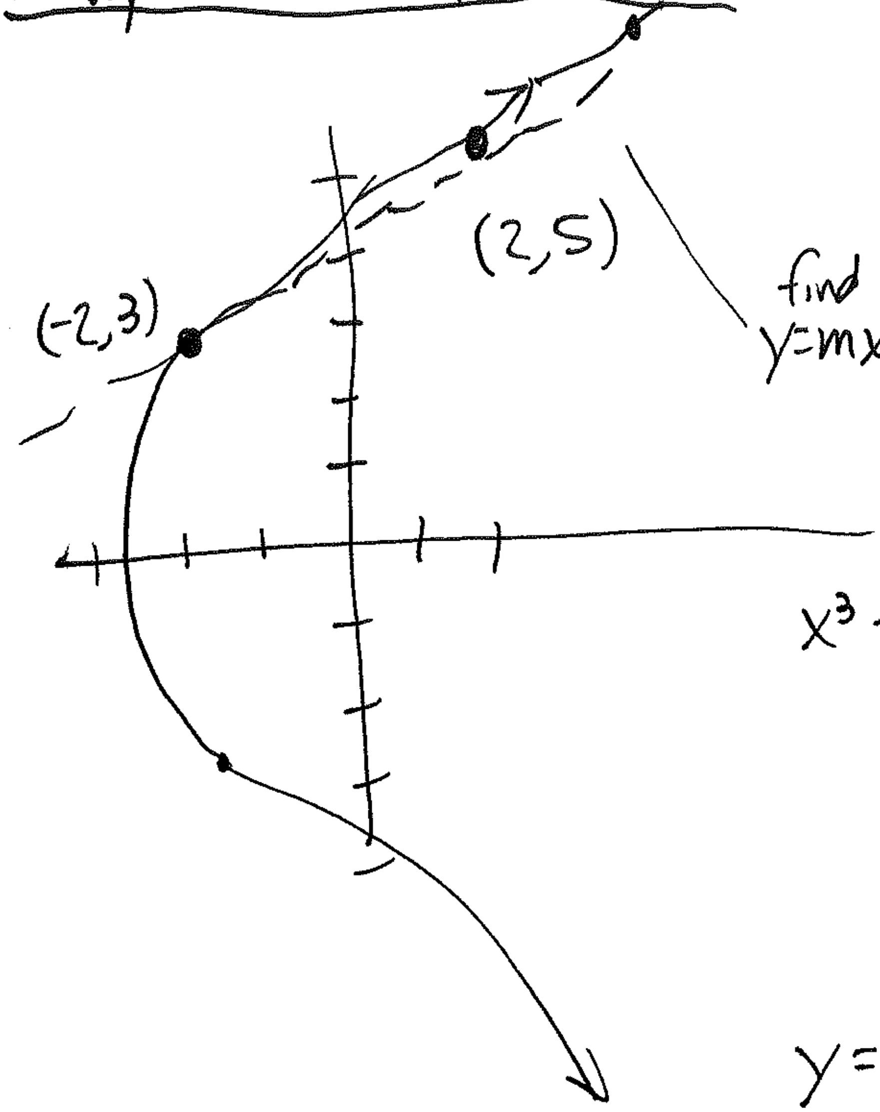
Today: More elliptic curves



$$y^2 = x^3 + 17$$

find $y = mx + b$ plug to here, solve for x

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

negative sum of roots

$$y = \frac{1}{2}x + 4$$

$$\left(\frac{1}{2}x + 4\right)^2 = x^3 + 17$$

$$\frac{1}{4}x^2 + 4x + 16 = x^3 + 17$$

$$x^3 - \frac{1}{4}x^2 - 4x + 1 = 0$$

$\left.\begin{array}{l} x = -2 \\ x = 2 \end{array}\right)$ already knew

$x = 1/4$

$$y=\frac{1}{2}x+4=\frac{1}{2}\left(\frac{1}{4}\right)+4=\frac{33}{8}$$

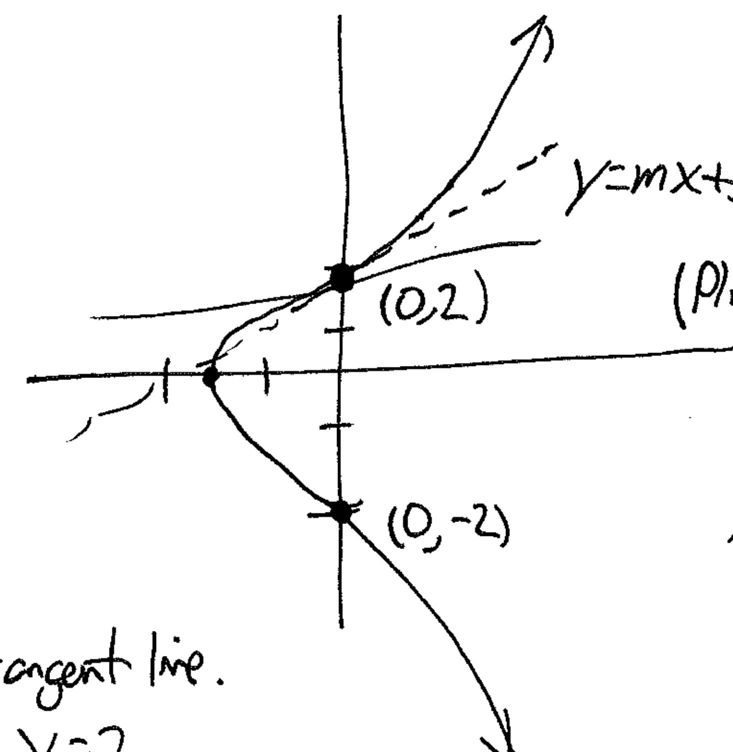
Third point: $\left(\frac{1}{4}, \frac{33}{8}\right)$

"Sum" of solutions:

$$(-2,3)+(2,5)=\left(\frac{1}{4}, -\frac{33}{8}\right)$$

Another: $y^2=x^3+4$

$(0,2)+(0,2)$



$y=mx+b$ tangent line.

(Plug in to cubic eqn, find third point)

$$2y\frac{dy}{dx}=3x^2$$

tangent line.

$y=2$

$$\frac{dy}{dx}=\frac{3x^2}{2y}=0.$$

plug in: $y^2=x^3+4$

$$4=x^3+4 \longrightarrow x^3=0$$

third point is also $(0,2)$.

$(0,2)+(0,2)=(0,-2)$.

what's $(0,2)+(0,-2)$?

line between points is: vertical.

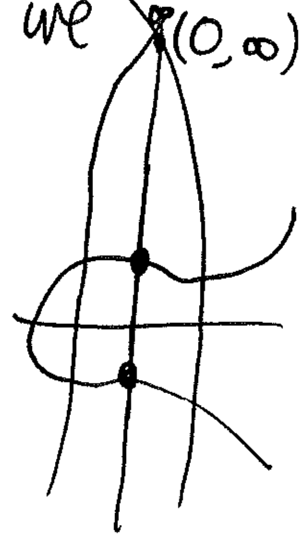
Where does vertical line hit $y^2=x^3+4$?

only hits it at $(0,2)$ & $(0,-2)$!!

Solution: Add a point at infinity, denoted "∞".

← pretend it's another solution

To make addition of points always work, we declare that $(x,y)+(x,-y)=\infty$.



We also declare

$(x,y)+\infty=(x,y)$

Def A group is a set G with a binary operation $\times$ satisfying

two elements of G as input, one element of G as output.

- associative:

  $(x \times y) \times z = x \times (y \times z)$

- identity element:

  there's some $e \in G$ where $x \times e = x$, $e \times x = x$

- inverse:

  for any $x \in G$, there's a y in the group so $x \times y = e$.

Examples $G = \mathbb{R}^* = \{$all real numbers other than $0\}$

$\times$ is normal multiplication.

$e = 1$

(but $\mathbb{Z}^*$ wouldn't work; no inverses)

One more group:

G = the rational points on an elliptic curve E, plus ∞.

$\times$ = the addition operation we defined.

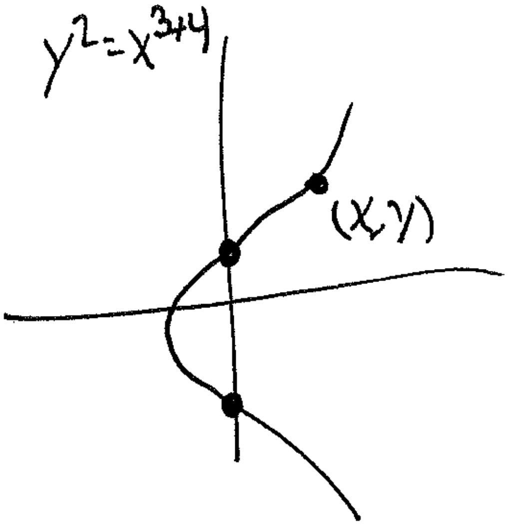
This is a group! (Trust me, it's associative.)

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

This is why we do the weird flip-the-y-coordinate trick.

What's identity?

∞



$(x,y)+\infty = (x,y)$.

What's inverse of $(0,2)$?

$(0,-2)$

$(0,2)+(0,-2) = \infty$.

$G = \mathbb{Z}$ (or $\mathbb{R}$, or $\mathbb{C}$)

$\times$ is addition.

$e = 0$

G = integers from 0 to $n-1$.

add

Operation = addition mod n (add them and take remainder when divided by n)

$\boxed{\begin{array}{l} \text{e.g if } n=10 \\ 6+7=3 \end{array}}$

$e = 0$

(inverse of 6 if $n=10$: 4)

G = 2×2 matrices with determinant not 0

$\times$ = multiplication.

$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

ABELIAN

"non-abelian group" since not commutative.

weird feature: $X \times Y \neq Y \times X$ in general

For cryptography, we look at mod-n solutions to elliptic curve eqns $y^2 = x^3 + ax + b$

(only has to work mod n)

How to solve $3x \equiv 2 \mod 5$?

(x must be integer)

$x = 4$ works.

$x^2 \equiv 2 \mod 7$

$x = 3$ or 4 (aka -3)

$x^2 \equiv 3 \mod 7$

no solutions!

x	$x^2 \mod 7$
0	0
1	1
2	4
3	2
4	2
5	4
6	1

Elliptic curves mod n: use the same trick for finding new solutions.

$$y^2 = x^3 - x - 1 \mod 5$$

$(x_1, y_1) = (4, 3)$

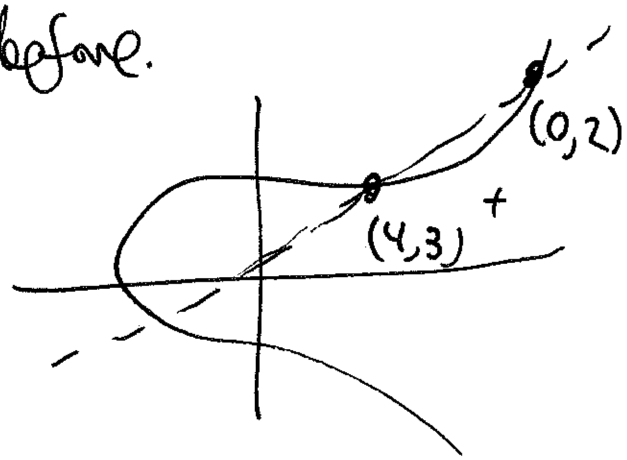
$(x_2, y_2) = (0, 2)$ are solutions.

$$3^2 \stackrel{?}{=} 4^3 - 4 - 1 \mod 5$$

$$9 \stackrel{?}{=} 64 - 4 - 1 \mod 5$$

$$9 \equiv 59 \mod 5 \checkmark$$

use these two to generate a new solution, as before.



$4 \cdot 4 \equiv 1 \bmod 5$

so "$\frac{1}{4}$" mod 5 is just 4.

line $=$ $y = \frac{1}{4}x + 2$

$$y \overset{\text{mod } 5}{=} 4x+2$$

$$(4x+2)^2 = x^3 - x - 1 \bmod 5$$

$$16x^2 + 16x + 4 = x^3 - x - 1 \bmod 5$$

$$x^3 - 16x^2 - 17x - 5 \equiv 0 \bmod 5$$

$$x^3 + 4x^2 + 3x \equiv 0 \bmod 5.$$

Know two roots: $x = 0$, $x = 4$

the other root is: $x = -8$ which mod 5 is $x = 2$

then $y = 4x + 2 = 10 = 0 \bmod 5$

$(2, 0)$ is our third pt.

$y^2 = x^3 - x - 1 \bmod 5?$

How many solutions are there to

$$y^2 = x^3 + ax + b \mod p?$$

At most p^2, but in fact:

Hasse bound: number is

$$p+1-2\sqrt{p} < \downarrow < p+1+2\sqrt{p}$$