for gp G, can solve
$g^n = h$ for n
DL for gps

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

Bezout's Theorem
C_1 curve of deg d
C_2 curve of deg e
have de pts of $\cap$.

- over $\mathbb{C}$ ✓
- up to multiplicity ✓
- w/ pts at ∞

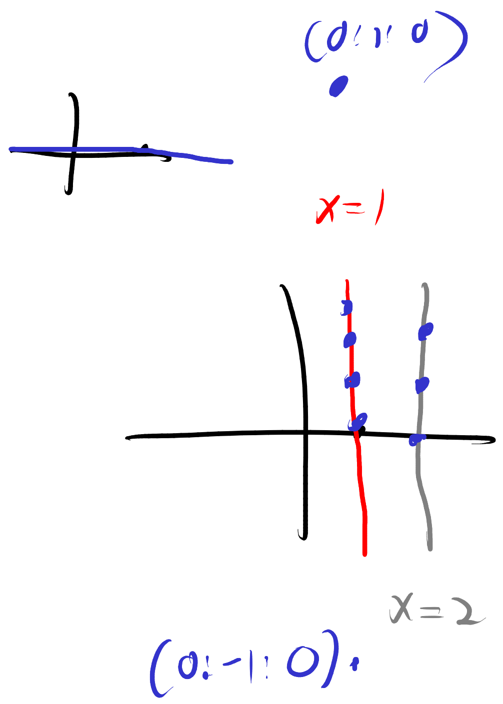
The projective plane

$$\mathbb{P}_2 = \left(\mathbb{R}^3 \setminus \{(0,0,0)\}\right) / \sim$$

$(a, b, c) \sim r(a, b, c)$

If $c \neq 0$, can divide by c to assume $c = 1$.

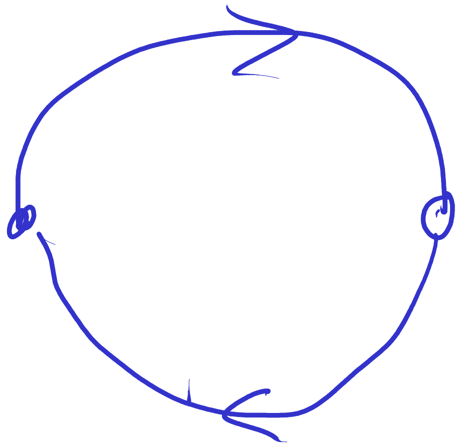
$(1:0:0)$



$y^2 = x^3 + 1$
pts $(0,1)$, $(0,-1)$, $(-1,0)$
$(0:1:1)$, $(0:-1:1)$, $(-1:0:1)$

homogenize
$$Y^2 Z = X^3 + Z^3$$

$x = 1$	$x = 2$
$X = Z$	$X = 2Z$
$(1:0:1)$	$(2:0:1)$
$(1:1:1)$ $(1:2:1)$	$(2:1:1)$ $(2:2:1)$
$(0:1:0)$	$(0:1:0)$



Group Law

$(x,y)+(a,b) = (x+a, y+b)$ X

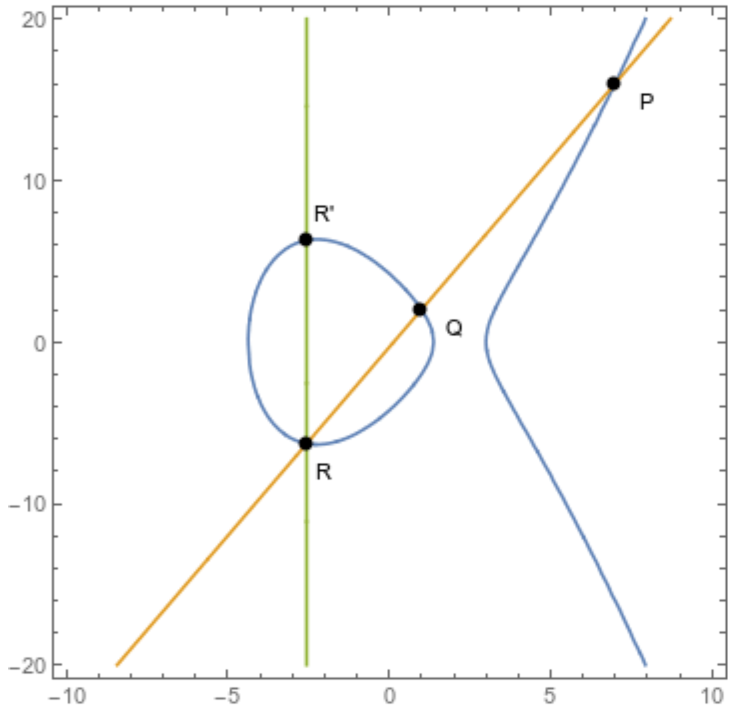
Dfn: Let $P, Q \in E$

draw line through P, Q

$\exists$ 3rd pt of $\cap$, called R

Let R' be the reflection of R across x-axis

define $R' = P \oplus Q$



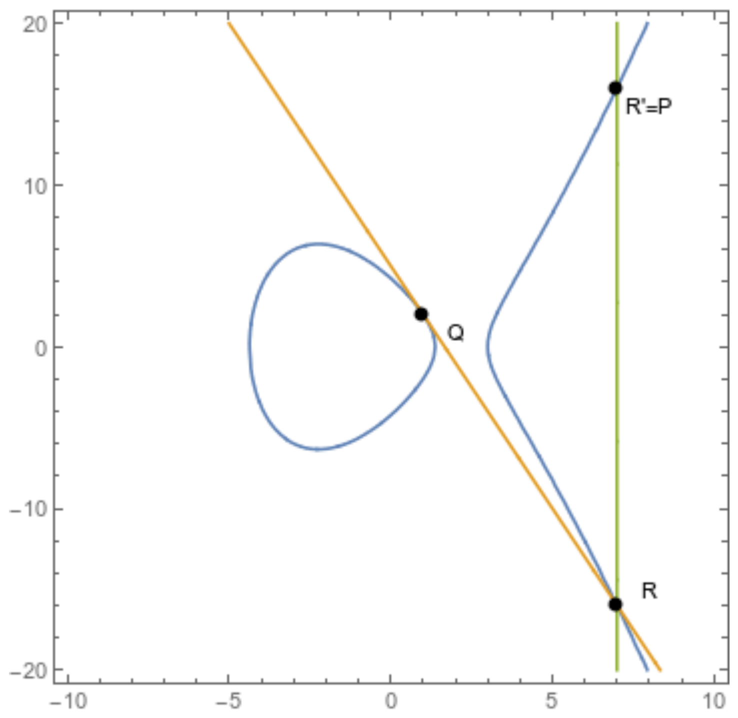
$y^2 = x^3 + ax + b$

$Y^2Z = X^3 + aXZ^2 + bZ^3$

what if $P = Q$?

want to go through P "twice".

draw line tangent to $P = Q$



$R \oplus R' = (0:1:0)$

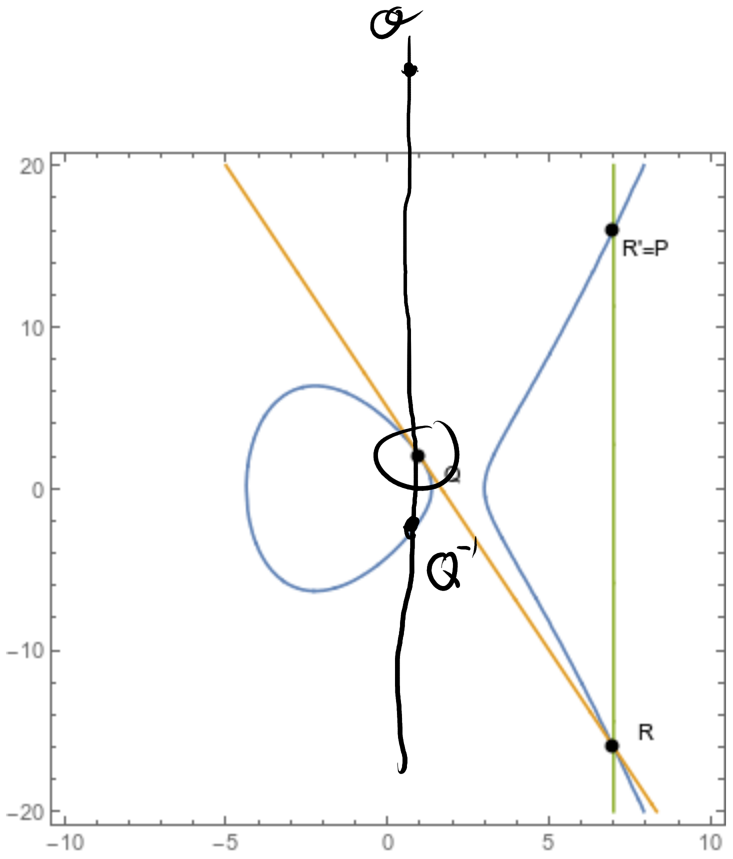
Dfn: $(0:1:0) = \mathcal{O}$

Fact: $\mathcal{O} \oplus P = P$

Dfn: $\mathcal{O} = (0:1:0)$

pt at (vertical) ∞

Fact: $\mathcal{O} \oplus Q = Q$

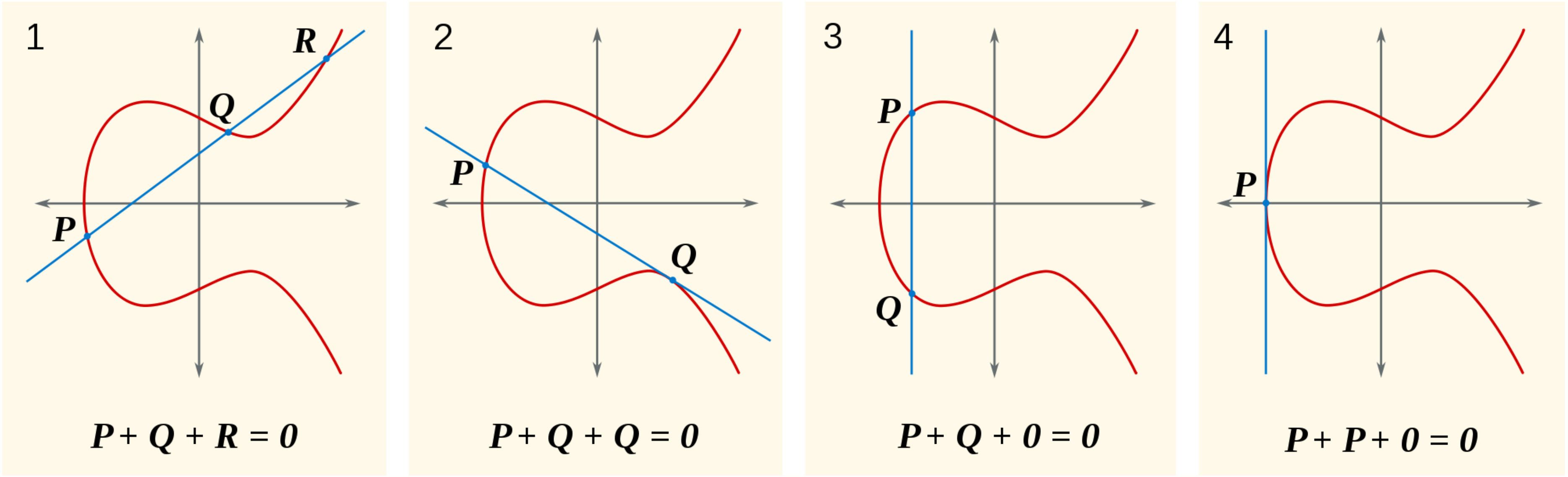


Under this operation, $E(K)$ forms a group.

in fact, forms an abelian gp.

Dfn: $P \oplus (-Q) = P - Q$

$P \oplus P \oplus \cdots \oplus P = nP$



Elliptic Curves over $\mathbb{Q}$

Fact: if $E(\mathbb{Q})$ is finite, then either $E(\mathbb{Q}) = \mathbb{Z}/n\mathbb{Z}$ for

$$n \in \{1, 2, 3, \dots, 9, 10, 12\}$$

or $E(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

for $n \in \{2, 4, 6, 8\}$

Conjecture: exactly 50% of curves are infinite.

(special case of Birch and Swinnerton-Dyer Conjecture)

BSD

$E: y^2 = x^3 - 15x + 18$

$P = (7, 16)$

$Q = (1, 2)$

what's $P \oplus Q$?

$$y = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) + y_1$$

$$y = \frac{16-2}{7-1}(x-1) + 2$$

$$y = \frac{7}{3}x - \frac{1}{3}$$

$$\left(\frac{7}{3}x - \frac{1}{3}\right)^2 = x^3 - 15x + 18$$

$$\Rightarrow x^3 - \frac{49}{9}x^2 - \frac{121}{9}x + \frac{161}{9} = 0.$$

two roots: 1, 7

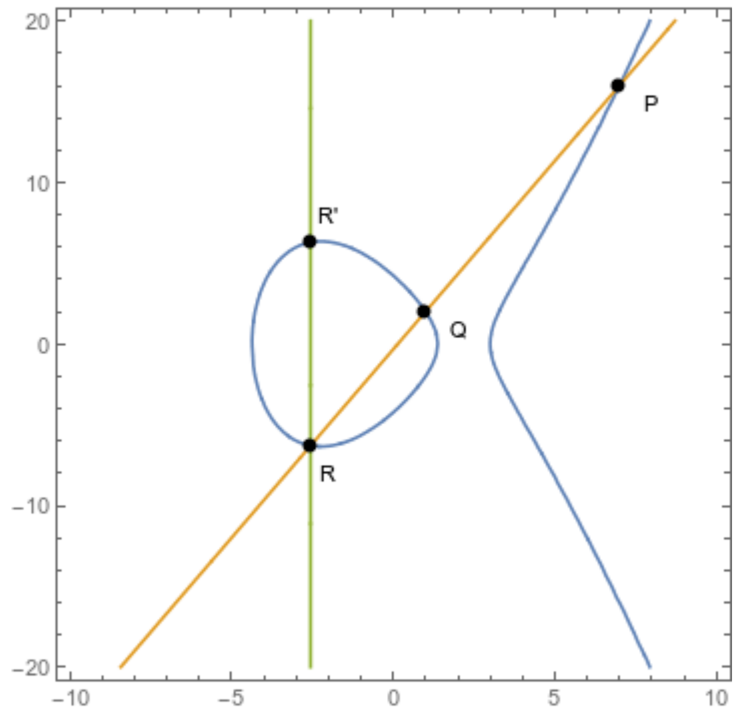
$$x^3 \boxed{-\frac{49}{9}} x^2 - \frac{121}{9}x + \frac{161}{9}$$

$$= (x-1)(x-7)(x-x_3)$$

$$= x^3 + \boxed{(-1 + -7 + -x_3)} x^2 + (\ )x + (\ )$$

So $$-\frac{49}{9} = -1 - 7 - x_3$$

$$x_3 = \frac{49}{9} - 8 = \frac{-23}{9}.$$



$$y_3 = \frac{7}{3}\left(\frac{-23}{9}\right) - \frac{1}{3}$$

$$= -\frac{170}{27}$$

$$R = \left(\frac{-23}{9}, \frac{-170}{27}\right)$$

$$P \oplus Q = \left(\frac{-23}{9}, \frac{170}{27}\right)$$

$E: y^2 = x^3 - 15x + 18$

$P = (7, 16)$

$Q = (1, 2)$

$Q \oplus Q$

need line through Q twice

Tangent line

$2yy' = 3x^2 - 15$

$x=1,\ y=2$

$4y' = 3 - 15$

$y' = -3$

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

$= -3x + 5$

$(5-3x)^2 = x^3 - 15x + 18$

$0 = x^3 \boxed{-9x^2} + 15x - 7$

$= (x-1)(x-1)(x-x_3)$

$= x^3 + \boxed{(-1-1-x_3)x^2} + (\ )x + (\ )$

$-9 = -1 - 1 - x_3$

$\Rightarrow x_3 = 7.$

$y_3 = -3(7) + 5$

$= -16$

$R = (7, -16)$

$Q \oplus Q = (7, 16)$