# Question 8: Finding an Inverse Modulo *n*

# Introduction about Euclidean Algorithm and Extended Euclidean Algorithm

## Euclidean Algorithm

The Euclidean algorithm is an efficient method for finding the greatest common divisor (GCD) of two integers. It is based on the principle that the GCD of two numbers does not change if the larger number is replaced by its difference with the smaller number.

### Example

Suppose you want to find the GCD of 48 and 18:

Subtract the smaller number, 18, from the larger number, 48 (48 - 18 = 30).

Repeat the step with the new pair of numbers: 30 and 18 (30 - 18 = 12).

Continue with the new pair: 18 and 12 (18 - 12 = 6).

Repeat: 12 and 6 (12 - 6 = 6).

Finally, when both numbers are equal, the GCD is 6.

## Extended Euclidean Algorithm

The extended Euclidean algorithm not only computes the GCD but also finds integers x and y such that ax + by = gcd(a, b). This is an extension of the basic Euclidean algorithm.

### Example

Suppose you want to find the GCD of 120 and 23, and also find integers x and y so that

120x + 23y = gcd (120, 23):

Apply the Euclidean algorithm to 120 and 23:

- 120 % 23 = 8 (120 - 5 \* 23 = 8)

- 23 % 8 = 7 (23 - 2 \* 8 = 7)

- 8 % 7 = 1 (8 - 7 = 1)

- 7 % 1 = 0 (Ends here, GCD is 1)

Now, we backtrack through the steps to find x and y:

- 1 = 8 - 7

- 1 = 8 - (23 - 2 \* 8) = 3 \* 8 - 23

- 1 = 3 \* (120 - 5 \* 23) - 23 = 3 \* 120 - 16 \* 23

Thus, x = 3 and y = −16y are the integers found.

# Introduction about inverse modul

In modular arithmetic, there is no traditional division operation. Instead, we have the concept of **modular inverses**. The modular inverse of a number A modulo C is a number such that (mod C).

In other words, that mod C = 1. This means that if gcd(A,C)≠1, then A does not have a modular inverse. Only numbers that share no common factors with C (i.e., their greatest common divisor with C is 1) have a modular inverse modulo C.

**Example to illustrate:** Let's take C = 14. We know that 14 is the product of the prime numbers 2 and 7. According to the definition, numbers that share no common factors with 14 are those not divisible by 2 or 7.

**Method for finding a modular inverse using the extended Euclidean algorithm:**

1. Use the Euclidean algorithm to find gcd(a,b)
2. Write down the equation ax + by = gcd (a,b) and solve for x and y.
3. If gcd (a,b) = 1, then x is the inverse of a modulo b. If x is negative, add b to it until you get a positive value.

**Example:** Choose the number 3 to check if it has an inverse modulo 14 and then calculate the modular inverse if it exists.

First, we need to calculate its gcd with 14 using the extended Euclidean algorithm:

* 14=4×3+2
* 3=1×2+1
* 2=2×1+0
* gcd(3,14)=1

Since gcd (3,14) =1, 3 has a modular inverse modulo 14.

Next, solve for x and y in the equation 3x + 14y = 1

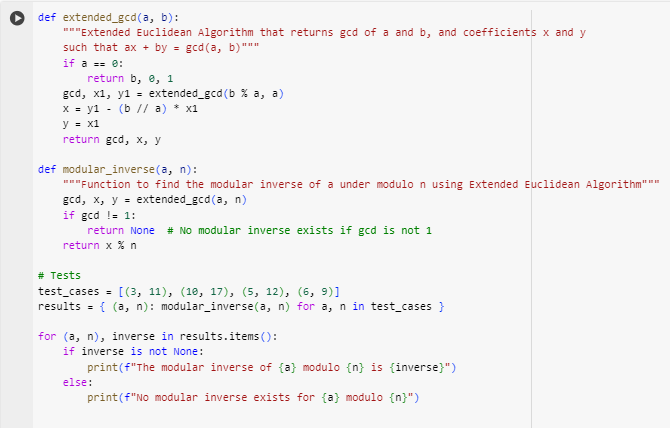
* 1=3×(−4)+14

So, x=−4. Add 14 to get a positive value:

* x=−4+14=10

Therefore, the inverse of 3 modulo 14 is 10 because 3×10 ≡ 30 ≡ 1 (mod14)

**Python implementation :**



Result :

