Fermat's little Theorem:

If p is a prime number and $p \nmid a$

then $a^{p-1} \equiv 1 \mod 5$

Ex 1 Let p be 5

$5 \nmid 2 \Rightarrow 2^{5-1} \equiv 1 \mod 5$

$2^4 \equiv 1 \mod 5$

Similarly $3^4 = 1 \mod 5$

$5 \mid 5$, theorem doesn't apply; $5^4 \equiv 0 \mod 5$

$5 \nmid 6, \Rightarrow 6^4 \equiv 1 \mod 5$

$7^4 \equiv 1 \mod 5$

$8^4 \equiv 1 \mod 5$

$9^4 \equiv 1 \mod 5$

$5 \mid 10$; theorem doesn't apply, $10^4 \equiv 0 \mod 5$

...

Ex 2 of app of Firmat's little theorem.

Find the remainder when you divide

$3^{100\,000}$ by 53.

here p ~~is~~ 53 is a prime number; $53 \nmid 3$ so:

Raise both side to a large power

$\frac{100\,000}{2} \Rightarrow q = 1923$ quotient

$r = 4$ remainder

$3^{52} \equiv 1 \bmod 53$ by Fermat's LT.

$(3^{52})^{1923} \equiv 1^{1923} \bmod 53$ raise both the sides to the power of 1923

$3^{99\,996} \equiv 1 \bmod 53$

$3^{4} \times (3^{99996}) \equiv 3^{4} \bmod 53$

$3^{100\,000} \equiv 81 \bmod 53$

$3^{100\,000} \equiv 28 \bmod 53$

which means that if we devide $3^{100\,000}$ over 53 we get a remainder equals to 28.

Proof of Fermat's Little Theorem.

if p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \bmod p$.

Ex Let $p = 7$

$\forall n \in \mathbb{Z} \quad n \equiv \{0, 1, 2, 3, 4, 5, 6\} \bmod 7$

consider $a = 12$.

Multiply all non zero congruence classes by 12:

$$12, 24, 36, 48, 60, 72 \equiv 5, 3, 1, 6, 4, 2 \bmod 7$$

This is a rearrangement of the values

$$1, 2, 3, 4, 5, 6.$$

Conclusion

if you multiply the congruence classes of a by a it simply reranges them.

Proof Assume p is prime and $p \nmid a$.

every integer is congruent to $0, 1, 2, \ldots, p-1 \bmod p$

Only focus on nonzero congruence classes, because $0 \bmod p$ contains all multiples of p (and $p \nmid a$). So we focus on C.C.

$$1, 2, \ldots, p-1.$$

Multiply all of these by a:

$$a, 2a, \ldots, a(p-1)$$

Show that this is simply a rearrangement of congruent classes $1, 2, \ldots, p-1$.

Case 1

None of these is congruent to 0

Suppose $r.a \equiv 0 \mod p.$, then $p | r.a$, but this is impossible since $p \nmid a$ and $p \nmid r$ (since $r < p$).

. so non of these are conguent to 0.

Case 2

these are distinct; no two are congruent to each other.

Pick two values $r.a$, $s.a$

$0 < r < p$ and $0 < s < p$.

Let's show that $a.r \not\equiv s.a \mod p$

so look at $r.a - s.a = a(r-s)$.

by assumption $p \nmid a$, so can p divide $r-s$?

$$\begin{array}{rl} & 0 < r < p \\ + & -p < -s < 0 \\ \hline & -p < r-s < p. \end{array}$$

As $r-s \neq 0$ because r and s are distinct congruence classes, so $p \nmid r-s$ which means $a, 2a, \dots, a(p-1)$ is just a rearrangement of one another so the product:

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

$$(p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p} \quad \cdots (1)$$

p doesn't divide $(p-1)!$ because $(p-1)!$ is the product of a set of numbers that are $< p$.

So we can divide both sides of (1) by $(p-1)!$ to get:

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

$\square$.