Modular Arithmetic

In modular arithmetic, each number x is represented by *x mod m,* where m is a constant and the resulting number is the remainder obtained by dividing x with m. The value of the remainder lies from *0* to *m-1*.
For Example: Let us say x is 10 and m is 3, then *10 mod 3 = 1.*

Properties of modular arithmetic:

- (x+y) mod m = ((x mod m) + (y mod m)) mod m
- (x-y) mod m = ((x mod m) - (y mod m) + m) mod m
- (x*y) mod m = ((x mod m) * (y mod m)) mod m
- x^n mod m = (x mod m)^n mod m
- (x/y) mod m = ((x mod m) * (y^{-1} mod m)) mod m, where y^{-1} is known as the multiplicative modular inverse of y and m.

Note: Modular division is different from modular addition,subtraction or multiplication, even for it to exist, the inverse of y must exist which is discussed in section "modular multiplicative inverse".

Why use modular arithmetic

Modular arithmetic and its properties are very useful in handling overflow scenarios and problems that involve combinatorics and probabilities where you are asked to compute a value that will overflow the limit of standard integer data types.
For Example: You are given two large numbers x = 10^16 and y = 10^15 and you need to compute the product z = x*y i.e (10^15)*(10^16) = 10^31 which certainly can't be stored in an integer data type. In such scenarios, you are always asked to compute the value under mod m(say 10^9 + 7), so
z = ((x mod m) * (y mod m)) mod m = 996570007

Examples of modular arithmetic:

Let x = 7, y = 5 and m = 3, then -

- *(x+y) mod m = ((x mod m) + (y mod m)) mod m => (12 mod 3) = 0 = ((7 mod 3) + (5 mod 3)) mod 3 = (4 + 2) mod 3 = 6 mod 3 = 0*
- *(x-y) mod m = ((x mod m) - (y mod m)) mod m => (2 mod 3) = 1 = (7 mod 3) - (5 mod 3) mod 3 = (1 - 2) mod 3 = -1 mod 3 = (-1 + 3) mod 3 = 2 mod 3 = 2 (Handling negative integers by adding m, as it does not affect the answer)*
- *(x*y) mod m = ((x mod m) * (y mod m)) mod m => (35 mod 3) = 2 = (7 mod 3) * (5 mod 3) mod 3 = (1 * 2) mod 3 = 2 mod 3 = 2*
- *x^n mod m = (x mod m)^n mod m => Let x = 5, n = 2 and m = 4 => (25 mod 4) = 1 = (5 mod 4)^2 mod 4 = 1 mod 4 = 1*
- *(x/y) mod m = ((x mod m) * (y^{-1} mod m)) mod m => Inverse of y exists, y^{-1} = 2 so the value becomes (7 mod 3) * (2 mod 3) mod 3 = (1*2) mod 3 = 2.*