Bharathidasan University
Tiruchirappalli - 620 024
Tamil Nadu, India

Programme: M.Sc., Mathematics

Course Title :Theory of Numbers
COurse Code : 21M04CC

Fermat's Theorem and Consequences

Dr. V. Piramanantham
Professor
Department of Mathematics

Euler's generalization of Fermat's Theorem

Theorem If $(a, m)=1$, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Proof: (outline)

$A = \{ r_1, r_2 \cdots r_{\varphi(m)} \}$ — RRS

$(a, m) = 1$

$B = \{ ar_1, ar_2 \cdots ar_{\varphi(m)} \}$ — RSS

$a_i \equiv b_i$

$\Rightarrow \prod a_i \equiv \prod b_i$

$\cancel{a}x \equiv \cancel{a}y$

$(a, m) = 1$

A is RSS

for each i, $(a, m) = 1, (r_i, m) = 1$

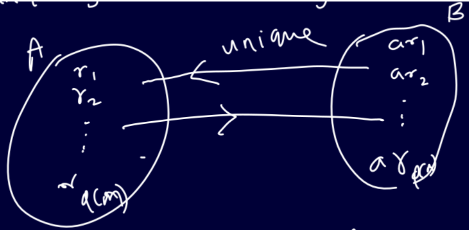
$(ar_i, m) = 1$

$\therefore$

$\exists$ unique j st $ar_i \equiv r_j \pmod{m}$

B

unique



B is RSS $\Rightarrow$ for each $r_k \in A$

$\exists$ unique $ar_l \in B$

s.t. $r_k \equiv ar_l \pmod{m}$

there is a bijection betn A & B

the bijection fn $f(r_i) \equiv ar_j$

$f : A \to B$

B is RRS $\Rightarrow$ f is 1-1

A is RRS $\Rightarrow$ f is onto

each member $ar_1, ar_2, \ldots, ar_{\phi(m)}$

is congruent to one member of

$r_1, r_2, \ldots, r_{\phi(m)}$, not necessarily

in same order

$$ar_1 \, ar_2 \cdots ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod m$$

$$a^{\phi(m)} r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod m \quad \text{—} (*)$$

$$ar_1\, ar_2 \cdots ar_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m}$$

$$a^{\phi(m)}\, r_1 r_2 \cdots r_{\phi(m)} \equiv r_1 r_2 \cdots r_{\phi(m)} \pmod{m} \quad \text{— } \circledast$$

Since $(r_i, m) = 1$, $\left(\prod_{i=1}^{\phi(m)} r_i, m\right) = 1$

Σ - Π

sum prod

cancelling $\prod_{i=1}^{\phi(m)} r_i$ in $\circledast$,

$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Fermat's Theorem: Let p be prime.

If $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$

For any a, $a^{p} \equiv a \pmod{p}$

Proof $m = p$, $\phi(p) = p-1$

$\{1, 2, \ldots, p-1\}$ RRS $(\bmod\ p)$

$p \nmid a \Rightarrow (a, p) = 1$

Euler's gen. $\Rightarrow$ $a^{p-1} \equiv 1 \pmod{p}$

of p

For any p, if $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$

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

$p \mid a$, $a = kp \Rightarrow a \equiv 0 \pmod{p}$

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

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

Theorem

(1) $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$

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

(2) a,

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

$$(a, p) = 1$$

$$\Rightarrow a \cdot a^{p-2} \equiv 1 \pmod{p}$$

$$b = a^{p-2}, \quad \boxed{ab \equiv 1 \pmod{p}}$$

$$\boxed{xy \equiv 1 \Rightarrow y \text{ is the inverse of } x}$$

b is the multiplicative inverse (mod p)

Definition Let $(a, m) = 1$. Then an integer $b \pmod{m}$ is called the multiplicative inverse of $a \pmod{m}$ if

$$ab \equiv 1 \pmod{m}.$$

Theorem: (1) If $(a, m) = 1$, then there is an integer x such that

$$ax \equiv 1 \pmod{m}$$

(2) If there is another integer y s.t.

$$ay \equiv 1 \pmod{m}$$

then $x \equiv y \pmod{m}$

(3) If $(a, m) > 1$, there is no such x.

Proof: ① $(a, m) = 1$

$\exists\, x$ & z s.t. $ax + mz = 1$

$\Rightarrow ax - 1 = mz$

$$\Rightarrow \quad ax \equiv 1 \pmod m \quad - (1)$$

(2) $\exists$ another y s.t. $\quad ay \equiv 1 \pmod m \quad - (2)$

From eqns (1) & (2),

$$ax \equiv ay \pmod m$$

$(a, m) = 1$, $\qquad x \equiv y \pmod m$

Note: If $\quad ab \equiv 1 \pmod m$

b is ~~the multiplicative~~ $\quad (*)$

** then $b \pmod m$ is the multiplicative inverse of $a \pmod m$

b	$b \pmod m$
b only	$\ldots b-2m, b-m, b, b+m, b+2m, \ldots$ arithmetic progression of b with c.d. m.

(3) If $(a, m) > 1$, $\nexists$ no x s.t. $ax \equiv 1 \pmod m$

Proof suppose $\exists\ x$ s.t.

$$ax \equiv 1 \pmod m$$

$$\Rightarrow m \mid ax - 1$$

$\exists\ z' \in \mathbb{Z}$ s.t.

$$ax - 1 = mz'$$

$$\Rightarrow ax - mz' = 1$$

$z = -z'$

$$\Rightarrow ax + mz = 1$$

Bezout's Thm

$(a,b) = g \Downarrow$

$\exists\ x \,\&\, y$ s.t.

$ax + by = g$

$\{ \quad / \ x, y \in \mathbb{Z}\}$

$$\longrightarrow 1 \in A$$

$A = \{at + ms \,/\, t, s \in \mathbb{Z}\}$

$t = x,\ s = z$

$at + ms = 1$

$$\Rightarrow (a, m) = 1$$

$$\Rightarrow \Leftarrow$$

to $(a, m) > 1$

$A = \{ax+by \mid \ldots\}$
Smallest +ve integ- g

$\nexists$ no x s.t. $ax \equiv 1 \pmod m$

The multiplicative inverse exists for all a s.t. $(a, m) = 1$

a^{-1}

$\boxed{1 \le a \le m}$

The multiplicative inverse of $a \pmod m$ is denoted by $\bar{a}$

$$a\bar{a} \equiv 1 \pmod{m}$$

$p | a$, a^{p-2} is the multiplicative inverse $\pmod{p}$

$(a, m) = 1$, $a^{\phi(m)} \equiv 1 \pmod{m}$

$\Rightarrow a^{\phi(m)-1}$ is the multiplicative inverse $\pmod{m}$

p is prime

$$p \mid ab \Rightarrow p \mid a \text{ or } p \mid b$$

$$a = 1 \Rightarrow \bar{a} = 1 \pmod{p}$$

$$a = -1 \Rightarrow \bar{a} = -1$$

$$(-1)(-1) \equiv 1 \pmod{p}$$

$\bar{a}$

$a \equiv b$

$\Rightarrow a - b \equiv 0$

$m \mid 0$

$\Leftarrow \Rightarrow m \mid a - b$

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

$a = -1, \quad \bar{a} = p-1$

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

$a = p-1, \quad \bar{a} = -1 \equiv p-1$

$a = p-1, \quad \bar{a} = p-1$

$$\boxed{\begin{array}{l} \bar{1} = 1 \\ \overline{p-1} = p-1 \quad \text{or} \quad \overline{-1} = -1 \end{array}}$$

If x is its own multiplicative inverse $(\text{mod } p)$,

$x^2 \equiv 1 \pmod{p}$

$\bar{x} = x$

$x\bar{x} \equiv 1$

$x^2 \equiv 1$

Converse

If x is an int s.t.

$x^2 \equiv 1 \pmod{p}$

$p \mid x^2 - 1$

$p \mid (x-1)(x+1)$

$\Rightarrow p \mid x-1$ or $p \mid x+1$

$\Rightarrow x \equiv 1$ or $x \equiv -1 \equiv p-1$

If $x^2 \equiv 1 \pmod{p}$, $x = 1$ & $x = p-1$ are their own invers

$1 \leq a \leq p-1 \quad , \quad (a, p) = 1$

$\{1, 2, \ldots \; p-1\}$

Among the integers $1, 2, \ldots, p-1$

1 & $p-1$ are the only integers

with their own inverse

$1 < a < p-1, \quad \bar{a} \neq a$