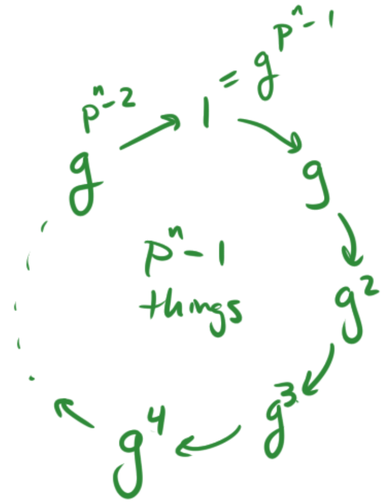
Discrete Log in Finite Fields

$(\mathbb{F}_{p^n})^*$ ← non-0 elements (unit group) — size $p^n - 1$.

Fact. $(\mathbb{F}_{p^n})^*$ has a multiplicative generator.

Call it g. This implies $g^{p^n-1} = 1$.



:o ☹

> **"Finite Field Euler Thm"** If $a \neq 0$, $a \in \mathbb{F}_{p^n}$, then
>
> $$a^{p^n-1} = 1.$$

Discrete Log Problem in $\mathbb{F}_{p^n}$

Given g, mult. generator in $\mathbb{F}_{p^n}^*$, and $h = g^x$, find x.

Same: • El Gamal, D-H Key Exchange.

• Birthday / Baby-Step-Giant-Step methods.

• Index Calculus is possible too!

$$g^x = \prod p_i^{a_i}$$

p_i: small polynomials not primes.

$$\Rightarrow x = \sum a_i L_g(p_i) \pmod{p^n - 1}$$

Different: • Runtime of Index Calculus is a bit better when p small, n large.

$O(e^{\sqrt[4]{\log n}})$ (faster) instead of $O(e^{\sqrt[3]{\log n}})$ (slower)

$\Rightarrow$ less secure.

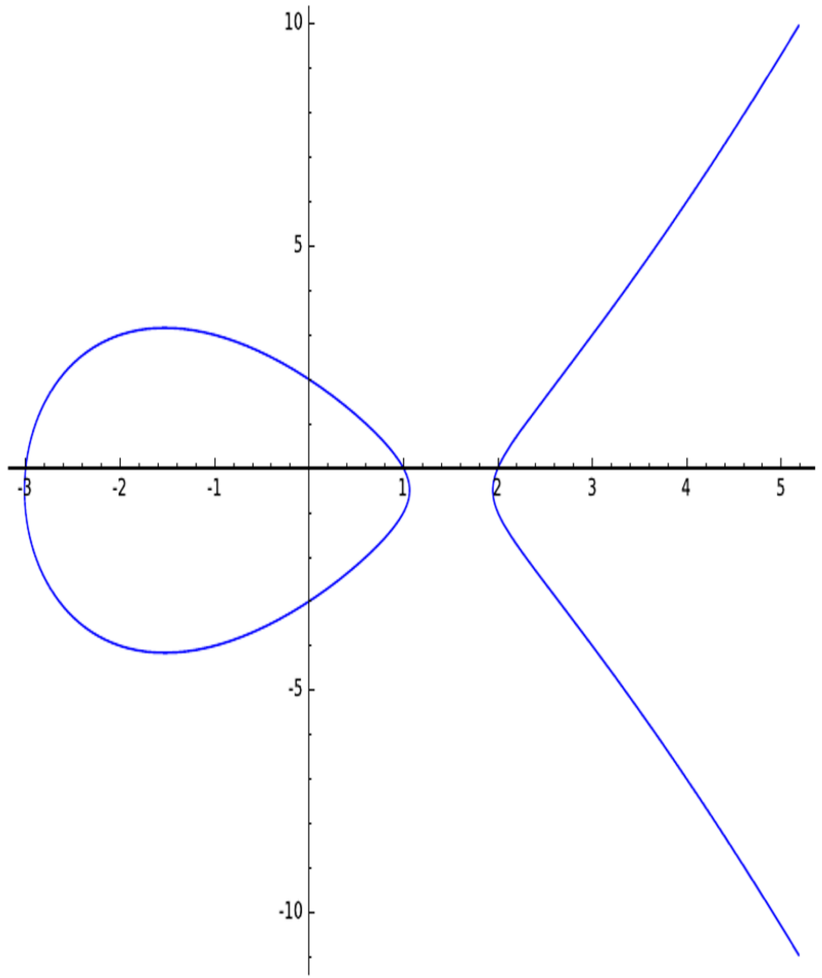
$\$$ Even faster for certain fields, particularly 2-power.

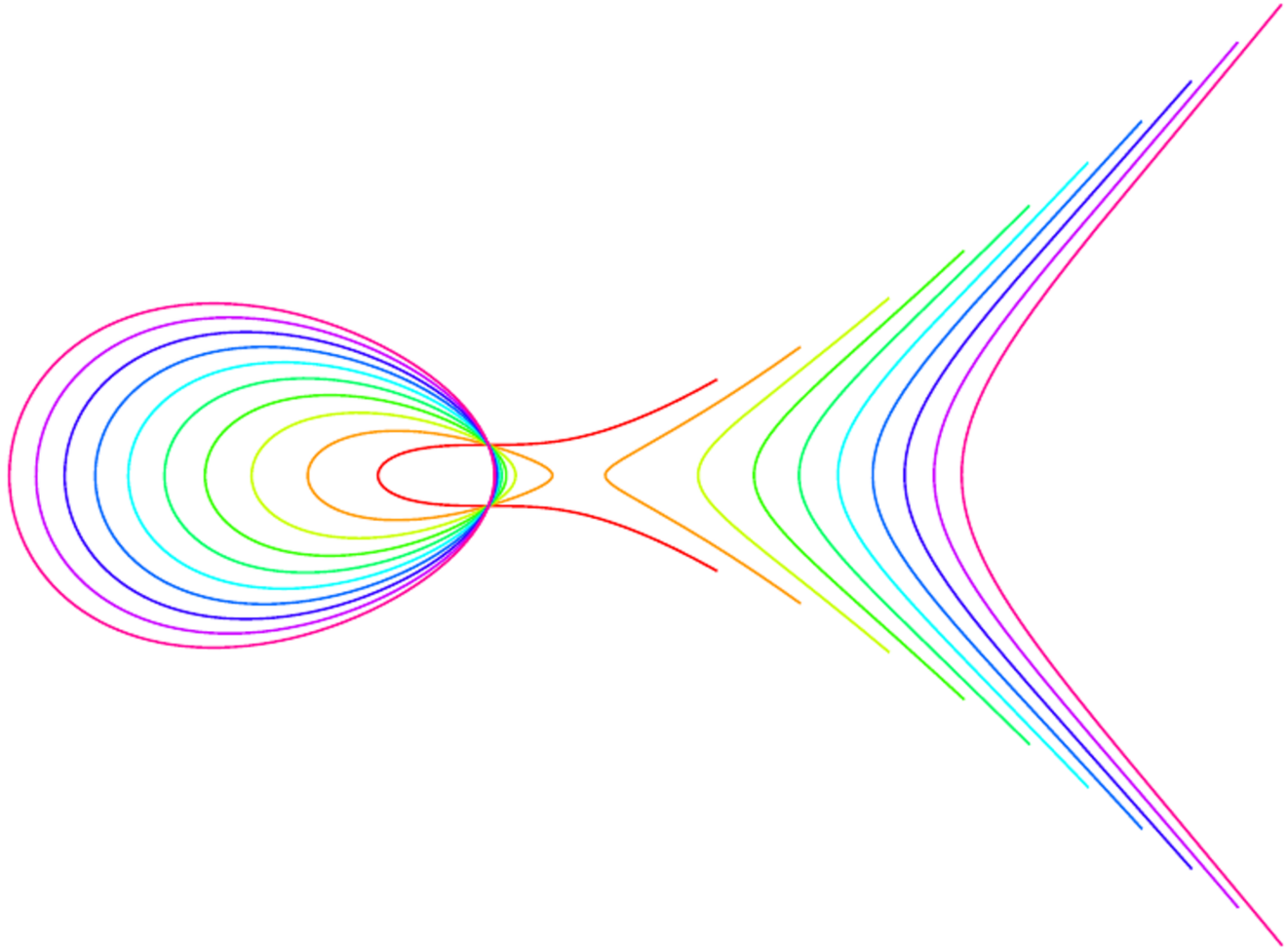
Records: 2014: $\mathbb{F}_{2^{9234}}$ (45 core-years)

2016: $\mathbb{F}_p$ $p = 768$ bits (6600 core-years)

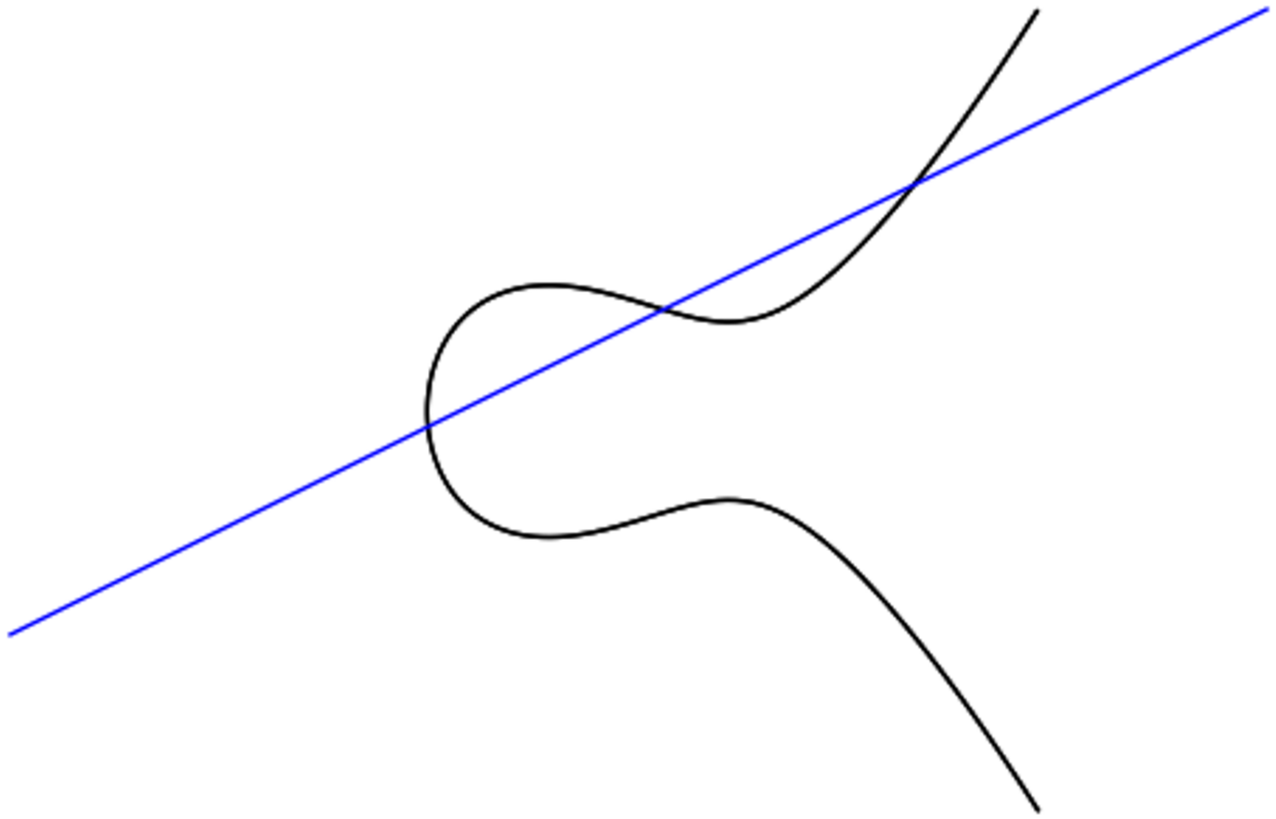
Elliptic Curves

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



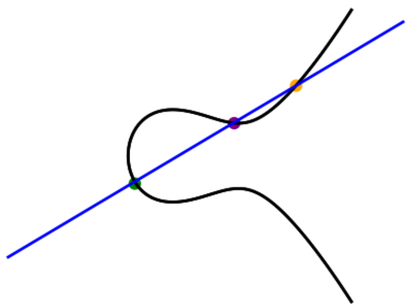


Since E is degree 3, a line intersects E at 3 places

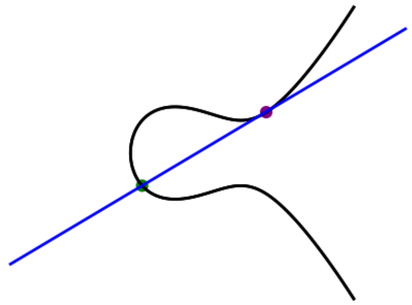


$$E: y^2 = x^3 + ax^2 + bx + c$$

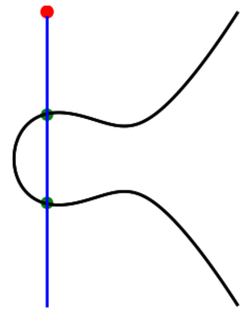
Since E is degree 3, a line intersects E at 3 places



3 real sol^{n}s

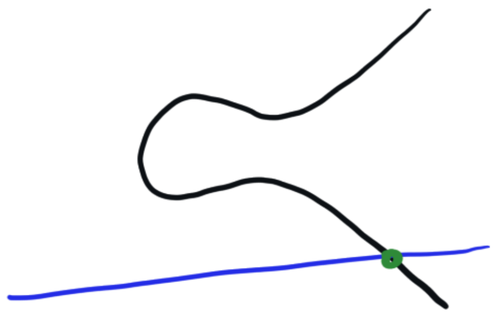


3 real sol^{n}s (1 repeated)

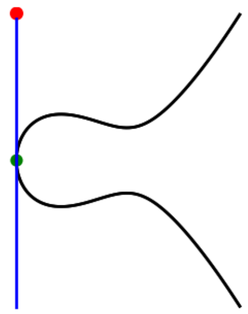


2 real sol^{n}s, 1 at ∞

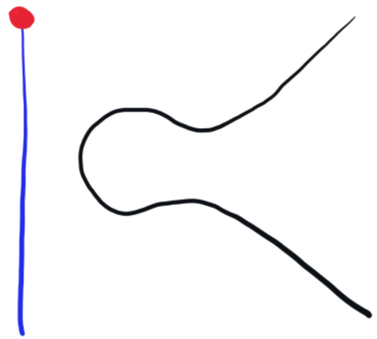
A line passes through ∞ if and only if it is vertical.



1 real sol^n,
2 complex sol^{n}s



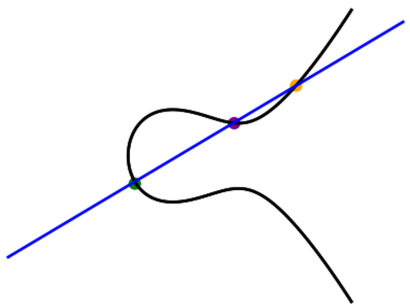
1 repeated real sol^n
1 at ∞



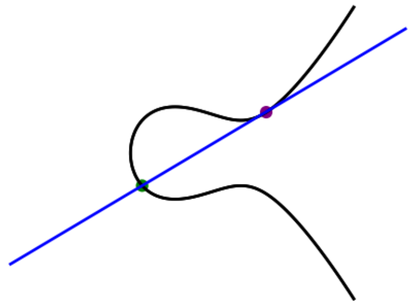
2 complex sol^{n}s,
1 at ∞

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

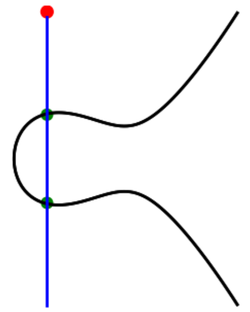
Since E is degree 3, a line intersects E at 3 places



3 real sol^{n}s

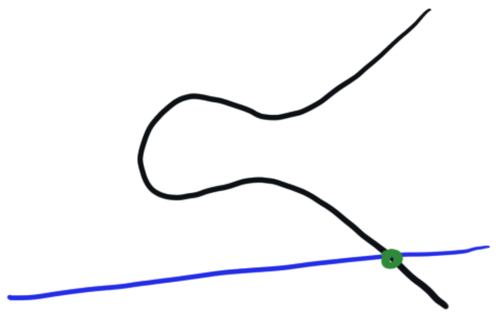


3 real sol^{n}s (1 repeated)

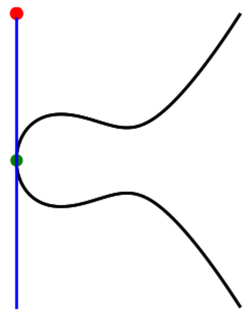


2 real sol^{n}s, 1 at ∞

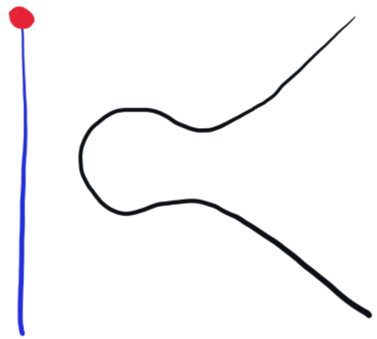
A line passes through ∞ if and only if it is vertical.



1 real sol^n,
2 complex sol^{n}s



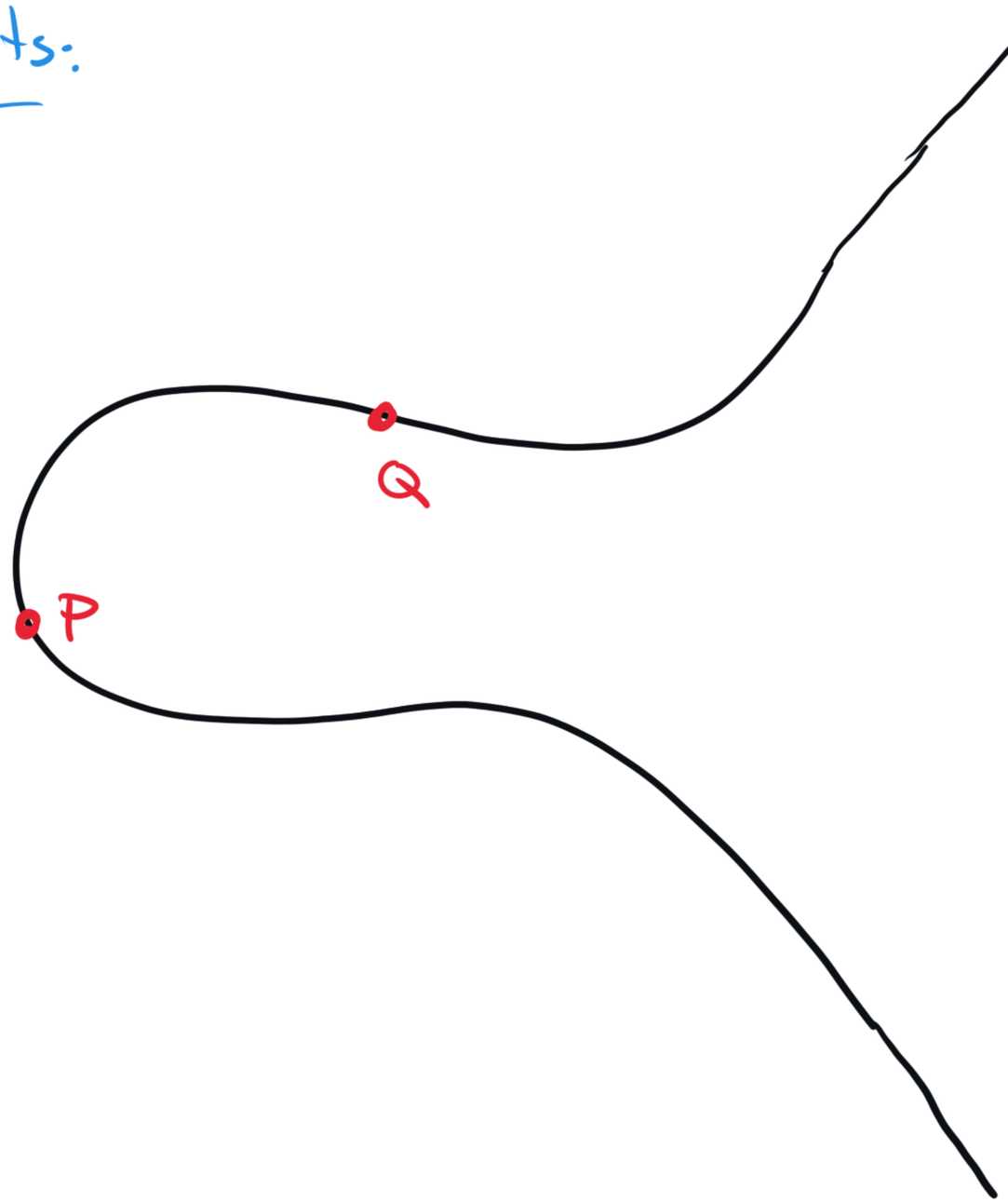
1 repeated real sol^n
1 at ∞



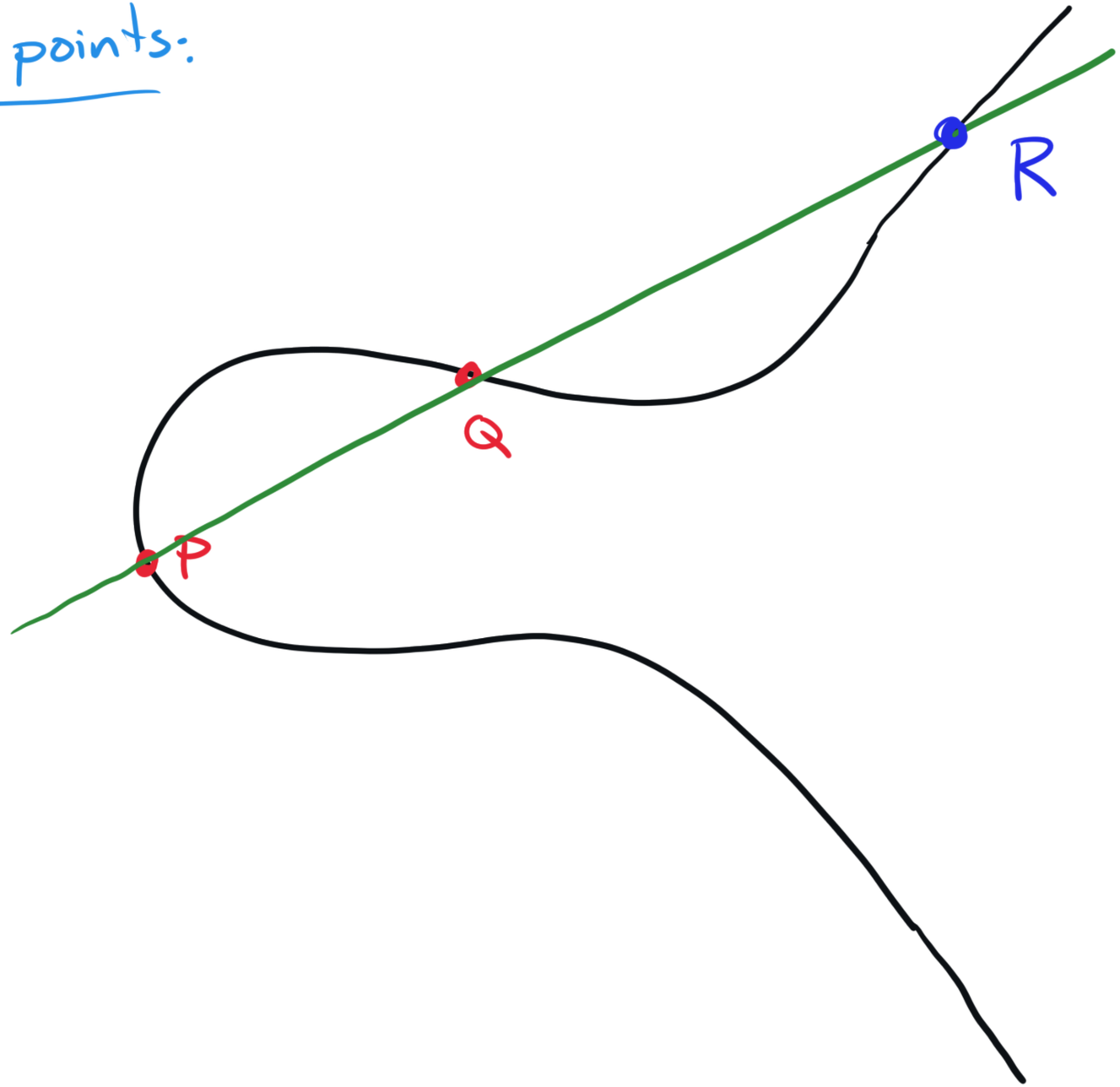
2 complex sol^{n}s,
1 at ∞

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

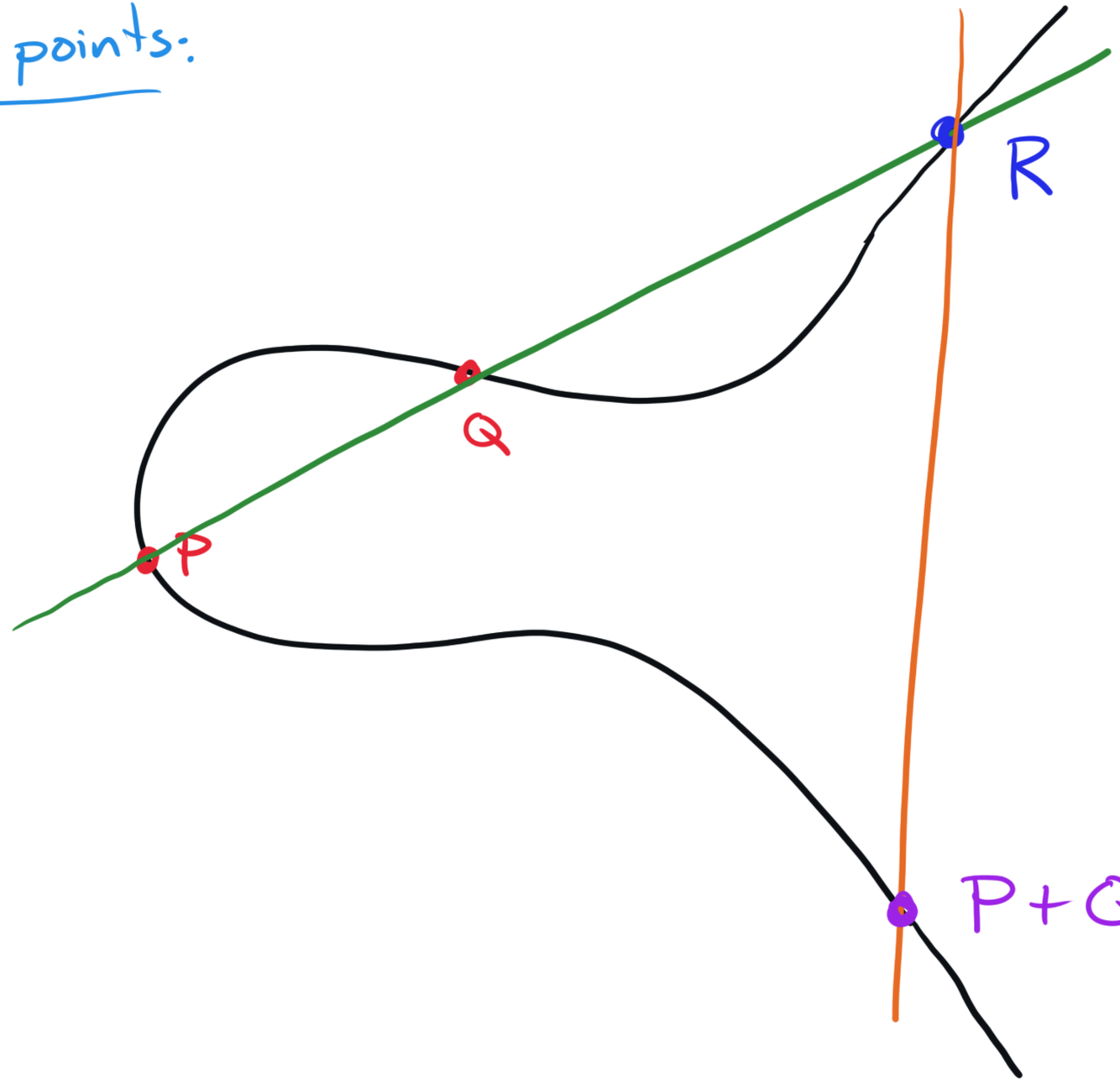
How to add points:



How to add points:



How to add points:



Rules:

$P+Q = Q+P$

$P+(Q+R) = (P+Q)+R$

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

For every P, there exists $-P$ s.t.

$P+(-P) = (P)+P = \infty$

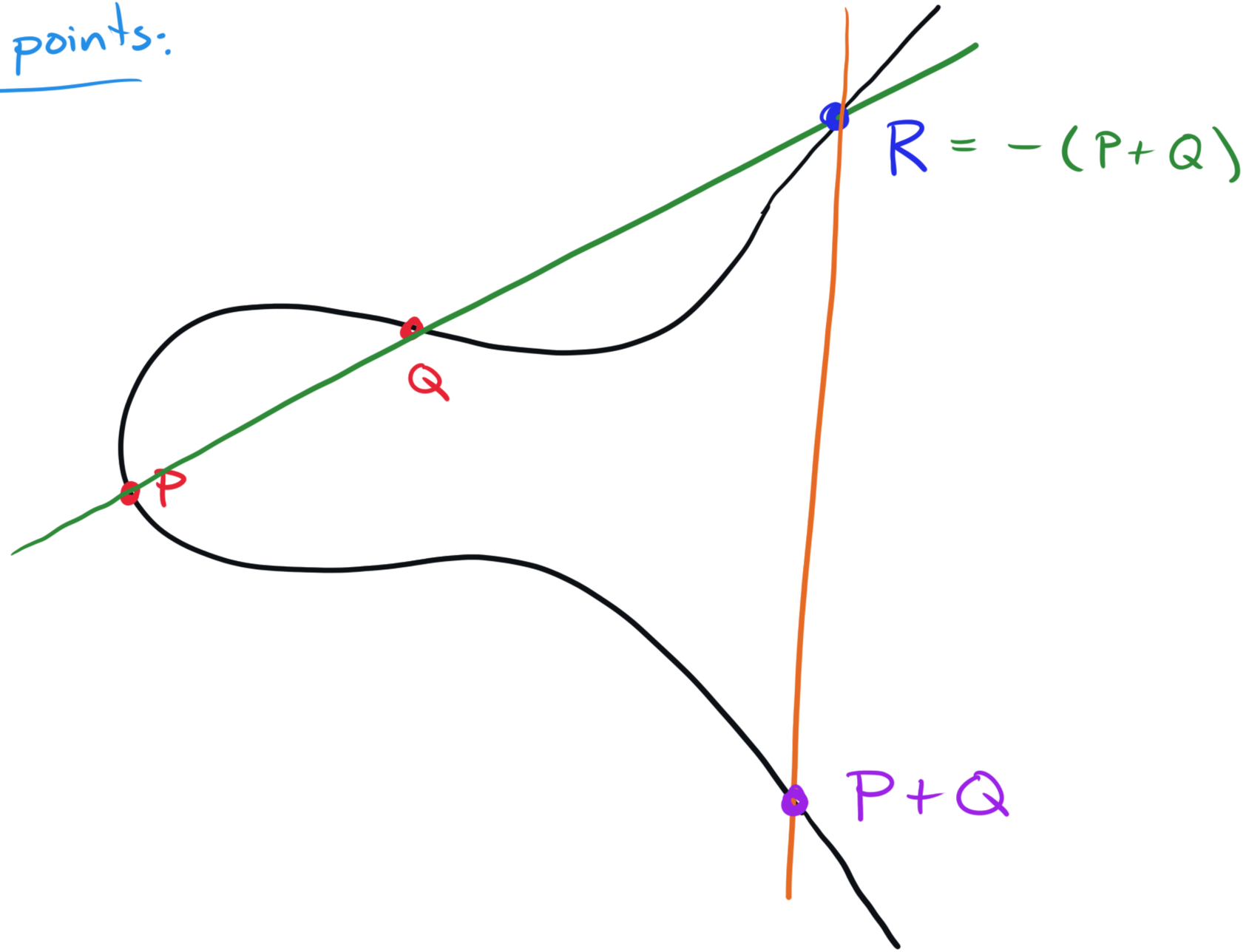
"an abelian group"

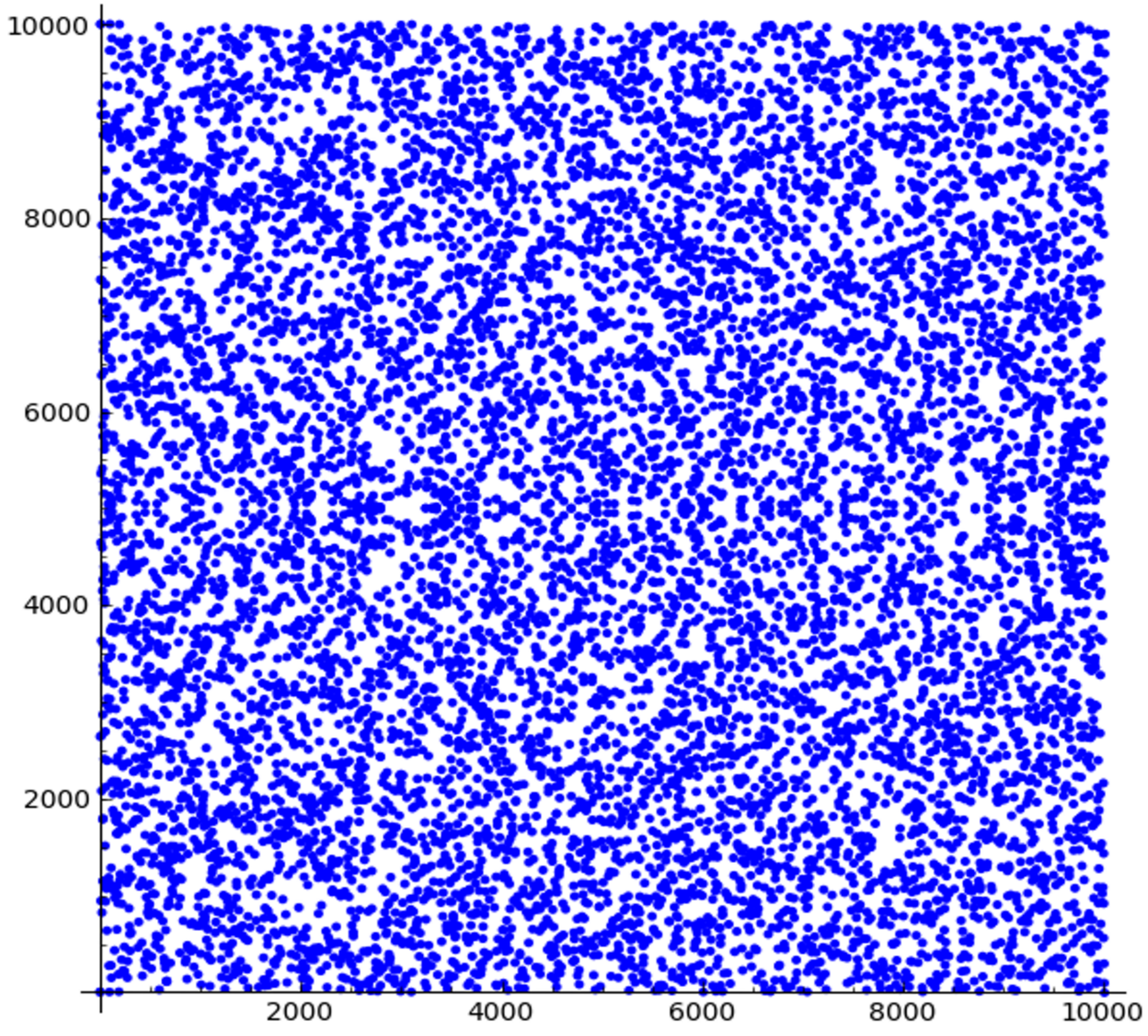
How to add points:

Key idea:

∞ = identity

collinear points add to ∞





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:

∞

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

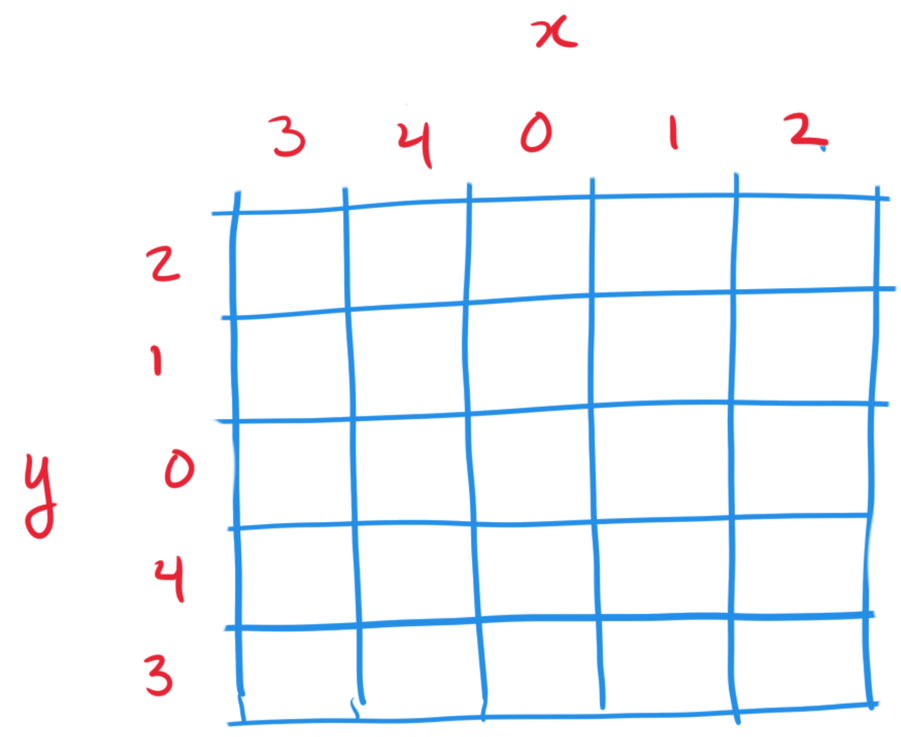
Example Mod 5

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

Points:

∞

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



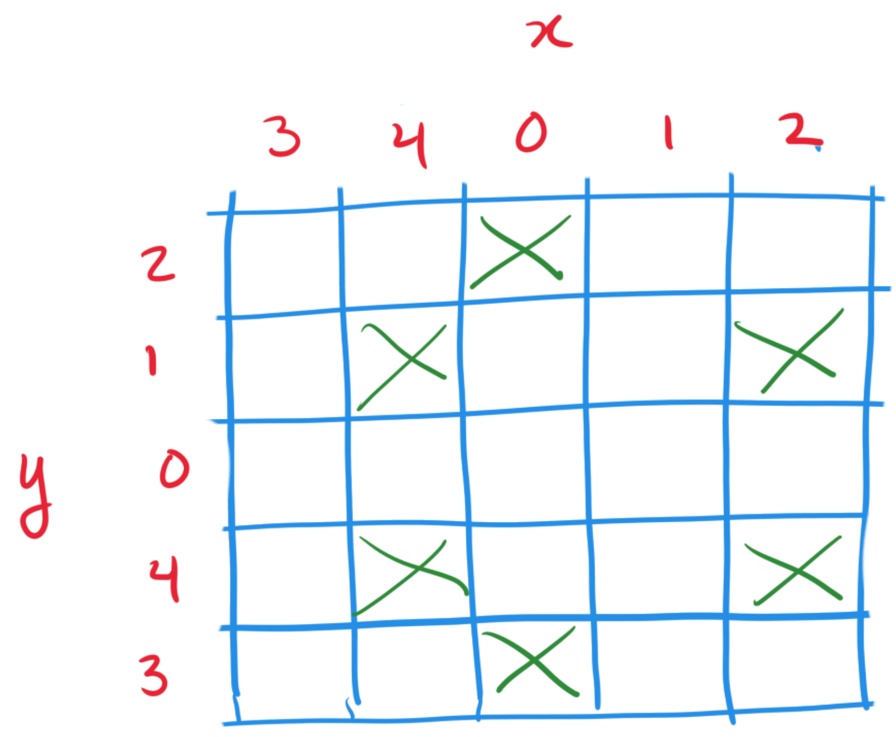
Example Mod 5

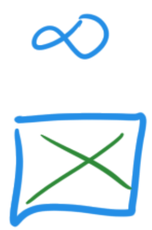
$$y^2 \equiv x^3 + 2x + 4 \pmod 5$$

Points:

∞

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





7 pants.

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 $(0,2)$ and $(2,4)$.

Example Mod 5

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

Points:

∞

$(0,2)$

$(0,3)$

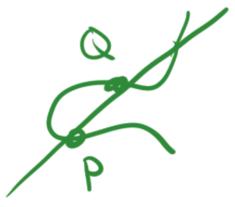
$(2,1)$

$(2,4)$

$(4,1)$

$(4,4)$

Task: Add $P = (0,2)$ and $Q = (2,4)$.



Line through P and Q:

$$y \equiv x + 2 \pmod 5$$

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

y-intercept $= 2$

Example Mod 5

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

Points:

∞

$(0,2)$

$(0,3)$

$(2,1)$

$(2,4)$

$(4,1)$

$(4,4)$

P Q

Task: Add $(0,2)$ and $(2,4)$.

Line through P and Q:

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

y-intercept $= 2$

$$y = x + 2$$

3rd intersection pt:

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

$$x^3 - x^2 - 2x = 0$$

Example Mod 5

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

Points:

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

P Q

Task: Add $(0,2)$ and $(2,4)$.

Line through P and Q:

$$y = x + 2$$

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

3rd intersection pt:

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

$$x^3 - x^2 - 2x = 0$$

$-(x^2$ coefficient$)$ = sum of roots

$$1 = 0 + 2 + x_R \Rightarrow x_R = -1 \equiv 4$$

Example Mod 5

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

Points:

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

P Q

Task: Add $(0,2)$ and $(2,4)$.

Line through P and Q:

$$y = x + 2$$

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

3rd intersection pt:

$$(x+2)^2 = x^3 + 2x + 4$$
$$x^3 - x^2 - 2x = 0$$

$-(x^2$ coefficient$)$
$=$ sum of roots

$$1 = 0 + 2 + x_R \implies x_R = -1 \equiv 4$$
$$y_R = x_R + 2 \equiv 1$$

$\boxed{(4,1)}$

Example Mod 5

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

$$(x-a)(x-b)(x-c) = x^3 + x^2(-a) + x^2(-b) + x^2(-c) + \cdots$$

Points:

∞

$(0,2)$

$(0,3)$

$(2,1)$

$(2,4)$

$(4,1)$

$(4,4)$

P Q

Task: Add $(0,2)$ and $(2,4)$.

Line through P and Q:

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

$$\text{y-intercept} = 2$$

$$y = x + 2$$

3rd intersection pt:

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

$$x^3 - x^2 - 2x = 0$$

(roots = x coords of P, Q, R.)

$-(-1)$ = sum of roots

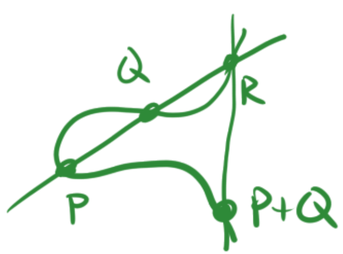
$-(x^2 \text{ coefficient})$ = sum of roots

$$1 = 0 + 2 + x_R \Rightarrow x_R = -1 \equiv 4$$

$= \text{coeff of } x^2 \text{ term}$

$$y_R = x_R + 2 \equiv 1$$

$(4,1)$



Reflect in x-axis:

$$P + Q = (4,4)$$