then $P + Q = (2, 5)$ on $y^2 = x^3 + 17$



Group Law (*cont.*)

- (eg) if $P = (-2, 3)$, $Q = (-1, 4)$, $\mathcal{O} = (-2, -3)$, then $P + Q = (2, 5)$ on $y^2 = x^3 + 17$



Group Law (*cont.*)

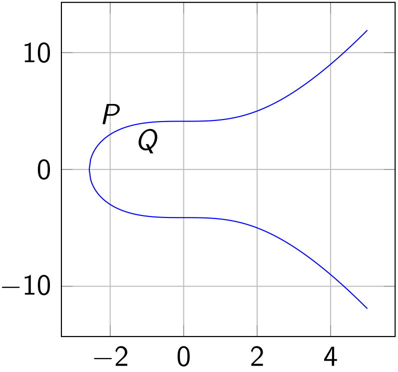
- Usually work in projective space, so during our Weierstrass transformation we make $\mathcal{O}$ become "the point at infinity" to make things easier

Group Law *(cont.)*

- Usually work in projective space, so during our Weierstrass transformation we make $\mathcal{O}$ become "the point at infinity" to make things easier
- Now $P + Q$ is just $P * Q$ reflected about the x-axis

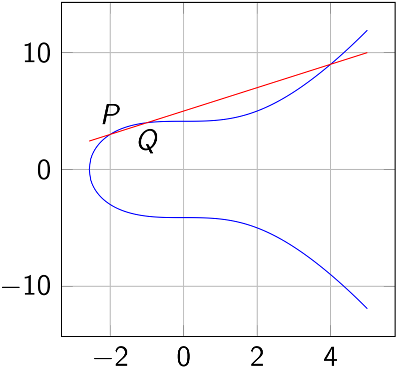
Group Law (*cont.*)

- Usually work in projective space, so during our Weierstrass transformation we make $\mathcal{O}$ become "the point at infinity" to make things easier
- Now $P + Q$ is just $P * Q$ reflected about the x-axis



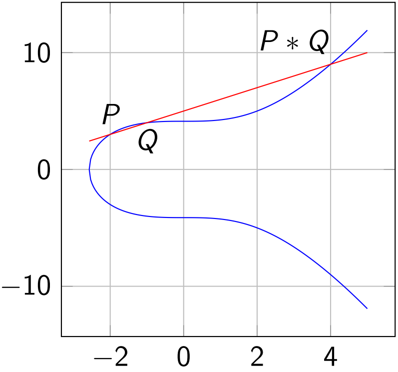
Group Law (*cont.*)

- Usually work in projective space, so during our Weierstrass transformation we make $\mathcal{O}$ become "the point at infinity" to make things easier
- Now $P + Q$ is just $P * Q$ reflected about the x-axis



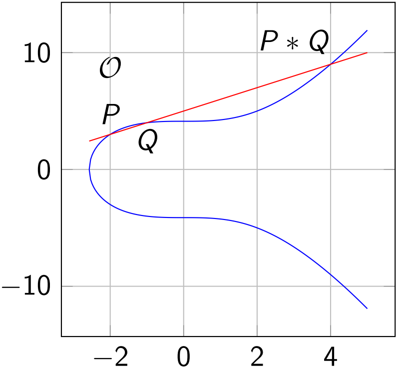
Group Law (*cont.*)

- Usually work in projective space, so during our Weierstrass transformation we make $\mathcal{O}$ become "the point at infinity" to make things easier
- Now $P + Q$ is just $P * Q$ reflected about the x-axis



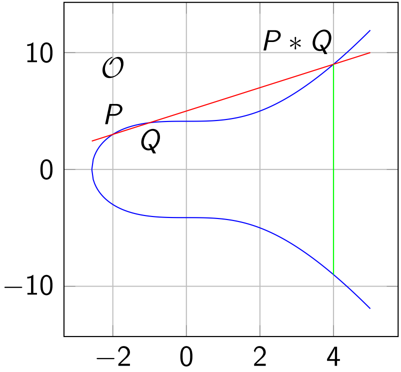
Group Law (*cont.*)

- Usually work in projective space, so during our Weierstrass transformation we make $\mathcal{O}$ become "the point at infinity" to make things easier
- Now $P + Q$ is just $P * Q$ reflected about the x-axis



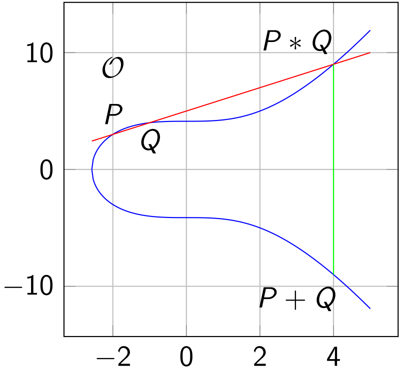
Group Law (*cont.*)

- Usually work in projective space, so during our Weierstrass transformation we make $\mathcal{O}$ become "the point at infinity" to make things easier
- Now $P + Q$ is just $P * Q$ reflected about the x-axis



Group Law (*cont.*)

- Usually work in projective space, so during our Weierstrass transformation we make $\mathcal{O}$ become "the point at infinity" to make things easier
- Now $P + Q$ is just $P * Q$ reflected about the x-axis



Group Law (*cont.*)

- Closure ✓

Group Law (*cont.*)

- Closure ✓
- Identity

Group Law (*cont.*)

- Closure ✓
- Identity
  $P + \mathcal{O} = (P * \mathcal{O}) * \mathcal{O} = P$

Group Law (*cont.)*

- Closure ✓
- Identity
  $P + \mathcal{O} = (P * \mathcal{O}) * \mathcal{O} = P$ ✓

Group Law (*cont.*)

- Closure ✓
- Identity
  $P + \mathcal{O} = (P * \mathcal{O}) * \mathcal{O} = P$ ✓
- Existence of Inverses

Group Law (*cont.*)

- Closure ✓
- Identity
  $P + \mathcal{O} = (P * \mathcal{O}) * \mathcal{O} = P$ ✓
- Existence of Inverses
  If $P = (x, y)$, then let $-P = (-x, y) \Rightarrow P + -P = \mathcal{O}$

Group Law (*cont.*)

- Closure ✓
- Identity
  $P + \mathcal{O} = (P * \mathcal{O}) * \mathcal{O} = P$ ✓
- Existence of Inverses
  If $P = (x, y)$, then let $-P = (-x, y) \Rightarrow P + -P = \mathcal{O}$ ✓

Group Law (*cont.*)

- Closure ✓
- Identity
  $P + \mathcal{O} = (P * \mathcal{O}) * \mathcal{O} = P$ ✓
- Existence of Inverses
  If $P = (x, y)$, then let $-P = (-x, y) \Rightarrow P + -P = \mathcal{O}$ ✓
- Associativity

Group Law (*cont.*)

- Closure ✓
- Identity
  $P + \mathcal{O} = (P * \mathcal{O}) * \mathcal{O} = P$ ✓
- Existence of Inverses
  If $P = (x, y)$, then let $-P = (-x, y) \Rightarrow P + -P = \mathcal{O}$ ✓
- Associativity ✓

Order

- Let the order of a point $P = (x, y)$ be the smallest $m \in \mathbb{Z}$ st $mP = \mathcal{O}$

Order

- Let the order of a point $P = (x, y)$ be the smallest $m \in \mathbb{Z}$ st $mP = \mathcal{O}$
- Let $\Phi = \{P = (x, y) \in C(\mathbb{Q}) \mid P \text{ has finite order}\} \cup \{\mathcal{O}\}$ be the torsion subgroup of $C(\mathbb{Q})$

Order

- Let the order of a point $P = (x, y)$ be the smallest $m \in \mathbb{Z}$ st $mP = \mathcal{O}$
- Let $\Phi = \{P = (x, y) \in C(\mathbb{Q}) \mid P \text{ has finite order}\} \cup \{\mathcal{O}\}$ be the torsion subgroup of $C(\mathbb{Q})$
  - This is clearly a subgroup:

Order

- Let the order of a point $P = (x, y)$ be the smallest $m \in \mathbb{Z}$ st $mP = \mathcal{O}$
- Let $\Phi = \{P = (x, y) \in C(\mathbb{Q}) \mid P \text{ has finite order}\} \cup \{\mathcal{O}\}$ be the torsion subgroup of $C(\mathbb{Q})$
  - This is clearly a subgroup:
    if $m_1 P_1 + m_2 P_2 = \mathcal{O} \Rightarrow m_1 m_2 (P_1 + P_2) = \mathcal{O}$

Order

- Let the order of a point $P = (x, y)$ be the smallest $m \in \mathbb{Z}$ st $mP = \mathcal{O}$
- Let $\Phi = \{P = (x, y) \in C(\mathbb{Q}) \mid P \text{ has finite order}\} \cup \{\mathcal{O}\}$ be the torsion subgroup of $C(\mathbb{Q})$
  - This is clearly a subgroup:
    if $m_1 P_1 + m_2 P_2 = \mathcal{O} \Rightarrow m_1 m_2 (P_1 + P_2) = \mathcal{O}$
- Because of a surprising theorem by Nagell-Lutz (both independently discovered), we know that if $P = (x, y) \in \Phi$, then $x, y \in \mathbb{Z}$

Field of Integers mod p

- Let $\mathbb{F}_p$ be the field of integers modulo a prime p

Field of Integers mod p

- Let $\mathbb{F}_p$ be the field of integers modulo a prime p
- Since our group law didn't use anything specific about $\mathbb{Q}$ (other than it's a field), $C(\mathbb{F}_p)$ is still a group

Field of Integers mod p

- Let $\mathbb{F}_p$ be the field of integers modulo a prime p
- Since our group law didn't use anything specific about $\mathbb{Q}$ (other than it's a field), $C(\mathbb{F}_p)$ is still a group
- Visualizing $C(\mathbb{F}_p)$ is difficult

Field of Integers mod p

- Let $\mathbb{F}_p$ be the field of integers modulo a prime p
- Since our group law didn't use anything specific about $\mathbb{Q}$ (other than it's a field), $C(\mathbb{F}_p)$ is still a group
- Visualizing $C(\mathbb{F}_p)$ is difficult
  - Remember it represents solutions to polynomial equations

Field of Integers mod p (*cont.*)

- Let $z \to \hat{z}$ be the "reduction modulo p" map

Field of Integers mod p (*cont.*)

- Let $z \to \hat{z}$ be the "reduction modulo p" map
  (eg) if $C : y^2 = x^3 + ax^2 + bx + c$, then $\hat{C} : y^2 = x^3 + \hat{a}x^2 + \hat{b}x + \hat{c}$

Field of Integers mod p (*cont.*)

- Let $z \to \hat{z}$ be the "reduction modulo p" map
  (eg) if $C : y^2 = x^3 + ax^2 + bx + c$, then $\hat{C} : y^2 = x^3 + \hat{a}x^2 + \hat{b}x + \hat{c}$
  (eg) if $P = (x, y) \in C(\mathbb{Q})$ st $x, y \in \mathbb{Z}$, then $\hat{P} = (\hat{x}, \hat{y}) \in \hat{C}(\mathbb{F}_p)$

Field of Integers mod p (*cont.*)

- Let $z \to \hat{z}$ be the "reduction modulo p" map
  (eg) if $C : y^2 = x^3 + ax^2 + bx + c$, then $\hat{C} : y^2 = x^3 + \hat{a}x^2 + \hat{b}x + \hat{c}$
  (eg) if $P = (x, y) \in C(\mathbb{Q})$ st $x, y \in \mathbb{Z}$, then $\hat{P} = (\hat{x}, \hat{y}) \in \hat{C}(\mathbb{F}_p)$
- We know $\hat{C}$ is non-singlular as long as its discriminant $\neq 0$

Field of Integers mod p (*cont.)*

- Let $z \to \hat{z}$ be the "reduction modulo p" map
  (eg) if $C : y^2 = x^3 + ax^2 + bx + c$, then $\hat{C} : y^2 = x^3 + \hat{a}x^2 + \hat{b}x + \hat{c}$
  (eg) if $P = (x, y) \in C(\mathbb{Q})$ st $x, y \in \mathbb{Z}$, then $\hat{P} = (\hat{x}, \hat{y}) \in \hat{C}(\mathbb{F}_p)$
- We know $\hat{C}$ is non-singlular as long as its discriminant $\neq 0$
  - $\hat{C}$'s discriminant is $\hat{D}$ where D is the discriminant of C

Field of Integers mod p (*cont.*)

- Let $z \to \hat{z}$ be the "reduction modulo p" map
  (eg) if $C : y^2 = x^3 + ax^2 + bx + c$, then $\hat{C} : y^2 = x^3 + \hat{a}x^2 + \hat{b}x + \hat{c}$
  (eg) if $P = (x, y) \in C(\mathbb{Q})$ st $x, y \in \mathbb{Z}$, then $\hat{P} = (\hat{x}, \hat{y}) \in \hat{C}(\mathbb{F}_p)$
- We know $\hat{C}$ is non-singlular as long as its discriminant $\neq 0$
  - $\hat{C}$'s discriminant is $\hat{D}$ where D is the discriminant of C
    (ie) $\hat{C}$ is non-singular as long as $p \nmid D$ (and $p \neq 2$)

Torsion Subgroup

- Since every $P \in \Phi$ has integer cordinates, our "reduction modulo p" map will make sense:

Torsion Subgroup

- Since every $P \in \Phi$ has integer cordinates, our "reduction modulo p" map will make sense:
  (ie) $\Phi \to \hat{C}(\mathbb{F}_p)$ st $P = (x, y) \mapsto \hat{P} = (\hat{x}, \hat{y})$ (note: $\mathcal{O} \mapsto \mathcal{O}$)

Torsion Subgroup

- Since every $P \in \Phi$ has integer cordinates, our "reduction modulo p" map will make sense:
  (ie) $\Phi \rightarrow \hat{C}(\mathbb{F}_p)$ st $P = (x, y) \mapsto \hat{P} = (\hat{x}, \hat{y})$ (note: $\mathcal{O} \mapsto \mathcal{O}$)
- This is a group homomorphism

Torsion Subgroup

- Since every $P \in \Phi$ has integer cordinates, our "reduction modulo p" map will make sense:
  (ie) $\Phi \rightarrow \hat{C}(\mathbb{F}_p)$ st $P = (x, y) \mapsto \hat{P} = (\hat{x}, \hat{y})$ (note: $\mathcal{O} \mapsto \mathcal{O}$)
- This is a group homomorphism
  - In fact, $ker(\hat{}) = \mathcal{O}$ so it is one-one

Torsion Subgroup

- Since every $P \in \Phi$ has integer cordinates, our "reduction modulo p" map will make sense:
  (ie) $\Phi \to \hat{C}(\mathbb{F}_p)$ st $P = (x, y) \mapsto \hat{P} = (\hat{x}, \hat{y})$ (note: $\mathcal{O} \mapsto \mathcal{O}$)
- This is a group homomorphism
  - In fact, $ker(\hat{}) = \mathcal{O}$ so it is one-one
- $\#\Phi$ divides $\#\hat{C}(\mathbb{F}_p)$

Example

- Let $C : y^2 = x^3 + 3$

Example

- Let $C : y^2 = x^3 + 3$
- $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$

Example

- Let $C : y^2 = x^3 + 3$
- $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = -243$

Example

- Let $C : y^2 = x^3 + 3$
- $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = -243 = -3^5$

Example

- Let $C : y^2 = x^3 + 3$
- $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = -243 = -3^5$
- Now we know there is a 1-1 group homomorphism between Φ and $\hat{C}(\mathbb{F}_p)$ for all primes ≥ 5

Example

- Let $C : y^2 = x^3 + 3$
- $D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2 = -243 = -3^5$
- Now we know there is a 1-1 group homomorphism between Φ and $\hat{C}(\mathbb{F}_p)$ for all primes ≥ 5
- Let's look at $\hat{C}(\mathbb{F}_5)$ and $\hat{C}(\mathbb{F}_7)$

Example (*cont.*)

- $\hat{C}(\mathbb{F}_5)$:

x	$x^2 \pmod 5$	$x^3 + 3 \pmod 5$
0	0	3
1	1	4
2	4	1
3	4	0
4	1	2

Example (*cont.*)

- $\hat{C}(\mathbb{F}_5)$:

x	$x^2 \pmod 5$	$x^3 + 3 \pmod 5$
0	0	3
1	1	4
2	4	1
3	4	0
4	1	2

- $\hat{C}(\mathbb{F}_5) = \{(1,2),(1,3),(2,1),(2,4),(3,0),\mathcal{O}\}$

Example (*cont.*)

- $\hat{C}(\mathbb{F}_5)$:

x	$x^2 \pmod 5$	$x^3 + 3 \pmod 5$
0	0	3
1	1	4
2	4	1
3	4	0
4	1	2

- $\hat{C}(\mathbb{F}_5) = \{(1,2),(1,3),(2,1),(2,4),(3,0),\mathcal{O}\}$
  $\Rightarrow \#\hat{C}(\mathbb{F}_5) = 6$

Example (*cont.*)

- $\hat{C}(\mathbb{F}_7)$:

x	$x^2 \pmod 7$	$x^3 + 3 \pmod 7$
0	0	3
1	1	4
2	4	4
3	2	2
4	2	4
5	4	2
6	1	2

Example (*cont.*)

- $\hat{C}(\mathbb{F}_7)$:

x	$x^2 \pmod 7$	$x^3 + 3 \pmod 7$
0	0	3
1	1	4
2	4	4
3	2	2
4	2	4
5	4	2
6	1	2

- $\hat{C}(\mathbb{F}_7) =$
  $\{(1,2),(1,5),(2,2),(2,5),$
  $(3,3),(3,4),(4,2),(4,5),$
  $(5,3),(5,4),(6,3),(6,4),\mathcal{O}\}$

Example (*cont.*)

- $\hat{C}(\mathbb{F}_7)$:

x	$x^2 \pmod 7$	$x^3 + 3 \pmod 7$
0	0	3
1	1	4
2	4	4
3	2	2
4	2	4
5	4	2
6	1	2

- $\hat{C}(\mathbb{F}_7) =$
$\{(1,2),(1,5),(2,2),(2,5),$
$(3,3),(3,4),(4,2),(4,5),$
$(5,3),(5,4),(6,3),(6,4),\mathcal{O}\}$
$\Rightarrow \#\hat{C}(\mathbb{F}_7) = 13$

Example (*cont.*)

- $\hat{C}(\mathbb{F}_7)$:

x	$x^2 \pmod 7$	$x^3 + 3 \pmod 7$
0	0	3
1	1	4
2	4	4
3	2	2
4	2	4
5	4	2
6	1	2

- $\hat{C}(\mathbb{F}_7) =$
  $\{(1,2),(1,5),(2,2),(2,5),$
  $(3,3),(3,4),(4,2),(4,5),$
  $(5,3),(5,4),(6,3),(6,4),\mathcal{O}\}$
  $\Rightarrow \#\hat{C}(\mathbb{F}_7) = 13$
  $\Rightarrow \#\Phi$ divides both 6 and 13

Example (*cont.*)

- $\hat{C}(\mathbb{F}_7)$:

x	$x^2 \pmod 7$	$x^3 + 3 \pmod 7$
0	0	3
1	1	4
2	4	4
3	2	2
4	2	4
5	4	2
6	1	2

- $\hat{C}(\mathbb{F}_7) =$
$\{(1,2),(1,5),(2,2),(2,5),$
$(3,3),(3,4),(4,2),(4,5),$
$(5,3),(5,4),(6,3),(6,4),\mathcal{O}\}$
$\Rightarrow \#\hat{C}(\mathbb{F}_7) = 13$
$\Rightarrow \#\Phi$ divides both 6 and 13
$\Rightarrow \#\Phi = 1$

Example (*cont.*)

- $\hat{C}(\mathbb{F}_7)$:

x	$x^2 \pmod 7$	$x^3 + 3 \pmod 7$
0	0	3
1	1	4
2	4	4
3	2	2
4	2	4
5	4	2
6	1	2

- $\hat{C}(\mathbb{F}_7) =$
  $\{(1,2),(1,5),(2,2),(2,5),$
  $(3,3),(3,4),(4,2),(4,5),$
  $(5,3),(5,4),(6,3),(6,4),\mathcal{O}\}$
  $\Rightarrow \#\hat{C}(\mathbb{F}_7) = 13$
  $\Rightarrow \#\Phi$ divides both 6 and 13
  $\Rightarrow \#\Phi = 1 \Rightarrow \Phi = \{\mathcal{O}\}$