Euclidean Algorithm

The Euclidean algorithm is a way to find the greatest common divisor of two positive integers.

GCD of two numbers is the largest number that divides both of them

The Algorithm

The Euclidean Algorithm for finding GCD(A,B) is as follows:

- If A = 0 then GCD(A,B)=B, since the GCD(0,B)=B, and we can stop.
- If B = 0 then GCD(A,B)=A, since the GCD(A,0)=A, and we can stop.
- Write A in quotient remainder form ($A = B \cdot Q + R$)
- Find GCD(B,R) using the Euclidean Algorithm since GCD(A,B) = GCD(B,R)

Example

- Find the GCD of 270 and 192
- A=270, B=192
- A ≠0
- B ≠0
- Use long division to find that 270/192 = 1 with a remainder of 78. We can write this as:
- A=B*Q+R
- 270 = 192 * 1 +78
- Find GCD(192,78), since GCD(270,192)=GCD(192,78)
- A=192, B=78
- A ≠0
- B ≠0
- Use long division to find that 192/78 = 2 with a remainder of 36. We can write this as:
- A=B*Q+R
- 192 = 78 * 2 + 36

- Find GCD(78,36),
- A=78, B=36
- A $\neq 0$
- B $\neq 0$
- Use long division to find that 78/36 = 2 with a remainder of 6. We can write this as:
- $78 = 36 * 2 + 6$

- Find GCD(36,6),
- A=36, B=6
- A $\neq 0$
- B $\neq 0$
- Use long division to find that 36/6 = 6 with a remainder of 0. We can write this as:
- $36 = 6 * 6 + 0$

Find GCD(6,0),

- A=6, B=0
- A ≠0
- B =0, GCD(6,0)=6
- **So we have shown:**
- GCD(270,192) = GCD(192,78) = GCD(78,36) = GCD(36,6) = GCD(6,0) = 6

GCD(270,192) = 6

Modular Arithmetic

The Modulus

- If **a** is an integer and **n** is a positive integer, we define **a mod n** to be the **remainder** when **a** is divided by **n.** The integer **n** is called the **modulus.**
- Modular arithmetic is a system of arithmetic for integers, where numbers "wrap around" upon reaching a certain value called **modulus**
- 1:00 and and 13:00 hours are the same(1=13mod12)

Congruence

Integers that leave the same remainder when divided by the modulus m are somehow similar, however, not identical.

Such numbers are called **“congruent”.**

For instance, 1 and 13 and 25 and 37 are congruent mod 12 since they all leave the same remainder when divided by 12.

$a \equiv b \bmod m$

$15 \equiv 3 \pmod{12}$

$23 \equiv 11 \pmod{12}$

$33 \equiv 3 \pmod{10}$

$23 \equiv 3 \pmod{10}$

$38 \equiv 2 \pmod{12}$ q=3

$38 \equiv 14 \pmod{12}$ q=2

Computational Rules

- $((a \bmod m) + (b \bmod m)) \bmod m = (a + b) \bmod m$
- $((a \bmod m) - (b \bmod m)) \bmod m = (a - b) \bmod m$
- $((a \bmod m) * (b \bmod m)) \bmod m = (a * b) \bmod m$

Example

[(15 mod 8) + (11 mod 8)]mod 8=(15+11) mod 8

(7+3) mod 8 =26 mod 8

10 mod 8=26 mod 8

2=2

Properties of Modular Arithmetic

Property	Expression
Commutative Laws	$(a + b) \bmod n = (b + a) \bmod n$ $(a \times b) \bmod n = (b \times a) \bmod n$
Associative Laws	$[(a + b) + c] \bmod n = [a + (b + c)] \bmod n$ $[(a \times b) \times c] \bmod n = [a \times (b \times c)] \bmod n$
Distributive Laws	$[a \times (b + c)] \bmod n = [(a \times b) + (a \times c)] \bmod n$
Identities	$(0 + a) \bmod n = a \bmod n$ $(1 \times a) \bmod n = a \bmod n$
Additive Inverse	For each $a \in Z_n$, there exists a '$-a$' such that $a + (-a) \equiv 0 \bmod n$