Extra credit portfolio entries - Available, but going fast.

Exit Survey - complete by Friday to receive participation grade.

TCEs - please do them!

Review problems - coming soon

Thm 4.13: Let p be a prime, and a an integer not divisible by p (i.e. $(a,p)=1$).

Then $\{a, 2a, 3a, \ldots, pa\}$ is a complete residue system mod p.

Proof: The numbers in $\{a, 2a, 3a, \ldots, pa\}$ are pairwise incongruent mod p:

$$xa \equiv ya \pmod{p}$$

$$\Rightarrow x \equiv y \pmod{p} \quad \text{by Thm 1.45}$$

but the coefficients range from 1 to p, so no two distinct coefficients are congruent mod p.

$x \equiv y \pmod{p}$ and $1 \leq x, y \leq p$ $\rightarrow$ $x = y$

By Thm 3.17, this is a complete residue system. ∎

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

$\{1 \cdot 2, 2 \cdot 2, 3 \cdot 2, \ldots, 7 \cdot 2\}$

$= \{2, 4, 6, 8, 10, 12, 14\}$

CCRS $= \{0, 1, 2, 3, 4, 5, 6\}$

Thm 4.14: Let p prime, a not divisible by p.

Then

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \cdots (p-1) \pmod{p}$$

Proof: We just saw that

$$\{a, 2a, 3a, \ldots, (p-1)a, \boxed{pa}\}$$

and

$$\{\boxed{0}, 1, 2, 3, \ldots, p-1\}$$

are both complete residue systems.

We know $pa \equiv 0 \pmod{p}$.

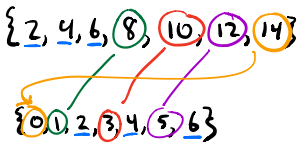
Also, each number in $\{a, 2a, 3a, \ldots, (p-1)a\}$ is congruent to exactly one number in $\{1, 2, 3, \ldots, p-1\}$

So

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}.$$

■

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



$$2 \cdot 4 \cdot 6 \cdot 8 \cdot 10 \cdot 12 \equiv 2 \cdot 4 \cdot 6 \cdot 1 \cdot 3 \cdot 5 \pmod{7}$$

$$\equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7}$$

Looking at this more closely,

$$2^6(1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6) \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \pmod{7}$$

Thm 1.45 → can cancel a number from both sides if it is relatively prime to 7

$$\Rightarrow \quad 2^6 \equiv 1 \pmod 7.$$

Note: We already saw $2^3 \equiv 1 \pmod 7$

$$2^6 = (2^3)^2 \equiv 1^2 \equiv 1 \pmod 7$$

Thm 4.16 (Fermat's Little Theorem):

If p is prime and $p \nmid a$ (i.e. a relatively prime to p) then

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

Proof: By 4.14,

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$$

$$\rightarrow \quad a^{p-1}(1 \cdot 2 \cdot 3 \cdots (p-1)) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod p$$

By Thm 1.45, we can cancel $1, 2, 3, \ldots, p-1$ because they are relatively prime to p.

$$a^{p-1} \equiv 1 \pmod p$$

Fermat's LT version 2

Thm 4.16: If p is prime and a is any integer, then

$$a^p \equiv a \pmod{p}$$

Proof:

Case 1: $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$ (Fermat version 1)

Multiply both sides by a:

$$a^p \equiv a \pmod{p}$$

Case 2: $p \mid a \Rightarrow a \equiv 0 \pmod{p}$

$$\Rightarrow a^p \equiv 0^p \equiv 0 \pmod{p}$$

So $a \equiv a^p \pmod{p}$. ∎

Ex: $512^{372} \equiv (512^{12})^{31} \pmod{13} \equiv 1^{31} \pmod{13}$

↑ FLT ($13 \nmid 512$)

$372 = 31 \cdot 12$

$\equiv 1 \pmod{13}$.

Ex: $3444^{3233} \equiv (3444^{16})^{202} \cdot 3444 \pmod{17}$

$3233 = 202 \cdot 16 + 1$

$\equiv 1^{202} \cdot 3444 \pmod{17}$

FLT

$17 \nmid 3444$

$3444 = 202 \cdot 17 + 10$

$\equiv 3444 \pmod{17}$

$\equiv 10 \pmod{17}$.

Cor (4.18 Thm): If p prime, $p \nmid a$, then

$\text{ord}_p(a)$ divides $p-1$.

smallest $k > 0$ such that $a^k \equiv 1 \pmod{p}$

Proof: By FLT, $a^{p-1} \equiv 1 \pmod{p}$.

By Thm 4.10, $\text{ord}_p(a)$ divides $p-1$.

∎

Ex: $\text{ord}_7(1) = 1$ divides $7-1 = 6$.

$\text{ord}_7(2) = 3$ divides 6.

$\text{ord}_7(3) = 6$ divides 6.

$\text{ord}_7(4) = 6$ divides 6.

$\text{ord}_7(5) = 3$ divides 6.

$\text{ord}_7(6) = 2$ divides 6.