Sunday, 16 December 2018

Modular Arithmetic

Some useful Identities

- (a*b) % n = (a%n * b%n) % n
- (a^b) % n = ((a%n)^b) % n
- (1/a) % n -> Modular Multiplicative Inverse
- ((a*b)%n * (1/a)%n) % n = b%n
- a % 2^n = a & (n-1)
- When -ve result -> (result+n)%n