

Math Counting — Illustrated Guide

=====

Core Tools

- 1) Fast Modular Exponentiation (modpow): $O(\log e)$
- 2) $nCr \% \text{mod}$ (prime mod): $O(n)$ precompute, $O(1)$ per query
- 3) gcd / lcm via Euclid: $O(\log \min(a,b))$
- 4) $nPr \% \text{mod}$ (prime mod): $O(n)$ precompute
- 5) Applications: m^k , subset count, lcm over list

Notes

- Fermat's Little Theorem: $a^{(p-1)} \equiv 1 \pmod{p}$ when p is prime and $\gcd(a,p)=1$.
 $\Rightarrow a^{(-1)} \equiv a^{(p-2)} \pmod{p}$, used for modular inverses.
- Always use integer division before multiply in lcm: $a // \gcd(a,b) * b$.
- For multiple queries with the same n upper bound, precompute factorial and inverse arrays once.

Examples Included

- $\text{modpow}(3, 13, 1e9+7) = 1594323$
- $nCr_mod(10, 3, 1e9+7) = 120$
- $\gcd(48,18) = 6, \text{lcm}(21,6) = 42$
- $nPr_mod(10, 3, 1e9+7) = 720$
- $26^{10} \% (1e9+7), (2^5 - 1) \% (1e9+7), \text{lcm}([4,6,8,14])$