**Fermat's little theorem** states that if *p* is a [prime number](https://en.wikipedia.org/wiki/Prime_number), then for any [integer](https://en.wikipedia.org/wiki/Integer) *a*, the number *ap* − *a* is an integer multiple of *p*. In the notation of [modular arithmetic](https://en.wikipedia.org/wiki/Modular_arithmetic), this is expressed as

{\displaystyle a^{p}\equiv a{\pmod {p}}.}

For example, if *a* = 2 and *p* = 7, then 27 = 128, and 128 − 2 = 126 = 7 × 18 is an integer multiple of 7.

If *a* is not divisible by *p*, Fermat's little theorem is equivalent to the statement that *ap*− 1 − 1 is an integer multiple of *p*, or in symbols:[[1]](https://en.wikipedia.org/wiki/Fermat%27s_little_theorem#cite_note-1)[[2]](https://en.wikipedia.org/wiki/Fermat%27s_little_theorem#cite_note-2)

{\displaystyle a^{p-1}\equiv 1{\pmod {p}}.}

For example, if *a* = 2 and *p* = 7, then 26 = 64, and 64 − 1 = 63 = 7 × 9 is thus a multiple of 7.

**a^p mod p = a ;**

**a ^ (p-1) mod p = 1 ( if a is not divisible by p )**

**a ^ (p-2) mod p = a^-1**