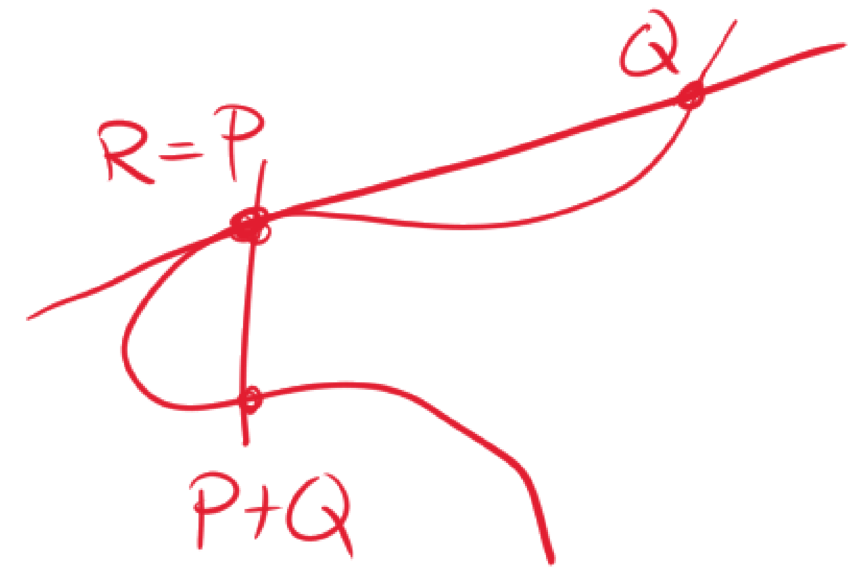
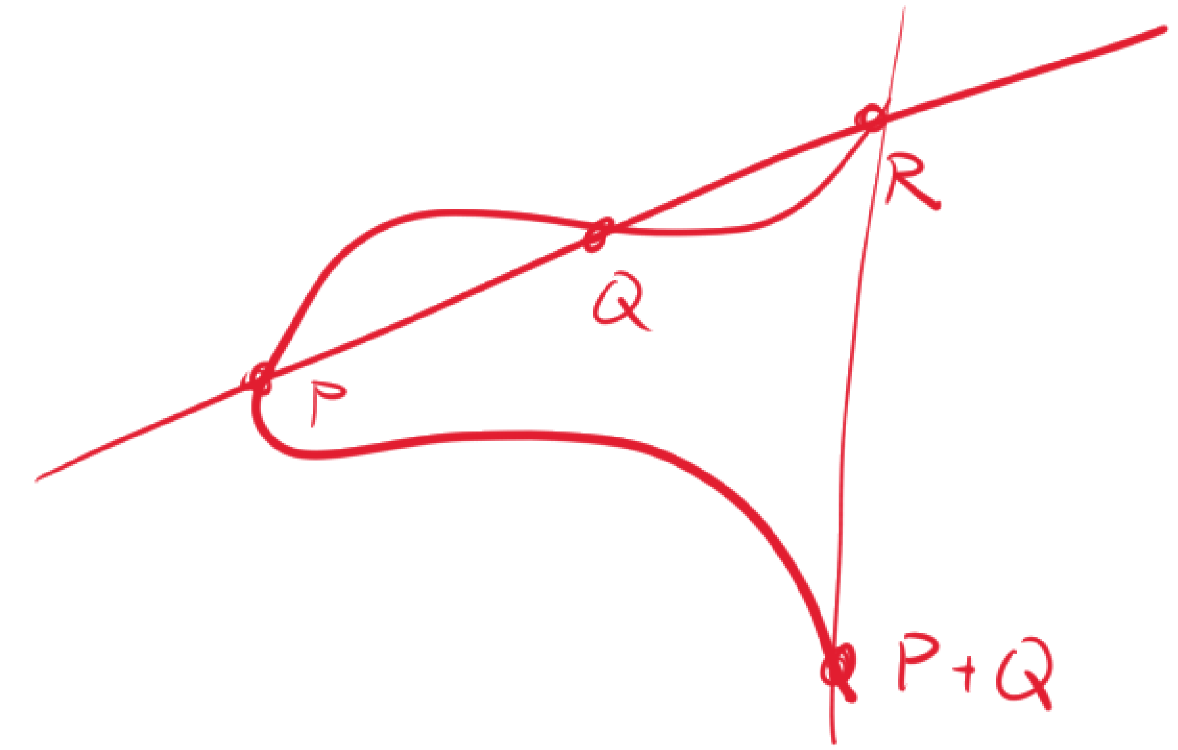
$E: \ y^2 = x^3 + x + 1 \pmod 7$.

$P = (0,1), \quad Q = (2,2)$.





⓪ Check P is on E: $1^2 = 0^3 + 0 + 1$ ✓

Check Q is on E: $2^2 = 4$

$2^3 + 2 + 1 = 8 + 3 = 11$

$\equiv 4$ ✓

① Line through P and Q: slope $= \frac{1}{2} \equiv 4 \pmod 7$

$2^{-1} \pmod 7$ $\qquad 2 \cdot 4 \equiv 8 \equiv 1 \pmod 7$

$$y = 4x + 1$$

② Solve for intersections:

$$(4x+1)^2 = x^3 + x + 1$$

$$2x^2 + x + 1 = x^3 + x + 1$$

$$x^3 + 5x^2 = 0$$

$$-5 = 0 + 2 + x_R$$

$$\Rightarrow x_R = 0 \quad \Rightarrow y_R = 4 \cdot 0 + 1 = 1$$

③ Reflect across the x-axis:

$$P + Q = (0, 6)$$

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

Example Mod 5

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

Points:

∞

$(0,2)$

$(0,3)$

$(2,1)$

$(2,4)$

$(4,1)$

$(4,4)$

Task: Add $(0,2)$ to itself.

Example Mod 5

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

Points:

∞

$(0,2)$

$(0,3)$

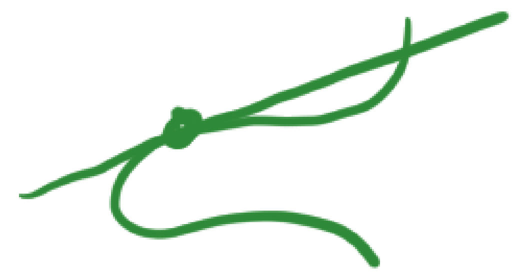
$(2,1)$

$(2,4)$

$(4,1)$

$(4,4)$

Task: Add $(0,2)$ to itself.



Tangent line @ $(0,2)$:

mod 5

$$2y\frac{dy}{dx} = 3x^2 + 2 \quad \Rightarrow \quad \frac{dy}{dx} = \frac{3x^2+2}{2y} = \frac{2}{4} = \frac{1}{2} \equiv 3$$

Example Mod 5

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

Points:

∞

$(0,2)$

$(0,3)$

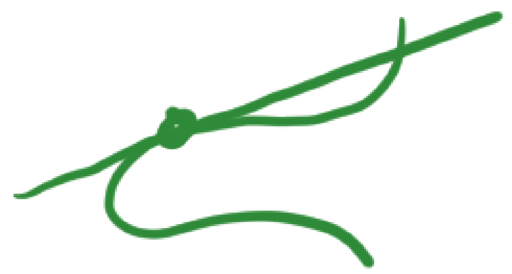
$(2,1)$

$(2,4)$

$(4,1)$

$(4,4)$

Task: Add $(0,2)$ to itself.



Tangent line @ $(0,2)$:

mod 5

$$2y\frac{dy}{dx} = 3x^2 + 2 \implies \frac{dy}{dx} = \frac{3x^2+2}{2y} = \frac{2}{4} = \frac{1}{2} \equiv 3$$

$$\left.\begin{array}{l} \text{slope} = 3 \\ y\text{-intercept} = 2 \end{array}\right\} \quad y = 3x + 2$$

Example Mod 5

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

Points:

∞

$(0,2)$

$(0,3)$

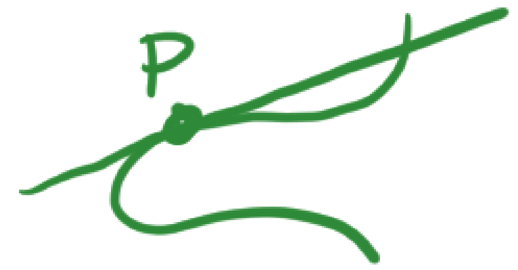
$(2,1)$

$(2,4)$

$(4,1)$

$(4,4)$

Task: Add $\overset{P}{(0,2)}$ to itself.

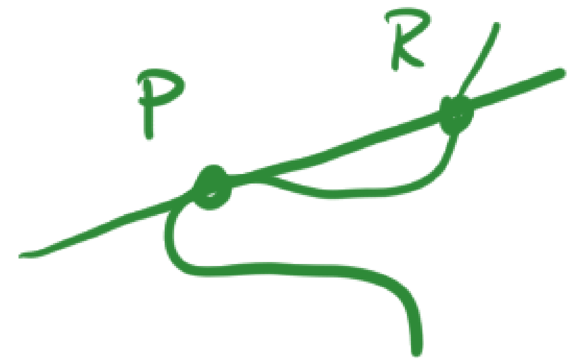


Tangent line @ $(0,2)$:

mod 5

$$2y\frac{dy}{dx} = 3x^2 + 2 \Rightarrow \frac{dy}{dx} = \frac{3x^2+2}{2y} = \frac{2}{4} = \frac{1}{2} \equiv 3$$

$$\left.\begin{array}{l}\text{slope} = 3 \\ y\text{-intercept} = 2\end{array}\right\} \quad y = 3x + 2$$



Find 3rd intersection pt:

$$(3x+2)^2 = x^3 + 2x + 4$$
$$9x^2 + 12x + 4 = x^3 + 2x + 4$$
$$x^3 - 9x^2 - 10x \equiv 0$$
$$x^3 - 4x^2 \equiv 0$$
$$x^2(x-4) \equiv 0$$
$$x_R = 4 \Rightarrow y_R = 3x_R + 2 = 4$$

$R = (4,4)$

Example Mod 5

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

Points:

∞

$(0,2)$

$(0,3)$

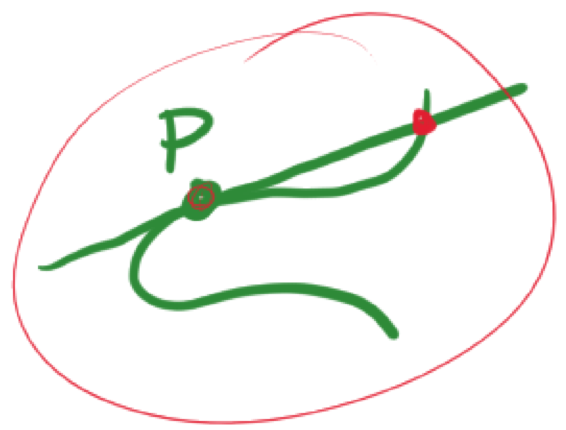
$(2,1)$

$(2,4)$

$(4,1)$

$(4,4)$

Task: Add $\overset{P}{(0,2)}$ to itself.

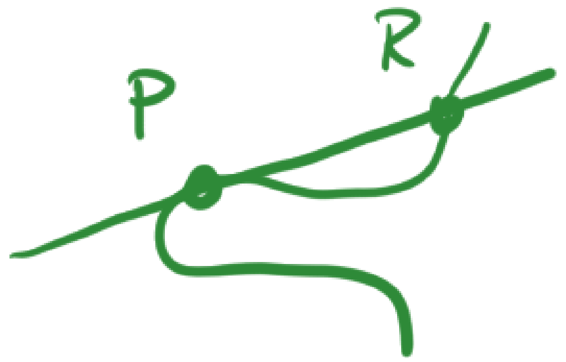


Tangent line @ $(0,2)$:

$$2y\frac{dy}{dx} = 3x^2 + 2 \Rightarrow \frac{dy}{dx} = \frac{3x^2+2}{2y} = \frac{2}{4} = \frac{1}{2} \underset{\text{mod } 5}{\equiv} 3$$

slope $= 3$

y-intercept $= 2$ $\Big\}$ $y = 3x + 2$



Find 3rd intersection pt:

$$(3x+2)^2 = x^3 + 2x + 4$$

$$9x^2 + 12x + 4 = x^3 + 2x + 4$$

$$x^3 - 9x^2 - 10x \equiv 0$$

$$x^3 - 4x^2 \equiv 0$$

$$x^2(x-4) \equiv 0$$

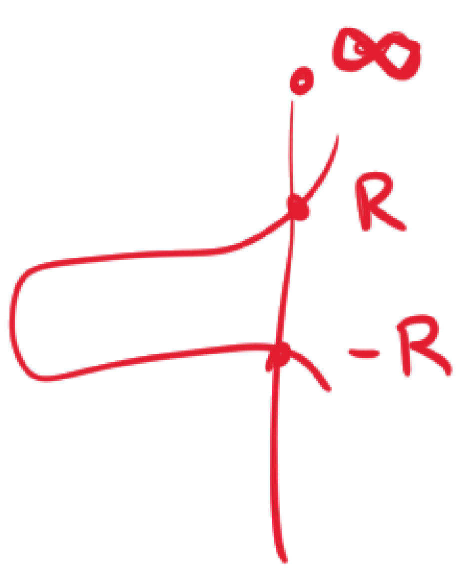
$$4 = 0 + 0 + x_R$$

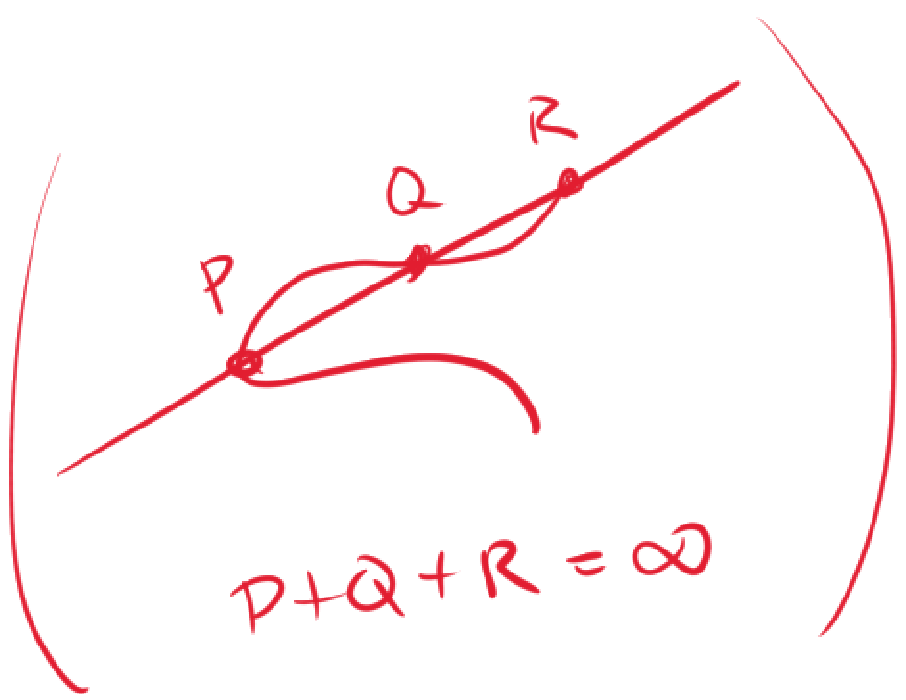
$$x_R = 4 \Rightarrow y_R = 3x_R + 2 = 4$$

$R = (4,4)$

Flip in x-axis:

$$\boxed{2P = (4,1)}$$





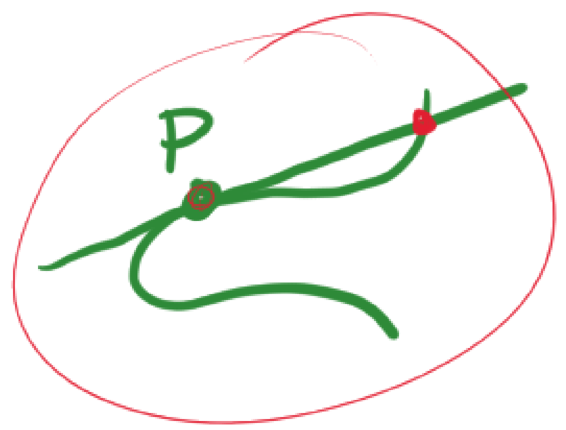
Example Mod 5

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

Points:

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

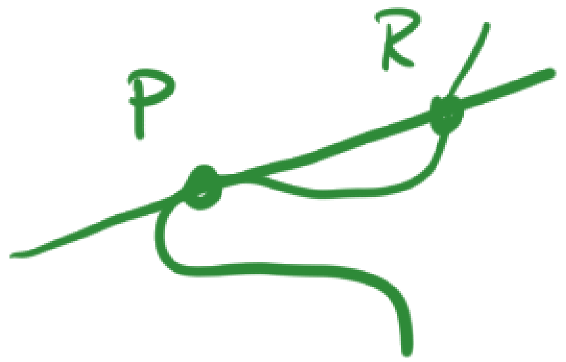
Task: Add $\overset{P}{(0,2)}$ to itself.



Tangent line @ $(0,2)$:

$$2y\frac{dy}{dx} = 3x^2 + 2 \Rightarrow \frac{dy}{dx} = \frac{3x^2+2}{2y} = \frac{2}{4} = \frac{1}{2} \underset{\text{mod } 5}{\equiv} 3$$

$$\left.\begin{array}{l}\text{slope} = 3\\ y\text{-intercept} = 2\end{array}\right\} \quad y = 3x + 2$$



Find 3rd intersection pt:

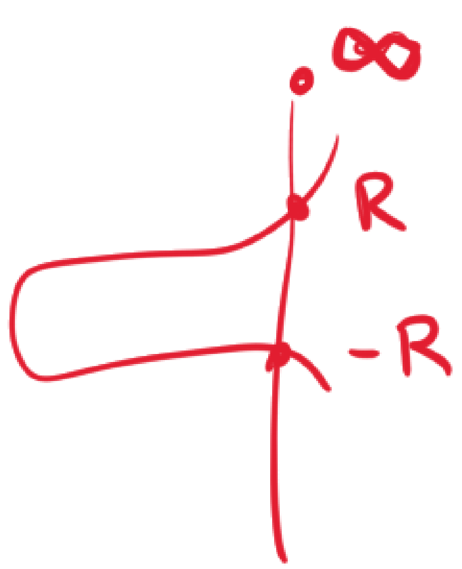
$$(3x+2)^2 = x^3 + 2x + 4$$
$$9x^2 + 12x + 4 = x^3 + 2x + 4$$
$$x^3 - 9x^2 - 10x \equiv 0$$
$$x^3 - 4x^2 \equiv 0$$
$$x^2(x-4) \equiv 0$$
$$x_R = 4 \Rightarrow y_R = 3x_R + 2 = 4$$

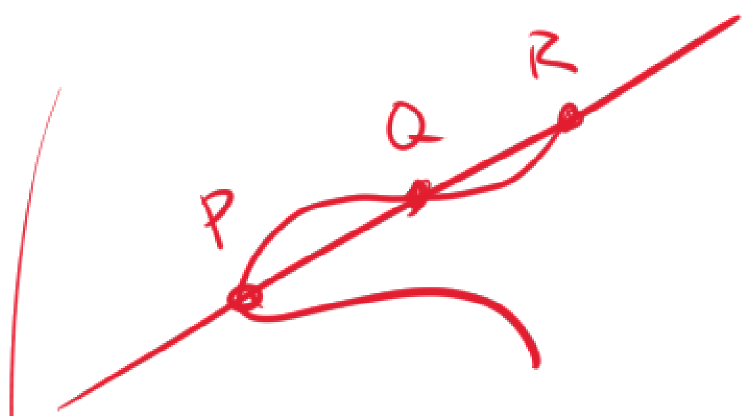
$4 = 0 + 0 + x_R$

$R = (4,4)$

Flip in x-axis:

$$\boxed{2P = (4,1)}$$





$P + Q + R = \infty$

Example Mod 5

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

Points:

$\mathcal{O} = \infty$

$P = (0,2)$

$(0,3)$

$(2,1)$

$(2,4)$

$2P = (4,1)$

$(4,4)$

Example Mod 5

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

Points:

$\mathcal{O} = \infty$

$P = (0,2)$

$(0,3)$

$(2,1)$

$(2,4)$

$2P = (4,1)$

$(4,4)$

SAGE can compute such things!

Example Mod 5

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

Points:

$O = \infty$

$P = (0,2)$

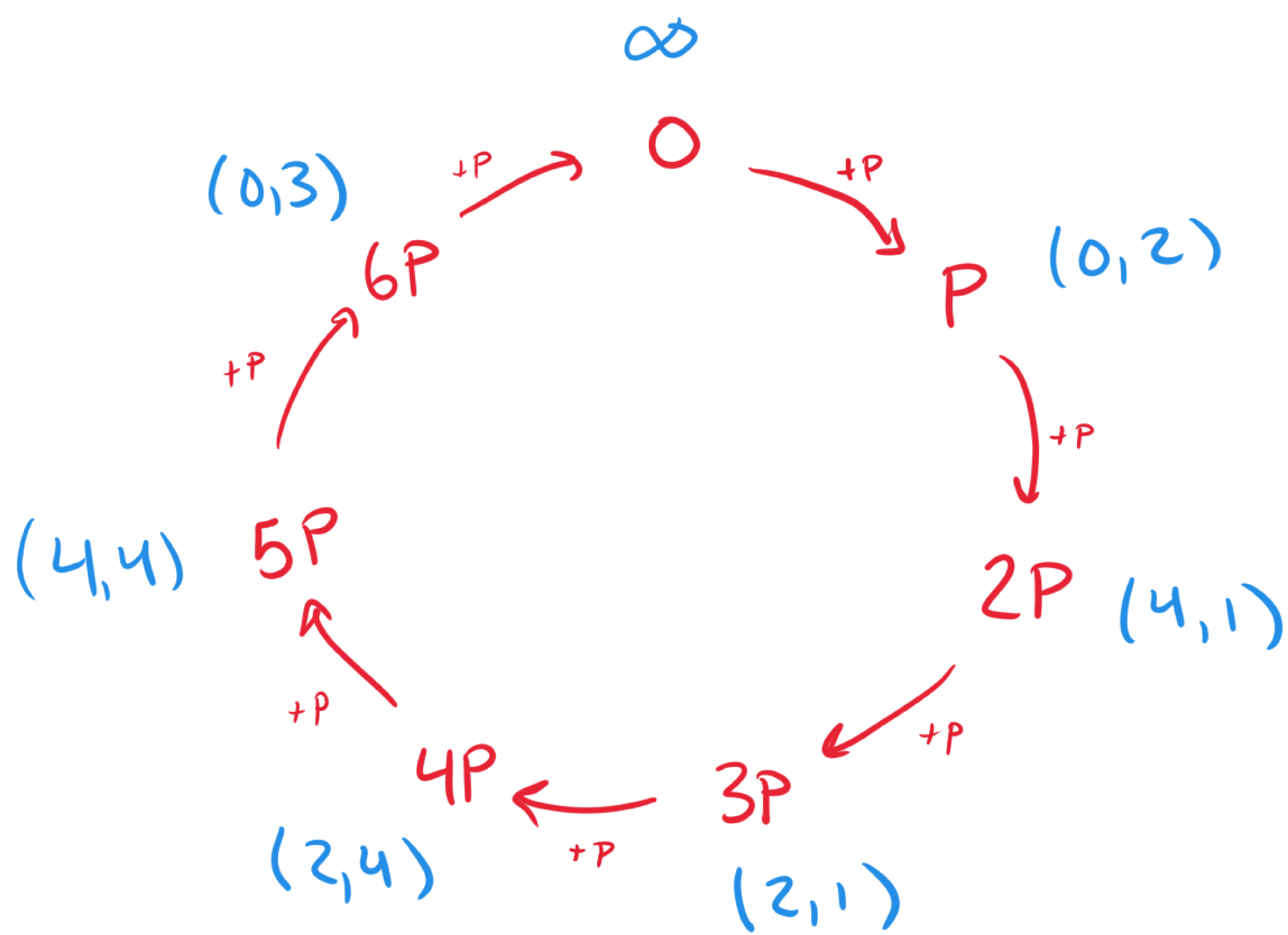
$6P = (0,3)$

$3P = (2,1)$

$4P = (2,4)$

$2P = (4,1)$

$5P = (4,4)$



Number of Points on an Elliptic Curve

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

Heuristic: Let $x = 0, 1, \ldots, p-1.$

usually: either 0 y's or 2 y's go with a given x.

Lemma: $\frac{1}{2}$ of the non-0 residues mod p are squares.
(from Module)

So $\begin{cases} \frac{1}{2} \text{ time no points for given } x \\ \frac{1}{2} \text{ time 2 points for given } x \end{cases}$

So we expect $2\frac{p}{2} + \underbrace{1}_{\text{pt at } \infty} = p+1$ points on average.

Hasse's Theorem. $\left| \overbrace{\#E(\mathbb{F}_p)}^{\#\text{ pts on } E \text{ over } \mathbb{F}_p} - p - 1 \right| < 2\sqrt{p}.$

Any value of $\#E(\mathbb{F}_p)$ allowed by bound <u>does</u> occur for some E.

Elliptic Curve Factoring

Recall the $(p-1)$-method for Factoring:

$$a \longrightarrow a^2 \longrightarrow a^{3!} \longrightarrow a^{4!} \longrightarrow a^{5!} \longrightarrow \cdots \longrightarrow a^{B!}$$

If $p-1$ divides $B!$ then $a^{B!} \equiv 1 \pmod{p}$. (FLT)

So try $\gcd(a^{B!}-1, n)$.

Idea:

$n = pq$

$$a \in \mathbb{Z}/n\mathbb{Z} \quad \nearrow a_1 \in \mathbb{Z}/p\mathbb{Z}, \quad \searrow a_2 \in \mathbb{Z}/q\mathbb{Z}$$

By CRT

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$$
$$a \longmapsto (a_1, a_2)$$

$$\begin{array}{ccccccc} a & \longrightarrow & a^2 & \longrightarrow & a^{3!} & \longrightarrow & \cdots \\ \text{\rotatebox{90}{$\cong$}} & & \text{\rotatebox{90}{$\cong$}} & & \text{\rotatebox{90}{$\cong$}} & & \\ (a_1, a_2) & & (a_1^2, a_2^2) & & (a_1^{3!}, a_2^{3!}) & & \\ & & & & \| & & \\ & & & & \boxed{(1, *)} & & \end{array}$$

something

DETECTOR $\boxed{\gcd(a^{B!}-1, n)}$

E.C. method

$$\begin{tikzcd}[row sep=small] & E/\mathbb{F}_p \\ E/(\mathbb{Z}/n\mathbb{Z}) \arrow[ur] \arrow[dr] & \\ & E/\mathbb{F}_q \end{tikzcd} \qquad \begin{tikzcd}[row sep=small] & \underset{\text{mod } p}{P_1} \\ \underset{\text{mod } n}{P} \arrow[ur] \arrow[dr] & \\ & \underset{\text{mod } q}{P_2} \end{tikzcd}$$

$$\begin{tikzcd} P \arrow[r, "\times 2"] \arrow[d] & 2P \arrow[r, "\times 3"] \arrow[d] & 3!P \arrow[r, "\times 4"] \arrow[d] & 4!P \arrow[r, "\times 5"] & 5!P \arrow[r] & \cdots \\ (P_1, P_2) & (2P_1, 2P_2) & (3!P_1, 3!P_2) \arrow[d, equal] & & & \\ & & \boxed{(\infty, \underset{\text{anything}}{*})} & \text{DETECT} & & \end{tikzcd}$$

Example. $\boxed{n = 18923}$

Choose $y^2 = x^3 + x + \square$?

$P = (0,1)$

Find $\square$ by plugging in $(0,1)$:

$1^2 = 0^3 + 0 + \square \implies \square = 1$

$E: y^2 = x^3 + x + 1$ $\boxed{\text{mod } n}$

why?

$7!P = \left(\frac{a}{d}, \frac{b}{d}\right)$

where $d \equiv 0 \pmod{p}$

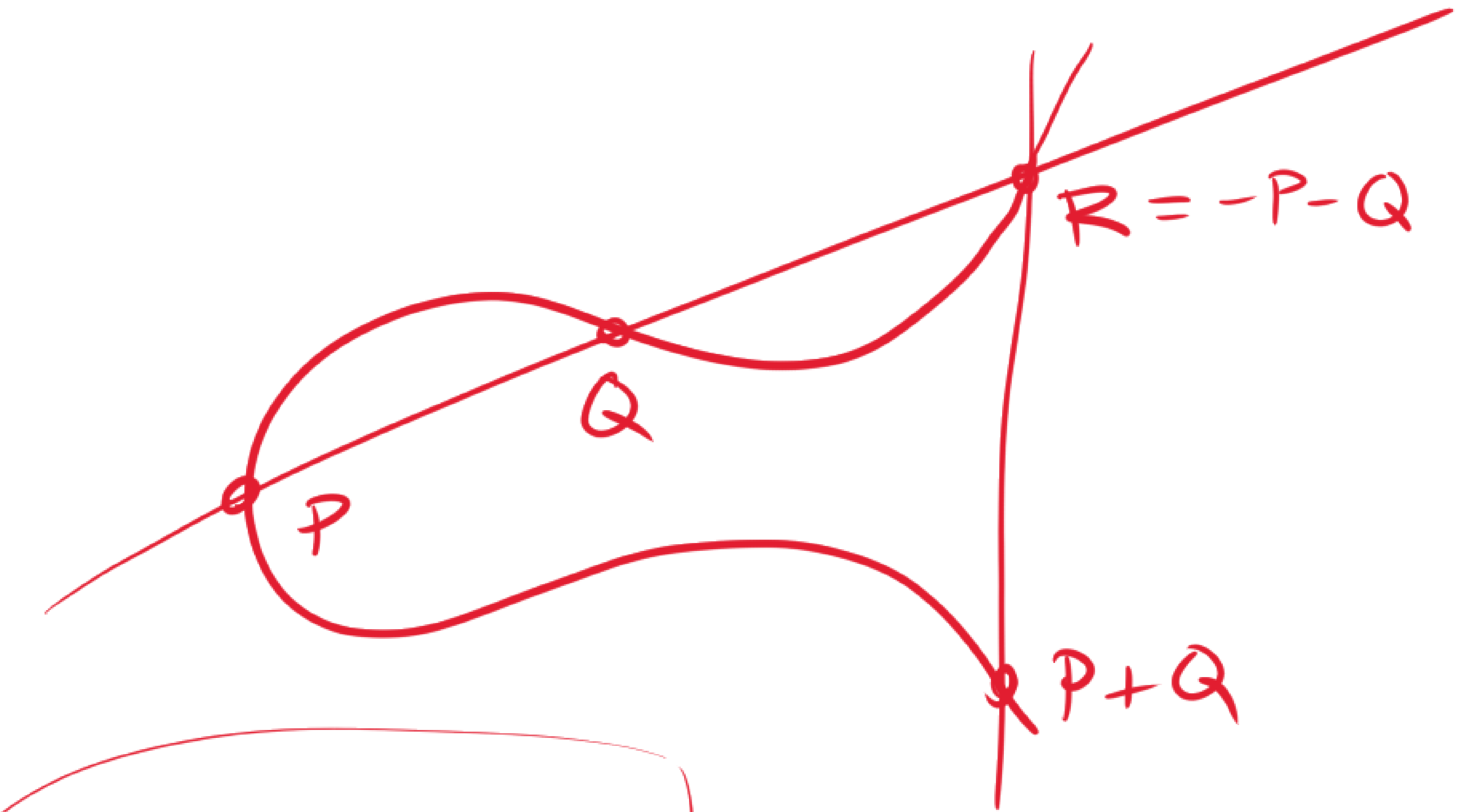
this happens iff

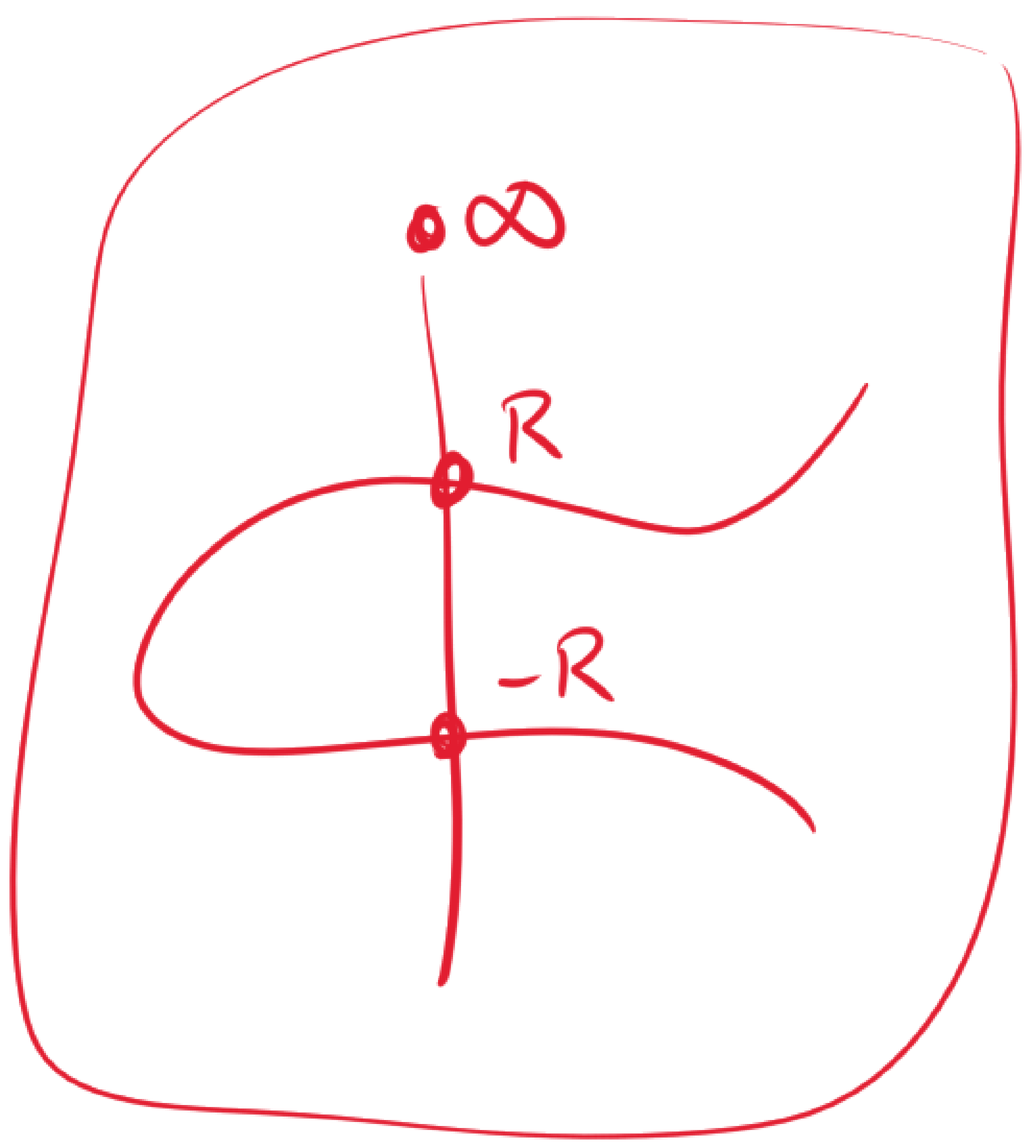
$\left(\frac{a}{d}, \frac{b}{d}\right) = \infty$ mod p.

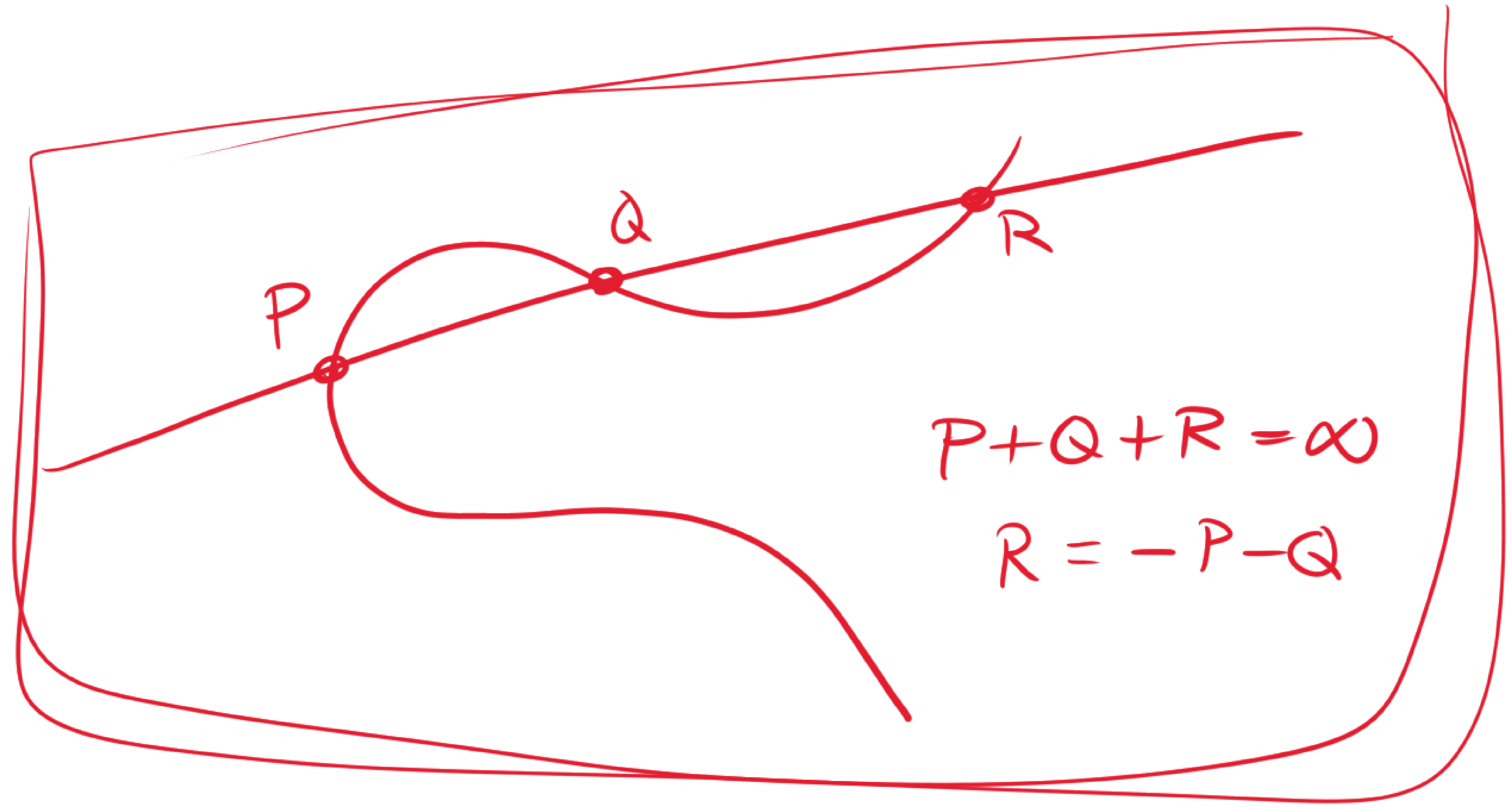
Ask Sage for $P \to 2P \to 3!P \to 4!P \to \ldots$

At $7!P$ it couldn't continue because it needed to invert 16002 mod n.

So take $\gcd(16002, n)$ for a nontrivial factor.


P
Q
R = -P-Q
P+Q


∞
R
-R


P
Q
R
P+Q+R = ∞
R = -P-Q