Fermat's Little Theorem:

15 October 2020 09:19

For every integer a and every prime p,

a^p modulo p = a modulo p

that is, $a^p \equiv a \pmod{p}$

Proof: Case-I: If $p \mid a$

If $p \mid a$, then $p \mid a^p$

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

Case-II: If $p \nmid a$

If $p \nmid a$, then by division algorithm,

$a = pm + r$, where $1 \leq r \leq p-1$.

$\Rightarrow a \equiv r \pmod{p}$, where $1 \leq r \leq p-1$. (1)

Now, $0 \leq r \leq p-1 \Rightarrow r \in U(p)$, where $U(p) = \{1, 2, 3, \ldots, p-1\}$

Now $U(p)$ is a group under multiplication modulo p and $r \in U(p)$

$\therefore r^{|U(p)|} \equiv 1 \pmod{p}$ $\quad \boxed{\because a^{|G|} = 1}$

$\Rightarrow r^{p-1} \equiv 1 \pmod{p}$ ——— (2)

from eq^n (1), $a \equiv r \pmod{p}$

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

$\Rightarrow a^{p-1} \equiv 1 \pmod{p}$ [from eq^n (2)]

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

<u>Another statement:</u> For every integer a that is coprime to p,

$a^{p-1} \equiv 1 \pmod{p}$, where p is a prime.

or.

If p is a prime and $p \nmid a$, then

$a^{p-1} \equiv 1 \pmod{p}$, where $a \in \mathbb{Z}$

Q. Find last digit of 9^{81}

1567 → 7

SG7

$\underline{101} \to 1,$ $\qquad 1567 \to 7$

$101 \equiv 1 \pmod{10}$ $\qquad 1567 \equiv 7 \pmod{10}$

2, 5

primes

$2 \nmid 9$

$\Rightarrow 9^{2-1} \equiv 1 \pmod 2$

$\Rightarrow 9 \equiv 1 \pmod 2$

$\Rightarrow 9^{80} \equiv 1 \pmod 2$ ——— (1)

$5 \nmid 9 \Rightarrow 9^{5-1} \equiv 1 \pmod 5$

$\Rightarrow 9^4 \equiv 1 \pmod 5 \Rightarrow 9^{80} \equiv (1)^{20} \pmod 5$

$\Rightarrow 9^{80} \equiv 1 \pmod 5$ ——— (2)

from eqⁿ (1) & (2), $2 \mid (9^{80}-1)$ & $5 \mid (9^{80}-1)$

$\because \gcd(2,5) = 1$, $\therefore (2)(5) \mid (9^{80}-1)$

$\Rightarrow 10 \mid (9^{80}-1)$

$\Rightarrow 9^{80} \equiv 1 \pmod{10}$

$\Rightarrow 9^{81} \equiv 9 \pmod{10}$

$\therefore$ last digit of 9^{81} is 9.

Q. Show that the Converse of Lagrange's Theorem is not true.

Sol

Soln Lagrange's Thm → order of a subgroup divides order of group

Converse →. If some number m divides $|G|$. then G must have subgroup of order m.

The group A_4 (Alternating group of degree 4) has order $\frac{4!}{2} = 12$ but A_4 has no subgroup of order 6, while $6 \mid 12$.

We know that the group A_4 has eight elements of order 3. | Cayley table of A_4.

Now, let a be any element of order 3 in A_4.

Suppose that H is a subgroup of A_4 and $|H| = 6$.

then $|A_4 : H| = \frac{|A_4|}{|H|} = \frac{12}{6} = 2$.

Now, $a \in A_4$ & $|a| = 3$.

∴ the possible cosets of H in A_4 are.

H, aH and $a^2 H$

$\because$ H has index 2 in A_4,

$\therefore$ at most two of the cosets H, aH & a^2H are distinct.

$\Rightarrow$ any two cosets from H, aH & a^2H must be equal.

If $H = aH \Rightarrow a \in H$

If $H = a^2H \Rightarrow aH = a^3H \Rightarrow aH = eH$

$\Rightarrow aH = H \Rightarrow a \in H$

If $aH = a^2H \Rightarrow a^2H = a^3H \Rightarrow a^2H = eH \Rightarrow a^2H = H$.

$\Rightarrow a^3H = aH \Rightarrow eH = aH \Rightarrow H = aH$

$\Rightarrow a \in H$.

$\therefore$ If $a \in G$ ($=A_4$) have order 3, and A_4 have subgroup H of order 6, then $a \in H$.

Thus, a subgroup of order 6 would have to contain eight element of order 3, which is a contradiction.

$\therefore$ A_4 has no subgroup of order 6.

$A_4 \rightarrow \{1, 2, 3, 4\}$

$(12)(13) \longrightarrow (1\,3\,2)$

$(132)(123) = \ldots$

$(13)(12) \to (123)$

$(14)(13) \to (134)$

$\vdots$

<u>Thm</u> For two finite subgroups H and K of a group G, define a set

$$HK = \{hk \mid h \in H,\ k \in K\}.$$

Then
$$|HK| = \frac{|H|\,|K|}{|H \cap K|}$$

$$\boxed{|HK| \le |G|.}$$

<u>Proof:</u>

· the set $HK = \{hk \mid h \in H, k \in K\}$
$h \to |H|$, $k \to |K|$

the set HK has $|H||K|$ products, but all of these products need not represent distinct group elements.

that is, we may have
$hk = h'k'$, where $h \neq h'$ & $k \neq k'$

$\mathbb{Z}_6$, $H = \{0, 2, 4\}$
$K = \{0, 3\}$
$2 \cdot 3 = 4 \cdot 3 = 0$.
$|HK| = |H||K| = (3)(2)$

& $k^{-1}k$

$$|HK| = \frac{|H||K|}{|H\cap K|} = \frac{(3)(2)}{1} = 6$$

for every t in $H\cap K$, the product hk can be written as

$hk = (ht)(t^{-1}k)$, where $ht \in H$ & $t^{-1}k \in K$.

So each group element in HK is represented by atleast $|H\cap K|$ products in HK.

$h\in H \Rightarrow h \to |H|$
$t \in H\cap K \Rightarrow t \to |H\cap K|$

But $hk = h'k'$

$\Rightarrow h^{-1}hk(k')^{-1} = h^{-1}h'k'(k')^{-1}$

$\Rightarrow k(k')^{-1} = h^{-1}h'$

$\Rightarrow \underbrace{h^{-1}h'}_{H} = \underbrace{k(k')^{-1}}_{K} = t \in H\cap K$

$\Rightarrow h' = ht$ and $(k')^{-1} = k^{-1}t$

$\Rightarrow h' = ht$ and $k' = t^{-1}k$

Thus, each element in HK is represented by exactly $|H\cap K|$ products.

Therefore, $|HK| = \dfrac{|H||K|}{|H \cap K|}$.

Example: Show that: A group of order 75 can have at most one subgroup of order 25.

Soln: Let G be a group of order 75.

Suppose that G have two subgroups H and K of order 25.

$\because$ H & K are subgroups of G

$\Rightarrow$ $H \cap K$ is a subgroup of H.

$\Rightarrow$ $|H \cap K|$ divides $|H|$

$\Rightarrow$ $|H \cap K|$ divides 25.

$\Rightarrow$ $|H \cap K|$ can be 1 or 5 or 25.

Case-I: If $|H \cap K| = 1$,

then $|HK| = \dfrac{|H||K|}{|H \cap K|} = \dfrac{(25)(25)}{1} = 625$

$\therefore$ $|HK| > |G|$ . . $(\because |HK| \leq |G|)$

$\longrightarrow\!\leftarrow$

Case - II: contradiction. $(|H \cap K| = 5)$

Case - III: If $|H \cap K| = 25$,

$\therefore |H| = 25, \; |K| = 25, \; |H \cap K| = 25.$

$\therefore H = K.$

$\Rightarrow$ G can have atmost one subgroup of order 25.

Q. Find last digit of 7^{72}?

Sol^n $2 \nmid 7 \Rightarrow 7^{2-1} \equiv 1 \pmod 2$

$\Rightarrow 7 \equiv 1 \pmod 2$

$\Rightarrow 7^{72} \equiv 1 \pmod 2$ —— (1)

$5 \nmid 7 \Rightarrow 7^{5-1} \equiv 1 \pmod 5$

$\Rightarrow 7^4 \equiv 1 \pmod 5$

$\Rightarrow (7^4)^{18} \equiv 1^{18} \pmod 5$

$\Rightarrow 7^{72} \equiv 1 \pmod 5$ —— (2)

$\because$ from eq^n ① & ②, $2 \mid (7^{72}-1)$ & $5 \mid (7^{72}-1)$

$\because \gcd(2,5)=1 \Rightarrow (2)(5) \mid (7^{72}-1)$

$\Rightarrow 7^{72} \equiv 1 \pmod{10}$

$\therefore$ last digit of 7^{72} is 1.

Q. Prove that if a is any integer relatively prime to n, then $a^{\phi(n)} \equiv 1 \pmod{n}$

$\boxed{\text{Euler's Theorem}}$

Sol^n// $\gcd(a,n)=1$.

If we divide a by n, then by division algorithm

$a = qn + r$, where $1 \le r < n$. —— ①

from eq^n ①, $a \equiv r \pmod{n}$

$\because \gcd(a,n)=1 \Rightarrow \gcd(r,n)=1$

and $1 \le r < n$

$\phi(n)$ is the no. of integers less than n and relatively prime to n.

$U(n) = \{1 \le a < n \mid \gcd(a,n)=1\}$.

$$\boxed{U(n) = \{ 1 \le a < n \mid \gcd(a, n) = 1 \}}$$

$\therefore\ r \in U(n)$

$\Rightarrow\ r^{|U(n)|} \equiv 1 \pmod{n}$

$\Rightarrow\ r^{\phi(n)} \equiv 1 \pmod{n}$ $\left(\because |U(n)| = \phi(n)\right)$ —— ②

from eqn ①, $a \equiv r \pmod{n}$

$\Rightarrow\ a^{\phi(n)} \equiv r^{\phi(n)} \pmod{n}$

$\Rightarrow\ a^{\phi(n)} \equiv 1 \pmod{n}$ (from eqn ②)

Q. Suppose H & K are subgroups of G. If $|H| = 12$ and $|K| = 35$, find $H \cap K$.

Soln: $H \cap K$ is a subgroup of H & K.

$\Rightarrow$ $|H \cap K|$ divides $|H|$ and $|H \cap K|$ divides $|K|$

$\Rightarrow$ $|H \cap K|$ divides 12 and $|H \cap K|$ divides 35

$\Rightarrow$ $|H \cap K|$ divides $\gcd(12, 35)$

$\Rightarrow$ $|H \cap K|$ divides 1

$\Rightarrow$ $|H \cap K| = 1$

$\Rightarrow \quad H \cap K = \{e\}.$