Euclid Division Algorithm:

Properties of GCD:

① GCD(0,A) = GCD(A,0) = A

② GCD(A,B) = GCD(B,A)

③ GCD(A,B) = GCD(A-B,B), where A ≥ B

Proof of GCD(A,B) = GCD(A-B,B):

GCD(A,B) = g ⟶ ①

A = gx B = gy

A - B = gx - gy

g(x-y)

∴ GCD(A-B, B) = g ⟶ ②

① = ②

Euclid Algorithm:

$$GCD(A,B) = \begin{cases} A, & \text{if } B = 0 \\ GCD(B, A \bmod B), & \text{otherwise} \end{cases}$$

↓ Logic

GCD(B, A-B-B-...) → Property ③ of GCD

↳ until it becomes the least +ve number (modulus)

Time complexity = O(log(max(A,B)))