Lecture 6 Friday, 12/8/2022

Note Title 8/11/2022

<u>Theorem 1</u>: Let $\gcd(a,m)=1$. Let $\{x_1, x_2, \ldots, x_m\}$ be a complete residue system modulo m. Then $\{ax_1, \ldots, ax_m\}$ is again a complete residue system mod m. If $\{r_1, \ldots, r_{\varphi(m)}\}$ is a reduced residue system modulo m, then $\{ar_1, \ldots, ar_{\varphi(m)}\}$ is also a reduced residue system modulo m.

<u>Proof</u>: We need to prove that $ax_i \not\equiv ax_j \pmod{m}$ whenever $i \neq j$.

Let $ax_i \equiv ax_j \pmod{m}$. Since $\gcd(a,m)=1$, so $x_i \equiv x_j \pmod{m}$.

Since, $\{x_1, \ldots, x_m\}$ is a complete residue system modulo m, so

$$x_i \not\equiv x_j \pmod{m} \text{ whenever } i \neq j.$$

$\therefore$ $ax_i \not\equiv ax_j \pmod{m}$ whenever $i \neq j$.

$\Rightarrow \{ax_1, \ldots, ax_m\}$ is a complete residue system modulo m.

Let $\{r_1, \ldots, r_{\varphi(m)}\}$ be a reduced residue system modulo m.

Since $\gcd(a, m) = 1$ and $\gcd(r_i, m) = 1$ $\forall i$, so $\gcd(ar_i, m) = 1$ $\forall i$.

Also, $ar_i \equiv ar_j \pmod{m} \Rightarrow r_i \equiv r_j \pmod{m}$.

Since $r_i \not\equiv r_j \pmod{m}$ if $i \neq j$, so $ar_i \not\equiv ar_j \pmod{m}$ if $i \neq j$.

$\therefore \{ar_1, \ldots, ar_{\varphi(m)}\}$ is a reduced residue system modulo m.

#

———x———

<u>Theorem 2 (Fermat's little theorem)</u>: Let p be a prime. Let a be an integer such that $p \nmid a$ (that is, $\gcd(p, a) = 1$). Then $a^{p-1} \equiv 1 \pmod{p}$.

<u>Proof</u>: Let $p = 2$. Then $p \nmid a \Rightarrow a$ is odd and hence $a^{p-1} = a^1 \equiv 1 \pmod{2}$.

Hence, the result is true if $p = 2$.

Let $p \geq 3$. Then, $\{1, 2, \dots, p-1\}$ is a reduced residue system mod p.
Since $\gcd(a, p) = 1$, so $\{1 \cdot a, 2 \cdot a, \dots, (p-1) \cdot a\}$ is also a reduced residue system modulo p.

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

$\Rightarrow a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$

$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$ $(\because \gcd(p, (p-1)!) = 1)$

__Corollary:__ For any integer a, $a^p \equiv a \pmod{p}$.

__Proof:__ If $\gcd(a, p) = 1$, then by Fermat's theorem, $a^{p-1} \equiv 1 \pmod{p}$
$\Rightarrow a^p \equiv a \pmod{p}$.

If $\gcd(a, p) \neq 1$, then $p \mid a$.

Hence, $p \mid (a^p - a) \Rightarrow a^p \equiv a \pmod{p}$.

#

__Theorem 3__ (Euler's generalization to Fermat's theorem):

Let $m \geq 1$. If $\gcd(a, m) = 1$, then $a^{\varphi(m)} \equiv 1 \pmod{m}$.

__Proof__: Let $\{r_1, \ldots, r_{\varphi(m)}\}$ be a reduced residue system modulo m.

Then, $\{ar_1, \ldots, ar_{\varphi(m)}\}$ is a reduced residue system modulo m.

$\therefore \quad ar_1 \cdot ar_2 \cdot \cdots \cdot ar_{\varphi(m)} \equiv r_1 \cdot r_2 \cdot \cdots \cdot r_{\varphi(m)} \pmod{m}$

$\Rightarrow \quad a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}$.

Since $\gcd(r_i, m) = 1$ for all $i = 1, 2, \ldots, \varphi(m)$, so $\gcd\left(\prod_{i=1}^{\varphi(m)} r_i, m\right) = 1$.

$\therefore \quad a^{\varphi(m)} \equiv 1 \pmod{m}$.

#

<u>Ex 1:</u> Prove that $17 \mid (11^{104} + 1)$.

<u>Solution:</u> $a = 11$, $p = 17$. By Fermat's theorem, $11^{16} \equiv 1 \pmod{17}$

Now, $104 = 16 \times 6 + 8$. Hence, $11^{104} = (11^{16})^6 \cdot 11^8 \equiv 11^8 \pmod{17}$

$\Rightarrow 11^{104} \equiv (-6)^8 \pmod{17} \equiv 36^4 \pmod{17} \equiv 2^4 \pmod{17} \equiv -1 \pmod{17}$

$\Rightarrow 11^{104} + 1 \equiv 0 \pmod{17} \Rightarrow 17 \mid (11^{104} + 1)$.

#

<u>Lemma 1:</u> Let p be a prime. Then, $x^2 \equiv 1 \pmod{p} \Leftrightarrow x \equiv \pm 1 \pmod{p}$.

<u>Proof:</u> If $x \equiv \pm 1 \pmod{p}$, then $x^2 \equiv 1 \pmod{p}$.

Conversely, suppose that $x^2 \equiv 1 \pmod{p}$. Then, $p \mid (x-1)(x+1)$.

$\Rightarrow p \mid (x-1)$ or $p \mid (x+1) \Rightarrow x \equiv \pm 1 \pmod{p}$.

#

<u>Lemma 2</u>: Given an integer a, the congruence $ax \equiv 1 \pmod{m}$ has a solution if and only if $\gcd(a,m) = 1$. Furthermore, if x_0 and x_1 satisfy $ax \equiv 1 \pmod{m}$, then $x_0 \equiv x_1 \pmod{m}$.

<u>Proof</u>: We know that $\gcd(a,m) = 1 \Leftrightarrow ax_0 + my_0 = 1$ for some $x_0, y_0 \in \mathbb{Z}$.

$\Leftrightarrow ax_0 \equiv 1 \pmod{m}$. Hence, $ax \equiv 1 \pmod{m}$ has a solution $\Leftrightarrow \gcd(a,m) = 1$.

Let $\gcd(a,m) = 1$, and $ax_0 \equiv 1 \pmod{m}$ and $ax_1 \equiv 1 \pmod{m}$.

Then, $ax_0 \equiv ax_1 \pmod{m}$

$\Rightarrow x_0 \equiv x_1 \pmod{m}$ since $\gcd(a,m) = 1$.

$\#$

Theorem 4 (Wilson's theorem): For a prime p, $(p-1)! \equiv -1 \pmod p$.

Proof: If $p=2$, then $(p-1)! = 1 \equiv -1 \pmod 2$.
If $p=3$, then $(p-1)! = 2 \equiv -1 \pmod 3$.
Hence, the result is true if $p=2,3$.

So, let $p \geq 5$.

Let $a \in \{1, 2, \cdots, p-1\}$. For each a, the equation $ax \equiv 1 \pmod p$ has an unique solution $b \in \{1, 2, \cdots, p-1\}$.

If $a = b$, then $a^2 \equiv 1 \pmod p \Leftrightarrow a = 1$ or $a = p-1$. (by Lemma 1).

Thus, for every $a \in \{2, 3, \cdots, p-2\}$, there exists unique $b \in \{2, 3, \cdots, p-2\}$ such that $ab \equiv 1 \pmod p$.

Now,
$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot (p-2)(p-1) = (p-1)\overbrace{\left[2 \cdot 3 \cdots (p-2)\right]}^{\frac{p-3}{2} \text{ pairs and each pair contribute } 1 \bmod p.}$$
$$\equiv p-1 \pmod p \equiv -1 \pmod p.$$

#

Theorem 5: Let p be a prime. Then, $x^2 \equiv -1 \pmod{p}$ has solutions if and only if $p=2$ or $p \equiv 1 \pmod{4}$.

Proof: If $p=2$, then $x=1$ satisfies $x^2 \equiv -1 \pmod{p}$.
Let $p \geq 3$. By Wilson's theorem, we have

$$\left(1 \cdot 2 \cdot \cdots j \cdots \frac{p-1}{2}\right)\left(\frac{p+1}{2} \cdots (p-j) \cdots (p-2)(p-1)\right) \equiv -1 \pmod{p}$$

$$\Rightarrow \prod_{j=1}^{\frac{p-1}{2}} j(p-j) \equiv -1 \pmod{p}$$

$$\Rightarrow \prod_{j=1}^{\frac{p-1}{2}} j(-j) \equiv -1 \pmod{p} \Rightarrow (-1)^{\frac{p-1}{2}} \prod_{j=1}^{\frac{p-1}{2}} j^2 \equiv -1 \pmod{p}$$

Since $p \equiv 1 \pmod{4}$, so $(-1)^{\frac{p-1}{2}} = 1$ and hence $\left(\prod_{j=1}^{\frac{p-1}{2}} j\right)^2 \equiv -1 \pmod{p}$.

$\Rightarrow x = \left(\frac{p-1}{2}\right)!$ is a solution of $x^2 \equiv -1 \pmod{p}$.

Conversely, suppose that $x^2 \equiv -1 \pmod p$ has a root, say x_0. Then, $\gcd(x_0, p) = 1$. If $p \geq 3$, then

$$(-1)^{\frac{p-1}{2}} \equiv (x_0^2)^{\frac{p-1}{2}} \pmod p \equiv x_0^{p-1} \equiv 1 \pmod p$$

(By Fermat's theorem)

$\Rightarrow \dfrac{p-1}{2}$ is even

$\Rightarrow p = 4k+1$ for some $k \geq 1$.

This completes the proof. $\neq$