MATH 565 Spring 2019 - Class Notes

3/5/19

Scribe: Kourtney Harrison

1 Congruences

Definition 1. *Congruent*

$$a \equiv b \pmod{c}$$

If $(b-a)$ is divisible by c.

Say: "a is congruent to b modulo c"

Ex: $7 \equiv 12 \pmod 5$ because (12-7)=5 and 5|5

Intuitively we think of numbers as the "the same" modulo c if they have the same remainder when divided by c

Ex(cont.):

- $7 \equiv 2 \pmod 5$
- $2 \equiv 7 \pmod 5$
- $7 \equiv 2 \equiv 10 + 2 \equiv 2(6) \equiv 5 \pmod 5$
- $7 \equiv -3 \pmod 5$
- $2 \not\equiv -2 \pmod 5$

Theorem 1. *If $a \equiv a' \pmod c$ and $b \equiv b' \pmod c$, then*

$$a \pm b \equiv a' \pm b' \pmod c$$
$$\text{and } ab \equiv a'b' \pmod c$$

Note: Division does not always work!

Proof. Suppose $a \equiv a' \pmod c$ and $b \equiv b' \pmod c$ so

$$(a' - a) \equiv kc \text{ for some } k \text{ and}$$
$$(b' - b) \equiv lc \text{ for some } l$$

Consider $(a' + b') - (a + b)$
$$= (a' - a) + (b' - b)$$
$$= kc + lc$$
$$= c(k + l)$$

So $c|(a' + b') - (a + b)$

So $a + b \equiv a' + b' \pmod{c}$

Now consider $a'b' - ab$
$$= a'b' - ab' + ab' - ab$$
$$= (a'b' - a'b) + (a'b - ab)$$
$$= a'(b' - b) + b(a' - a)$$
$$= a'(lc) + b(kc)$$
$$= c(a'l + bk)$$

So $c|(a'b') - (ab)$

So $ab \equiv a'b' \pmod{c}$

□

Theorem 2. *Properties of Modulo*

$$a \equiv a \pmod{c} \quad \textit{(Reflexive Property)}$$
$$a \equiv b \pmod{c} \Rightarrow \quad b \equiv a \pmod{c} \quad \textit{(Symmetric Property)}$$
$$\textit{If } a \equiv b \pmod{c} \textit{ and } b \equiv d \pmod{c}, \textit{ then } a \equiv d \pmod{c} \quad \textit{(Transitive Property)}$$

Proof. Transitive Property

Suppose $a \equiv b \pmod{c} \Rightarrow c|(b - a)$
and $b \equiv d \pmod{c} \Rightarrow c|(d - b)$

Now consider $d - a$
$$= d - b + b - a$$
$$= (d - b) + (b - a)$$

c divides both of these so c divides $(d - a)$

□

Ex:

$$3 \equiv 10 \pmod{7} \text{ and } 5 \equiv -2 \pmod{7}$$
3+5=10 and 10-2=8
$$\text{so } 3 + 5 \equiv 10 + (-2) \pmod{7}$$
3(5)=15 and 10(-2)=-20
$$\text{so } 15 \equiv -20 \pmod{7}$$
$$3(5) \equiv 10(-2) \pmod{7}$$

Theorem 3. *Cancellation Property*

If $bc \equiv bd \pmod{n}$ *and* $\gcd(b,n) = 1$, *then*
$$c \equiv d \pmod{n}$$

We can "divide" by $b \pmod{n}$ only if $\gcd(b,n) = 1$

Proof. If $bc \equiv bd \pmod{n}$, then

$$n|(bd - bc)$$
$$n|b(d - c)$$

because $\gcd(b,n) = 1$
we know $n|(d - c)$ so

$$c \equiv d \pmod{n}$$

□

Ex: $12 \equiv 6 \pmod{2}$
$3(4) \equiv 3(2) \pmod{2}$
Since $\gcd(3,2) = 1$ we can cancel out the 3's
$4 \equiv 2 \pmod{2}$
But $2(6) \equiv 2(3) \pmod{2}$ try cancelling out the 2's
$6 \not\equiv 3 \pmod{2}$ because $\gcd(2,2) = 2$

Definition 2. *Residue*

If $a \equiv b \pmod{n}$ *we'll say that* b *is a* <u>*residue*</u> *of* a *modulo* n.
We'll say that $\{r_1, r_2, ..., r_s\}$ *is a* <u>*complete residue system*</u> *modulo* n *if*

1. $r_i \not\equiv r_j \pmod{n}$ *if* $i \not\equiv j$

2. *Any integer* m *has* $m \equiv r_i \pmod{n}$ *for some* i

Ex: $\{0, 1, 2\}$ is a complete residue system $\pmod{3}$
So is $\{-1, 0, 1\}$, $\{0, 4, 8\}$, $\{-1, 3, 31\}$, or $\{1, 2, 3\}$

Our Favorite Complete Residue System:

$$\{0, 1, ..., n - 1\} \pmod{n}$$

Theorem 4. *If* $\{r_1, r_2, ..., r_s\}$ *is a complete residue system* $\pmod{n}$, *then* $s = n$

Theorem 5. *Fermat's Little Theorem*

If p *is prime, then*

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

Note: *If* $\gcd(n,p) = 1$*, then our cancellation property says we can cancel an* n *from both sides*

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

Theorem 6. *Wilson's Theorem*
If p *is prime, then*

$$(p-1)! \equiv -1 \pmod p$$

Ex: Wilson's Theorem
$p = 5$
$(p-1)! = 4! = 4(3)(2)(1) = 24$
$24 \equiv -1 \pmod 5$

Definition 3. *A* reduced residue system *modulo* n *is a set* $\{r_1, r_2, ..., r_s\}$
Satisfying:

1. $r_i \neq r_j \pmod n$
2. $\gcd(n, r_i) = 1$ *for each* i
3. *If* $\gcd(m,n) = 1$*, then* $m \equiv r_j \pmod n$ *for some* i

Ex: Reduced Residue System
Consider $n = 12$. Find a reduced residue system $\pmod n$.
$\{\cancel{0}, 1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}, \cancel{9}, \cancel{10}, 11\}$

To get the reduced residue system, start with a complete residue system and get rid of all numbers that are not relatively prime with n.

Reduced Residue System $\pmod{12}$: $\{1, 5, 7, 11\}$

Note: You can $\div$ by any number in the reduced residue system but you can only $+, -, or \times$ in the complete residue system

Definition 4. $\varphi(n) = \phi(n)$
$\varphi(n) =$ *size of a reduced residue system* $\pmod n$

$$\varphi(n) = \#\{o < a < n | \gcd(a,n) = 1$$

$\# \to$ *means count*
If p *is prime, then*

$$\varphi(p) = p - 1$$

Ex: $\varphi(12) = 4$

Theorem 7. *Euler's Theorem*
If $\gcd(a, n) = 1$, *then*

$$a^{\varphi(n)} \equiv 1 \pmod{n}$$

Ex: $n = 10$ and $a = 3$
$\gcd(10, 3) = 1$
$\varphi(10) = 4 \rightarrow$ reduced residue system $\{1, 3, 7, 9\}$
Euler's Theorem Says
$3^4 \equiv 9^2 \equiv 81 \equiv 1 \pmod{10}$

Proof. Let $\{r_1, r_2, ..., r_s\}$ be a reduced residue system $\pmod{n}$
Note: $s = \varphi(10)$
Multiply each r_i by a (from theorem)
$\{ar_1, ar_2, ..., ar_s\}$
all of these are coprime to n
Note that each $ar_i \equiv r_j$ for some j because
$\{r_1, r_2, ..., r_s\}$ is a reduced residue system

Ex: $n = 10$ and $a = 3$
$\{r_1, r_2, r_3, r_4\}$
$\{1, 3, 7, 9\}$

$$\begin{aligned} 3r_1 &\equiv 3 \pmod{10} \\ 3r_2 &\equiv 3(3) \equiv 9 \pmod{10} \\ 3r_3 &\equiv 3(7) \equiv 21 \equiv 1 \pmod{10} \\ 3r_4 &\equiv 3(9) \equiv 27 \equiv 7 \pmod{10} \end{aligned} \quad \rightarrow \quad \begin{aligned} 3r_1 &\equiv r_2 \pmod{10} \\ 3r_2 &\equiv r_4 \pmod{10} \\ 3r_3 &\equiv r_1 \pmod{10} \\ 3r_4 &\equiv r_3 \pmod{10} \end{aligned} \tag{1}$$

Notes that if $ar_i \equiv ar_j \pmod{n}$ the cancellation property says $r_i \equiv r_j \pmod{n}$

So $\{ar_1, ar_2, ..., ar_s\}$ is also a reduced residue system

Multiply together all things in this set
$(ar_1)(ar_2)...(ar_s) \equiv P \pmod{n}$
Since multiplying by a just changed the order of things in our reduced residue system
$(r_1)(r_2)...(r_s) \equiv P \pmod{n}$

$P \equiv (ar_1)(ar_2)...(ar_s) \pmod{n}$
$P \equiv a^s(r_1)(r_2)...(r_s) \pmod{n}$
$P \equiv a^{\varphi(n)}P \pmod{n}$ (use Cancellation Property)
$1 \equiv a^{\varphi(n)}P \pmod{n}$

$\square$

Corollary 1. *If* $n = p$ *is prime, then*

$$\varphi(p) = p - 1$$

If $\gcd(a, n) = 1$, *then*

$$a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \pmod{n}$$

Note that Fermat's Little Theorem $\rightarrow a^{p-1} \equiv 1 \pmod{n}$ *is a special case of Euler's Theorem*