Last time: $\mathbb{Z}_n$

saw: for $a \in \mathbb{Z}$, get $\bar{a} \in \mathbb{Z}_n$

$\bar{a}$ is a unit in $\mathbb{Z}_n$ iff $\gcd(a, n) = 1$

when we solved $49x \equiv 4 \pmod{999}$

worked... found we should mult. by 367

bec. $367 \cdot 49 \equiv 1 \pmod{999}$

in the ring $\mathbb{Z}_{999}$,

think of "multiply by 367"

as the same thing as "divide by 49"

caveat: can't divide by just anything:

$99x \equiv 4 \pmod{999}$ has no sol.
bec. $\gcd(99, 999) = 9$ doesn't divide 4.

OTOH, $99x = 9 \pmod{999}$ has many sols.

issue: $\overline{99} \in \mathbb{Z}_{999}$ is not a unit
it's a zero-divisor

in $\mathbb{Z}_p$, when p is prime, never have this issue:
$\forall a \quad 0 < a < p$, have $\gcd(a, p) = 1$
so everything in $\mathbb{Z}_p$ is a unit. $\mathbb{Z}_p$ is a field.

Rational Numbers

$\mathbb{Q}$ = set of rational numbers.
("quotients")

$\mathbb{Z}$ = Zahlen = numbers

low-brow model:

$$\mathbb{Q} = \left\{ \text{symbols } \frac{a}{b} \;\middle|\; a \in \mathbb{Z},\ b \in \mathbb{Z}_{>0},\ \gcd(a,b) = 1 \right\}$$

"fractions in lowest terms"

add: $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$ and then cancel common factors.

$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ and then cancel...

$$\frac{3}{4} + \frac{1}{6} = \left(\frac{18 + 4}{24} = \frac{22}{24} \right) = \frac{11}{12}$$

check: it's a field.

kind of a pain:

$$\left(\frac{a}{b} + \frac{c}{d} \right) + \frac{e}{f} = \frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f} \right)$$

add, cancel, add, cancel

add, cancel, add, cancel...

high-brow model:

$\mathbb{Q} = \{$ equivalence classes of symbols $\frac{a}{b}$:

$a, b \in \mathbb{Z} \qquad b \neq 0$

declare $\frac{a}{b}$ equivalent to $\frac{a'}{b'}$ if

$ab' = a'b.$ $\}$

example of such an equivalence class:

$\{ \frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \frac{4}{8}, \frac{-1}{-2}, \frac{-2}{-4}, \text{etc} \}$

define $\frac{a}{b} + \frac{c}{d}$ and $\frac{a}{b} \cdot \frac{c}{d}$ by same fmla.

need to check that it's well-defined:

if $\frac{a}{b} = \frac{a'}{b'}$ ($ab' = a'b$) and $\frac{c}{d} = \frac{c'}{d'}$ ($cd' = c'd$)

then $\frac{a}{b} + \frac{c}{d} = \frac{a'}{b'} + \frac{c'}{d'}$ and sim with multiplication.

$\frac{ad+bc}{bd} \qquad \frac{a'd' + b'c'}{b'd'}$

want: $(ad+bc)b'd' \overset{?}{=} (a'd'+b'c')bd$

$$\begin{aligned} (ad+bc)b'd' &= adb'd' + bcb'd' \\ &= a'dbd' + bc'b'd \end{aligned}$$

$(a'd'+b'c')bd = a'd'bd + b'c'bd$ — same!

mult. is similar but easier.

Ordered Fields

a field F ... (think $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ ...)

an *ordering* of F is

a subset $F^+ \subset F$ such that

- $\forall a \in F$, exactly one of these holds: $\begin{cases} a \in F^+ \\ -a \in F^+ \\ a = 0 \end{cases}$
- $\forall a, b \in F^+$, $a+b$ and $a \cdot b \in F^+$

a field might admit several orderings, or no ordering...

saw that $\mathbb{Z}_3$ can't be ordered bec. $1+1+1=0$

on $\mathbb{Q}$, standard ordering:

$$\mathbb{Q}^+ = \left\{ \frac{a}{b} \;\middle|\; a>0 \text{ and } b>0 \text{ OR } a<0 \text{ and } b<0 \right\}$$