Modular Arithmetic

CS 2800: Discrete Structures, Fall 2014

Sid Chaudhuri

Follow-up exercise

Read up on **Euclid's Algorithm** for finding the Greatest Common Divisor of two natural numbers

Congruence (modulo m)

- Informally: Two integers are ***congruent*** modulo a natural number m if and only if they have the same remainder upon division by m

Congruence (modulo m)

- Informally: Two integers are ***congruent* modulo a natural number m** if and only if they have the same remainder upon division by m

NOT the definition!

Congruence (modulo m)

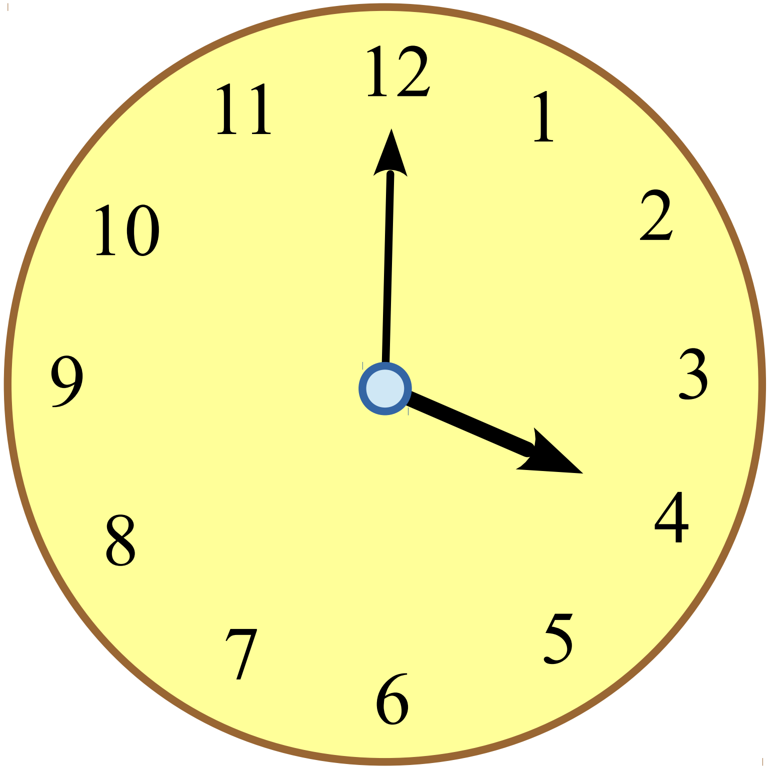
- Informally: Two integers are ***congruent*** modulo a natural number m if and only if they have the same remainder upon division by m

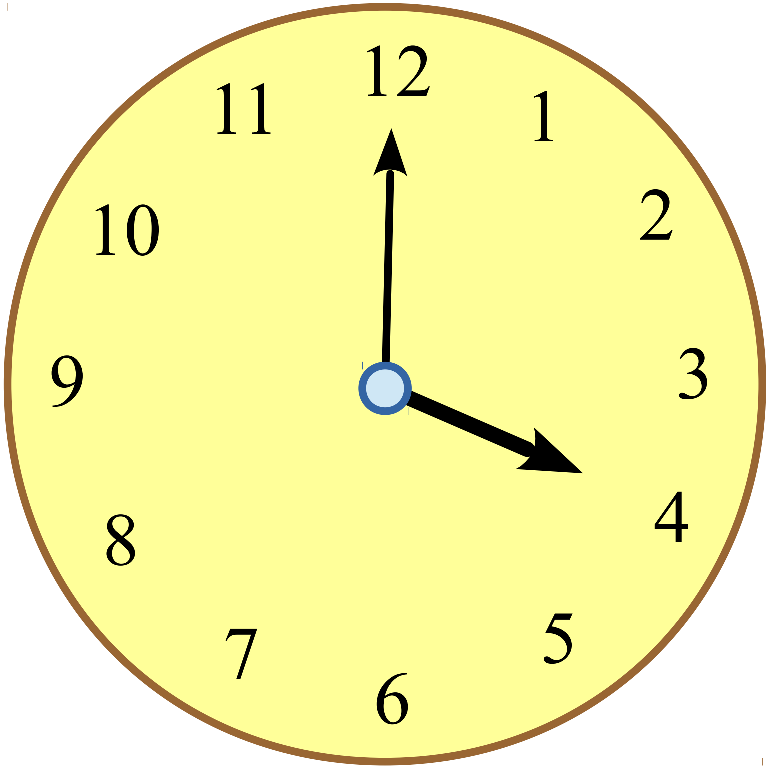
E.g.

$$\begin{aligned} 3 &\equiv 7 \pmod 2 \\ 9 &\equiv 99 \pmod{10} \\ 11^{999} &\equiv 1 \pmod{10} \end{aligned}$$

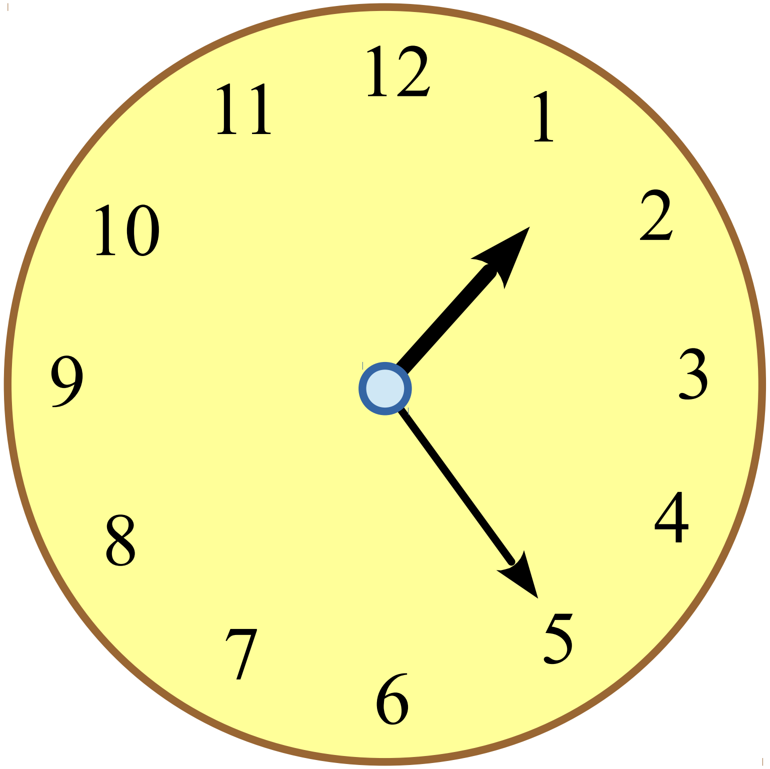
4am $\equiv$ 4pm (modulo 12h)

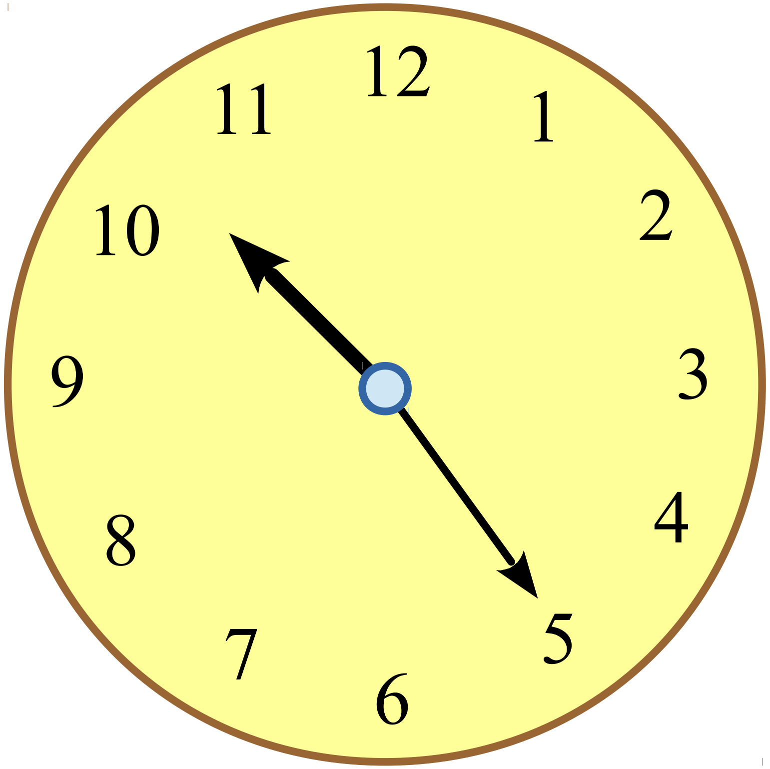
4pm Nov 12 $\equiv$ 4pm Nov 13 (modulo 24h)



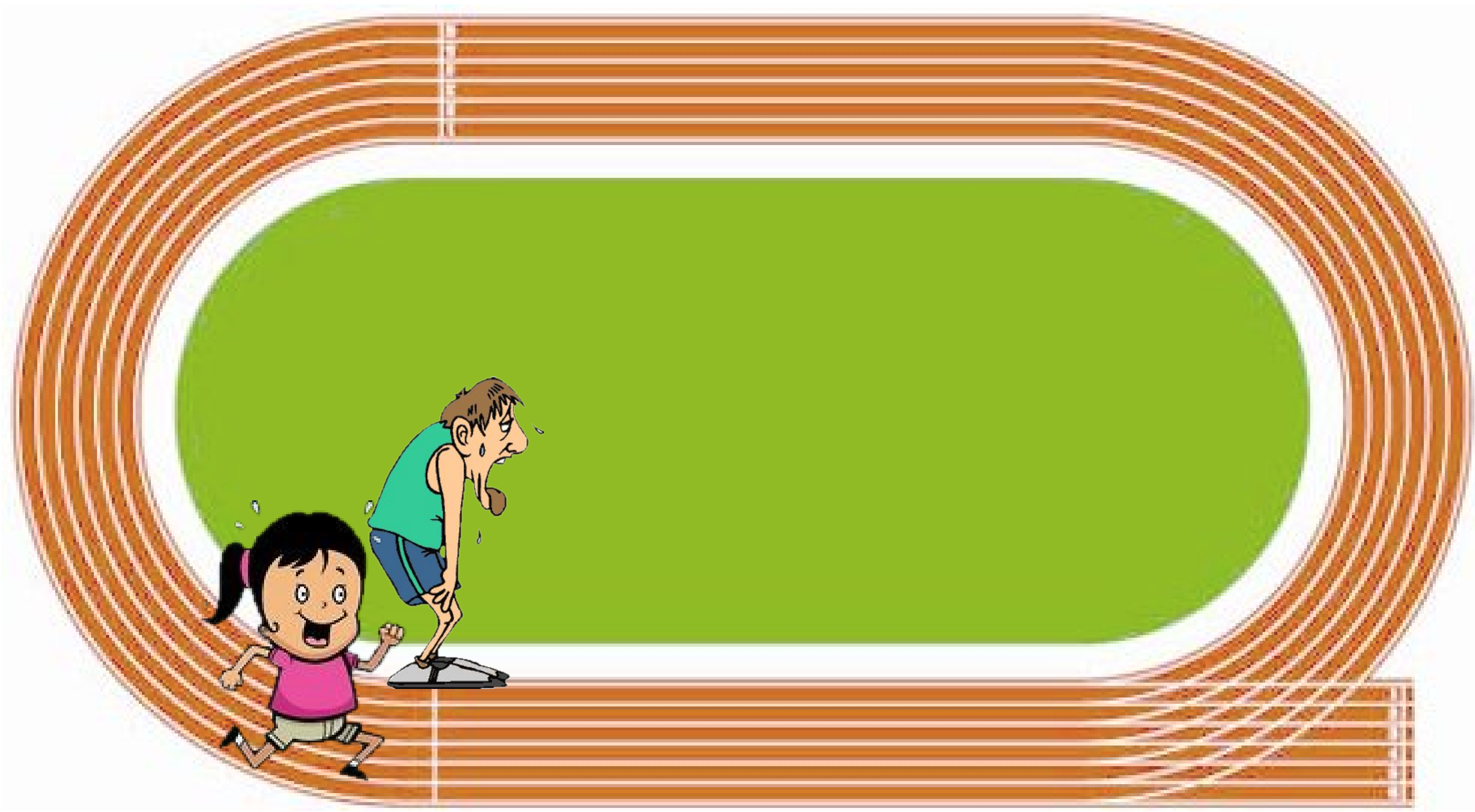


$$1{:}25 \equiv 10{:}25 \text{ (modulo 60 mins)}$$

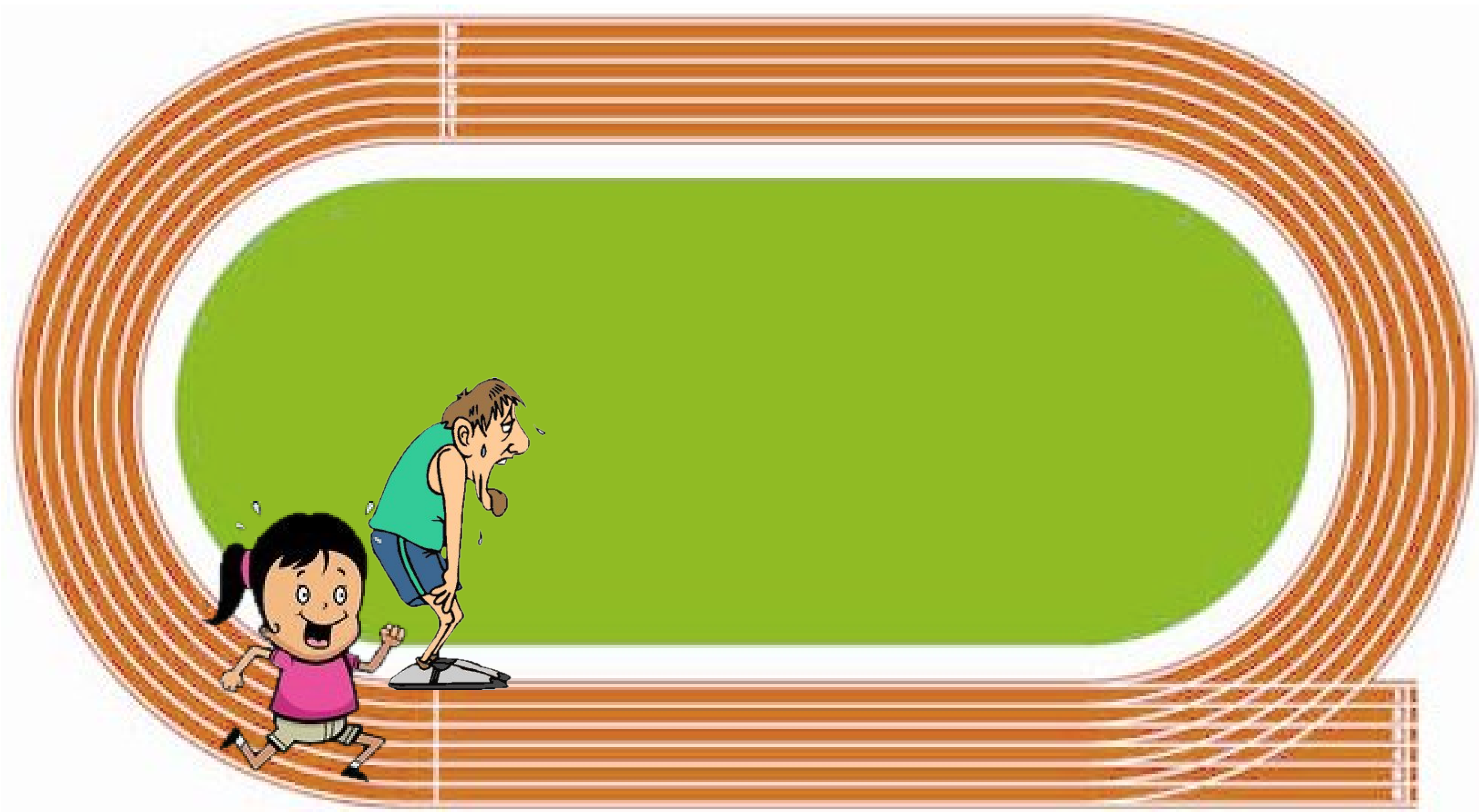




$$300\text{m} \equiv 9900\text{m} \pmod{400}$$



$300\text{m} \equiv 9900\text{m} \pmod{400}$



Discards absolute information (days, hours, laps...)!

The formal definition

- Let $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. a and b are said to be congruent modulo m, written $a \equiv b \pmod{m}$, if and only if $a - b$ is divisible by m
  - ... i.e. iff $m \mid a - b$
  - ... i.e. iff there is some integer k such that $a - b = km$

The formal definition

Doesn't include zero

- Let $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. a and b are said to be congruent modulo m, written $a \equiv b \pmod{m}$, if and only if $a - b$ is divisible by m
  - ... i.e. iff $m \mid a - b$
  - ... i.e. iff there is some integer k such that $a - b = km$

The formal definition

Doesn't include zero

- Let $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. a and b are said to be congruent modulo m, written $a \equiv b \pmod{m}$, if and only if $a - b$ is divisible by m
  - ... i.e. iff $m \mid a - b$
  - ... i.e. iff there is some integer k such that $a - b = km$

- Note: this does *not* directly say a and b have the same remainder upon division by m
  - That is a *consequence* of the definition

Congruence ⇔ Same remainder

- Claim: $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$

Congruence $\Leftrightarrow$ Same remainder

- Claim: $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$
- Proof:

  $(\Leftarrow)$

  Given: $a \bmod m = b \bmod m$

Congruence ⇔ Same remainder

- Claim: $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$
- Proof:

  $(\Leftarrow)$

  Given: $a \bmod m = b \bmod m$

  $\Rightarrow \exists\, q_1, q_2, r$ such that $a = q_1 m + r,\ \ b = q_2 m + r$

Congruence ⇔ Same remainder

- Claim: $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$
- Proof:

  ($\Leftarrow$)

  Given: $a \bmod m = b \bmod m$

  $\Rightarrow \exists\, q_1, q_2, r$ such that $a = q_1 m + r,\ \ b = q_2 m + r$

  $\Rightarrow a - b\ = q_1 m - q_2 m = m(q_1 - q_2)$

Congruence $\Leftrightarrow$ Same remainder

- Claim: $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$
- Proof:

  $(\Leftarrow)$

  Given: $a \bmod m = b \bmod m$

  $\Rightarrow \exists\, q_1, q_2, r$ such that $a = q_1 m + r,\ \ b = q_2 m + r$

  $\Rightarrow a - b\ = q_1 m - q_2 m = m(q_1 - q_2)$

  $\Rightarrow m \mid a - b$

Congruence ⇔ Same remainder

- Claim: $a \equiv b \pmod{m}$ iff $a \bmod m = b \bmod m$
- Proof:

$(\Leftarrow)$

Given: $a \bmod m = b \bmod m$

$\Rightarrow \exists\, q_1, q_2, r$ such that $a = q_1 m + r,\ \ b = q_2 m + r$

$\Rightarrow a - b \ = q_1 m - q_2 m = m(q_1 - q_2)$

$\Rightarrow m \mid a - b$

$\Rightarrow a \equiv b \pmod{m}$

Congruence $\Leftrightarrow$ Same remainder

- Proof: ($\Rightarrow$) Given: $a \equiv b \pmod{m}$

Congruence ⇔ Same remainder

- Proof: ($\Rightarrow$) Given: $a \equiv b \pmod{m}$

  Let $a = q_1 m + r_1,\ \ b = q_2 m + r_2$, where $0 \le r_1, r_2 < m$

Congruence ⇔ Same remainder

Division Algorithm!

- Proof: (⇒) Given: $a \equiv b \pmod{m}$

  Let $a = q_1 m + r_1,\ \ b = q_2 m + r_2$, where $0 \le r_1, r_2 < m$

Congruence $\Leftrightarrow$ Same remainder

Division Algorithm!

- Proof: $(\Rightarrow)$ Given: $a \equiv b \pmod{m}$

  Let $a = q_1 m + r_1,\ \ b = q_2 m + r_2$, where $0 \le r_1, r_2 < m$

  $$m \mid a - b$$

  $$\Rightarrow m \mid q_1 m + r_1 - q_2 m - r_2$$

Congruence ⇔ Same remainder

Division Algorithm!

- Proof: ($\Rightarrow$) Given: $a \equiv b \pmod{m}$

  Let $a = q_1 m + r_1,\ \ b = q_2 m + r_2$, where $0 \le r_1, r_2 < m$

  $$
  \begin{aligned}
  & m \mid a - b \\
  \Rightarrow\ & m \mid q_1 m + r_1 - q_2 m - r_2 \\
  \Rightarrow\ & m \mid r_1 - r_2
  \end{aligned}
  $$

Congruence ⇔ Same remainder

Division Algorithm!

- Proof: ($\Rightarrow$) Given: $a \equiv b \pmod{m}$

  Let $a = q_1 m + r_1$, $b = q_2 m + r_2$, where $0 \le r_1, r_2 < m$

  $$m \mid a - b$$

  $$\Rightarrow m \mid q_1 m + r_1 - q_2 m - r_2$$

  $$\Rightarrow m \mid r_1 - r_2$$

Exercise: Prove that

If a|b and a|c, then a|(b - c)

Congruence $\Leftrightarrow$ Same remainder

Division Algorithm!

- Proof: ($\Rightarrow$) Given: $a \equiv b \pmod{m}$

  Let $a = q_1 m + r_1$, $b = q_2 m + r_2$, where $0 \le r_1, r_2 < m$

  $m \mid a - b$

  $\Rightarrow m \mid q_1 m + r_1 - q_2 m - r_2$

  Exercise: Prove that

  If a|b and a|c, then a|(b - c)

  $\Rightarrow m \mid r_1 - r_2$

  But $-(m-1) \le r_1, r_2 \le (m-1)$

Congruence $\Leftrightarrow$ Same remainder

Division Algorithm!

- Proof: ($\Rightarrow$) Given: $a \equiv b \pmod{m}$

  Let $a = q_1 m + r_1$, $b = q_2 m + r_2$, where $0 \le r_1, r_2 < m$

  $$m \mid a - b$$

  $$\Rightarrow m \mid q_1 m + r_1 - q_2 m - r_2$$

  Exercise: Prove that

  If a|b and a|c, then a|(b - c)

  $$\Rightarrow m \mid r_1 - r_2$$

  But $-(m-1) \le r_1, r_2 \le (m-1)$

  $$\Rightarrow r_1 - r_2 = 0$$

Congruence $\Leftrightarrow$ Same remainder

Division Algorithm!

- Proof: ($\Rightarrow$) Given: $a \equiv b \pmod{m}$

  Let $a = q_1 m + r_1,\ \ b = q_2 m + r_2$, where $0 \le r_1, r_2 < m$

  $$m \mid a - b$$

  $$\Rightarrow m \mid q_1 m + r_1 - q_2 m - r_2$$

  Exercise: Prove that

  If a|b and a|c, then a|(b - c)

  $$\Rightarrow m \mid r_1 - r_2$$

  But $-(m-1) \le r_1, r_2 \le (m-1)$

  $$\Rightarrow r_1 - r_2 = 0$$

  $$\Rightarrow r_1 = r_2$$

Congruence $\Leftrightarrow$ Same remainder

Division Algorithm!

- Proof: $(\Rightarrow)$ Given: $a \equiv b \pmod{m}$

  Let $a = q_1 m + r_1,\ \ b = q_2 m + r_2$, where $0 \le r_1, r_2 < m$

  $$m \mid a - b$$

  $$\Rightarrow m \mid q_1 m + r_1 - q_2 m - r_2$$

  Exercise: Prove that

  If a|b and a|c, then a|(b - c)

  $$\Rightarrow m \mid r_1 - r_2$$

  But $-(m-1) \ \le\ r_1, r_2 \ \le\ (m-1)$

  $$\Rightarrow r_1 - r_2 = 0$$

  $$\Rightarrow r_1 = r_2$$

  $$\Rightarrow a \bmod m = b \bmod m$$

Properties of congruence

- If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then
  - $a + c \equiv b + d \pmod{m}$
  - $ac \equiv bd \pmod{m}$

E.g. $11 \equiv 1 \pmod{10} \Rightarrow 11^{999} \equiv 1^{999} \equiv 1 \pmod{10}$

$9 \equiv -1 \pmod{10} \Rightarrow 9^{999} \equiv (-1)^{999} \pmod{10}$

$7^{999} \equiv 49^{499}.7 \equiv (-1)^{499}.7 \equiv -7 \equiv 3 \pmod{10}$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Rightarrow a + c \equiv b + d \pmod{m}$$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Longrightarrow a + c \equiv b + d \pmod{m}$$

Proof: $a \equiv b \pmod{m},\ c \equiv d \pmod{m}$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Longrightarrow a + c \equiv b + d \pmod{m}$$

Proof: $a \equiv b \pmod{m},\ c \equiv d \pmod{m}$

$\Rightarrow\ m \mid a - b$ and $m \mid c - d$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Longrightarrow a + c \equiv b + d \pmod{m}$$

Proof: $a \equiv b \pmod{m},\ c \equiv d \pmod{m}$

$\Rightarrow\ m \mid a - b$ and $m \mid c - d$

$\Rightarrow\ m \mid ((a - b) + (c - d))$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Rightarrow a + c \equiv b + d \pmod{m}$$

Proof: $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$

$\Rightarrow\ m \mid a - b$ and $m \mid c - d$

$\Rightarrow\ m \mid ((a - b) + (c - d))$

Exercise: Prove that
if $a|b$ and $a|c$, then $a|(b + c)$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Rightarrow a + c \equiv b + d \pmod{m}$$

Proof: $a \equiv b \pmod{m},\ c \equiv d \pmod{m}$

$\Rightarrow\ m \mid a - b$ and $m \mid c - d$

$\Rightarrow\ m \mid ((a - b) + (c - d))$

Exercise: Prove that

If a|b and a|c, then a|(b + c)

$\Rightarrow\ m \mid ((a + c) - (b + d))$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Rightarrow a + c \equiv b + d \pmod{m}$$

Proof: $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$

$\Rightarrow\ m \mid a - b$ and $m \mid c - d$

$\Rightarrow\ m \mid ((a - b) + (c - d))$

Exercise: Prove that
If a|b and a|c, then a|(b + c)

$\Rightarrow\ m \mid ((a + c) - (b + d))$

$\Rightarrow\ a + c \equiv b + d \pmod{m}$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Rightarrow ac \equiv bd \pmod{m}$$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\implies ac \equiv bd \pmod{m}$$

Proof: $a \equiv b \pmod{m},\ c \equiv d \pmod{m}$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Rightarrow ac \equiv bd \pmod{m}$$

Proof: $a \equiv b \pmod{m},\ c \equiv d \pmod{m}$

$\Rightarrow\ \exists\ r, r'$ such that

$$a = q_1 m + r \qquad\qquad b = q_2 m + r$$
$$c = q'_1 m + r' \qquad\qquad d = q'_2 m + r'$$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Rightarrow ac \equiv bd \pmod{m}$$

Proof: $a \equiv b \pmod{m},\ c \equiv d \pmod{m}$

we proved congruence

$\Leftrightarrow$ same remainder

$\Rightarrow\ \exists\ r, r'$ such that

$$a = q_1 m + r \qquad b = q_2 m + r$$
$$c = q'_1 m + r' \qquad d = q'_2 m + r'$$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Rightarrow ac \equiv bd \pmod{m}$$

Proof: $a \equiv b \pmod{m},\ c \equiv d \pmod{m}$

we proved congruence

$\Leftrightarrow$ same remainder

$\Rightarrow\ \exists\ r, r'$ such that

$$a = q_1 m + r \qquad b = q_2 m + r$$
$$c = q'_1 m + r' \qquad d = q'_2 m + r'$$

$$\Rightarrow\ ac = q_1 m \cdot q'_1 m + q_1 m \cdot r' + q'_1 m \cdot r + rr'$$
$$bd = q_2 m \cdot q'_2 m + q_2 m \cdot r' + q'_2 m \cdot r + rr'$$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Rightarrow ac \equiv bd \pmod{m}$$

Proof: $a \equiv b \pmod{m},\ c \equiv d \pmod{m}$

we proved congruence

$\Leftrightarrow$ same remainder

$\Rightarrow\ \exists\ r, r'$ such that

$$a = q_1 m + r \qquad b = q_2 m + r$$
$$c = q'_1 m + r' \qquad d = q'_2 m + r'$$

$$\Rightarrow\ ac = q_1 m \cdot q'_1 m\ + q_1 m \cdot r'\ + q'_1 m \cdot r\ + rr'$$
$$bd = q_2 m \cdot q'_2 m\ + q_2 m \cdot r'\ + q'_2 m \cdot r\ + rr'$$

$$\Rightarrow\ ac \equiv bd \pmod{m}$$

$$a \equiv b \pmod{m},\ c \equiv d \pmod{m}$$
$$\Rightarrow ac \equiv bd \pmod{m}$$

Proof: $a \equiv b \pmod{m}$, $c \equiv d \pmod{m}$

we proved congruence $\Leftrightarrow$ same remainder

$\Rightarrow\ \exists\, r, r'$ such that

$$a = q_1 m + r \qquad b = q_2 m + r$$
$$c = q'_1 m + r' \qquad d = q'_2 m + r'$$

$$\Rightarrow\ ac = q_1 m \cdot q'_1 m + q_1 m \cdot r' + q'_1 m \cdot r + rr'$$
$$bd = q_2 m \cdot q'_2 m + q_2 m \cdot r' + q'_2 m \cdot r + rr'$$

$$\Rightarrow\ ac \equiv bd \pmod{m}$$

Note: But rr' is <u>not</u> in general the remainder (since it can be $\geq m$)