Elliptic Curves
RTG Presentation

Alex Tao
University of Arizona

8th December 2011

The General Cubic

Consider the general cubic equation in 2 variables

$$\begin{aligned} C_0 : f(x,y) = & k_1x^3 + k_2x^2y + k_3xy^2 + k_4y^3 + k_5x^2 \\ & + k_6xy + k_7y^2 + k_8x + k_9y + k_{10} = 0 \end{aligned}$$

$k_i \in \mathbb{Z}$.
The homogenisation of the cubic produces the projective closure of C_0:

$$\begin{aligned} C : F(X,Y,Z) = & k_1X^3 + k_2X^2Y + k_3XY^2 + k_4Y^3 + k_5X^2Z \\ & + k_6XYZ + k_7Y^2Z + k_8XZ^2 + k_9YZ^2 + k_{10}Z^3 = 0 \end{aligned}$$

Smoothness

Suppose $P \in C$, we say that P is singular if it is singular in some affine chart of C containing P. For example, if P is in the chart $\mathbb{A}_{Z=0}$, then

$$f(P) = 0 = \frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial x}(P)$$

i.e. The tangent line is *not* defined at P.
Otherwise, P is called non-singular.
If P is non-singular for all $P \in C$, we say C is non-singular or smooth.

Note that this means distinct roots.

Weierstrass Form

Let C be as before and let $C(k)$ be non-empty for some number field k. Suppose $P \in C(k)$.

Claim
There exists a projective transformation $\mathbb{P}^2 \to \mathbb{P}^2$ taking $P \mapsto \mathcal{O} = [0, 1, 0]$, the point at infinity which is an inflection point, and $f = 0$ to an equation of the form:

$$C_1 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 = 0$$

This is called the Weierstrass form.

General Idea

Let C be nonsingular projective plane curve over k and let $\mathcal{O}$ be a point of inflection in $C(k)$:

- There is a linear change of variables such that $\mathcal{O} \mapsto [0, 1, 0]$, and tangent line at $\mathcal{O}$ is $L_\infty : Z = 0$.
- If the above is satisfied then the equation of C has Weierstrass form.

Sketch Proof

Recall that

$$C : F(X, Y, Z) = k_1X^3 + k_2X^2Y + k_3XY^2 + k_4Y^3 + k_5X^2Z + k_6XYZ + k_7Y^2Z + k_8XZ^2 + k_9YZ^2 + k_{10}Z^3 = 0$$

and suppose that we have $\mathcal{O} = [0, 1, 0] \in C$.
We can immediately deduce $k_4 = 0$.
The tangent line at $\mathcal{O}$ in the chart $\mathbb{A}^2 = \{[x, y, z] \mid y = 1\}$ is given by

$$k_3X + k_7Z = 0$$

which is $L_\infty : Z = 0$ so $k_3 = 0$. C non-singular $\implies$ $k_7 \neq 0$.

Finally, consider intersection of L_∞ and C at $[0, 1, 0]$. Which reduces to

$$\text{Intersection number of } Z \text{ and } k_1 X^3 + k_2 X^2$$

Since $\mathcal{O}$ is a point of inflection, the intersection number is 3 which forces $k_2 = 0$.

Collecting all results, we divide through by k_1 (which is non-zero otherwise Z would divide C) and rescale Z, we arrive at the Weierstrass form.

Riemann-Roch for Elliptic Curves

For C defined over K

$$\ell(n(\mathcal{O})) = \dim \mathcal{L}(n(\mathcal{O})) = n \qquad n \geq 1$$

where $n(\mathcal{O})$ is a formal sum of $\mathcal{O}$ and $\mathcal{L}(n(\mathcal{O}))$ is the "K-vector space of functions with a pole at most at $n(\mathcal{O})$".

e.g. $\mathcal{L}(3(P)) =$ functions with a pole of order ≤ 3 and no other poles.

Existence of Weierstrass Form

For a curve C with $\mathcal{O} \in k$:

$$\mathcal{L}(1(\mathcal{O})) = k =< 1 >$$
$$\mathcal{L}(2(\mathcal{O})) =< 1, x > \qquad x \text{ has double pole at } \mathcal{O}$$
$$\mathcal{L}(3(\mathcal{O})) =< 1, x, y > \qquad y \text{ has triple pole at } \mathcal{O}$$
$$\mathcal{L}(4(\mathcal{O})) =< 1, x, y, x^2 >$$
$$\mathcal{L}(5(\mathcal{O})) =< 1, x, y, x^2, xy, >$$
$$\mathcal{L}(6(\mathcal{O})) =< 1, x, y, x^2, xy, x^3, y^2 >$$

$\ell(6(\mathcal{O})) = 6 \implies$ there is a linear relation between the functions.

Char $\neq 2, 3$

For a number field k where $\mathrm{char}(k) \neq 2, 3$, we may do a further transformation taking $f_1 = 0$ to

$$C_2 : y^2 = x^3 + Ax + B$$

Example

$$C_0 : x^2y + xy^2 = 6(xy - 1)$$

Take $(x, y) \mapsto (-\frac{y}{x}, \frac{x^2}{y})$ gives Weierstrass form

$$C_1 : y^2 + 6xy + 6y = x^3$$

and completing the square on LHS and rescaling gives the simplified Weierstrass form

$$C_2 : y^2 = x^3 - 9x + 9$$

Definition

The following are equivalent definitions of an elliptic curve E over a field k:

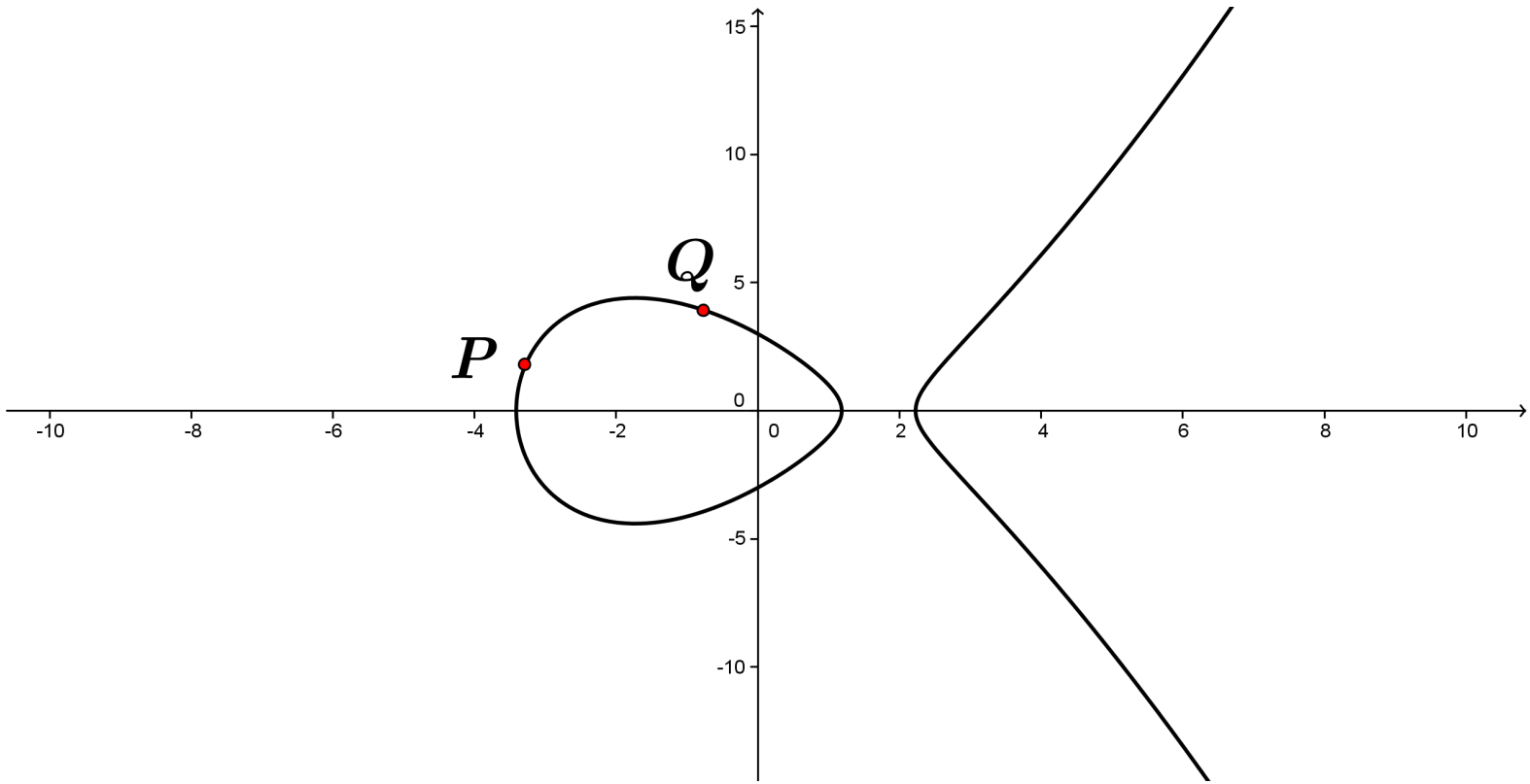
- E is a non-singular projective plane curve of degree 3 with a point $\mathcal{O} \in E(k)$.
- E is non-singular projective plane curve over k given by

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

- E is a non-singular projective curve of genus 1 together with a point $\mathcal{O} \in E(k)$.

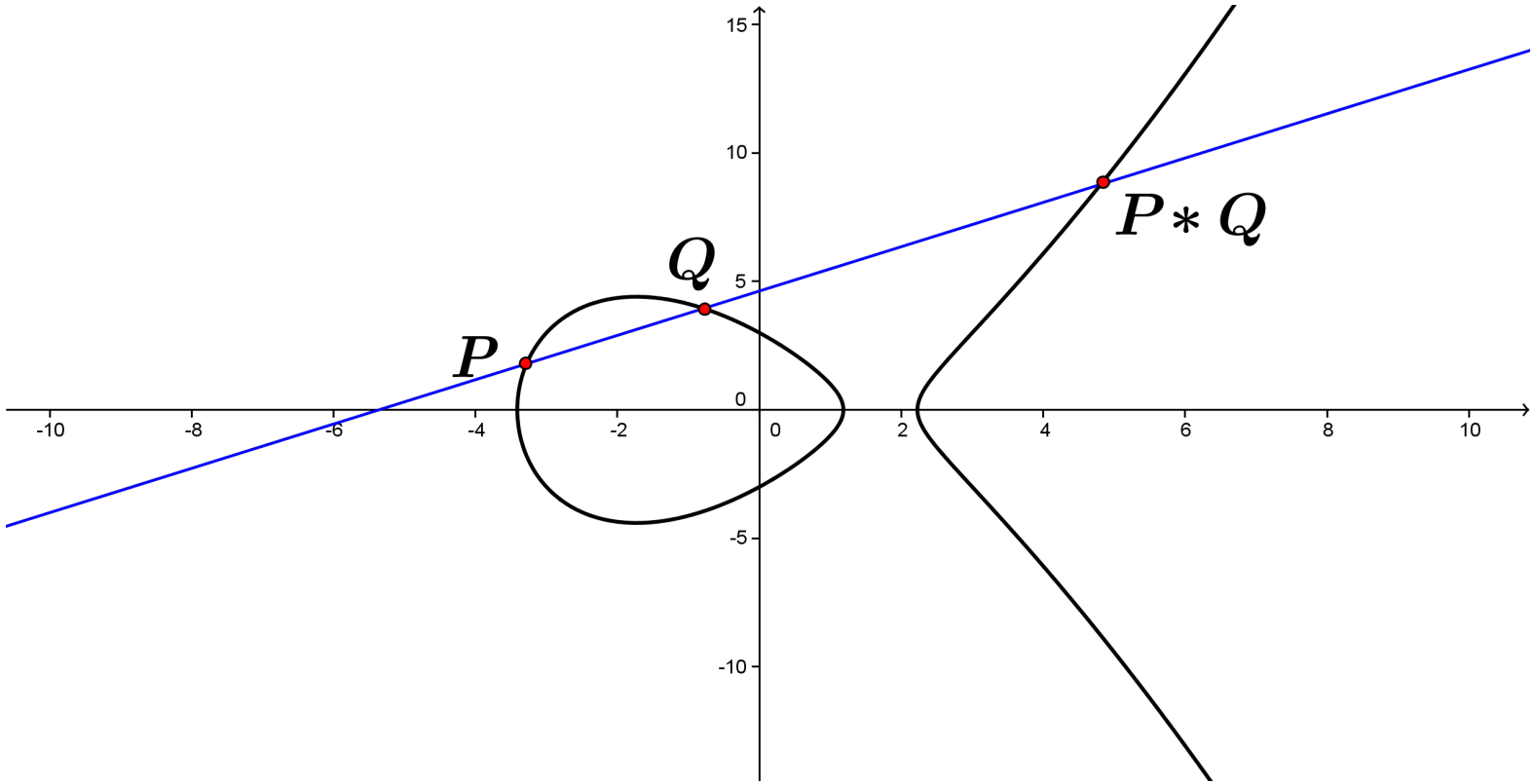
Group Law

Adding points: $P + Q$



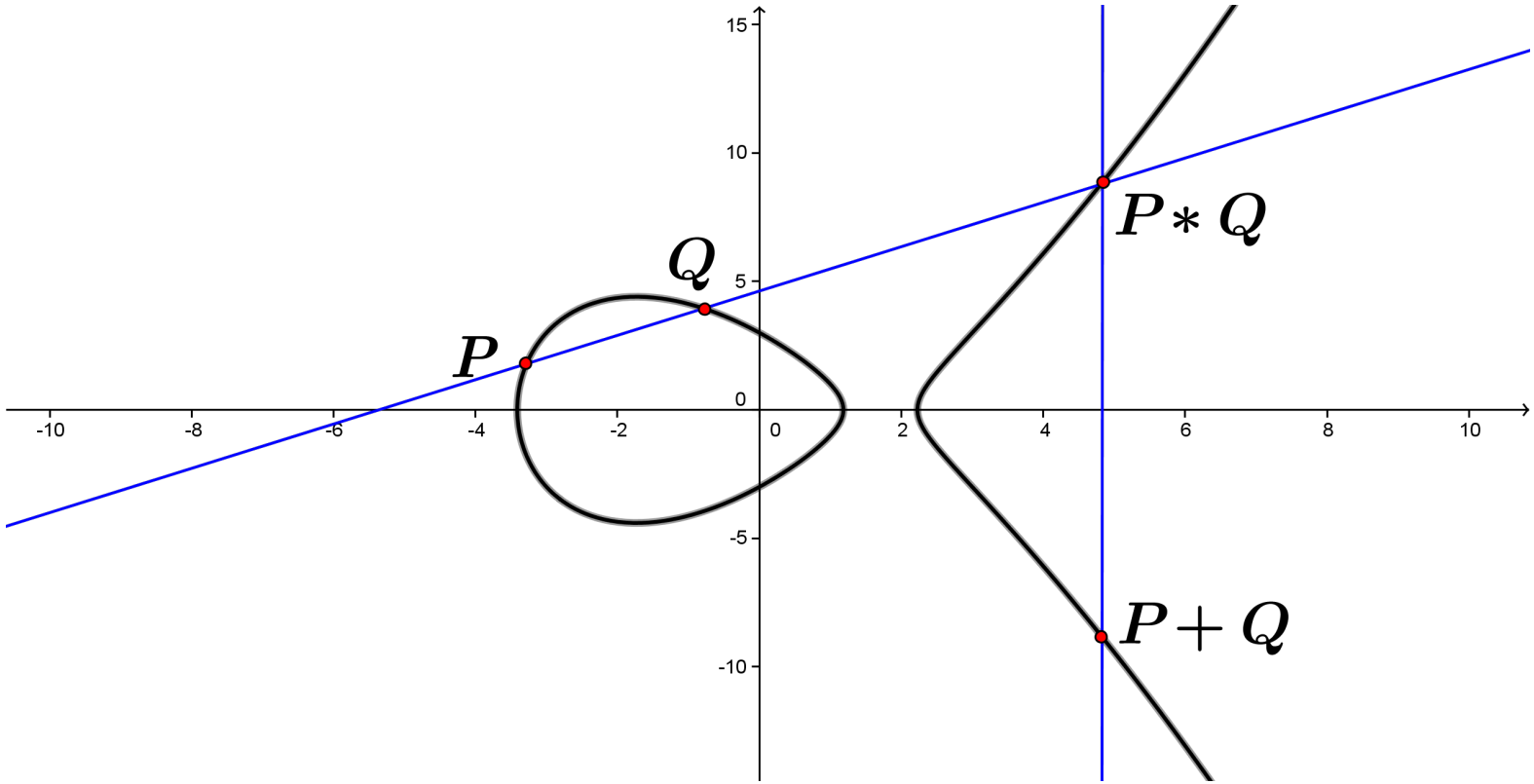
Group Law

Adding points: $P + Q$



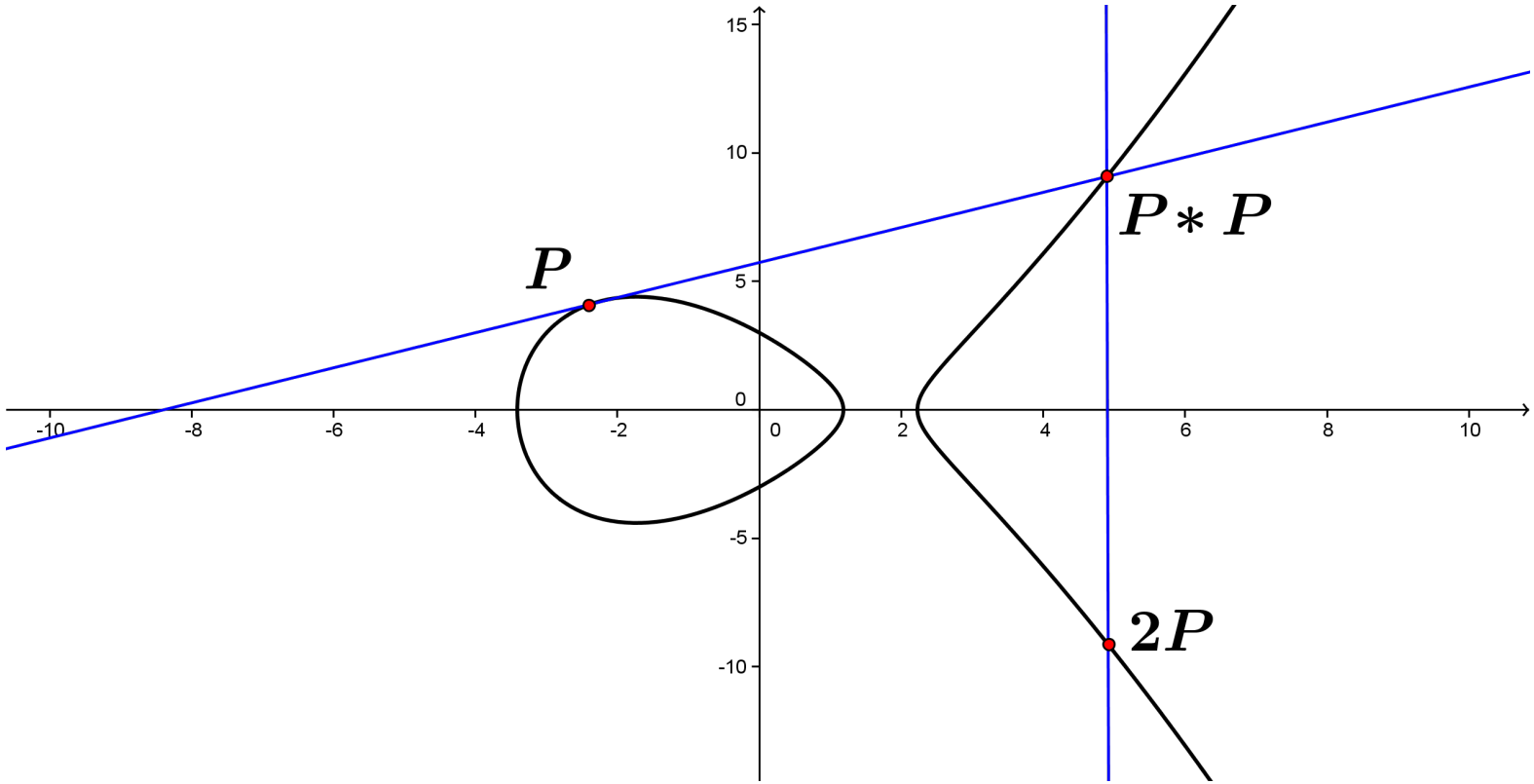
Group Law

Adding points: $P + Q$



Group Law

Duplicating a point P



Mordell-Weil Theorem

Let K be a number field and E/K an elliptic curve, then $E(K)$ is finitely generated. In particular,

$$E(K) \cong E_{\text{tors}}(K) \times \mathbb{Z}^r.$$

where $r \in \mathbb{Z}_{\geq 0}$ is the **rank** of the elliptic curve and $E_{\text{tors}} \times \mathbb{Z}^r$ is the finite **torsion subgroup** of $E(K)$.

Mazur's Theorem

Let E be an elliptic curve, and suppose that $E(\mathbb{Q})$ contains a point of finite order m. Then either

$$1 \leq m \leq 10 \qquad \text{or} \qquad m = 12.$$

More precisely, T forms a subgroup which has one of the following two forms:

(i) C_N with $1 \leq N \leq 10$ or $N = 12$.

(ii) $C_2 \times C_{2N}$ with $1 \leq N \leq 4$.

Nagell-Lutz Theorem

Let $P = (x, y)$ be a rational point of finite order on the elliptic curve

$$E : y^2 = f(x) = x^3 + ax + b$$

$a, b \in \mathbb{Z}$; and let $\triangle_E$ be the discriminant of $f(x)$,

$$\triangle_E = -4a^3 - 27b^2.$$

Then:

(i) $x, y \in \mathbb{Z}$

(ii) Either $y = 0$ or $y^2 | D$

Remark: Converse is not true.

Computation

Consider our elliptic curve in simplified Weierstrass form given by

$$E : y^2 = x^3 - 9x + 9$$

$\triangle_E = -3^6$.
Nagell-Lutz $\implies$ possible values of $y(P)$ are $0, \pm 3, \pm 9 \pm 27$ for any torsion point P. Furthermore, P is torsion then $x(P) \in \mathbb{Z}$ must satisfy one of the followings:

$$x^3 - 9x + 9 = 0$$
$$x^3 - 9x = 0$$
$$x^3 - 9x - 72 = 0$$
$$x^3 - 9x - 720 = 0$$

We may check for integral solutions by looking for solutions modulo some small primes:

$$\begin{aligned}
x^3 - 9x + 9 &= x^3 + x + 1 \mod 2 && \text{has no solution} \\
x^3 - 9x &= x(x^2 - 9) && \implies x = 0, \pm 3 \\
x^3 - 9x - 72 &= x^3 - 2x - 2 \mod 7 && \text{has no solution} \\
x^3 - 9x - 720 &= x^3 - 9x + 16 \mod 23 && \text{has no solution}
\end{aligned}$$

This shows that the only *possible* torsion points are $(0, \pm 3), (\pm 3, \pm 3)$.

Remark: If P is torsion, then $[n]P$ is torsion where $[n] : E \to E$ is the multiplication-by-n map.
If we can find an n such that $[n]P$ does not have integral coordinates, then P is not torsion.
By the duplication formula, we compute $[2](0,3) = (\frac{9}{4}, \frac{3}{8})$ which does not have integral coefficients. Since $(0,-3)$ is the inverse of $(0,3)$, it is also not torsion.
Similarly, we compute that $[2](3,3) = (3,-3)$ so if we write $P = (3,3)$, we have $[2]P = -P \implies [3]P = \mathcal{O}$.

Reduction Mod p

Let E/K be an elliptic in simplified Weierstrass form

$$y^2 = x^3 + ax + b$$

such that D is minimal and $a, b \in \mathbb{Z}$, then E is called minimal.

In such case, we can reduce E mod p for some prime p

$$\bar{E} : y^2 = x^3 + \bar{a}x + \bar{b}$$

Reduction Types

If $p \neq 2, p \nmid D$ then we have good reduction and $\bar{E}$ is non-singular. In particular, $E(\mathbb{Q}) \to \bar{E}(\mathbb{F}_p)$ is a homomorphism.

If $p \mid D$ then we have bad reduction, and the $\bar{E}$ is singular with the following two cases:

- $\bar{E}$ is singular with a cusp. e.g. $\bar{E} : y^2 = x^3$. This is called additive reduction. $\bar{E}$ is isomorphic to the additive group $\mathbb{G}_a$.
- $\bar{E}$ is singular with a node. e.g. $\bar{E} : y^2 = x^2(x+1)$. This is called multiplicative reduction. $\bar{E}$ is isomorphic to the multiplicative group $\mathbb{G}_m$.

Application on Torsion

The homomorphism

$$E(\mathbb{Q})_{\text{tors}} \to \bar{E}(\mathbb{F}_p)$$

is injective.

This restricts drastically the size of the torsion subgroup of $E(\mathbb{Q})$.

Computation

Let $E : y^2 = x^3 - 9x + 9$ as above with $\triangle_E = -3^6$, so E has good reduction at every prime $p > 3$.

$$\begin{aligned} p = 5 &\implies \bar{E} : \ y^2 = x^3 + x - 1 \\ &\implies \bar{E}(\mathbb{F}_5) = \{(0, \pm 2), (1, \pm 1), (2, \pm 3), (-2, \pm 2)\} \\ &\implies |\bar{E}(\mathbb{F}_5)| = 9 \end{aligned}$$

$$\begin{aligned} p = 11 &\implies \bar{E} : \ y^2 = x^3 + 2x - 2 \\ &\implies \bar{E}(\mathbb{F}_{11}) = \{(0, \pm 2), (1, \pm 1), (2, \pm 1), (4, \pm 2), \\ &\qquad\qquad (-4, \pm 5), (5, \pm 1), (-5, \pm 2)\} \\ &\implies |\bar{E}(\mathbb{F}_{11})| = 15 \end{aligned}$$

The only group that injects into a group of order 9 and a group of order 15 is C_3.