Congruences: arithmetic (mod n)

Def: \( a \equiv b \pmod{n} \) iff \( n \mid (a - b) \)

example: \( 30 \equiv 12 \pmod{9} \)

since

9 divides \((30 - 12)\)

Congruence mod n

\begin{align*}
\text{Remainder Lemma} \\
a \equiv b \pmod{n} \\
\text{iff} \\
\text{rem}(a,n) = \text{rem}(b,n)
\end{align*}

example: \( 30 \equiv 12 \pmod{9} \)

since

\( \text{rem}(30,9) = 3 = \text{rem}(12,9) \)
Remainder Lemma

\[ a \equiv b \pmod{n} \]

iff

\[ \text{rem}(a,n) = \text{rem}(b,n) \]

abbreviate: \( r_{b,n} \)

proof: \((\iff)\)

\[
\begin{align*}
a &= q_a n + r_{a,n} \\
b &= q_b n + r_{b,n}
\end{align*}
\]

conversely,

\( n | (a-b) \) means

\[ n | ((q_a-q_b)n + (r_{a,n}-r_{b,n})) \]

so

\( n | (a-b) \) \IMPLIES \( r_{a,n} = r_{b,n} \)

proof: \((\iff)\)

\[
\begin{align*}
a &= q_a n + r_{a,n} \\
b &= q_b n + r_{b,n}
\end{align*}
\]

if rem's are =, then

\[ a-b=(q_a-q_b)n \]

so \( n | (a-b) \)
**Remainder Lemma**

\[ a \equiv b \pmod{n} \]

iff

\[ \text{rem}(a,n) = \text{rem}(b,n) \]

QED

**Corollaries**

**symmetric**

\[ a \equiv b \pmod{n} \text{ implies } b \equiv a \pmod{n} \]

**transitive**

\[ a \equiv b \& b \equiv c \pmod{n} \text{ implies } a \equiv c \pmod{n} \]

**Remainder arithmetic**

**Corollary:**

\[ a \equiv \text{rem}(a,n) \pmod{n} \]

pf: \( 0 \leq r_{a,n} < n \), so

\[ r_{a,n} = \text{rem}(r_{a,n},n) \]

**Congruence \( \pmod{n} \)**

If \( a \equiv b \pmod{n} \), then

\[ a+c \equiv b+c \pmod{n} \]

pf: \( n \mid (a - b) \) implies

\[ n \mid ((a+c) - (b+c)) \]
If \( a \equiv b \pmod{n} \), then
\[ a \cdot c \equiv b \cdot c \pmod{n} \]

Proof (pf): \( n \mid (a - b) \) implies
\[ n \mid (a - b) \cdot c, \text{ and so} \]
\[ n \mid ((a \cdot c) - (b \cdot c)) \]

Corollary:
If \( a \equiv b \pmod{n} \) &
\[ c \equiv d \pmod{n} \],
then \( a \cdot c \equiv b \cdot d \pmod{n} \)

Cor: If \( a \equiv a' \pmod{n} \),
then replacing \( a \) by \( a' \) in any arithmetic formula gives an \( \equiv (\pmod{n}) \) formula

So arithmetic \((\pmod{n})\) a lot like ordinary arithmetic
Remainder arithmetic

important: congruence &

\[ a \equiv \text{rem}(a,n) \pmod{n} \]

keeps \((\pmod{n})\) arithmetic
in the remainder range

\([0,n)\)