Modular numbers

- A modular number $[a]_m$ is an equivalence class under $\equiv_m$

  $$\mathbb{Z}_m := \mathbb{Z}/(\equiv_m) = \{[0]_m, [1]_m, \ldots, [m-1]_m\}$$

- We defined $[a]_m + [b]_m := [a + b]_m$

- We defined $[a]_m[b]_m := [ab]_m$

- We checked that + and \cdot are well-defined

- We tried to define $[a]^{[b]} := [a^b]$ but it was not well-defined

In Java: can redefine .equals()

\[
\begin{bmatrix}
"2:00 PM"
\end{bmatrix} = \begin{bmatrix}
"14:00"
\end{bmatrix}
\]

If you define equals you must redefine "hashCode"

need to ensure if $a.equals(b)$ then $a.hashCode()$ equals $b$.hashCode

\{ \text{hashCode should be "well-defined"} \}

and other methods!
Solve for $x \in \mathbb{Z}$:

\[ 2x = 5 \]

- Find $2 \cdot \frac{1}{2} \pmod{8}$
- $2 \cdot 4 \equiv 0 \pmod{8}$
- No inverse of $2$, $\pmod{8}$.

**Def**: If $x$ has a multiplicative inverse, $x$ is called a "unit".
Units

- **Defn**: A *(multiplicative)* inverse of \( x \) is an element \( y \) with \( xy = 1 \)
- **Defn**: A *unit* is an element with a multiplicative inverse
- **Defn**: \( \mathbb{Z}_m^* \) is the set of units of \( \mathbb{Z}_m \)

**Question**: What are the units of \( \mathbb{Z}_8 \) of \( \mathbb{Q} \) of \( \mathbb{Z}_7 \) of \( \mathbb{Z}_8 \)?

\[
\mathbb{Z}_8^* = \{ [1], [3], [5], [7] \}
\]

\[
\mathbb{Z}_7^* = \{ [1], [3], [5], [6] \}
\]

\[
\phi(8) = 4
\]

\[
\phi(7) = 6
\]

**Defn**: The totient of \( m \) (written \( \phi(m) \))

is the number of units of \( \mathbb{Z}_m \).

(i.e. the size of \( \mathbb{Z}_m^* \))
How can we find a unit?

Claim: \([a]_m\) is a unit iff \(\gcd(a, m) = 1\)

Fact (proved in discussion): There exist Bézout coefficients \(s\) and \(t\) satisfying

\[\gcd(a, b) = sa + tb\]

Proof of claim:

Assume \(\gcd(a, m) = 1\).

Then \(-\exists s, t\) with \(1 = sa + tm\), by

Then \([1] = [sa + tm] = [s][a] + [t][m] = [0]\) \((\text{mod } m)\).

\[= [s][a] + [0] = [s][a].\]

So \([s]\) is an inverse of \([a]\), so \([a]\) is a unit.
Computing $\varphi(m)$

- $\varphi(n)$ is the number of units mod $m$.
- $[a]_m$ is a unit if $\gcd(a,m) = 1$.
  i.e. $a \in \mathbb{Z}_m$ have no factors in common.

Q: If $p$ is prime (only factors are 1 and $p$)

What is $\varphi(p)$?

$\mathbb{Z}_p^* := \{ [1], [2], [3], \ldots, [p-1] \}$

$\varphi(p) = p-1$, if $p$ is prime.