Elliptic Curves

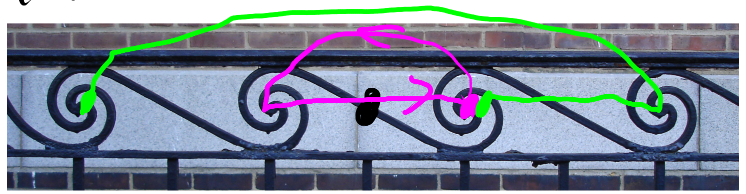
Groups and Fields

Dfn: a **group** is a set G and a binary operation $*: G \times G \to G$ such that:

- There is an **identity element** $e \in G$, s.t. $e * g = g * e = g$ $\forall g \in G$.
- $\forall g \in G$, $\exists$ **inverse elt** g^{-1} s.t. $g g^{-1} = g^{-1} g = e$.
- $*$ is associative $(f * g) * h = f * (g * h)$.

(• closed under $*$)

- $(\mathbb{Z}, +)$
- $(\mathbb{Q}, +)$
- $(\mathbb{Q} \setminus \{0\}, \times)$
- $(\mathbb{Z}/n\mathbb{Z}, +)$
- $(GL(n), \times)$ the set of invertible $n \times n$ matrices

  $(AB)^{-1} = B^{-1} A^{-1}$
- $(SL(n), \times)$ set of det 1 matrices
- Rotations of the circle
- 

Non-examples

- $(\mathbb{N}, +)$
- $(\mathbb{Q}, \times)$
- $(M_n, \times)$
- matrices of det 2

- set of permutations of a n-elt set S_n

$\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$

Dfn: if $g * h = h * g$ $\forall g, h \in G$, say G is an abelian gp.

Dfn: Let $g \in G$. The set $\{g^n \mid n \in \mathbb{Z}\} = \langle g \rangle$ the subgroup generated by g.

if $\exists g$ s.t. $\langle g \rangle = G$, say G is cyclic and g is a generator (or a PR).

The size of $\langle g \rangle$ is the order of g, $\mathrm{ord}_G(g)$. $g^{\mathrm{ord}_G(g)} = e$.

Fact: if $\# G = n$, $g \in G$, then $\mathrm{ord}_G(g) \mid n$.

In any gp, can define discrete log problem:

given fixed $g \in G$,

given $h \in G$, find n s.t. $g^n = h$.

Field

Dfn: a field is a set K, w/ 2 operations $+$ and $\cdot$ s.t.

1) $(K, +)$ is ab gp
2) $(K \setminus \{0\}, \cdot)$ is ab gp
3) $k(x+y) = kx + ky$

Ex: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Non-ex: $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{N}$

$\mathbb{Z}/n\mathbb{Z}$ is not a field <u>unless</u> $n = p$ is prime.

$\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ is a field of order p.

If we want to solve an eqn, have to choose a field.

$x^2 - 2 = 0$ in $\mathbb{R}$, not in $\mathbb{Q}$

$x^2 + 2 = 0$ in $\mathbb{C}$, not in $\mathbb{R}$.

Elliptic Curves

Dfn: an elliptic curve over a field K is a smooth projective curve over K of genus 1 with a K-rational pt.

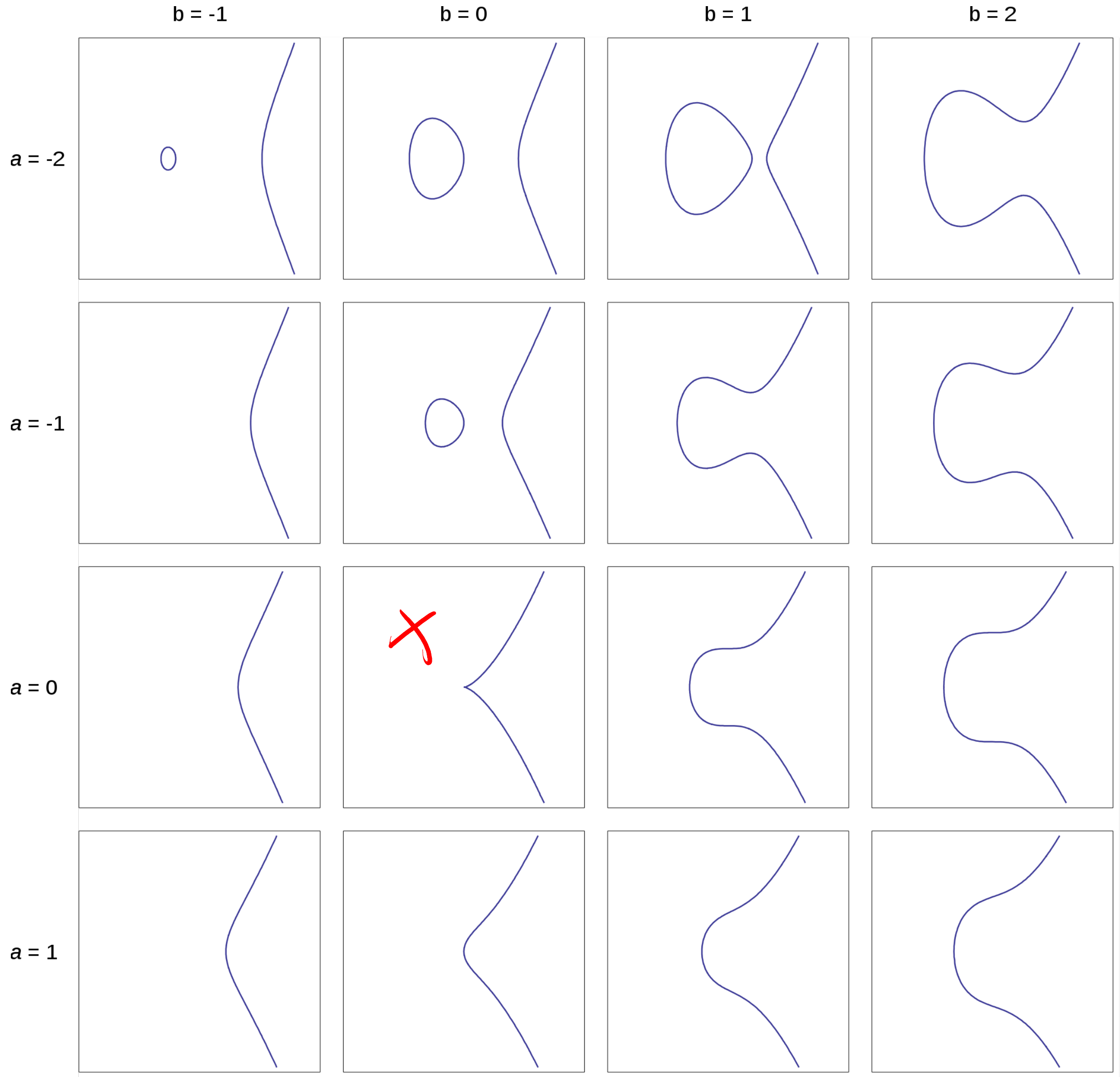
Dfn: $y^2 = x^3 + Ax + B$

s.t. $A, B \in K$, and the discriminant

$$\Delta = 4A^3 + 27B^2 \neq 0.$$

Set of solns is $E(K)$

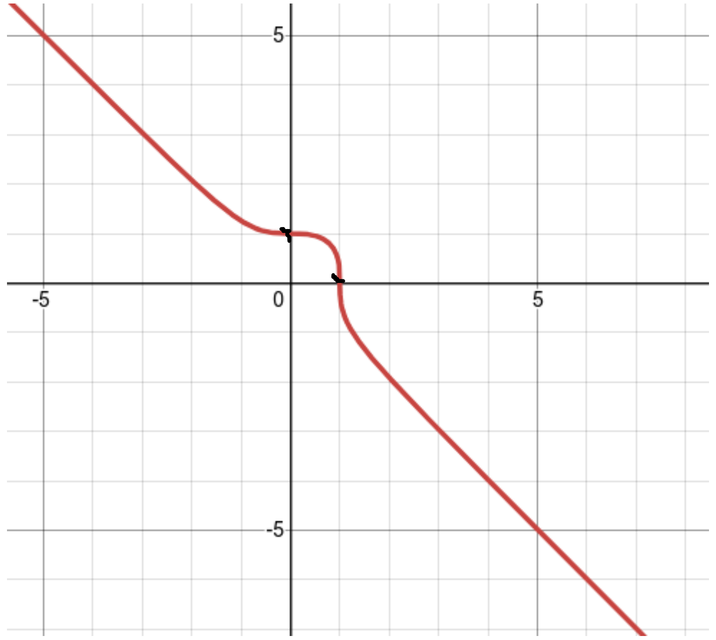
This is Weierstrass form.



$E(\mathbb{R})$

The rule $\Delta \neq 0$ prevents cusps and repeated roots.

$x^3 + y^3 = 1$



$X^2 + Y^2 = Z^2 \quad / \mathbb{Z}$

$\Updownarrow$

$\left(\frac{X}{Z}\right)^2 + \left(\frac{Y}{Z}\right)^2 = 1 \quad / \mathbb{Z}$

$x^2 + y^2 = 1 \quad / \mathbb{Q}$

Bezout's Thm:

Suppose C_1 degree d

C_2 degree e

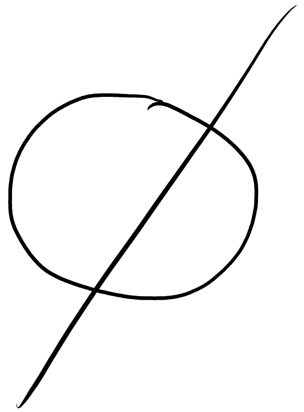
then $\exists$ exactly de pts of intersection in $C_1 \cap C_2$.

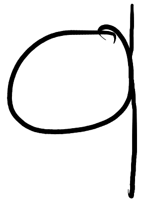
(up to technical conditions)

1) over $\mathbb{C}$

2) "up to multiplicity"

3) allowing pts 'at infinity' in the "projective plane".





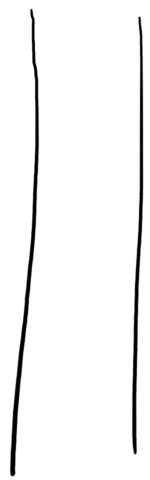
$x^2+y^2=1$

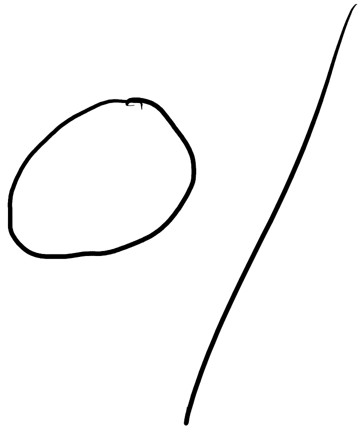
$x=1$

$\Rightarrow$ $1+y^2=1$

$y^2=0$

$y=0, 0$





$x^2+y^2=1$

$y=x-10$

$(x-10)^2+x^2=1$