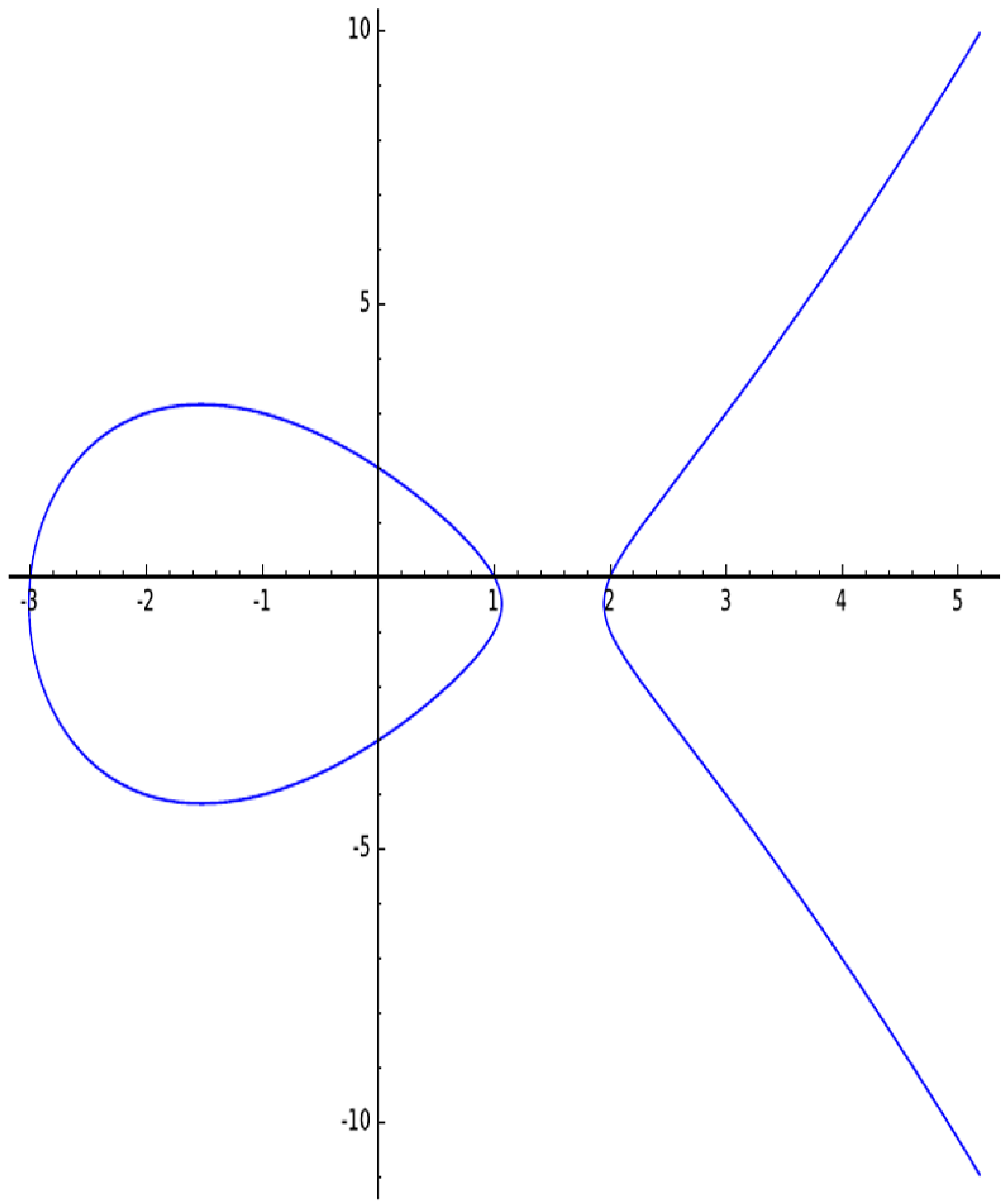
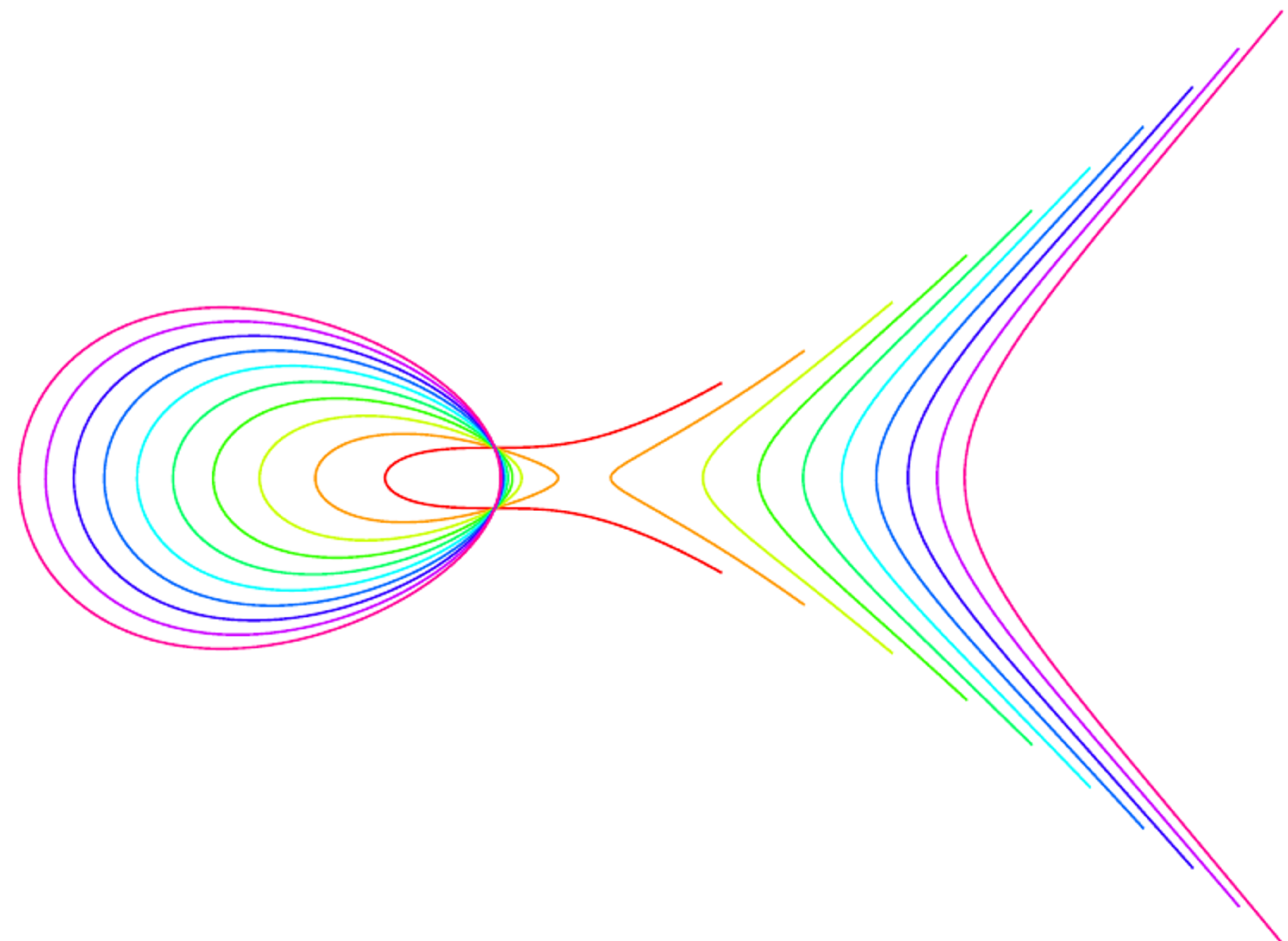
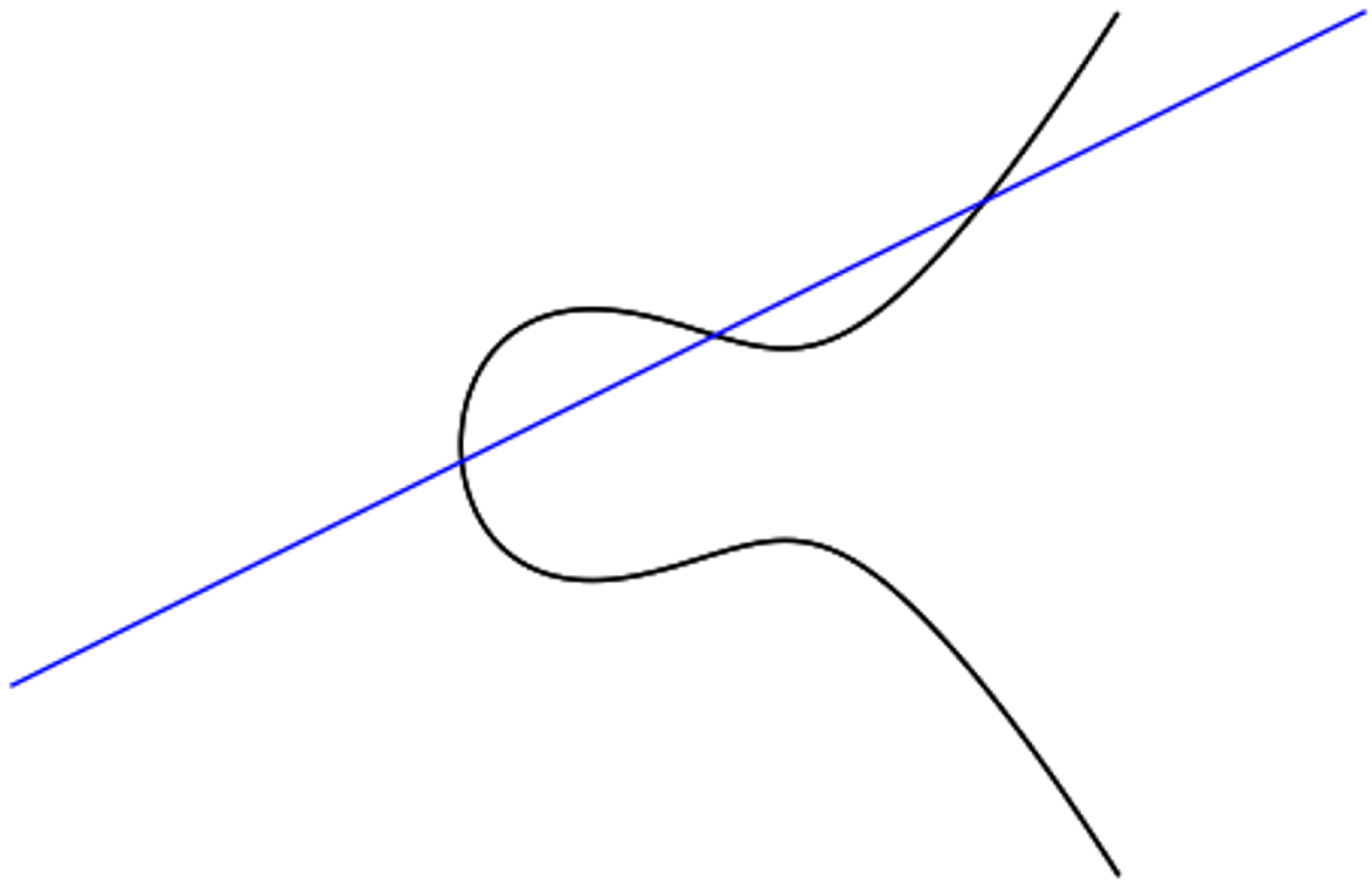
Elliptic Curves

$$E: \quad y^2 = x^3 + ax^2 + bx + c$$





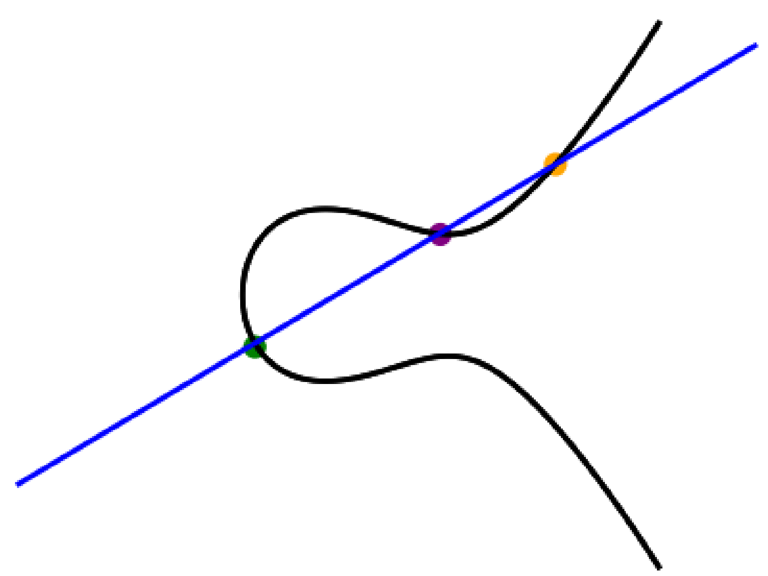
a line intersect E at 3 points



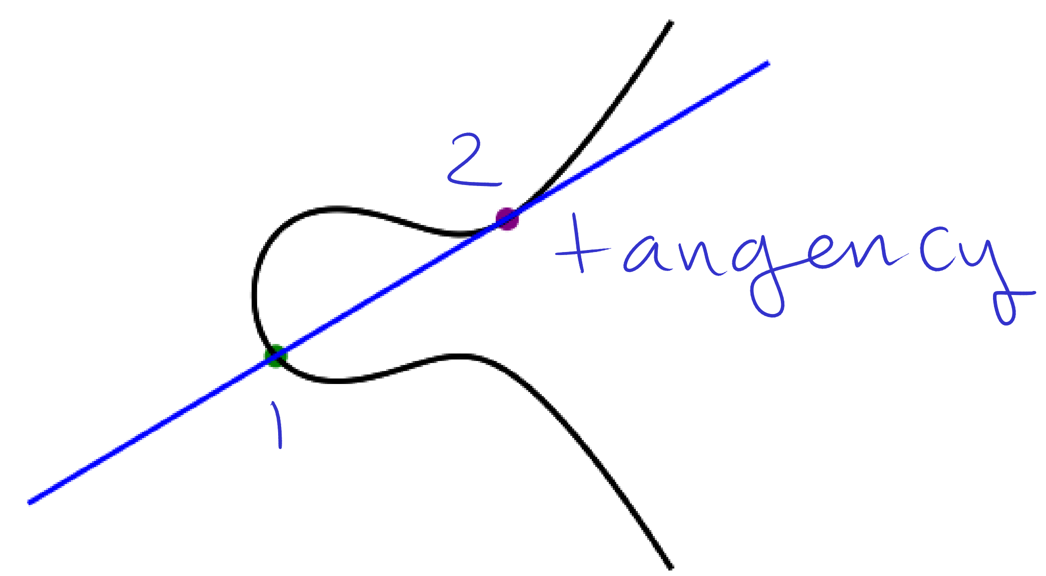
$\cap$ w/ $y = mx + n$

$E: y^2 = x^3 + ax^2 + bx + c$

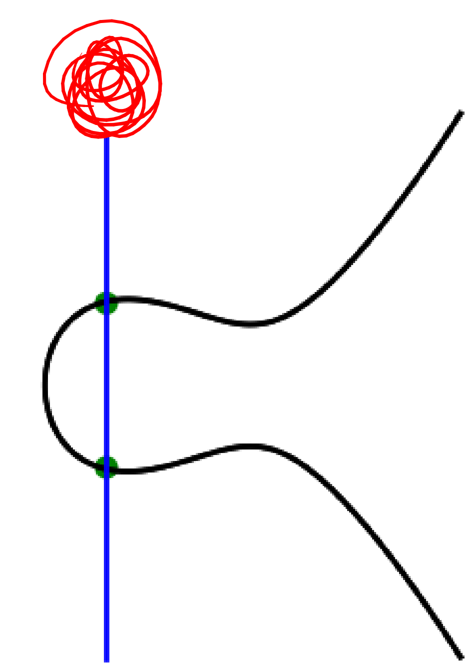
Since E is degree 3, a line intersects E at 3 places



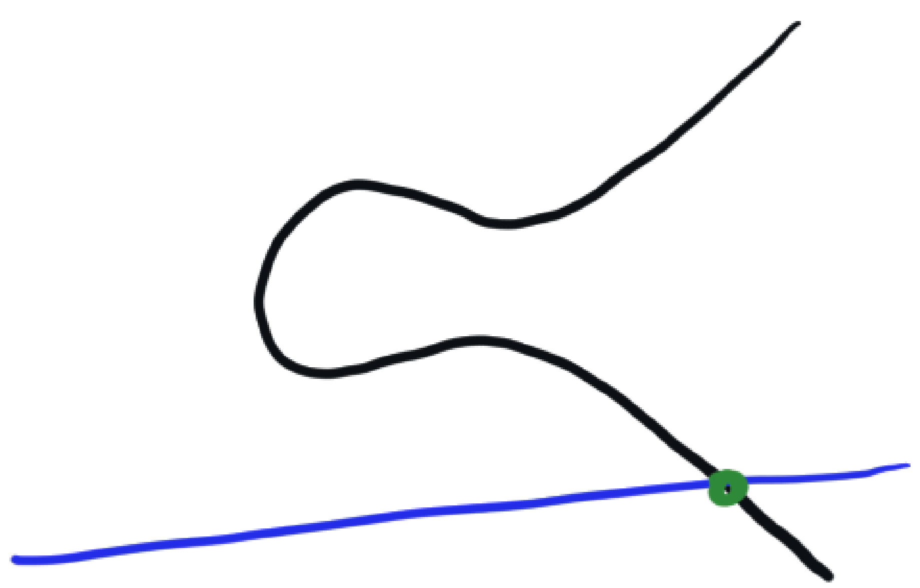
3 real roots



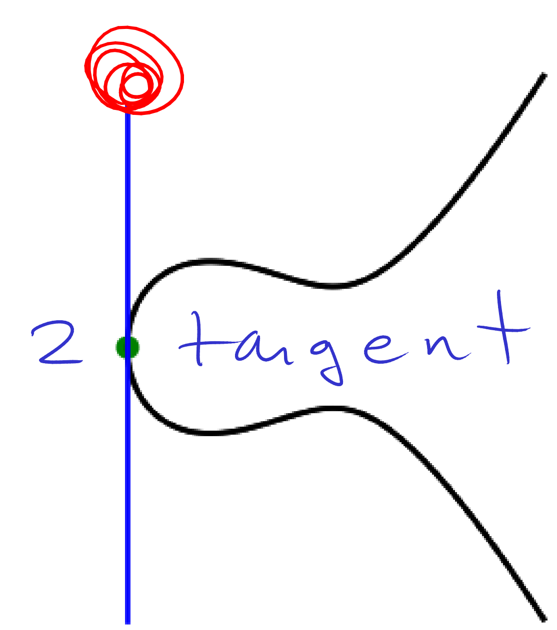
3 real (1 repeated)



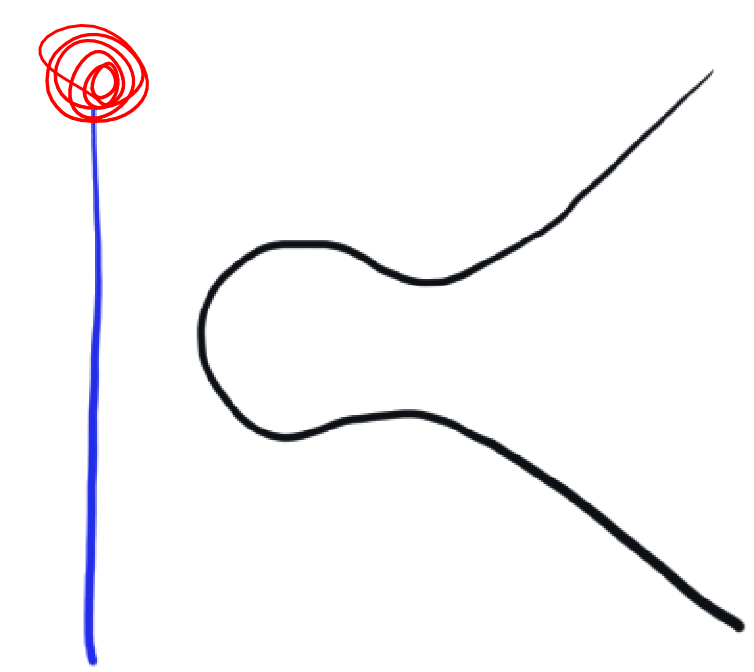
2 real, 1 is ∞



1 real, 2 complex



1 real repeated root + ∞



2 complex + ∞

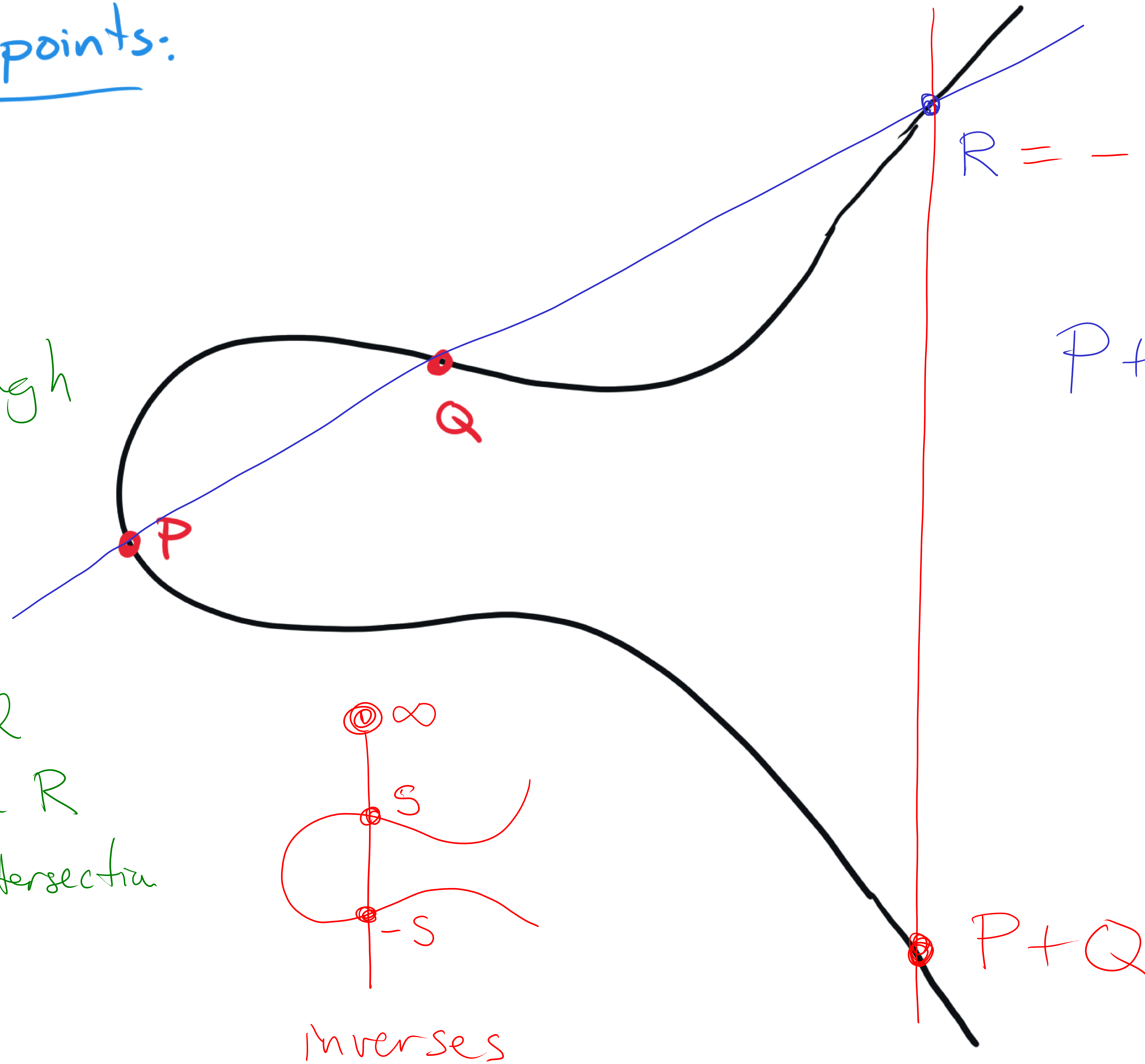
$$E : y^2 = x^3 + ax^2 + bx + c$$

How to add points:

Rules

① take line through
P & Q
get a 3rd
intersection point R

② take vertical
line through R
get 2nd intersection
P+Q



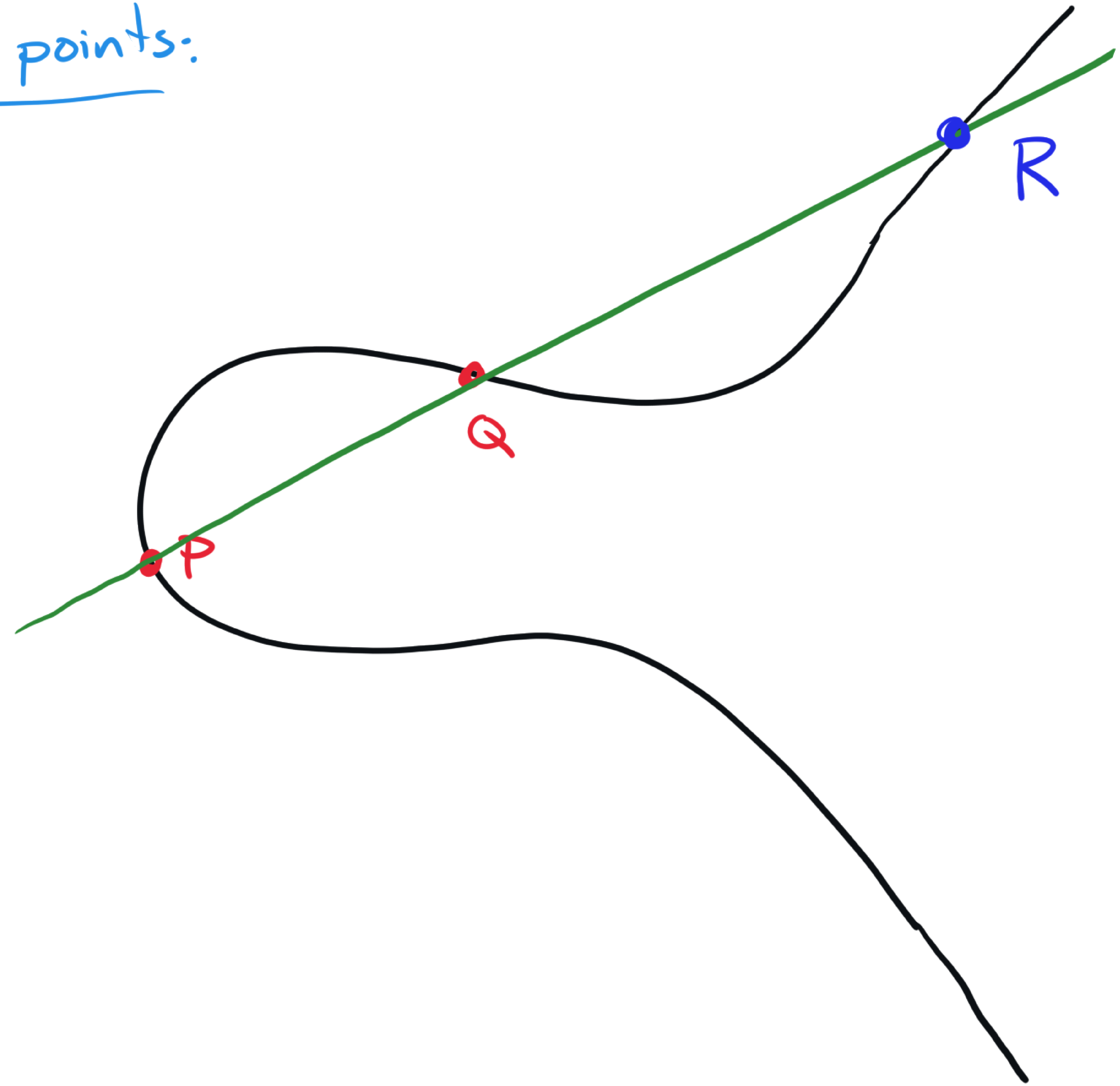
$R = -(P+Q)$

$\Uparrow$

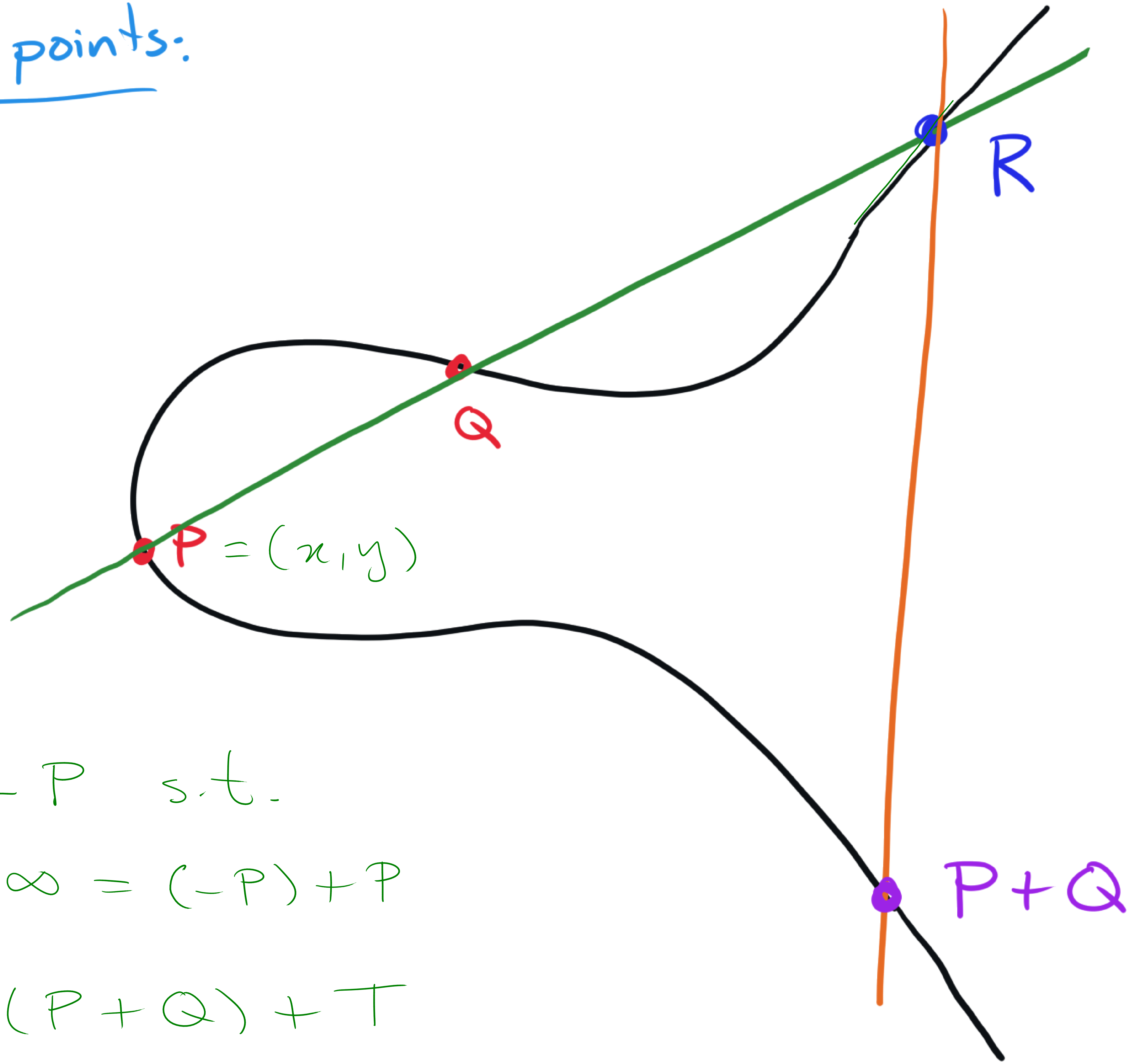
$P+Q+R = \infty$

identity in group

How to add points:



How to add points:



Group laws:

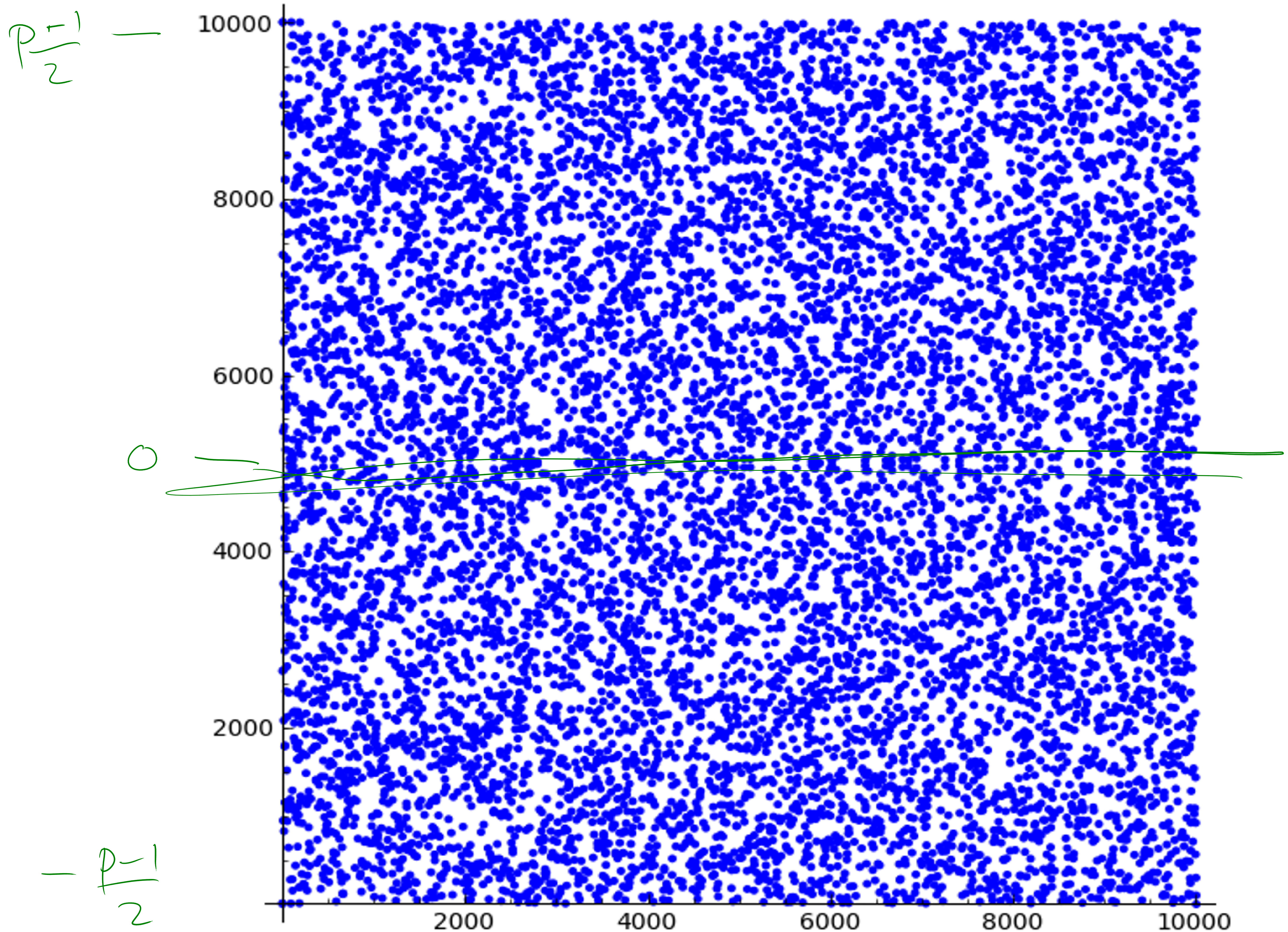
$P + Q = Q + P$

$\infty + P = P + \infty$
$= P$

For every P,
there exists $-P$ s.t.
$P + (-P) = \infty = (-P) + P$

$P + (Q + T) = (P + Q) + T$

If adding
$P + P$
the "line through
P and P"
is the tangent
line @ P



An elliptic curve over $\mathbb{F}_p$ for big p.

$$\{(x,y) : x, y \in \mathbb{F}_p, \ y^2 = ax^3 + bx^2 + cx + d\}$$

Example Mod 5

$$y^2 \equiv x^3 + 2x + 4 \pmod 5$$

Points:

$O = \infty$

$P = (0,2)$

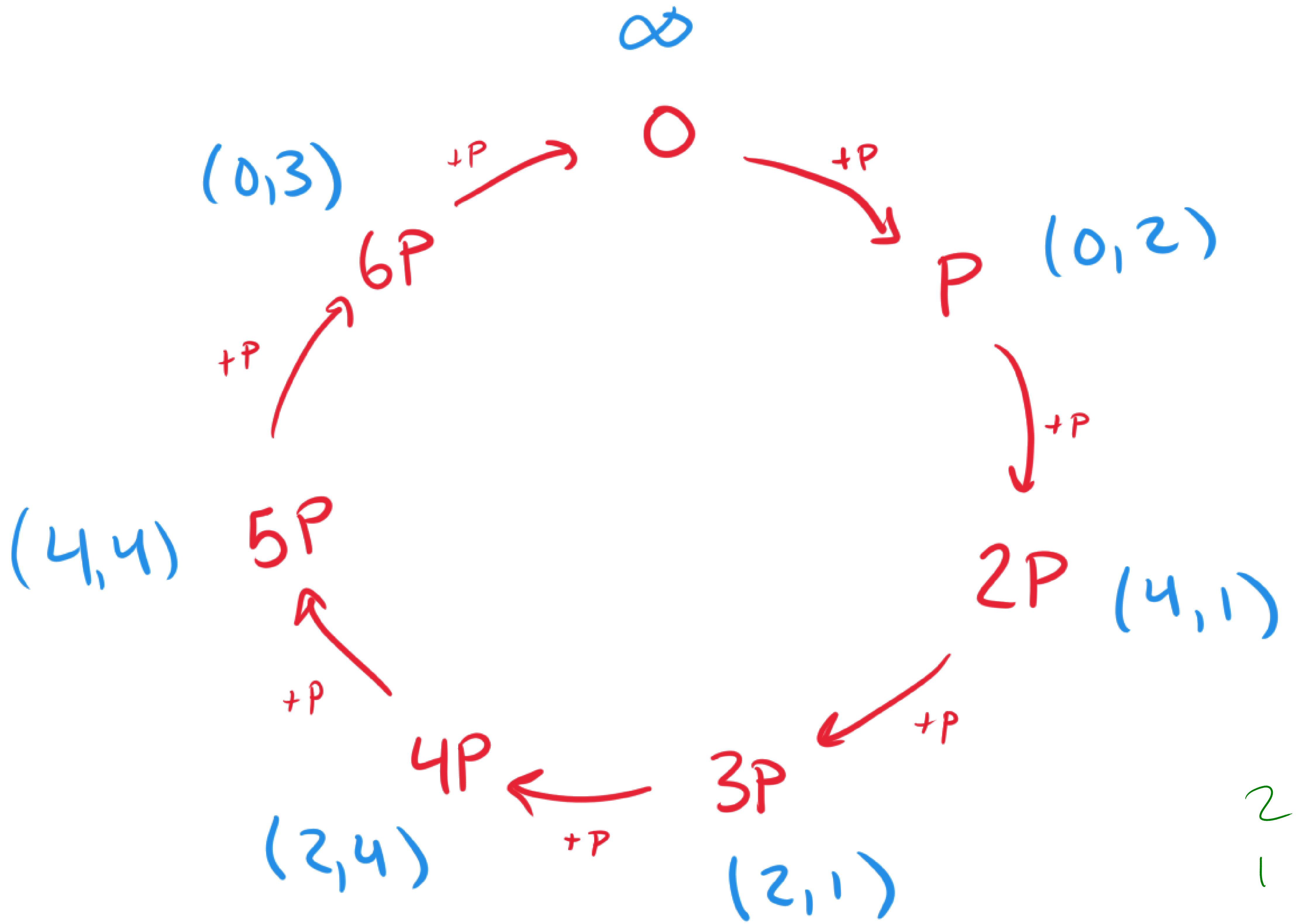
$6P = (0,3)$

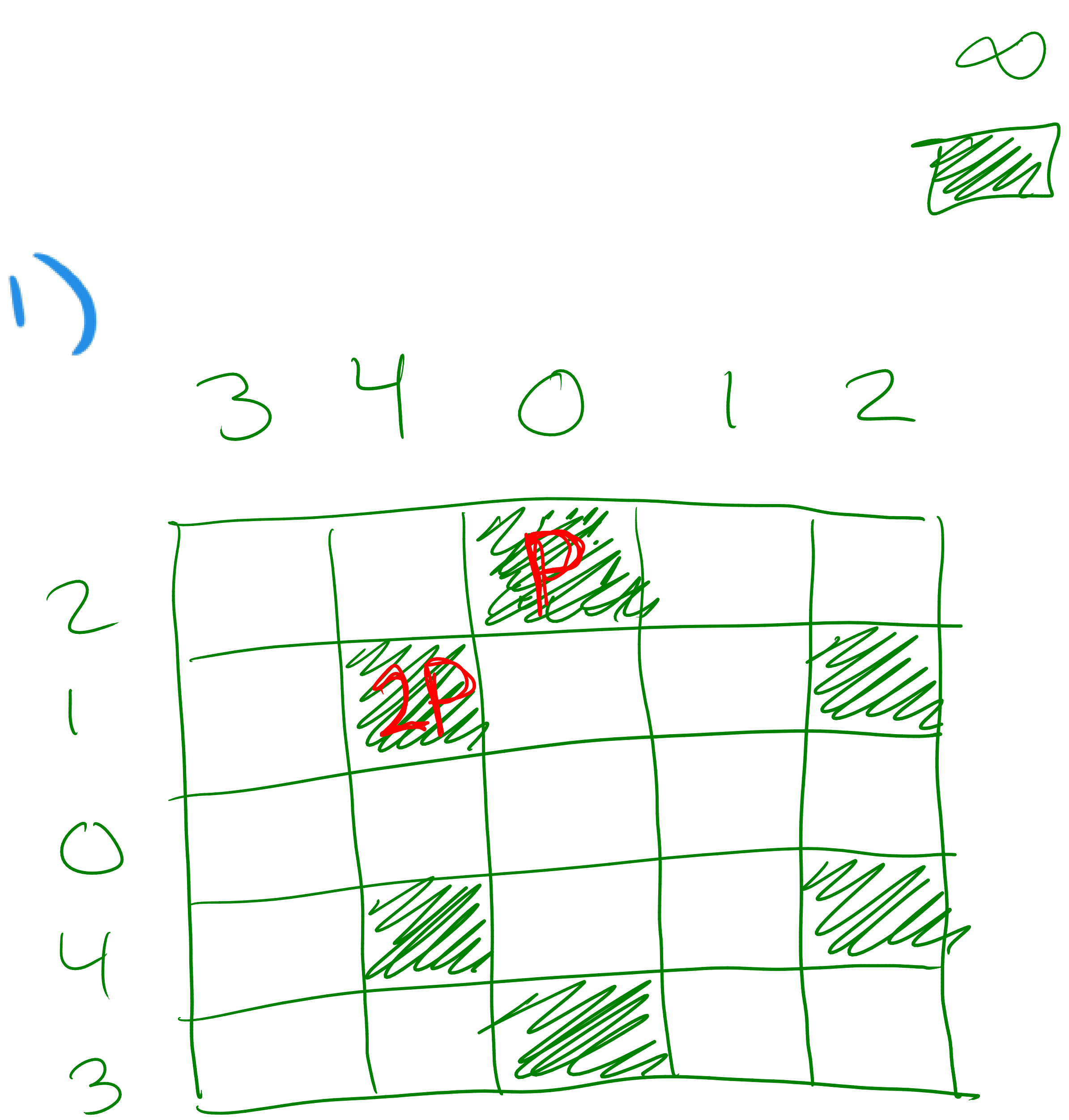
$3P = (2,1)$

$4P = (2,4)$

$2P = (4,1)$

$5P = (4,4)$





Example Mod 5

$$y^2 \equiv x^3 + 2x + 4 \pmod{5}$$

Points:

$O = \infty$

$P = (0,2)$

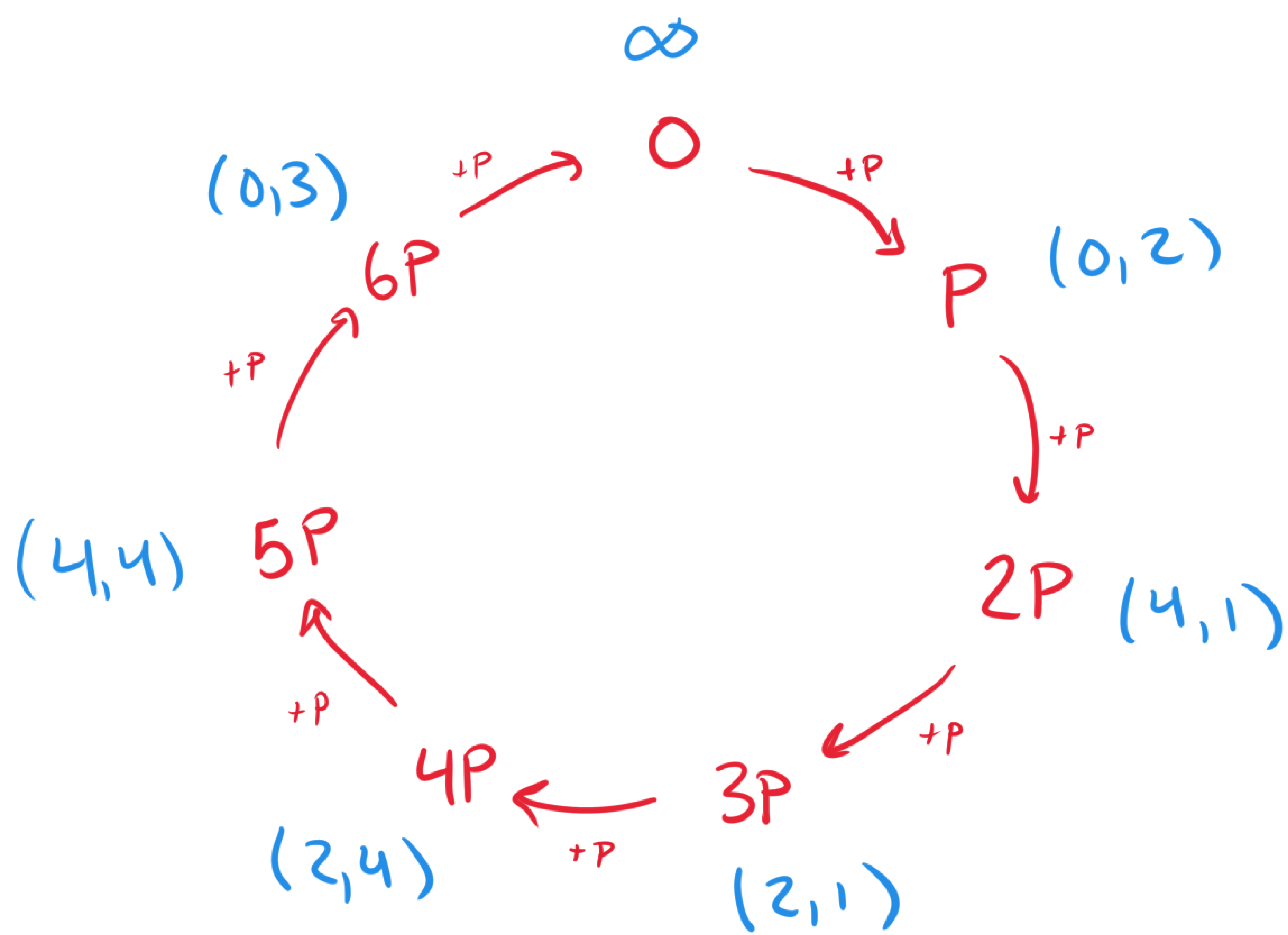
$6P = (0,3)$

$3P = (2,1)$

$4P = (2,4)$

$2P = (4,1)$

$5P = (4,4)$



$E: y^2 \equiv x^3 + 2x + 4 \pmod 5$

<u>Points</u>

∞
$(0,2)$
$(0,3)$
$(2,1)$
$(2,4)$
$(4,1)$
$(4,4)$

<u>Task:</u> Add $\underset{P}{(0,2)}$ to $\underset{Q}{(2,4)}$

① line through P and Q:

slope $= \frac{4-2}{2-0} = \frac{2}{2} = 1$ y-intercept $= 2$

Line $L: y \equiv x + 2 \pmod 5$

② 3^{rd} intersection pt of L w/ E

$(x+2)^2 \equiv x^3 + 2x + 4$

$x^3 - x^2 - 2x \equiv 0$

we know 0, 2 are solns, want 3^{rd}

trace $\equiv 1 \equiv 0 + 2 + x_R$

$\Rightarrow x_R \equiv -1 \equiv 4$

So $y_R \equiv x_R + 2$ (from L)
$\equiv 4 + 2$
$\equiv 1$

$\Rightarrow \underset{(3^{rd}\text{ pt})}{R} = (4,1)$

<u>aside:</u>

$x^3 + ax^2 + bx + c = 0$

trace is $-a$

$= \Sigma$ of roots

③ $P + Q$

$\equiv -R \equiv (x_R, -y_R)$

$\equiv (4,4)$