Lecture 18 Elliptic Curves §6.1

Why elliptic Curves

- They are groups w/ more confusing addition laws than $(\mathbb{Z}/p\mathbb{Z})^\times$ $\Rightarrow$ harder DLP.

Most modern cryptography uses Elliptic curve Diffie-Hellman to exchange a symmetric encryption key.

- Curves with a B-smooth number of points can be used to factor integers & compute discrete logs.

Lenstra's Algorithm

For instance, if we know of an elliptic curve over $\mathbb{F}_p$ w/ a B-smooth # of points then we can use an oracle for Diffie-Hellman to solve Discrete Log.

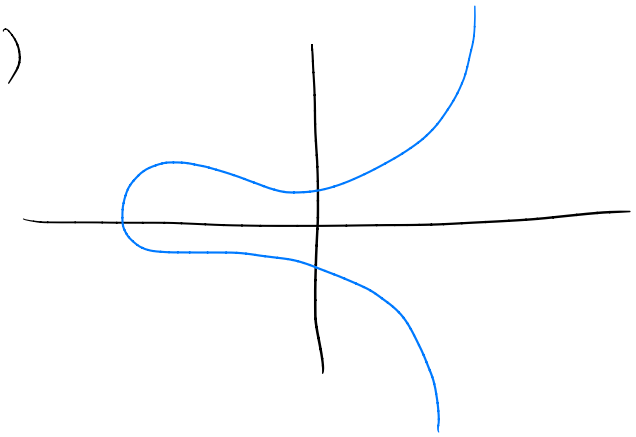
Elliptic curves

Def A Weierstrass Cubic is an eqn of the form

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

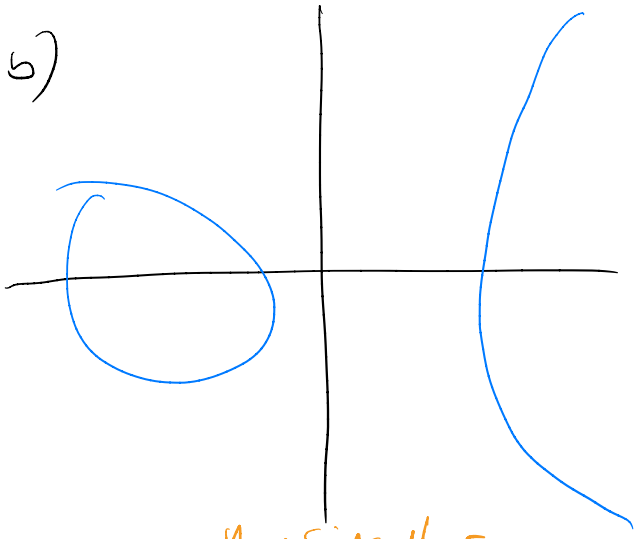
The pairs $(x, y) \in \mathbb{R}^2$ satisfying this eqn look like one of the following:

(a)



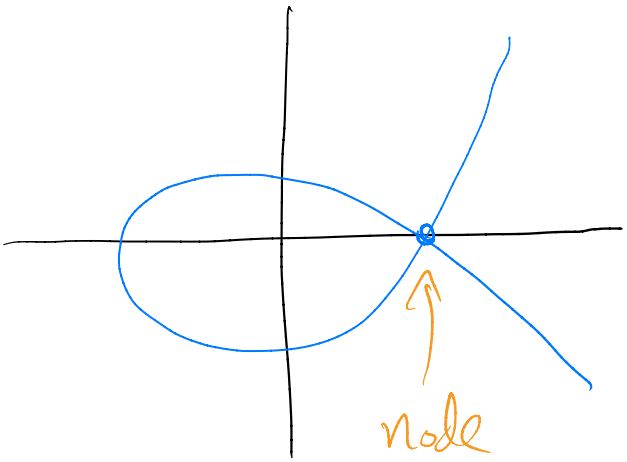
Nonsingular

(b)



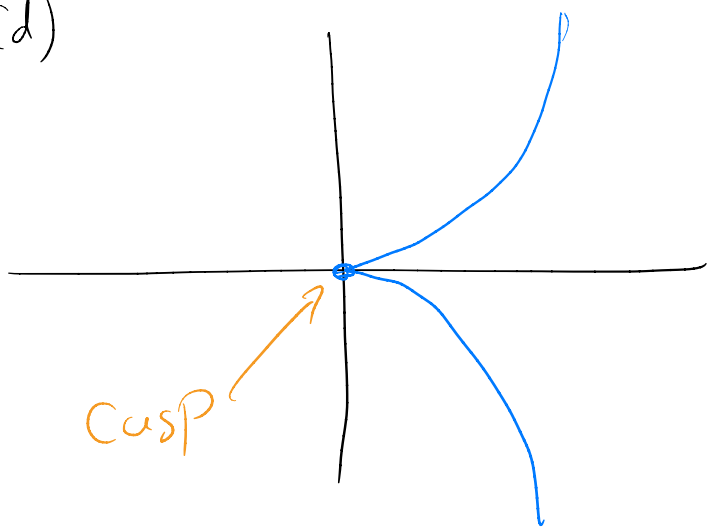
Nonsingular

(c)



Singular

(d)



Singular

The set of solutions of a nonsingular Weierstrass eqn is an <u>elliptic curve</u>.

(a) & (b) are nonsingular & are elliptic curves.

(c) has a node called a "nodal cubic"

(d) has a cusp called a "cuspidal cubic"

(c) & (d) are <u>not</u> elliptic curves.

A weierstrass equation $y^2 = x^3 + Ax + B$ is nonsingular if and only if $f(x) = x^3 + Ax + B$ has no repeated roots.

<u>Def</u> Suppose $p(x)$ is a polynomial which factors as $p(x) = (x-r_1)\cdots(x-r_n)$. The discriminant of $p(x)$ is $D = \prod_{i \neq j} (r_i - r_j)$.

If the roots r_i are distinct, $D \neq 0$.

If there is a repetition, then $D = 0$.

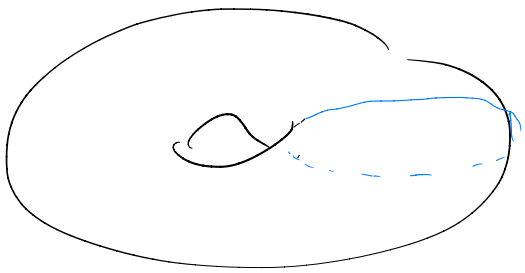
Conveniently, D can be expressed in terms of the coeffizents of $p(x)$!

Fact If $f(x) = x^3 + Ax + B$ then

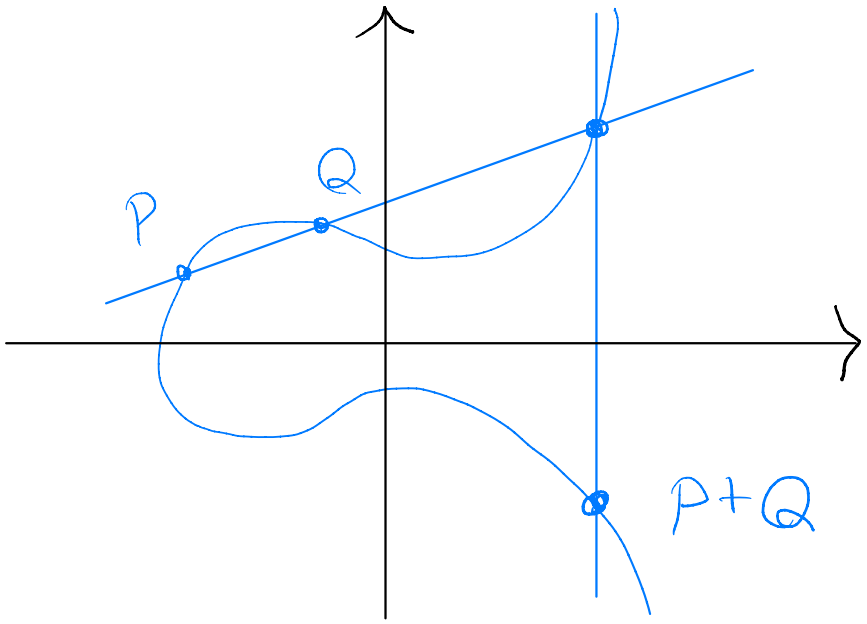
$$D = -4A^3 - 27B^3.$$

Thus, any Weierstrass equ w/ $D = -4A^3 - 27B^3 \neq 0$ is an elliptic curve.

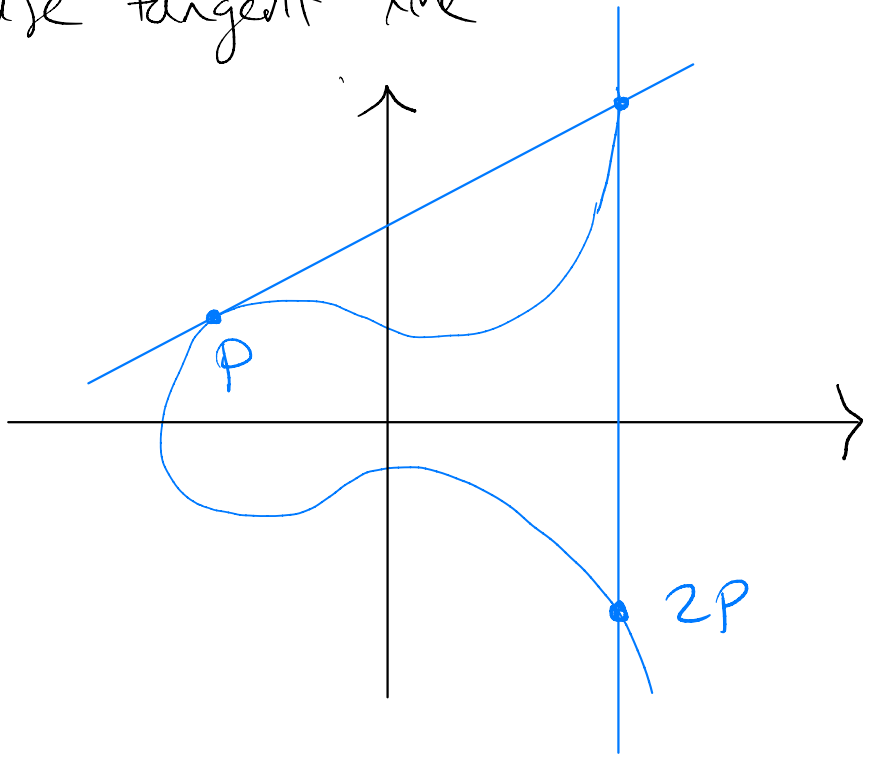
Geometrically, the complex solutions look like a donut:



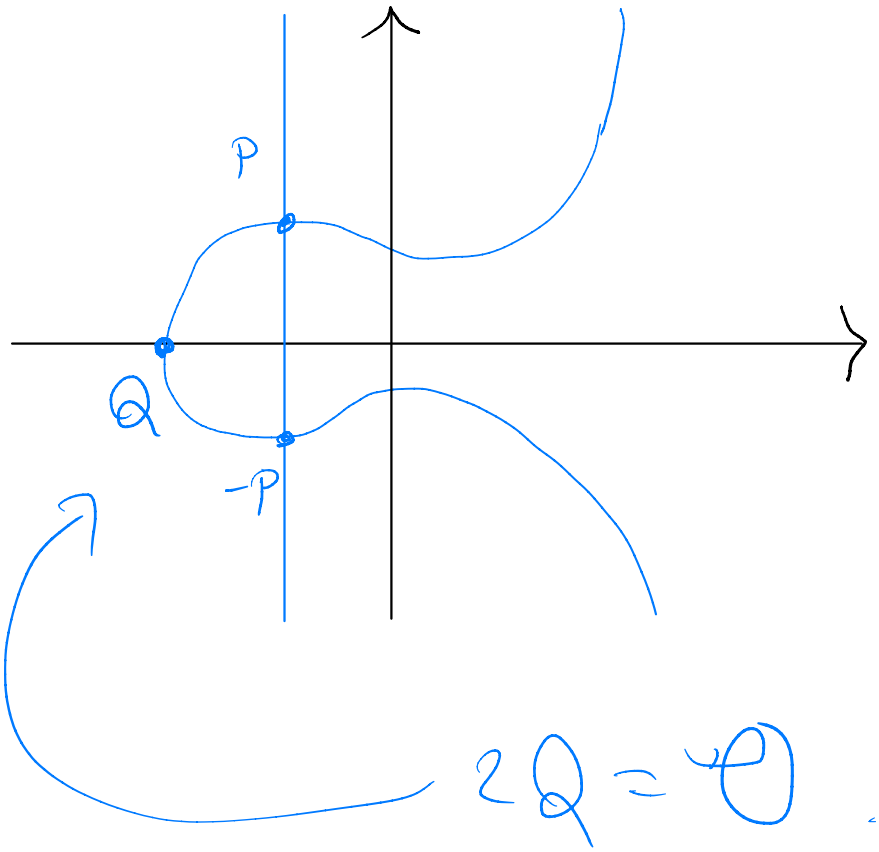
We can add points on an elliptic curve:



Each line intersects the curve in exactly 3 points counting repetitions. To double a point, use tangent line instead of secant line.



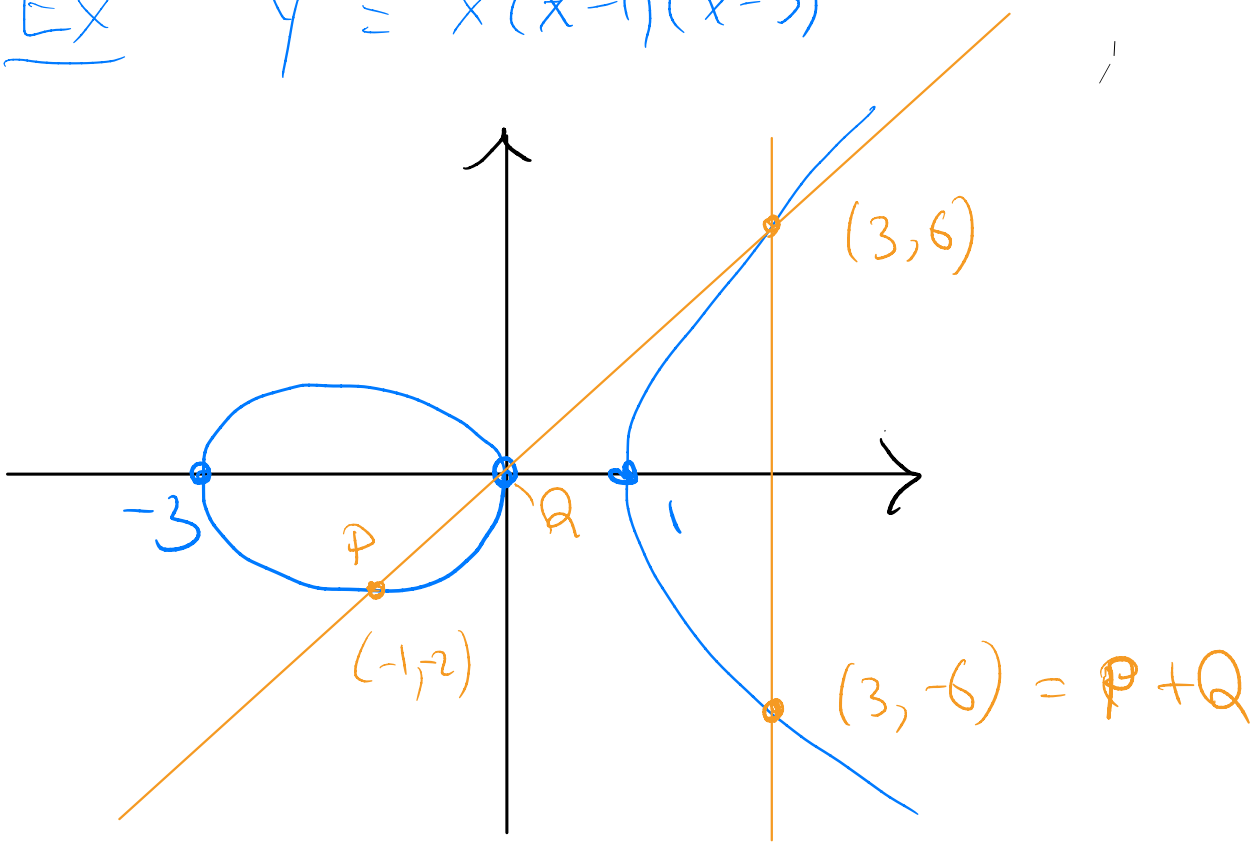
Also, vertical lines only intersect curve twice, so we add an extra point $\mathcal{O}$ and say it is on every vertical line. $P + \mathcal{O} = P$, so $\mathcal{O}$ is the identity.



<u>Fact</u> This addition is a group structure on the points of the curve.

<u>Rmk</u> We don't need a Weierstrass cubic, any cubic w/ nonvanishing discriminant works.

Ex $y^2 = x(x-1)(x-3)$



$P = (-1,-2)$ $Q = (0,0)$. The line through P & Q is $y = 2x$, so the third point of intersection is

$$(2x)^2 = x(x-1)(x+3)$$

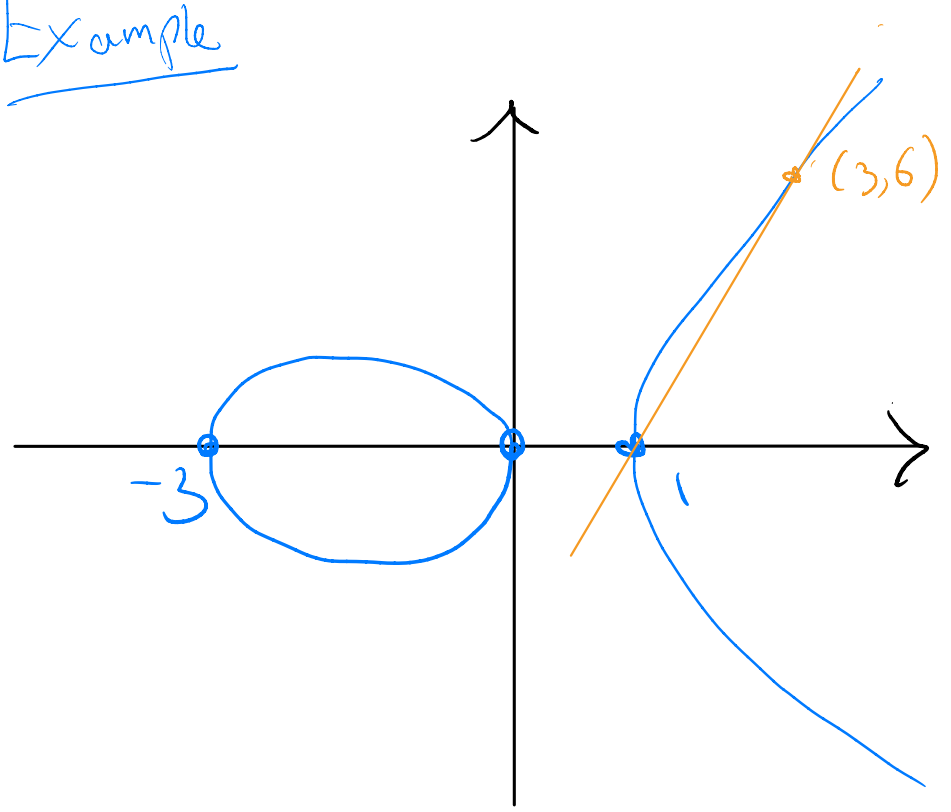
$$\Rightarrow \quad 4x^2 = x^3 + 2x^2 - 3x$$

$$x^3 - 2x^2 - 3x = 0$$

$$\underbrace{x(x+1)}_{\text{known roots}}\underbrace{(x-3)}_{\text{third intersection point}} = 0$$

$y = 2x \Rightarrow (3,6) \Rightarrow P+Q = (3,-6)$.

Example



2. $(3,6) = (1,0)$

Tangent line

$$y^2 = x(x-1)(x+3) = x^3 + 2x^2 - 3x$$

implicit differentiation $\Rightarrow$ $2yy' = 3x^2 + 4x - 3$

Plug in $(x,y) = (3,6)$ $\Rightarrow$ $12y' = 27 + 12 - 3 = 36$

$\Rightarrow$ $y' = 3$

$\Rightarrow$ tangent line is $y = 3(x-3) + 6$

$= 3x - 3$

Plug tangent line back into elliptic curve eqn:

$$(3x-3)^2 = x^3 + 2x^2 - 3x$$

$$9x^2 - 18x + 9 = x^3 + 2x^2 - 3x$$

$$x^3 - 7x^2 + 15x - 9 = 0$$

Root sum must be 7. b/c

$$(x-a)(x-b)(x-c) = x^3 - (a+b+c)x^2 + \cdots$$

$3 + 3 + \_ = 7 \Rightarrow$ third root is 1.

$\Rightarrow x = 1$ & $y = 3(1) - 3 = 0$.

Reflect wrt x-axis gives $(1, -0) = \boxed{(1,0)}$