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