CLASS: Msc MATHEMATICS IV SEM

SUBJECT CODE: H-4049
SUBJECT NAME: NUMBER THEORY

TAUGHT BY:DR SATISH KUMAR
ASSOCIATE PROFESSOR
DEPARTMENT OF MATHEMATICS
DN PG COLLEGE MEERUT

Fermat's Factorization method

Let n be an odd integer then

$$n = x^2 - y^2 = (x-y)(x+y)$$

$$\Rightarrow x^2 - n = y^2$$

select x as $x_1 < \sqrt{n} < x$

then search y such that

$$x^2 - n = y^2$$

$$\Rightarrow x^2 - y^2 = n \Rightarrow n = (x-y)(x+y)$$

ex (1) $n = 10541$

Solution Given $n = 10541$

To find factors of n

We observe that $102 < \sqrt{10541} < 103$

not a perfect sq

so $103^2 - 10541 = 10609 - 10541 = 68$

$104^2 - 10541 = 10816 - 10541 = 275$, not a perfect sq

$105^2 - 10541 = 11025 - 10541 = 484 = 22^2$, a perfect sq

ii $105^2 - 22^2 = 10541$

$\Rightarrow 10541 = 105^2 - 22^2 = (105-22)(105+22)$

$10541 = 83 \times 127$

which is required factors of 10541.

(2) Factorize $(2^{11}-1)$ by Farmat's method.

Sol Let $n = 2^{11} - 1 = 2048 - 1 = 2047$

$45^2 < \sqrt{2047} < 46^2$

ii $46^2 - 2047 = 69$, not a perfect square

$47^2 - 2047 = 162$, not a perfect square

$48^2 - 2047 = 257$, not a perfect square

$49^2 - 2047 = 354$, not a perfect square

$50^2 - 2047 = 453$, not a perfect square

$51^2 - 2047 = 554$, not a perfect square

$52^2 - 2047 = 657$, not a perfect square
$53^2 - 2047 = 762$, not a perfect square
$54^2 - 2047 = 869$, not a perfect square
$55^2 - 2047 = 978$, not a perfect square
$56^2 - 2047 = 1089 = 33^2$, a perfect square

$\Rightarrow 56^2 - 33^2 = 2047$

$\Rightarrow 2047 = 56^2 - 33^2 = (56-33)(56+33)$

$\Rightarrow 2047 = (23) \times (89)$

which is required factorization of $(2^{11}-1)$. Ans.

* State and prove Fermat's Theorem (OR Fermat's little theorem)

Statement. If p is a prime, a is positive integer

Let $(a, p) = 1$ then $a^{p-1} \equiv 1 \pmod{p}$

Proof. Let p is a prime. Let $(a, p) = 1$

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

We know that

$$(x_1+x_2)^p = x_1^p + {}^pC_1\, x_1^{p-1} \cdot x_2 + {}^pC_2\, x_1^{p-2} x_2^2 + \cdots + {}^pC_{p-1}\, x_1 \cdot x_2^{p-1} + x_2^p.$$

$(x_1+x_2)^p = x_1^p + x_2^p +$ terms divisible by p.

$\Rightarrow (x_1+x_2)^p \equiv (x_1^p + x_2^p +$ term divisible by $p) \pmod{p}$

$(x_1+x_2)^p \equiv (x_1^p + x_2^p) \pmod{p}$

Similarly $(x_1+x_2+x_3)^p \equiv (x_1^p + x_2^p + x_3^p) \pmod{p}$

— — —

$$(\underbrace{x_1+x_2+x_3+\cdots+x_a}_{\text{total } a \text{ terms}})^p \equiv (x_1^p + x_2^p + x_3^p + \cdots + x_a^p) \pmod{p} \quad \text{— (1)}$$

Putting $x_1 = x_2 = \cdots = x_a = 1$ in (1), we get

$$(\underbrace{1+1+1+\cdots+1}_{\text{total } a \text{ terms}})^p \equiv (\underbrace{1^p+1^p+1^p+\cdots+1^p}_{\text{total } a \text{ terms}}) \pmod{p}$$

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

(3)

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

$\Rightarrow a^{p-1} \equiv 1 \left[\text{mod } \frac{p}{(a,p)}\right]$

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

, proved.

Examples on Fermat's theorem

(1) Show that $(8^{30}-1)$ is divisible by 31.

Soln Let $a=8, p=31 \Rightarrow (8,31)=1$

so by Fermat theorem

$8^{31-1} \equiv 1 \pmod{31}$ [$\because a^{p-1} \equiv 1 \pmod{p}$, p is prime]

$\Rightarrow 8^{30} \equiv 1 \pmod{31}$

$\Rightarrow (31) \mid (8^{30}-1)$. proved.

(2) Find the remainder when 72^{1001} is divided by 31.

Soln To find the remainder when 72^{1001} is divided by 31.

We have $72 \equiv 10 \pmod{31}$

By Fermat's theorem

$10^{30} \equiv 1 \pmod{31}$ [$\because a^{p-1} \equiv 1 \pmod{p}$, p is prime, $(a,p)=1$]

$\Rightarrow (10^{30})^{33} \equiv 1^{33} \pmod{31}$ Here $(10,31)=1$

$\Rightarrow 10^{990} \equiv 1 \pmod{31}$ —— (1)

$1001 = 990 + 8 + 2 + 1$

$\therefore (72)^{1001} \equiv (10)^{1001} \pmod{31}$ [$\because 72 \equiv 10 \pmod{31}$]

$(72)^{1001} \equiv (10^{990} \times 10^{8} \times 10^{2} \times 10^{1}) \pmod{31}$ —— (2)

We also have

$10 \equiv 10 \pmod{31}$ —— (3)

$10^{2} \equiv 7 \pmod{31}$ —— (4)

$10^9 \equiv 7^2 \pmod{31}$

$10^4 \equiv -13 \pmod{31}$

$10^8 \equiv 169 \pmod{31}$

$10^8 \equiv 14 \pmod{31}$ — (5)

[$49 + 31k = 49 - 62$

$169 + 31k$
$169 - 155 = 14$
$k = 5$]

Using (1), (3), (4) & (5)

equation (2) $\Rightarrow$

$(72)^{1001} \equiv (10^{990} \times 10^8 \times 10^2 \times 10) \pmod{31}$

$\equiv (1 \times 14 \times 7 \times 10) \pmod{31}$

$(72)^{1001} \equiv (98 \times 10) \pmod{31}$

$\equiv (5 \times 10) \pmod{31}$

$\equiv 50 \pmod{31}$

[$98 = 98 + 31k$
$= 5 \quad k = -3$]

$(72)^{1001} \equiv (50 + 31k) \pmod{31}$

$\equiv 19 \pmod{31}$

$\Rightarrow$ Required remainder is 19.

(3) If $7 \nmid a$, prove either (a^3+1) or (a^3-1) is divisible by 7.

Solution Given $7 \nmid a \Rightarrow (a, 7) = 1$

$\Rightarrow a^6 \equiv 1 \pmod{7}$ [Fermat's theorem $a^{p-1} \equiv 1 \pmod{p}$, $(a, p) = 1$]

$\Rightarrow 7 \mid (a^6 - 1)$

$\Rightarrow 7 \mid (a^3-1)(a^3+1)$

$\Rightarrow 7 \mid (a^3-1)$ or $7 \mid (a^3+1)$, proved.

(4) Show $5^{38} \equiv 4 \pmod{11}$

Soln To show $5^{38} \equiv 4 \pmod{11}$

Here $a=5$, $p=11$, $(5,11)=1$

$\Rightarrow 5^{11-1} \equiv 1 \pmod{11}$ [Fermat's theorem $a^{p-1} \equiv 1 \pmod{p}$, $(a,p)=1$, p is prime]

$5^{10} \equiv 1 \pmod{11}$

$5^{30} \equiv 1^3 \pmod{11}$

Now $5^{30} \equiv 1 \pmod{11}$ ——— (1)

$5^2 \equiv (25+11k) \pmod{11}$

$5^2 \equiv 3 \pmod{11}$ [For $k=-2$]

$5^4 \equiv 9 \pmod{11}$

$5^8 \equiv 81 \pmod{11}$

$\equiv (81+11k) \pmod{11}$

$5^8 \equiv 4 \pmod{11}$ (For $k=-7$) ——— (2)

ii (1) and (2) $\Rightarrow$

$5^{38} \equiv 1 \times 4 \pmod{11}$

$5^{38} \equiv 4 \pmod{11}$, proved.

(5) Find the remainder 41^{75} is divided by 3.

Solution Let $a=41$, $p=3$ then $(41,3)=1$

$\Rightarrow 41^{3-1} \equiv 1 \pmod{3}$ [Fermat's $a^{p-1} \equiv 1 \pmod{p}$ if $(a,p)=1$]

$\Rightarrow 41^2 \equiv 1 \pmod{3}$

$\Rightarrow (41)^{74} \equiv 1 \pmod{3}$ [$(41^2)^{37} \equiv 1^{37} \pmod{3}$]

Now $(41)^{75} \equiv 41 \times 1 \pmod{3}$

$\equiv (41+3k) \pmod{3}$

$(41)^{75} \equiv 2 \pmod{3}$

So, Required remainder is 2.

(6) Find the remainder when $2^{10,00000}$ is divided by 7.

Sol. To find remainder when $2^{10,00000}$ is divided by 7.

Here $(2,7)=1$, so by Fermat's we have

$$2^6 \equiv 1 \pmod 7 \quad \left[\text{Fermat's } a^{p-1} \equiv 1 \pmod p,\ (a,p)=1,\ a=2\right]$$

$$(2^6)^{166666} \equiv 1^{166666} \pmod 7$$

$$\Rightarrow 2^{999996} \equiv 1 \pmod 7$$

$$\Rightarrow 2^{10,00000} \equiv 2^{9,99,996} \cdot 2^4 \pmod 7$$

$$\equiv 1 \cdot 2^4 \pmod 7$$

$$\equiv 16 \pmod 7$$

$$\equiv (16+7k) \pmod 7$$

$$2^{10,00000} \equiv 2 \pmod 7 \quad (\text{for } k=-2)$$

Req. remainder is 2.

(7) What is the remainder when 3^{287} is divided by 23.

Sol. Here $(3,23)=1$

so by Fermat's

$$3^{22} \equiv 1 \pmod{23} \quad \left[a^{p-1} \equiv 1 \pmod p,\ (a,p)=1,\ p \text{ is prime} \text{ — Fermat's theorem}\right]$$

$$(3^{22})^{13} \equiv 1^{13} \pmod{23}$$

$$3^{286} \equiv 1 \pmod{23}$$

$$\Rightarrow 3^{287} \equiv 3^{286} \times 3^1 \pmod{23}$$

$$3^{287} \equiv 1 \times 3 \pmod{23}$$

$\therefore$ Required remainder is 3.

(08) Find the remainder when 5^{11} is divided by 7

Soln We have (MU 01, 07)

$(5,7) = 1$

$\Rightarrow 5^6 \equiv 1 \pmod 7$ —— (1) [Fermat's $a^{p-1} \equiv 1 \pmod p$, $(a,p)=1$, p is prime]

$5^2 \equiv 25 \pmod 7$

$5^2 \equiv 4 \pmod 7$

$5^4 \equiv 16 \pmod 7$

$5^4 \equiv 2 \pmod 7$ [$\because 16 + 7k \equiv 2 \pmod 7$] —— (2)

$\therefore 5^{11} \equiv 5^6 \times 5^4 \times 5 \pmod 7$

$\equiv 1 \times 2 \times 5 \pmod 7$

$\equiv 10 \pmod 7$

$\equiv (10 + 7k) \pmod 7$

$5^{11} \equiv 3 \pmod 7$ for $k = -1$

$\therefore$ Required remainder is 3.

- **Pseudo prime** Let $(2, n) = 1$ then n is called a (absolute) pseudo prime if

$$2^n \equiv 2 \pmod n$$

ex 341 is pseudo prime as

$2^{341} \equiv 2 \pmod{341}$ [Note $341 = 11 \times 31$]

Note: pseudo prime is not prime but every prime is pseudo prime as $2^p \equiv 2 \pmod p$

Ex (1) Show 561 is an absolute pseudo prime

Sol We have $561 = 3 \times 11 \times 17$

Let $(a,3) = 1 \Rightarrow a^2 \equiv 1 \pmod 3$ —— (1)

$(a,11) = 1 \Rightarrow a^{10} \equiv 1 \pmod{11}$ —— (2)

$(a,17) = 1 \Rightarrow a^{16} \equiv 1 \pmod{17}$ —— (3)

(1) $\Rightarrow a^2 \equiv 1 \pmod 3$

$(a^2)^{280} \equiv 1 \pmod 3$

$\Rightarrow a^{560} \equiv 1 \pmod 3$

$\Rightarrow a^{561} \equiv a \pmod 3$ ——— (4)

(2) $\Rightarrow a^{10} \equiv 1 \pmod{11}$

$\Rightarrow (a^{10})^{56} \equiv 1 \pmod{11}$

$\Rightarrow a^{560} \equiv 1 \pmod{11}$

$\Rightarrow a^{561} \equiv a \pmod{11}$ ——— (5)

(3) $\Rightarrow a^{16} \equiv 1 \pmod{17}$

$(a^{16})^{35} \equiv 1 \pmod{17}$

$\Rightarrow a^{560} \equiv 1 \pmod{17}$

$\Rightarrow a^{561} \equiv a \pmod{17}$

(4), (5) & (6) $\Rightarrow$ ——— (6)

$a^{561} \equiv a \bmod (3 \times 11 \times 17)$

$\Rightarrow a^{561} \equiv a \pmod{561}$

$\Rightarrow$ 561 is absolutely pseudo prime

$\left[\begin{array}{l} a \equiv b \pmod{m_1} \\ a \equiv b \pmod{m_2} \\ a \equiv b \pmod{m_3} \end{array}\right] \Rightarrow a \equiv b \pmod{m_1 m_2 m_3}$, $(m_i, m_j) = 1$, $i \neq j$

Ex (2). Show 1729 is an absolute pseudo prime

Soln. $1729 = 7 \times 13 \times 19$

$(a,7) = 1 \Rightarrow a^6 \equiv 1 \pmod 7$ — (1), if $(a,7) = 1$, $(a,13) = 1$, $(a,19) = 1$

$(a,13) = 1 \Rightarrow a^{12} \equiv 1 \pmod{13}$ — (2)

$(a,19) = 1 \Rightarrow a^{18} \equiv 1 \pmod{19}$ — (3)

(1) $\Rightarrow$ $a^6 \equiv 1 \pmod 7$

$(a^6)^{288} \equiv 1 \pmod 7$

$a^{1729} = a^{1728} \cdot a \equiv a \pmod 7$ ——— (4)

(2) $\Rightarrow$ $a^{12} \equiv 1 \pmod{13}$

$(a^{12})^{144} \equiv 1 \pmod{13}$

$\Rightarrow a^{1728} \equiv 1 \pmod{13}$

$\Rightarrow a^{1729} \equiv a \pmod{13}$ ——— (5)

(3) $\Rightarrow a^{18} \equiv 1 \pmod{19}$

$(a^{18})^{96} \equiv 1 \pmod{19}$

$a^{1728} \equiv 1 \pmod{19}$

$a^{1729} \equiv a \pmod{19}$ ——— (6)

(4), (5) & (6) $\Rightarrow$

$a^{1729} \equiv a \pmod{7 \times 13 \times 19}$

$\Rightarrow a^{1729} \equiv a \pmod{1729}$

$\Rightarrow$ 1729 is a absolutely pseudo prime.

[If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, $a \equiv b \pmod{m_3}$ $\Rightarrow a \equiv b \pmod m$, $m = m_1 m_2 m_3$, $(m_i, m_j) = 1$, $i \neq j$]

(10) Number Theory
Dr Satish Kr Gupta

State and prove Wilson's Theorem

Statement. If p is a prime then $\lfloor p-1 \equiv -1 \pmod p$ i.e. $p \mid \{\lfloor p-1 + 1\}$

Proof. Let p is prime, let a be any integer such that $1 \le a \le p-1$ then $(a, p) = 1$

$\Rightarrow$ $ax \equiv 1 \pmod p$ has a unique solution modulo p, ——— (1)

Let b be the unique solution of (1), we have

$$a.b \equiv 1 \pmod p$$

If put $b = a$, we have

$$a^2 \equiv 1 \pmod p \quad \text{——— (2)}$$

$$\Rightarrow p \mid (a^2 - 1) \Rightarrow p \mid (a-1) \text{ (i) or } p \mid (a+1) \text{ (ii)}$$

If $p \mid (a-1) \Rightarrow a \equiv 1 \pmod p$ ——— (3)

OR, $p \mid (a+1) \Rightarrow a \equiv -1 \pmod p$

$\Rightarrow a \equiv p-1 \pmod p$ [$\because a \equiv -1 \pmod p \Rightarrow a = -1 + pk$ for $k = 1$, $a = p-1$] ——— (4)

Here we observe that

if $S = \{2, 3, 4, \cdots, (p-2)\}$

then for each $b \in S$, $\exists\ b' \in S$ such that

$$bb' \equiv 1 \pmod p$$

as $2 \le b \le p-2$

$2 \le b' \le p-2$

$\Rightarrow 2 \times 3 \times 4 \times \cdots \times (p-2) \equiv 1 \pmod p$

$\Rightarrow \lfloor p-2 \equiv 1 \pmod p$

$\Rightarrow (p-1) \lfloor p-2 \equiv (p-1) \pmod p$

$\Rightarrow \lfloor p-1 \equiv (p-1) \pmod p$

$\equiv (p-1+pk) \pmod p$

$\lfloor p-1 \equiv -1 \pmod p$ [For $k = (-1)$]

This proves the Wilson's theorem.

Ex. Take $p = 7$
$S = (2, 3, 4, 5)$ ($p-2 = 7-2 = 5$)
Take $b = 2$
$\Rightarrow \exists\ b' = 4$ s.t
$bb' \equiv 1 \pmod 7$
$b = 3$, $b' = 5$

[$a \equiv b \pmod p \Rightarrow ac \equiv bc \pmod p$, c is positive integer]

(2) Converse of Wilson's theorem

If $\{m \mid \lfloor m-1 + 1\}$ then m must be prime

Proof. Suppose $m \mid \{\lfloor m-1 + 1\}$ ——— (1)

To prove m must be prime

Suppose if possible m is a composite number

$\Rightarrow$ m has atleast three factors namely 1, m and any other factor say d such that $1 < d \leq (m-1)$

$\Rightarrow d \mid 1.2.3.4.\ldots.(m-1)$

$\Rightarrow d \mid \lfloor m-1$

$\Rightarrow d \nmid (\lfloor m-1 + 1)$ ——— (2)

But $d \mid m$ and $m \mid (\lfloor m-1 + 1)$

$\Rightarrow$ d must divide $(\lfloor m-1 + 1)$ ——— (3)

But (2) and (3) are contradictory in nature

i.e. m must be prime.

This is the proof of converse of Wilson's proof.

Theorem: The quadratic congruence $x^2 \equiv -1 \pmod{p}$) p is prime, has a solution iff $p \equiv 1 \pmod{4}$

Proof. Let p be a prime

"If part" Suppose $x^2 \equiv -1 \pmod{p}$ has a solution ——— (1)

To prove $p \equiv 1 \pmod{4}$

Let $x \equiv a \pmod{p}$ be a solution of (1), we have

$$a^2 \equiv -1 \pmod{p}, \quad (a, p) = 1 \quad \text{——— (2)}$$

By Fermat's theorem

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

$$\Rightarrow (a^2)^{\frac{p-1}{2}} \equiv 1 \pmod{p} \quad \text{——— (3)}$$

We know that if $p > 2$ then p is an odd

From (2) and (3), we have

$\Rightarrow \frac{p-1}{2}$ is always even [!! $a^2 \equiv -1 \pmod{p}$
$\Rightarrow (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$]
$\equiv 1 \pmod{p}$

$$\Rightarrow \frac{p-1}{2} = 2k$$

$$\Rightarrow p = 4k + 1$$

$$\Rightarrow 4 \mid p-1$$

$$\Rightarrow p \equiv 1 \pmod{4}$$

"Only if part" Suppose $p \equiv 1 \pmod{4}$

To prove $x^2 \equiv (-1) \pmod{p}$ has solution

We know that Wilson's theorem states that

$$\lfloor p-1 \equiv -1 \pmod{p}$$

$$\Rightarrow 1 \times 2 \times 3 \times \cdots \times \left(\frac{p-1}{2}\right) \times \left(\frac{p+1}{2}\right) \times \left(\frac{p+3}{2}\right) \cdots (p-1) \equiv -1 \pmod{p} \quad \text{——— (4)}$$

But
$$\left.\begin{aligned} \frac{p+1}{2} &\equiv -\left(\frac{p-1}{2}\right) \pmod{p} \\ \frac{p+3}{2} &\equiv -\left(\frac{p-3}{2}\right) \pmod{p} \\ &\cdots\cdots \\ (p-1) &\equiv -1\,(1) \pmod{p} \end{aligned}\right\} \quad \text{——— (5)}$$

Eqn (4) can be re-written as

$$\{1\times2\times3\times\cdots\left(\frac{p-3}{2}\right)\left(\frac{p-1}{2}\right)\}\{(p-1)(p-2)\cdots\cdots\left(\frac{p+3}{2}\right)\left(\frac{p+1}{2}\right)\}\equiv -1 \pmod p \quad (6)$$

Here

$$\left.\begin{aligned} p-1 &\equiv -1\ (1) \pmod p \\ p-2 &\equiv (-1)(2) \pmod p \\ &\cdots \\ \left(\frac{p+3}{2}\right) &\equiv (-1)\left(\frac{p-3}{2}\right) \pmod p \\ \left(\frac{p+1}{2}\right) &\equiv (-1)\left(\frac{p-1}{2}\right) \pmod p \end{aligned}\right\} \quad (7)$$

ii LHS of (6) & (7) $\Rightarrow$

$$(-1)^{\frac{p-1}{2}}\left[1\times2\times3\times\cdots\left(\frac{p-1}{2}\right)\right]^2 \equiv (-1) \pmod p$$

$$(-1)^{2k}\left[\left\lfloor\frac{p-1}{2}\right\rfloor\right]^2 \equiv -1 \pmod p \quad \left[\begin{array}{l} \because p\equiv 1 \pmod 4 \\ \Rightarrow p-1=4k \\ \Rightarrow \frac{p-1}{2}=2k \end{array}\right.$$

$$\left(\left\lfloor\frac{p-1}{2}\right\rfloor\right)^2 \equiv -1 \pmod p$$

This shows that $\left\lfloor\frac{p-1}{2}\right\rfloor$ is a solution of

$x^2 \equiv -1 \pmod p$. proved.

Q. For any prime p, prove $p \mid \{a^p + \lfloor p-1 \rfloor, a\}$, a is any integer.

Soln By Fermat's theorem

$$p \mid (a^{p-1}-1) \quad \left[\because a^{p-1}\equiv 1 \pmod p\right] \quad (1)$$

By Wilson's theorem

$$p \mid (\lfloor p-1 \rfloor + 1) \quad (2)$$

(1) & (2) $\Rightarrow$

$$p \mid \{a^{p-1}-1+\lfloor p-1 \rfloor + 1\} \quad \left[\begin{array}{l} p\mid a,\ p\mid b \\ \Rightarrow p\mid(a+b) \end{array}\right]$$

$\Rightarrow p \mid (a^{p-1} + \lfloor p-1 \rfloor) \Rightarrow p \mid a(a^{p-1} + \lfloor p-1 \rfloor)$ $\left[\because p\mid\alpha \Rightarrow p\mid a\alpha\right]$

$\Rightarrow p \mid (a^p + a\lfloor p-1 \rfloor)$, proved.

Q For any prime p, show that $p \mid \{\lfloor p-1 \cdot a^p + a\}$

Soln We know by Wilson's

$$p \mid \{\lfloor p-1 + 1\}$$
$$\Rightarrow p \mid a^p \{\lfloor p-1 + 1\} \quad [\because p \mid \alpha \Rightarrow p \mid a^p \alpha]$$
$$\Rightarrow p \mid \{a^p \lfloor p-1 + a^p\}$$
$$\Rightarrow p \mid \{a^p \lfloor p-1 + a^p + a - a\}$$
$$\Rightarrow p \mid \{a^p \lfloor p-1 + (a^p - a) + a\}$$
$$\Rightarrow p \mid \{a^p \lfloor p-1 + a\} \quad [\because a^p \equiv a \pmod p \Rightarrow a^p - a \equiv 0 \pmod p)$$

Numerical Examples on Wilson

(1) Show that 17 is a prime by showing $\lfloor 16 \equiv -1 \pmod{17}$

Soln We know $bb' \equiv 1 \pmod p$, $b, b' \in \{2, 3, 4, \ldots 15\}$

Take $b = 2 \Rightarrow b' = 9$ etc

$2 \times 9 \equiv 1 \pmod{17}$
$3 \times 6 \equiv 1 \pmod{17}$
$4 \times 13 \equiv 1 \pmod{17}$
$5 \times 7 \equiv 1 \pmod{17}$
$8 \times 15 \equiv 1 \pmod{17}$
$10 \times 12 \equiv 1 \pmod{17}$
$11 \times 14 \equiv 1 \pmod{17}$ multiplying

$$\lfloor 15 \equiv 1 \pmod{17}$$
$$\Rightarrow 16 \lfloor 15 \equiv 16 \pmod{17}$$
$$\Rightarrow \lfloor 16 \equiv -1 \pmod{17} \quad [\because 16 + 17k = -1 \text{ for } k = -1]$$
$$\Rightarrow \lfloor p-1 \equiv -1 \pmod p$$

By Wilson's theorem p is prime $\Rightarrow 17$ is prime. proved

(2) Find the remainder when $2\lfloor 28$ is divided by 31.

Soln. By Wilson's theorem, we have

$$\lfloor p-1 \equiv -1 \pmod p$$
$$(p-1)\lfloor (p-2) \equiv -1 \pmod p$$
$$\Rightarrow p\lfloor p-2 - \lfloor p-2 \equiv -1 \pmod p$$
$$\Rightarrow 0 - \lfloor p-2 \equiv -1 \pmod p$$
$$\Rightarrow \lfloor p-2 \equiv 1 \pmod p$$
$$\Rightarrow (p-2)\lfloor p-3 \equiv 1 \pmod p$$
$$\Rightarrow p\lfloor p-3 - 2\lfloor p-3 \equiv 1 \pmod p$$
$$\Rightarrow 0 - 2\lfloor p-3 \equiv 1 \pmod p$$
$$\Rightarrow 2\lfloor p-3 \equiv -1 \pmod p \quad \text{— (1)}$$

put $p = 31$

$$\Rightarrow 2\lfloor 28 \equiv -1 \pmod{31}$$
$$\Rightarrow 2\lfloor 28 \equiv (-1+31k) \pmod{31}$$
$$\Rightarrow 2\lfloor 28 \equiv 30 \pmod{31} \quad (\text{For } k=1)$$

$\therefore$ Required remainder is 30.

(3) Corollary in Q (2), eqn (1)

$$\Rightarrow 2\lfloor p-3 \equiv -1 \pmod p$$
$$\Rightarrow 2(p-3)\lfloor p-4 \equiv -1 \pmod p$$
$$\Rightarrow 2p\lfloor p-4 - 6\lfloor p-4 \equiv -1 \pmod p$$
$$\Rightarrow 0 - 6\lfloor p-4 \equiv -1 \pmod p$$
$$\Rightarrow 6\lfloor p-4 \equiv 1 \pmod p$$

put $p = 31$

$$6\lfloor 27 \equiv 1 \pmod{31}$$

$\Rightarrow$ 1 is remainder when $(6\lfloor 27)$ is divided by 31.

etc.