Fermat's Little Theorem (F.L.T.):-

If p is a prime and $p \nmid a$ then $a^{p-1} \equiv 1 \pmod{p}$

Proof :-

Claim:- The set $\{0a, 1\cdot a, 2a, 3a, \ldots, (p-1)a\}$ is complete set of residues mod p.

In fact, $ia \equiv ja \pmod{p}$

$\Rightarrow p \mid (i-j)a$, for $0 \leq i, j < p$.

$\Rightarrow p \mid i-j$, as $p \nmid a$

$\Rightarrow i = j$ $(\because i, j < p)$

Hence, the set is a complete set of residues modulo p.

$\Rightarrow a, 2a, \ldots, (p-1)a$ are simply rearrangement of $1, 2, 3, \ldots, p-1$ when considered modulo p.

$\Rightarrow a \cdot 2a \cdot 3a \cdots (p-1)a$

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

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

$\Rightarrow p \mid (p-1)!\left[a^{p-1} - 1\right]$

$\Rightarrow p \mid a^{p-1} - 1$, as $p \nmid (p-1)!$

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

Note:- If p is a prime, then $a^p \equiv a \pmod{p}$ for any integer p.

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \cdots\cdots + \binom{p}{p-1} a + 1.$$

(Binomial theorem)

$$\binom{p}{k} = \frac{p!}{k!\,(p-k)!}, \text{ for } 1 \le k \le p-1$$

$$\Rightarrow k! \binom{p}{k} = \frac{p!}{(p-k)!}$$

$$= p(p-1)\cdots(p-k+1)$$

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

$$\Rightarrow p \mid (k!)\binom{p}{k}$$

$$\Rightarrow p \mid \binom{p}{k}, \text{ as } p \nmid k! \text{ when } 1 \le k \le p-1.$$

$$\Rightarrow \binom{p}{k} \equiv 0 \pmod{p},$$

for $1 \leq k \leq p-1$

$$\therefore (a+1)^p \equiv a^p + 1 \pmod{p}$$

For $a=1$, $1^p \equiv 1 \pmod{p}$

Assuming, $a^p \equiv a \pmod{p}$ for some $a>1$,

we have, $(a+1)^p \equiv a^p + 1 \pmod{p}$

$$\Rightarrow (a+1)^p \equiv a+1 \pmod{p}$$

$$\Rightarrow a^p \equiv a \pmod{p}, \quad \forall\, a$$

(by induction)

Lemma:- If p and q are distinct primes with $a^p \equiv a \pmod{q}$ and $a^q \equiv a \pmod{p}$, then

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

Proof:- We know that-

$a^p \equiv a \pmod{p}$, for any a.

$\therefore (a^q)^p \equiv a^q \pmod{p}$

But- $a^q \equiv a \pmod{p}$ (given)

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

Similarly, $a^{pq} \equiv a \pmod{q}$

As $\gcd(p, q) = 1$, we have

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

Ex:- Prove that 17 divides $11^{104}+1$.

To prove $17 \mid 11^{104}+1$

i.e., to prove $11^{104}+1 \equiv 0 \pmod{17}$

i.e., to prove $11^{104} \equiv -1 \pmod{17}$

We have $11^{16} \equiv 1 \pmod{17}$,

as $17 \nmid 11$ and 17 is a prime

(by F. L. T.)

$104 = 16 \times 6 + 8$ (Division Algorithm)

$\therefore 11^{104} = 11^{16\times 6+8}$

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

$\equiv 1^6 \cdot 11^8 \pmod{17}$

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

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

$\therefore 11^4 \equiv 4 \pmod{17}$

$11^8 \equiv 16 \pmod{17} \equiv -1 \pmod{17}$

$\therefore 11^{104} \equiv 11^8 \equiv -1 \pmod{17}$

$\Rightarrow 17 \mid 11^{104} + 1$

Ex:- If g.c.d.$(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$

35 is not a prime.

$35 = 5 \times 7$.

$(a, 35) = 1 \Rightarrow (a, 5) = (a, 7) = 1$.

$\therefore$ FLT $\Rightarrow \begin{cases} a^4 \equiv 1 \pmod{5} \\ a^6 \equiv 1 \pmod{7} \end{cases}$

$$\Rightarrow \begin{cases} a^{12} = (a^4)^3 \equiv 1^3 \equiv 1 \pmod 5 \\ a^{12} = (a^6)^2 \equiv 1^2 \equiv 1 \pmod 7 \end{cases}$$

$$\Rightarrow a^{12} \equiv 1 \pmod{5\times 7}$$

$(\because \gcd(5,7) = 1)$

$$\Rightarrow a^{12} \equiv 1 \pmod{35}$$

Ex:- If $\gcd(a, 42) = 1$, prove that 168 divides $a^6 - 1$.

$$168 = 3 \times 7 \times 8 = 2^3 \times 3 \times 7$$

$$42 = 2 \times 3 \times 7.$$

$$(a, 42) = 1 \Rightarrow (a,2) = (a,3) = (a,7) = 1.$$

$$\Rightarrow a \equiv 1 \pmod 2$$
$$a^2 \equiv 1 \pmod 3$$
$$a^6 \equiv 1 \pmod 7$$

$a \equiv 1 \pmod 2 \Rightarrow a^6 \equiv 1 \pmod 2$

$a^2 \equiv 1 \pmod 2 \Rightarrow a^6 \equiv 1^3 \equiv \pmod 2$

Now $2 \mid a^6 - 1$ $(\because a^6 \equiv 1 \pmod 2)$

$\Rightarrow 2 \mid (a-1)(a^5 + a^4 + a^3 + a^2 + 1)$

$a^5 + a^4 + a^3 + a^2 + a + 1$

$= a^3(a^2 + a + 1) + a^2 + a + 1$

$= (a^3 + 1)(a^2 + a + 1)$

$= (a+1)(a^2 - a + 1)(a^2 + a + 1)$

$\therefore 2 \mid (a-1)(a+1)(a^2 - a + 1)(a^2 + a + 1)$

Note that a is odd

$(\because a \equiv 1 \pmod 2)$

$\Rightarrow |a| > 1$

If $a > 0$, then $a \geq 3$.

$\therefore 2 \mid a-1 \Rightarrow 4 \mid a+1$

$\Rightarrow 8 \mid (a-1)(a+1)$

$\Rightarrow 8 \mid a^6 - 1$

If $a < 0$, then, $a \leq -3$

$\Rightarrow 2 \mid a+1 \Rightarrow 4 \mid a-1$

$\Rightarrow 8 \mid a^6 - 1$

Now $a^6 \equiv 1 \pmod 8$

$a^6 \equiv 1 \pmod 3$

$a^6 \equiv 1 \pmod 7$

$\Rightarrow a^6 \equiv 1 \pmod{3 \times 7 \times 8}$

$\Rightarrow a^6 \equiv 1 \pmod{168}$

$\Rightarrow 168 \mid a^6 - 1$

Ex:- If $\gcd(a, 133) = \gcd(b, 133) = 1$,

then show that $133 \mid a^{18} - b^{18}$

$133 = 7 \times 19$

$\Rightarrow \gcd(a, 19) = \gcd(b, 19) = 1$

F.L.T. $\Rightarrow a^{18} \equiv 1 \pmod{19}$

$b^{18} \equiv 1 \pmod{19}$

$\therefore a^{18} - b^{18} \equiv 0 \pmod{19}$

$\Rightarrow 19 \mid a^{18} - b^{18} \longrightarrow (1)$

Also, $\text{g.c.d.}(a, 7) = \gcd(b, 7) = 1$

FLT $\Rightarrow \begin{cases} a^6 \equiv 1 \pmod{7} \\ b^6 \equiv 1 \pmod{7} \end{cases}$

$\Rightarrow a^6 - b^6 \equiv 0 \pmod 7$

$\Rightarrow 7 \mid a^6 - b^6$

But $a^{18} - b^{18} = (a^6)^3 - (b^6)^3$

$= (a^6 - b^6)\left((a^6)^2 + a^6 b^6 + (b^6)^2\right)$

$\Rightarrow 7 \mid a^{18} - b^{18}$

$\therefore \quad 7 \times 19 = 133 \mid a^{18} - b^{18}$

Ex:- If g.c.d$(a, 30) = 1$, show that 60 divides $a^4 + 59$.

g.c.d$(a, 2)$ = gcd$(a, 3)$ = gcd$(a, 5) = 1$

$(\because 30 = 2 \times 3 \times 5)$

$\Rightarrow a \equiv 1 \pmod 2$

$a^2 \equiv 1 \pmod 3$

$a^4 \equiv 1 \pmod 5$

} F.L.T.

$\Rightarrow a^2 \equiv 1 \pmod 2$
$a^4 \equiv 1 \pmod 3$

$a^2 \equiv 1 \pmod 2 \Rightarrow a^2 \equiv -1 \pmod 2$

$(\because 1 \equiv -1 \pmod 2)$

$\therefore 2 \mid a^2-1$ and $2 \mid a^2+1$

$\Rightarrow 4 \mid (a^2-1)(a^2+1) = a^4-1$

Now, $3 \mid a^4-1$, $4 \mid a^4-1$ and $5 \mid a^4-1$.

$\Rightarrow 3 \times 4 \times 5 = 60 \mid a^4-1$

$\Rightarrow a^4 \equiv 1 \pmod{60}$

$\Rightarrow a^4 \equiv -59 \pmod{60}$

$\Rightarrow 60 \mid a^4+59$

Ex:- Find the units digit of 3^{100} using Fermat's theorem.

Ans: $3^{100} \pmod{10}$ — units digit

$10 = 2 \times 5$

$3 \equiv 1 \pmod{2} \Rightarrow 3^{100} \equiv 1 \pmod{2}$

$3^2 \equiv -1 \pmod{5} \Rightarrow 3^{100} = (3^2)^{50}$

$\equiv (-1)^{50}$

$\equiv 1 \pmod{5}$

$\therefore 3^{100} \equiv 1 \pmod{2 \times 5}$

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

$\Rightarrow$ 1 is the units digit of 3^{100}

Ex:- Prove that $1835^{1910} + 1986^{2061} \equiv 0 \pmod{7}$

$1835 \equiv 1 \pmod{7}$ $(\because 1835 = 7 \times 262 + 1)$

$\Rightarrow 1835^{1910} \equiv 1 \pmod{7}$

$1986 \equiv 5 \pmod 7$

$(\because 1986 = 7 \times 283 + 5)$

$5^2 = 25 \equiv 4 \pmod 7$

$5^3 = 5^2 \times 5 = 4 \times 5 = 20 \equiv -1 \pmod 7$

Now $2061 = 3 \times 687$

$\therefore 1986^{2061} \equiv (-1)^{687} \equiv -1 \pmod 7$

$\therefore 1835^{1910} + 1986^{2061} \equiv 1 - 1 \equiv 0 \pmod 7$

Ex:- If p is odd prime, then prove that

$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod p$

By F.L.T.,

$LHS \equiv 1 + 1 + \cdots + 1$ ($p-1$ times)

$= p - 1$

$\equiv -1 \pmod p$

Ex:- If p is an odd prime, then prove that

$1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$

$LHS \equiv 1 + 2 + 3 + \cdots + (p-1)$

$(\because a^p \equiv a \pmod{p})$

$\equiv \frac{p(p-1)}{2}$ [note that $p-1$ is even]

$\equiv 0 \pmod{p}$

Ex:- Prove that if p is odd prime, and k is an integer, $1 \le k \le p-1$, then

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}$$

$$\binom{p-1}{k} = \frac{(p-1)!}{k!\,(p-k-1)!}$$

$$= \frac{(p-1)(p-2)\cdots(p-k)}{k!}$$

$$\Rightarrow k! \binom{p-1}{k} = (p-1)(p-2)\cdots(p-k)$$

$$\equiv (-1)(-2)\cdots(-k) \pmod{p}$$

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

$$\Rightarrow \binom{p-1}{k} \equiv (-1)^k \pmod{p}$$

$(\because p \nmid (k!)$, as $1 \le k \le p-1)$

Ex:- Two odd primes p and q are such that $p-1 \mid q-1$.

If $\gcd(a, pq) = 1$, then

Now that $a^{q-1} \equiv 1 \pmod{pq}$

$\gcd(a, pq) = 1$

$\Rightarrow \gcd(a, p) = \gcd(a, q) = 1$

$\Rightarrow \left.\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \\ a^{q-1} &\equiv 1 \pmod{q} \end{aligned}\right\}$ F. L. T.

Now $p-1 \mid q-1 \Rightarrow q-1 = k(p-1)$

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

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

Now $\left.\begin{aligned} a^{q-1} &\equiv 1 \pmod{p} \\ a^{q-1} &\equiv 1 \pmod{q} \end{aligned}\right\} \Rightarrow$

$\Rightarrow a^{q-1} \equiv 1 \pmod{pq}$

Ex:- If p and q are distinct primes, then

prove that

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

$$p^{q-1} \equiv 1 \pmod{q} \quad (F.L.T.)$$

And $q^{p-1} \equiv 0 \pmod{q}$

$$\therefore p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$$

Similarly, $p^{q-1} + q^{p-1} \equiv 1 \pmod{p}$

$$\Rightarrow p^{q-1} + q^{p-1} \equiv 1 \pmod{pq},$$

$(\because \gcd(p, q) = 1)$
