# MAT200: Logic Language and Proof

Lecture 25 - May 5 2021

Recently:

- Modular arithmetic (Ch 19)
- Applications of modular arithmetic multiplication and addition
- Division in modular arithmetic

Today: some applications of division in modular arithmetic
- Fermat's little theorem (1640)
- Wilson's theorem (1871)

**Proposition 19.3.2:** Suppose gcd(a, m) =1.
Then $ab_1 \equiv ab_2 \mod m \implies b_1 \equiv b_2 \mod m$.

**Theorem 20.1.5.** Suppose $\gcd(a, m) = 1$. Then $ax \equiv b \mod m$ has a unique (modulo m) solution.

**Theorem:** Suppose $p$ is prime. If $a \in \mathbb{Z}$ and $p \nmid a$, then $a^{p-1} - 1$ is divisible by $p$.

Need: $p \nmid a$: a is not a multiple of p

**Proposition 19.3.2:** Suppose gcd(a, m) =1.
Then $ab_1 \equiv ab_2 \mod m \implies b_1 \equiv b_2 \mod m$.

**Theorem 20.1.5.** Suppose $\gcd(a, m) = 1$. Then $ax \equiv b \mod m$ has a unique (modulo m) solution.

**Proof:** Suppose p prime, and $p \nmid a$.

* Let

$$f: \{0, 1, \ldots, p-1\} \to \{0, 1, \ldots, p-1\}.$$

$$f(x) = \begin{cases} \text{The unique} \\ b \in \{0, \ldots, p-1\} \end{cases} \text{ s.t. } ax \equiv b \mod p$$

Example: $p = 7$, $a = 2$

$f(6) =$ a) 1, b) 2, c) 5, d) 12

$$f(6) = \begin{cases} \text{The unique} \\ b \in \{0, \ldots, 6\} \end{cases} \text{ s.t. } 12 \equiv b \mod 7$$

Example:

$p = 7$

$a = 2$

$2^{7-1} - 1 = 63$.

Indeed, $7 \mid 63$.

Example:

$a = 7$

Then $7^{7-1} - 1$ clearly not divisible by 7, remainder is 6. ($7^{7-1} - 1 = 7^6 - 7 + 6$).

Example:

$p = 7$

$a = 3$

$3^{7-1} \equiv 3^6 \mod 7$

Now $3^2 \equiv 2 \mod 7$

$3^3 \equiv 6 \mod 7$

$3^4 \equiv 18 \equiv 4 \mod 7$

$3^5 \equiv 12 \equiv 5 \mod 7$

$3^6 \equiv 15 \equiv 1 \mod 7$.

Theorem 17.3.2, if $\gcd(a,p)=1$, $p \mid ab \Rightarrow p \mid b$.

**Theorem:** Suppose $p$ is prime. If $a \in \mathbb{Z}$ and $p \nmid a$, then $a^{p-1} - 1$ is divisible by $p$.

Need:

**Proposition 19.3.2:** Suppose gcd(a, m) =1.
Then $ab_1 \equiv ab_2 \mod m \implies b_1 \equiv b_2 \mod m$.

**Theorem 20.1.5.** Suppose $\gcd(a, m) = 1$. Then $ax \equiv b \mod m$ has a unique (modulo m) solution.

Proof: Suppose p prime, and $p \nmid a$.

* Let

$f: \{0,1,\dots,p-1\} \to \{0,1,\dots,p-1\}$.

$f(x) =$ {The unique $b \in \{0,\dots,p-1\}$ s.t. $ax \equiv b \mod p$

---

Example: $p=7$, $a=2$

$f(6) =$ a) 1 b) 2 c) 5 d) 12

$f(6) =$ {The unique $b \in \{0,\dots,6\}$ s.t. $12 \equiv b \mod 7$

* Claim:
f is a bijection.

Proof:

Injective:

- by definition. $ax \equiv f(x) \mod p$. $ay \equiv f(y) \mod p$

Suppose $f(x)=f(y)$,

- so $ax \equiv ay \mod p$.
- so $p \mid a(x-y)$.
- since $p \nmid a$, $\Rightarrow p \mid x-y$.
- So $x \equiv y \mod p$.
- So $x=y$.

Surjective:

Suppose $b \in \{0,1,\dots,p-1\}$.

By Thm 20.1.5, there exists $x \in \mathbb{Z}$ such that

$ax \equiv b \mod p$.

So $f(x) = b$. QED.

slight mistake/gap here too.

Theorem 17.3.2, if $\gcd(a,p)=1$, $p \mid ab \Rightarrow p \mid b$.

**Theorem:** Suppose $p$ is prime. If $a \in \mathbb{Z}$ and $p \nmid a$, then $a^{p-1} - 1$ is divisible by $p$.

Need:

**Proposition 19.3.2:** Suppose gcd(a, m) =1.
Then $ab_1 \equiv ab_2 \mod m \implies b_1 \equiv b_2 \mod m$.

**Theorem 20.1.5.** Suppose $\gcd(a, m) = 1$. Then $ax \equiv b \mod m$ has a unique (modulo m) solution.

Proof: Suppose p prime, and $p \nmid a$.

* Let

$$f: \{0,1,\dots,p-1\} \to \{0,1,\dots,p-1\}.$$

$$f(x) = \begin{cases} \text{The unique} \\ b \in \{0,\dots,p-1\} \end{cases} \text{ s.t. } ax \equiv b \mod p$$

---

Example: $p=7$, $a=2$

$f(6) =$ 0) 1, 1) 2, 2) 5, 3) 12

$$f(6) = \begin{cases} \text{The unique} \\ b \in \{0,\dots,6\} \end{cases} \text{ s.t. } 12 \equiv b \mod 7$$

* Claim:
f is a bijection.

Example: $p=7$ $a=2$.

$f(0) = 0$
$f(1) = 2$
$f(2) = 4$
$f(3) = 6$
$f(4) = 1$
$f(5) = 3$
$f(6) = 5$

Example: $p=7$ $a=3$

$f(0) = 0$
$f(1) = 3$
$f(2) = 6$
$f(3) = 2$
$f(4) = 5$
$f(5) = 1$
$f(6) = 4$

Theorem 17.3.2, if $\gcd(a,p)=1$, $p \mid ab \Rightarrow p \mid b$.

**Theorem:** Suppose $p$ is prime. If $a \in \mathbb{Z}$ and $p \nmid a$, then $a^{p-1} - 1$ is divisible by $p$.

Need: Used in primality.

**Proposition 19.3.2:** Suppose gcd(a, m) =1.
Then $ab_1 \equiv ab_2 \mod m \implies b_1 \equiv b_2 \mod m$.

**Theorem 20.1.5.** Suppose $\gcd(a, m) = 1$. Then $ax \equiv b \mod m$ has a unique (modulo m) solution.

Proof: Suppose p prime, and $p \nmid a$.

* Let

$f: \{0,1,\dots,p-1\} \to \{0,1,\dots,p-1\}$.

$f(x) =$ {The unique $b \in \{0,\dots,p-1\}$ s.t. $ax \equiv b \mod p$

* Claim:

f is a bijection, and $f(0)=0$.

So f is actually a bijection

$f: \{1,\dots,p-1\} \to \{1,\dots,p-1\}$.

Therefore

$f(1) \cdots f(p-1) \equiv 1 \cdot 2 \cdots (p-1) \mod p$

So

$(a \cdot 1) \cdots (a \cdot (p-1)) \equiv (p-1)! \mod p$

So

$a^{p-1}(p-1)! \equiv (p-1)! \mod p$.

$\gcd((p-1)!, p) = 1$, so

$a^{p-1} \equiv 1 \mod p$.

So $p \mid a^{p-1} - 1$.

1771

**Theorem (Wilson):** Let $p$ be prime. Then $(p-1)! + 1$ is divisible by $p$.

Need:

**Proposition 19.3.2:** Suppose gcd(a, m) =1.
Then $ab_1 \equiv ab_2 \mod m \implies b_1 \equiv b_2 \mod m$.

**Theorem 20.1.5.** Suppose $\gcd(a, m) = 1$. Then $ax \equiv b \mod m$ has a unique (modulo m) solution.

Relating Thm 20.1.5 to example:

9 is paired with 5 because
$9 \cdot 5 \equiv 1 \mod 11$
To find the 5, solved
$9x \equiv 1 \mod 11$.

$\{2, \ldots, p\}$

Proof: Define $f: \{2, \ldots, p-2\} \to \{2, \ldots, p-2\}$
$f(a)$ = the unique $x$ such that $ax \equiv 1 \mod p$.

Then
$(p-1)! \equiv (p-1) \cdot (p-2) \cdot \cdots \cdot 2 \mod p$
$\equiv (-1) \cdot (p-2) \cdot \cdots \cdot 2 \mod p$

because $f$ pairs up all the elements in the domain.

$\equiv (-1) \mod p$.

So $p \mid (p-1)! + 1$.

Example:

$p=5$, $(p-1)! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$

$24+1$ is divisible by 5

Example:

$p=11$

$10! = 10 \times (9 \times 5) \times (8 \times 7) \times (6 \times 2) \times (4 \times 3)$
$\equiv (-1) \times (1) \times (1) \times (1) \times (1) \mod 11$

$10! \equiv -1 \mod 11$

So
$11 \mid 10! + 1$.

This worked because we could pair up $\{1, \ldots, p-2\}$, such that product of pair is equivalent to 1.

**Theorem (Wilson):** Let $p$ be prime. Then $(p-1)!+1$ is divisible by $p$.

Need:

**Proposition 19.3.2:** Suppose gcd(a, m) =1.
Then $ab_1 \equiv ab_2 \mod m \implies b_1 \equiv b_2 \mod m$.

**Theorem 20.1.5.** Suppose $\gcd(a,m)=1$. Then $ax \equiv b \mod m$ has a unique (modulo m) solution.

**Theorem 17.3.2.** If $p$ is prime, $p \mid ab \implies p \mid a$ or $p \mid b$.

$f: \{2, \dots, p-2\} \to \{2, \dots, p-2\}$
$f(a)$ = the unique $x$ such that $ax \equiv 1 \mod p$.

Need: 1) $a \neq f(a)$
2) $a \neq b \implies f(a) \neq f(b)$ ←

1): Suppose $a = f(a)$, then $a^2 \equiv 1 \mod p$.

Then $a^2 - 1 \equiv 0 \mod p$.

$(a-1)(a+1) \equiv 0 \mod p$.

So $p \mid (a-1)(a+1) \implies p \mid a-1$ or $p \mid a+1$.

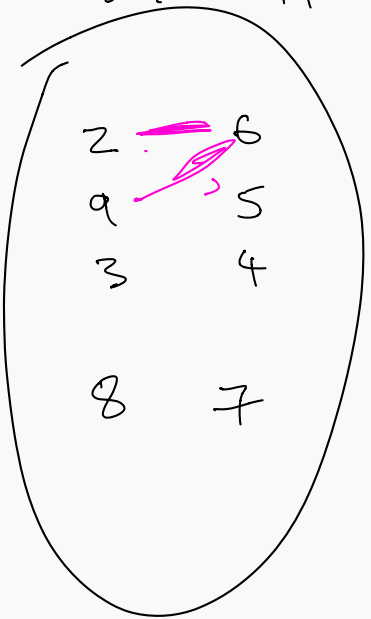
$\implies a \equiv 1$ or $a \equiv p-1 \mod p$.

if $f(a) = f(b)$, then
$af(a) \equiv 1$
$bf(a) \equiv 1$
so $a \equiv b \mod p$.

so $a, b$ solve $xf(a) \equiv 1$.

$\{2, \dots, p-2\}$

$p = 11$



**Theorem:** Let $p$ be not prime. Then $(p-1)!+1$ is not divisible by $p$.