Math 412: Number Theory
Lecture 7: Wilson's theorem

Gexin Yu
gyu@wm.edu

College of William and Mary

Congruent classes

- A complete system of residues modulo m is a set of integers such that every integer is congruent modulo m to exactly one integer of the set.
- Ex: A set of m incongruent integers modulo m forms a complete set of residues modulo m.
- Ex: If $r_1, \ldots, r_m$ is a complete system of residues modulo m, and if $a \in N$ and $(a, m) = 1$, then $ar_1 + b, ar_2 + b, \ldots, ar_m + b$ is a complete system of residues modulo m for any integer b.

$\mathbb{Z}_m = (\mathbb{Z}_m, +)$ group.

Reduced System of residues modulo m

- Let $\phi(n)$ be the number of integers in $1, 2, \ldots, n$ that are coprime to n.

$\phi(2) = 1$. $1, \cancel{2}$

$\phi(3) = 2$ $1, 2, \cancel{3}$

$\phi(8) = 4$ $1, \cancel{2}, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}$

Euler phi-function

Reduced System of residues modulo m

- Let $\phi(n)$ be the number of integers in $1, 2, \ldots, n$ that are coprime to n.

- A reduced system of residue modulo n is a set of $\phi(n)$ integers such that each element of the set is relatively prime to n, and no two different elements of the set are congruent modulo n.

$\underline{n=8}$:   1, 3, 5, 7
1, 3, -3, -1
1, 11, -3, 15.

unit group
$U(n)$

[Every element in a r.s.r. mn has an inverse
& the inverse is congruent to an element in the set.

Reduced System of residues modulo m

- Let $\phi(n)$ be the number of integers in $1, 2, \ldots, n$ that are coprime to n.
- A reduced system of residue modulo n is a set of $\phi(n)$ integers such that each element of the set is relatively prime to n, and no two different elements of the set are congruent modulo n.
- Ex: If $r_1, \ldots, r_m$ is a reduced system of residues modulo m, and if $a \in N$ and $(a, m) = 1$, then $ar_1, ar_2, \ldots, ar_m$ is a reduced system of residues modulo m.

① $(ar_i, m) = (r_i, m) = 1$

② $ar_i \equiv ar_j \pmod{m} \iff r_i \equiv r_j \pmod{m} \iff i = j$

- Wilson's Theorem: If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

Pf: For each $i \in \{1, 2, \dots, p-1\}$, $i^{-1} \in \{1, 2, \dots, p-1\}$.

So if $i^{-1} \neq i$, then $i \cdot i^{-1} \equiv 1 \pmod{p}$.

Consider $\underline{x \in \{1, 2, \dots, p-1\}}$ s.t. $x^{-1} \equiv x \pmod{p}$

$\boxed{x^2 \equiv 1 \pmod{p}} \Rightarrow p \mid x^2 - 1 = (x-1)(x+1)$

$\Rightarrow p \mid x-1$ or $p \mid x+1$ (Euclid Lemma)

$\Rightarrow x \equiv 1$ or $-1 \pmod{p}$

$\Rightarrow x = 1$ or $p-1$.

So $(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$

- Wilson's Theorem: If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

- Let $n \geq 2$ be a positive integer. Then $(n-1)! \equiv -1 \pmod{n}$ if and only if n is a prime.

Pf. Let $(n-1)! \equiv -1 \pmod{n}$.

Suppose that n is not a prime. Let $n = n_1 n_2$, $n_1, n_2 > 1$

If $n_1 \neq n_2$. $(n-1)! = 1 \cdots n_1 \cdots n_2 \cdots (n-1) \equiv 0 \pmod{n}$

If $n_1 = n_2$. Then $n = p^2$ for some prime p.

Then $(n-1)! = 1 \cdots p \cdots (p^2-1)$ is a multiple of p, so not congruent to $-1 \bmod p^2$.

- Wilson's Theorem: If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

- Let $n \geq 2$ be a positive integer. Then $(n-1)! \equiv -1 \pmod{n}$ if and only if n is a prime.

- More general, If $r_1, \ldots, r_{p-1}$ is a reduced system of residues modulo p, then $r_1 r_2 \cdots r_{p-1} \equiv -1 \pmod{p}$.

$r_1 r_2 \cdots r_{p-1} = \prod_{r_i^{-1} \neq r_i} (r_i \cdot r_i^{-1}) \cdot \left(\prod_{r_i = r_i^{-1}} r_i\right) \equiv \prod_{x^2 \equiv 1} x \pmod{p} \equiv 1 \cdot (-1) \equiv -1$

Consider $x^2 \equiv 1 \pmod{p} \Rightarrow p \mid x^2 - 1 = (x-1)(x+1) \Rightarrow p \mid x-1$ or $p \mid x+1 \pmod{p}$

$\Rightarrow p \equiv 1$ or $p \equiv -1 \pmod{p}$

- THM: let $r_1, r_2, \ldots, r_{\phi(m)}$ be a reduced system of residues modulo $m = p^l$, where p is odd prime, then $\prod_i r_i \equiv -1 \pmod{p^l}$.

Pf: $\prod_i r_i = \left(\prod_{r_i^{-1} \neq r_i} r_i r_i^{-1}\right) \cdot \left(\prod_{r_i^{-1} = r_i} r_i\right) \equiv \prod_{x^2=1} x \pmod{p^l}$

Consider $x^2 \equiv 1 \pmod{p^l} \Rightarrow p^l \mid x^2 - 1 = (x-1)(x+1)$

$(x-1, x+1) = (x-1, 2) = 1$ or 2.

If $(x-1, x+1) = 1$, then $p^l \mid x-1$ or $p^l \mid x+1 \Rightarrow x \equiv 1$ or $-1 \pmod{p^l}$

$\boxed{\text{If } (x-1, x+1) = 2, \text{ then } \left(\frac{x-1}{2}, x+1\right) = 1 \text{ or } \left(x-1, \frac{x+1}{2}\right) = 1}$

In either case, $p^l \mid x-1$ or $p^l \mid x+1$. So $x \equiv 1$ or $-1 \pmod{p^l}$

So $\prod_i r_i \equiv \prod_{x^2 \equiv 1} x \equiv 1 \cdot (-1) \equiv -1 \pmod{p^l}$.

- THM: let $r_1, r_2, \ldots, r_{\phi(m)}$ be a reduced system of residues modulo $m = p^l$, where p is odd prime, then $\prod_i r_i \equiv -1 \pmod{p^l}$.
- THM: let $r_1, r_2, \ldots, r_{\phi(m)}$ be a reduced system of residues modulo $m = 2p^l$, where p is odd prime, then $\prod_i r_i \equiv -1 \pmod{2p^l}$.

(hw)

So $x \equiv 1, -1 \bmod 2^l$
or $1, -1 \bmod 2^{l-1}$

- THM: let $r_1, r_2, \ldots, r_{\phi(m)}$ be a reduced system of residues modulo $m = 2^l$, where $l \geq 3$, then $\prod_i r_i \equiv 1 \pmod{2^l}$.

$1 \cdot (-1) \cdot (1 + k \cdot 2^{l-1})(-1 + t \cdot 2^{l-1}) \equiv (-1)(-1 + (k+t) 2^{l-1} + kt 2^{2l-2})$ k, l odd

$\equiv (-1)(-1)$
$\equiv 1 \pmod{2^l}$

Pf: $\prod_i r_i = \left(\prod_{r_i^{-1} \neq r_i} (r_i \cdot r_i^{-1})\right)\left(\prod_{r_i^{-1} = r_i} r_i\right) \equiv \prod_{x^2 \equiv 1} x \pmod{2^l}$

consider $x^2 \equiv 1 \pmod{2^l} \Rightarrow 2^l \mid x^2 - 1 = (x-1)(x+1)$

Note that $(x-1, x+1) = 2$ or 1

1. If $(x-1, x+1) = 1$, then $2^l \mid x-1$ or $2^l \mid x+1 \Rightarrow x \equiv 1$ or $-1 \pmod{2^l}$

2. If $(x-1, x+1) = 2$, then $\left(\frac{x-1}{2}, x+1\right) = 1$ or $\left(x-1, \frac{x+1}{2}\right) = 1$.

2.1 $\left(\frac{x-1}{2}, x+1\right) = 1$: $2^{l-1} \mid \frac{x-1}{2} \cdot (x+1) \Rightarrow 2^{l-1} \mid \frac{x-1}{2}$ or $2^{l-1} \mid x+1 \Rightarrow x \equiv 1 \bmod 2^l$ or $x \equiv -1 \bmod 2^{l-1}$

2.2 $\left(x-1, \frac{x+1}{2}\right) = 1$: $2^{l-1} \mid (x-1) \cdot \frac{x+1}{2} \Rightarrow 2^{l-1} \mid x-1$ or $2^{l-1} \mid \frac{x+1}{2} \Rightarrow x \equiv 1 \pmod{2^{l-1}}$ or $x \equiv -1 \pmod{2^l}$

- Ex: let, $r_1, r_2, \ldots, r_{p-1}$ and, $r_1', r_2', \ldots, r_{p-1}'$ are two complete system of residues modulo p, where p is odd prime, then, $r_1 r_1', r_2 r_2', \ldots, r_{p-1} r_{p-1}'$ is not a complete system of residues modulo p.

Pf: Assume that $r_1 r_1', \ldots, r_{p-1} r_{p-1}'$ is a reduced system.

Note that $r_1, \ldots, r_{p-1}$ & $r_1', \ldots, r_{p-1}'$ are reduced systems.

By Wilson's Theorem, $r_1 r_2 \cdots r_{p-1} \equiv -1 \pmod p$
$r_1' r_2' \cdots r_{p-1}' \equiv -1 \pmod p$

& $(r_1 r_1') \cdots (r_{p-1} r_{p-1}') \equiv -1 \pmod p$

$\wr\wr$

$(r_1 \cdots r_{p-1})(r_1' \cdots r_{p-1}') \equiv (-1)\cdot(-1) \equiv 1$

$\Rightarrow 1 \equiv -1 \pmod p$, a contradiction to the fact that p is odd

- Ex: let p be an odd prime. Then

$$1^2 \cdot 3^2 \cdot \ldots (p-2)^2 \equiv (-1)^{(p+1)/2} \pmod{p}$$

$$(p-1)! = 1\cdot 2\cdot 3 \cdots (p-2)(p-1)$$

$$= [1\cdot(p-1)]\cdot[2\cdot(p-2)]\,[3\cdot(p-3)]\cdots\left[\tfrac{p-1}{2}\cdot\tfrac{p+1}{2}\right]$$

$$\equiv [1\cdot(-1)]\cdot[(-1)\cdot(p-2)^2]\,[3\cdot(-3)]\cdots\left[\tfrac{p-1}{2}\cdot(-1)\tfrac{p-1}{2}\right] \pmod{p}$$

$$= (-1)^{\frac{p-1}{2}}\cdot 1^2\cdot(p-2)^2\cdot 3^2\cdots\left(\tfrac{p-1}{2}\right)^2$$

$$= (-1)^{\frac{p-1}{2}}\cdot 1^2\cdot 3^2\cdots(p-2)^2 \pmod{p}$$

$$\Rightarrow 1^2\cdot 3^2\cdots(p-2)^2 \equiv (-1)^{\frac{p-1}{2}}\cdot(p-1)! \underset{\text{thm}}{\overset{\text{Wilson's}}{=\!=\!=}} (-1)^{\frac{p-1}{2}}\cdot(-1) = (-1)^{\frac{p+1}{2}} \pmod{p}$$

- Ex: find the least nonnegative residue of 70! (mod 5183). (Note that $5183 = 71 \cdot 73$)

$$70! \equiv t \pmod{5183} \iff \begin{cases} 70! \equiv t \pmod{71} \\ 70! \equiv t \pmod{73} \end{cases}$$

$$\boxed{\text{By Wilson's thm } t \equiv 70! \equiv -1 \pmod{71}}$$

$$\Rightarrow 71 \cdot 72 \cdot t \equiv 70! \cdot 71 \cdot 72 \pmod{73}$$

$$\Rightarrow (-2)(-1)t \equiv 72! \pmod{73}$$

$$\Rightarrow 2t \equiv (-1) \pmod{73}$$

$$\Rightarrow t \equiv 36 \pmod{73}$$

$$\Rightarrow \begin{cases} t \equiv -1 \pmod{71} \\ t \equiv 36 \pmod{73} \end{cases} \xrightarrow{\text{CRT}} t \equiv 73 \cdot 36 \cdot (-1) + 71 \cdot 36 \cdot 36 \pmod{71 \cdot 73} \equiv 2591 \pmod{5183}$$

$m_1 = 71,\ M_1 = 73,\ M_1^{-1} \equiv 36$ $\qquad 73 \cdot M_1^{-1} \equiv 1 \pmod{71} \Rightarrow 2M_1^{-1} \equiv 1 \pmod{71}$

$m_2 = 73,\ M_2 = 71,\ M_2^{-1} = 36$ $\qquad 71 \cdot M_2^{-1} \equiv 1 \pmod{73} \Rightarrow -2M_2^{-1} \equiv 1 \pmod{73}$

- Fermat Little Theorem: Let p be a prime and $(a, p) = 1$. Then

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

Pf: Consider $r_1, r_2, \cdots, r_{p-1}$, a reduced system of residues mod p.

Then $ar_1, ar_2, \cdots, ar_{p-1}$ is also a r.s.o.r. mod p.

Then $(ar_1)(ar_2)\cdots(ar_{p-1}) \equiv -1 \pmod p$ by Wilson's Thm.

$a^{p-1} \cdot (\underline{r_1 r_2 \cdots r_{p-1}}) \equiv -1 \pmod p \Rightarrow a^{p-1} \cdot (-1) \equiv -1 \pmod p$

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

Cor: a^{p-2} is an inverse of $a \pmod p$!