# Binary Exponential and mod **m**:

1. If **m** is a prime number we can speed up a bit this algorithm by calculating **xn mod(m-1)** instead of **xn** This follows directly from [Fermat's little theorem](https://cp-algorithms.com/algebra/module-inverse.html#toc-tgt-2).

Proof:

let

n= x+y ; where x=z\*(m-1)

n mod(m-1)= 0+y

xn mod(m-1)  = x0+y =x0. xy

1. We know , thus binary exponents can be used to calculate nth Fibonacci number.
2. Applying a permutation k times. For example [RIFFLES](https://www.codechef.com/JAN221B/problems/RIFFLES)

# Extended Euclidean Algorithm:

The extended Euclidean algorithm is an algorithm to compute integers *x* and *y* such that

given *a* and *b*.

The existence of such integers is guaranteed by [Bézout's lemma](https://brilliant.org/wiki/bezouts-identity/).