Last Time:

Def: A group is a set G with a binary operation $*$ which has three properties

(1) $*$ is associative

(2) $*$ has an identity in G (usually called e)

(3) $*$ every element in G has an inverse in G.

Aside: If G just satisfies (1), it's called a semigroup

If G satisfies (1) and (2), it's called a monoid

If G satisfies (1), (2), and (3) and $*$ is commutative, it's called an Abelian group

A group G where $*$ is not commutative is called non-Abelian.

Modular arithmatic:

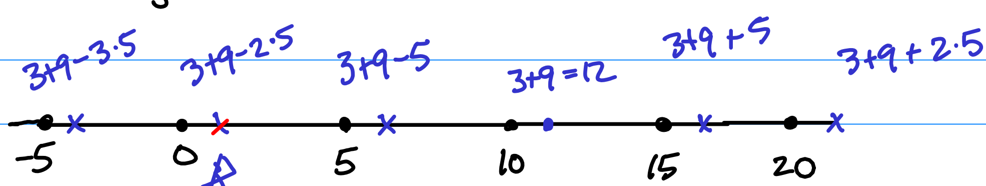
If $a, b \in \mathbb{R}$ and $t \in \mathbb{R}$ with $t > 0$,

$a +_t b$ = unique element in $[0, t)$ satisfying

$a + b = (a +_t b) + kt$ for some integer k

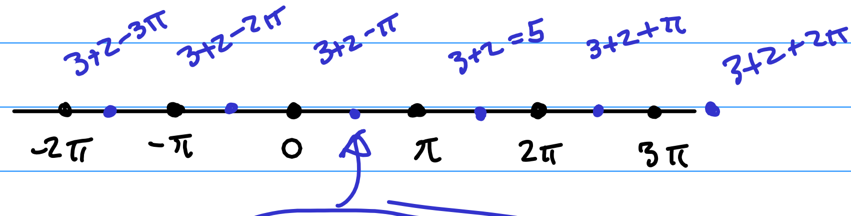
$a +_t b = a + b - kt$

Ex: $3 +_5 9 = ?$



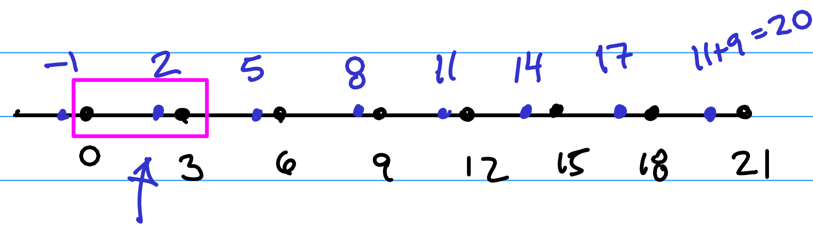
$3 +_5 9 = 2$.

Ex: $3 +_\pi 2 = ??$



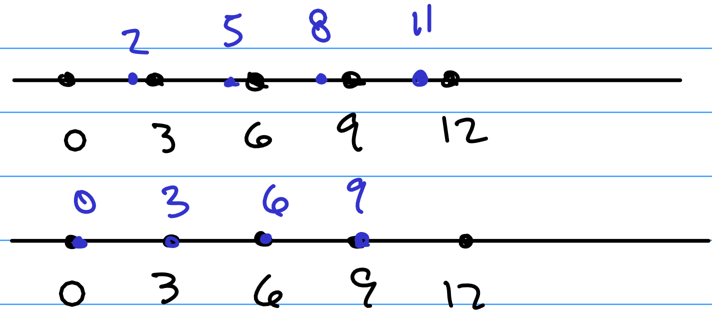
$5 - \pi = 3 +_\pi 2$

Ex: $11 +_3 9 = ?$ Try it out!!



$11 +_3 9 = 2$

Alternative method:



11 is equivalent to 2 modulo 3

9 is equivalent to 0 modulo 3.

$11 +_3 9 = 2 +_3 0 = 2$

Theorem: The set $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ with binary operation $+_n$ is an Abelian group.

Proof:

Associativity?

$a, b, c \in \mathbb{Z}_n$

$a +_n b = a + b - kn$ for some $k \in \mathbb{Z}$
$b +_n c = b + c - jn$ for some $j \in \mathbb{Z}$.

$\underline{(a +_n b) +_n c} = (a + b - kn) +_n c$

$= a + b - kn + c - \tilde{k}n$ for some $\tilde{k} \in \mathbb{Z}$
$= a + b + c - (k + \tilde{k})n \in \{0, 1, 2, \dots, n-1\}$

$\underline{a +_n (b +_n c)} = a +_n (b + c - jn)$
$= a + b + c - jn - \tilde{j}n$ for some $\tilde{j} \in \mathbb{Z}$
$= a + b + c - (j + \tilde{j})n \in \{0, 1, 2, \dots, n-1\}$

There's a <u>unique</u> integer $l \in \mathbb{Z}$ with
$a + b + c - ln \in [0, n)$

$\therefore j + j = k + \tilde{k}$

Thus $a + b + c - (k + \tilde{k})n = a + b + c - (j + \tilde{j})n$
$(a +_n b) +_n c = a +_n (b +_n c)$.

Thus $+_n$ is associative!

Identity? $\left.\begin{aligned} a +_n 0 &= a \\ 0 +_n a &= a \end{aligned}\right\}$ 0 is ~~an~~ the identity

Inverses? $0 +_n 0 = 0$
$a +_n (n - a) = 0$

$a +_n (n - a) = a + (n - a) - kn$
$= n - kn \in [0, n) \quad \therefore k = 1$
$= 0$.

Abelian?

NTS $a +_n b = b +_n a$ for all $a, b \in \mathbb{Z}_n$.

Defined using $+$, which is commutative!
So of course $+_n$ is still commutative $\square$

Complex Numbers: A complex number is something of the form $a+ib$, $a, b \in \mathbb{R}$.

Addition: $(a+ib)+(c+id) = (a+c) + i(b+d)$

Multiply: $(a+ib)(c+id) = (ac-bd) + i(bc+ad)$

Key: $i^2 = -1 \rightsquigarrow \sqrt{-1} = i$

$$\begin{aligned}(2+i3)(1+i) &= 2\cdot 1 + (i3)\cdot 1 + 2\cdot i + (i3)i \\ &= 2 + 3i + 2i + 3i^2 \\ &= 2 + 3i + 2i - 3 \\ &= -1 + 5i\end{aligned}$$

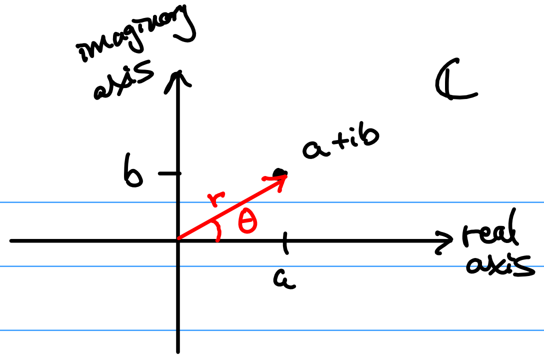
Subtract: Obvious
Divide: Complicated - omitted for now!

Def: $e^{i\theta} = \cos\theta + i\sin\theta$ Euler's Formula

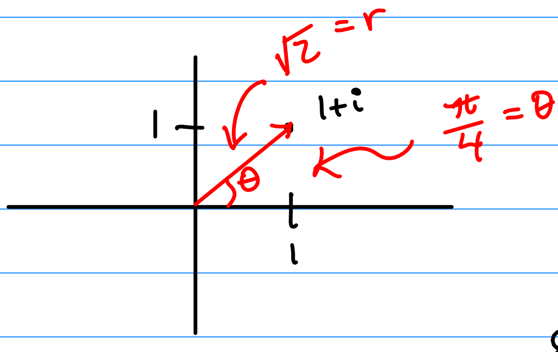
Using Euler's formula, we can write any complex # in its polar form $re^{i\theta}$, $r > 0$, $\theta \in [0, 2\pi)$.

Ex: $1+i = re^{i\theta}$ for some r, θ ...

$a+ib = re^{i\theta} \rightsquigarrow r = \sqrt{a^2+b^2}$



$$a+ib = re^{i\theta}$$



$$1+i = \sqrt{2}\, e^{i\pi/4}$$

<u>Q</u>: What is $(1+i)^8 = \left(\sqrt{2}\, e^{i\pi/4}\right)^8$

$$= (\sqrt{2})^8 \left(e^{i\pi/4}\right)^8$$

$$= 16 \quad e^{(i\pi/4)\cdot 8}$$

$$= 16 \quad e^{i2\pi}$$

$$= 16\left(\cos(2\pi) + i\sin(2\pi)\right)$$

$$= 16\,(\,1 + i\cdot 0\,)$$

$$= 16\,(1) \qquad = 16$$

<u>Roots of Unity</u>:

$$U_n = \{ z \in \mathbb{C} \mid z^n = 1 \}$$

<u>Fundamental Theorem of Algebra</u>: A poly of degree n has exactly n roots, counting multiplicity.

$\therefore$ U_n should have n elements! (It does!!)

$$z^n = 1$$

Secret sauce = use polar form!

$$\left(re^{i\theta}\right)^n = 1 \qquad \Rightarrow \qquad r = 1$$

$$e^{in\theta} = 1$$

$$\cos(n\theta) + i\sin(n\theta) = 1$$

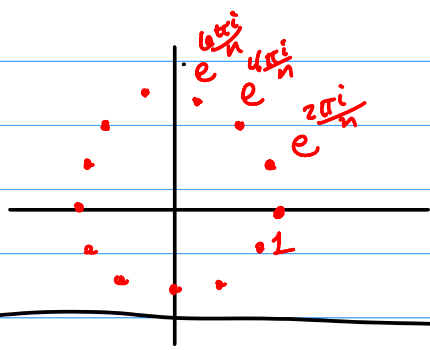
$$\therefore \cos(n\theta) = 1 \text{ and } \sin(n\theta) = 0$$

$$n\theta = 2\pi \cdot k \quad , \; k \in \mathbb{Z}$$

$$\theta = \frac{2\pi \cdot k}{n}$$

$$\boxed{e^{i\frac{2\pi k}{n}} \text{ is an } n^{th} \text{ root of unity!}}$$

REPEATS $e^{2\pi i} = 1$



$$z^n = 1$$

$$\boxed{U_n = \left\{ e^{\frac{2\pi i k}{n}} \;\middle|\; k = 0, 1, 2, \ldots, n-1 \right\}}$$

This is a group using complex multiplication!