# EE4013 Assignment-1 Presentation

Krishna Srikar Durbha (EE18BTECH11014)

16th August 2021

# Euclidean Algorithm by Subtraction I

Euclidean Algorithm is a recursive method of finding Greatest Common Divisor of 2 numbers. For some positive integers $a$ and $b$, it works by repeatedly subtracting the smaller number from the larger one until they become equal. At this point, the value of either term is the greatest common divisor of our inputs.

**Algorithm:**

Step-1: If $a = b$, then return the value of a

Step-2: Otherwise, if a > b then let a = a - b and return to Step-1

Step-3: Otherwise, if a < b, then let b = b - a and return to Step-1

**Proof**:

Proof involves proving that, subtracting between $a$ and $b$ doesn't change GCD. Let $a$, $b$ be 2 positive integers such that $gcd(a, b) = m$ and $a > b$. So, it can be written as,

$$a = a_1 \times m \tag{1}$$

$$b = b_1 \times m \tag{2}$$

$$gcd(a, b) = m \implies gcd(a_1, b_1) = 1 \tag{3}$$

# Euclidean Algorithm by Subtraction II

We need to prove that $gcd(a-b, b) = m$. We will prove it by contradiction. Let $gcd(a-b, b) = M$ where $M > m \implies k \neq 1$

$$
\begin{aligned}
a - b &= (a_1 - b_1) \times m && (4)\\
b &= b_1 \times m && (5)\\
gcd(a-b, b) = M \implies M &= k \times m \text{ (For some integer } k\text{)} && (6)\\
a - b \equiv 0 \pmod{M} &\text{ and } b \equiv 0 \pmod{M} && (7)\\
\implies a - b \equiv 0 \pmod{km} &\text{ and } b \equiv 0 \pmod{km} && (8)\\
\implies a_1 - b_1 \equiv 0 \pmod{k} &\text{ and } b_1 \equiv 0 \pmod{k} && (9)\\
\implies a_1 \equiv 0 \pmod{k} &\text{ and } b_1 \equiv 0 \pmod{k} && (10)
\end{aligned}
$$

We know that $gcd(a_1, b_1) = 1$, so there doesn't exist a $M \neq m$ such that $gcd(a-b, b) = M$. So, from contradiction, $gcd(a, b) = gcd(a-b, b) = M$ for $a > b$. Worst Case Time-Complexity is $\mathcal{O}(a+b)$.

# Euclidean Algorithm by Division I

Euclidean Algorithm by Division involves divison rather than subtraction. For some positive integers $a$ and $b$, $gcd(a, b) = gcd(b, a \mod b)$. We repeat the procedure until convergence.

Let $a$, $b$ be 2 positive integers such that $a > b$. By applying Euclid's Algorithm from $0^{th}$-step ,

$$a = q_0 b + r_0 \tag{11}$$

$$b = q_1 r_0 + r_1 \tag{12}$$

$$r_0 = q_2 r_1 + r_2 \tag{13}$$

$$r_1 = q_3 r_2 + r_3 ... \tag{14}$$

Here $a > b$, $b > r_0$, $r_0 > r_1$, $r_1 > r_2$.. and so on. So, remainders are decreasing after each step.

# Euclidean Algorithm by Division II

Let at $n^{th}$-step $r_{n-2} = q_n r_{n-1}$ i.e $r_n = 0$.

$$r_{n-2} = q_n r_{n-1} \tag{15}$$

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \tag{16}$$

$$\implies r_{n-1} \text{ divides } r_{n-2}, r_{n-3}, r_{n-4}, ..., r_1, r_0, b, a \tag{17}$$

$$\implies a \equiv 0 \pmod{r_{n-1}} \text{ and } b \equiv 0 \pmod{r_{n-1}} \tag{18}$$

So, the proof goes as $gcd(a, b) = r_{n-1}$. We will prove it by contraction. Let $gcd(a, b) = M \implies M > r_{n-1}$,

$$a = a_1 \times M \text{ and } b = b_1 \times M \tag{19}$$

$$r_0 = a - q_0 b = M(a_1 - q_0 b_1) \tag{20}$$

$$r_1 = b - q_1 r0 = M(b_1 - a_1 + q_0 b_1) \tag{21}$$

# Euclidean Algorithm by Division III

So, M divides $a, b, r_0, r_1, ...$ and so on all the following remainders. So, $M$ should divide $r_{n-1}$, which implies $r_{n-1} \geq M$ which is a contraction from $M > r_{n-1}$.

So, there doesn't exist a $M > r_{n-1}$ which is a divisor of $a$ and $b$. So, $gcd(a, b) = r_{n-1}$.