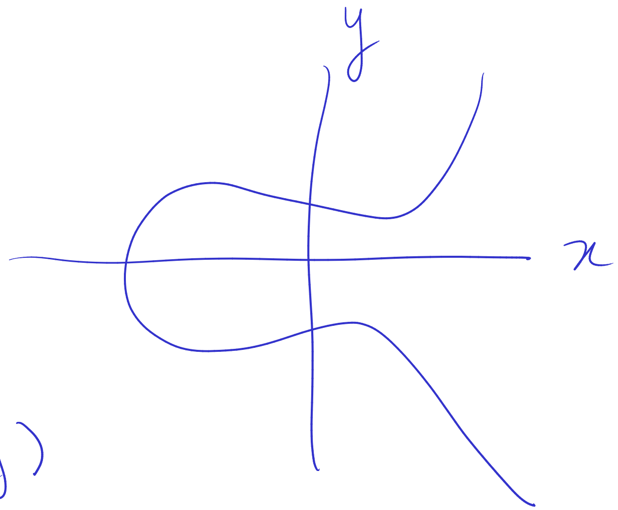
$E: \boxed{Y^2 Z = X^3 + aXZ^2 + bZ^3}$ in $\mathbb{P}^2$ $[X,Y,Z]$

$Z \neq 0$

$Z = 0$



$[X,Y,Z]$
$\|$
$[\frac{X}{Z}, \frac{Y}{Z}, 1]$
$\|$
$[x,y,1] \leftrightarrow (x,y)$

$x = \frac{X}{Z}$

$y = \frac{Y}{Z}$

$[X,Y,0]$

$Y^2 \cdot 0 = X^3 + aX \cdot 0^2 + b \cdot 0^3$

$0 = X^3$

$0 = X$

$[0,Y,0] = [0,1,0]$

1 pt!

called ∞

Number of points on an elliptic curve over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

$$y^2 = x^3 + ax^2 + bx + c \mod p$$

Given x, check if $x^3 + ax^2 + bx + c$ is a square.

If so, 2 pts (x, y), $(x, -y)$ } Probability $1/2$

If not, no pts } Prob. $1/2$

So expect $p \underset{(\text{pt} @ \infty)}{+1}$ points on average.

Hasse's Theorem

$$|\underbrace{\#E(\mathbb{F}_p)}_{\substack{\#\text{ of points on} \\ E \text{ defined} \\ \text{over } \mathbb{F}_p}} - (p+1)| < 2\sqrt{p}.$$

Interesting fact: every value of $\#E(\mathbb{F}_p)$ in this interval is attained for some E.

We will:

- use $E(\mathbb{F}_p)$ as the group for $\left\{ \begin{array}{l} \text{discrete log} \\ \text{Diffie-Hellman} \\ \text{El Gamal} \end{array} \right.$

- use $E(\mathbb{Z}/n\mathbb{Z})$ to factor n.