2) Fermat's Little theorem or fermat's theorem

fermat's theorem : Let p be prime and suppose that $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$

(proof) Considering first $p-1$ positive multiplies of a.

i.e integers $a, 2a, 3a, \ldots, (p-1)a$

clearly, none of these numbers is congruent modulo p to any other nor is any congruent to zero.

Since $ra \equiv sa \pmod{p}$ $\because 1 \le r < s \le p-1$

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

$\Rightarrow r \equiv s \pmod{p}$ which is not true as $r < s$

Also if $at \equiv 0 \pmod{p}$ $\because 1 \le t \le p-1$

$\Rightarrow at \equiv 0 \pmod{p}$

$\Rightarrow p \mid at$

$\Rightarrow p \mid a$ or $p \mid t$ (Not possible $\because p \nmid a$ & $1 \le t \le p-1$)

$\therefore$ Set of integers (above) must be congruent modulo p to $1, 2, 3, \ldots, p-1$, taken in some order.

Multiply all these congruences together,

$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$

$a \cdot a \cdots a \; 1 \cdot 2 \cdots (p-1)$

$(p-1)$ $(p-1)\, a^{p-1}$ $(p-1)!$

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

Also $p \nmid (p-1)!$ $\Rightarrow \gcd(p, (p-1)!) = 1$

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

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

Corollary 1
If p is prime then $a^p \equiv a \pmod p$ for any integer a.

(pf) When $p \mid a \Rightarrow a \equiv 0 \pmod p$
$\Rightarrow a^{p-1} \equiv 0 \pmod p$ (property: $a \equiv b \pmod p \Rightarrow a^k \equiv b^k \pmod p$, k is positive integer)
$\Rightarrow a^p \equiv 0 \pmod p$
$\equiv a \pmod p$ (as $p \mid a$)

If $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod p$ (By Fermat's thm)
$\Rightarrow a^p \equiv a \pmod p$

If $a \equiv a \pmod p$
$a^p \equiv 0 \pmod p$
& $a \equiv 0 \pmod p$ ($\because p \mid a$)
$\Rightarrow a^p \equiv a \pmod p$

Remark Another proof given in Book (for collary)

Application of Fermat's theorem

Verify $5^{38} \equiv 4 \pmod{11}$
$p = 11$ (prime)
$a = 5$
As $p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod p$
$\Rightarrow 5^{10} \equiv 1 \pmod p$

$5^{38} = (5^{10})^3 (5^2)^4$
$= 1 \cdot 3^4 \equiv 81 \equiv 4 \pmod{11}$

(lemma) If p and q are distinct primes with $a^p \equiv a \pmod q$ and $a^q \equiv a \pmod p$ then $a^{pq} \equiv a \pmod{pq}$

(pf) By above corollary
As p & q are prime (given) &
and $a^p \equiv a \pmod q$ — (1) & $a^q \equiv a \pmod p$

As q is prime
Now $a^{pq} = (a^q)^p$
$\equiv (a^q)^p \bmod p$ (use)
$\equiv a^p \pmod p$ (As we need $\bmod pq$)
$\equiv a \pmod p$ By corollary ($a^p \equiv a \pmod p$)
$\Rightarrow p \mid a^{pq} - a$ — (A)

& similarly $a^{pq} = (a^p)^q$
$\equiv a^q \pmod q$ (use (1))
$\equiv a \pmod q$ (By corollary)

$l \mid a^{pl} - a$ — (AA)

from (*) & (AA)

$p \mid a^{pl} - a$ & $l \mid a^{pl} - a$

$\gcd(p, l) = 1$ & p & l are distinct prime

(as prime divisors) $\Rightarrow p \cdot l \mid a^{pl} - a$

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

[Using $a \mid c$ & $b \mid c$, $\gcd(a, b) = 1 \Rightarrow a \cdot b \mid c$]

Converse of Fermat's theorem may not be true.

(e.g) $2^{340} \equiv 1 \pmod{341}$ but 341 is not prime. $\because 2 \times 341$

(How) $\because$ since $341 = 11 \times 31$

Also. $2^{11} = 2 \cdot 2^{10} \equiv 2 \cdot 1^{*} \equiv 2 \pmod{31}$

$2^{31} = 2(2^{10})^3 \equiv 2 \cdot 1^3 \equiv 2 \pmod{11}$

By lemma above

$2^{11 \times 31} \equiv 2 \pmod{11 \times 31}$

$2^{341} \equiv 2 \pmod{341}$

$2^{340} \equiv 1 \pmod{341}$

Exercise (5.2)

(Q-1) Use Fermat's theorem to verify that 17 divides $11^{104} + 1$ (Also show $11^{104} + 1 \equiv 0 \pmod{17}$)

(Sol^{n}) $a = 11$ $p = 17$ & $p \nmid a$ then by Fermat's theorem

$11^{17-1} \equiv 1 \pmod{17}$

$11^{16} \equiv 1 \pmod{17}$ ★ (done power 16 then split 104 into 16 multiples)

$11^{104} = (11^{16})^6 \cdot 11^8$

$11 \equiv 11 \pmod{17}$

$11^2 \equiv 121 \equiv 2 \pmod{17}$

$11^8 \equiv 2^4 \pmod{17}$

$\equiv 16 \pmod{17}$

$\therefore\therefore$

$11^{104} \equiv (1)^6 \cdot 16 \pmod{17}$

$\equiv 16 \pmod{17}$

$11^{104} + 1 \equiv 16 + 1 \pmod{17}$

$\equiv 0 \pmod{17}$

(Q-4) Derive each of following congruence

(a) $a^{21} \equiv a \pmod{15}$ for all a

Now $15 = 3 \times 5$, 5 & 3 are prime

By Fermat corollary ☆

$a^5 \equiv a \pmod 5$ and $a^3 \equiv a \pmod 3$

$(a^5)^4 \equiv a^4 \pmod 5$ and $(a^3)^7 \equiv a^7 \pmod 3$

$a^{20} \equiv a^4 \pmod 5$ $\quad a^{21} \equiv a^7 \pmod 3$

$a^{21} \equiv a^5 \pmod 5$ $\quad = (a^3)^2 \cdot a \pmod 3$

$\equiv a \pmod 5$ $\quad \equiv a \pmod 3$

$\Rightarrow 5 \mid a^{21} - a$ $\quad 3 \mid a^{21} - a$

and 5 & 3 are prime $\Rightarrow gcd(5,3) = 1$

$\Rightarrow 5 \cdot 3 \mid a^{21} - a$

$\Rightarrow a^{21} \equiv a \pmod{15}$

Use: $a \mid c$ & $b \mid c$, $gcd(a,b) = 1 \Rightarrow a \cdot b \mid c$

(c) $a^{13} \equiv a \pmod{3 \cdot 7 \cdot 13}$ for all a (by fermat's corollary)

$a^3 \equiv a \pmod 3$, $a^7 \equiv a \pmod 7$, $a^{13} \equiv a \pmod{13}$

(Q-5) (a) find the units digit of 3^{100} by use of Fermat's Theorem (10)

(Since $10 = 2 \times 5$) and base is 3

Since $gcd(3,5) = 1$ & $gcd(3,2) = 1$ By fermat's th

$3^4 \equiv 1 \pmod 5$, $3^1 \equiv 1 \pmod 2$

$\Rightarrow 5 \mid 3^4 - 1$ & $2 \mid 3^4 - 1$ $\Rightarrow 3^4 \equiv 1 \pmod 2$

If $a \mid c$ & $b \mid c$ & $gcd(a,b) = 1 \Rightarrow ab \mid c$

$gcd(5,2) = 1 \Rightarrow 10 \mid 3^4 - 1$

$\Rightarrow 3^4 \equiv 1 \pmod{10}$

$\Rightarrow (3^4)^{25} \equiv 1^{25} \pmod{10}$

$\Rightarrow 3^{100} \equiv 1 \pmod{10}$

0° unit digit of 3^{100} is 1.