DISCRETE MATHEMATICS PROJECT

Assigned by : Professor Manish K Gupta
Course : SC 205
DISCRETE MATHEMATICS
DA-IICT
GANDHINAGAR

Made by: Dhameliya Sanny
ID : 201901031

Euclid Algorithm

Dhameliya Sanny,
201901031,
DAIICT,
GANDHINAGAR,
GUJARAT,
INDIA
201901031@daiict.ac.in

June 28, 2022

Abstract

Euclid (named after the Greek mathematician Euclid) algorithm is an approach for finding the Greatest Common Divisor (GCD) of two positive integers, which can be used to reduce fractions to their simplest form, and is a part of many other number-theoretic and cryptography.

1 INTRODUCTION

[1] Probably the most common use of the Euclidean Algorithm around the world is for finding modular inverse there is a simple tweak of it that allows you given two integers a,b to calculate integers X,Y such that

$$aX + bY = GCD(a, b)$$

This is known as the extended Euclid Algorithm.In fact, you can skip calculating Y entirely.

2 PROBLEM FRAMEWORK

Well, if a,b are co-prime this will find you interwar such that

$$aX + bY = 1$$

Which to say that

$$aX \equiv 1 \mod b$$

that is it will find integer X that is inverse of a mod b. since the extended Euclid Algorithm runs quite quickly even for integer it,is efficient method for computing modular inverse. This is very important, because countless cryptography schemes require finding modular inverses as a basic building block. For example, in RSA you need to calculate a modular inverse as part of key generation. In ElGamal, modular inverse is used as part of decryption. As variations of all of these different schemes are used any time that you want to send information in a secure manner over the Internet (which is to say, any time you want to do virtually anything on the Internet), it is unlikely that there is another area in which the Euclidean algorithm is called more often.

3 THE SEQUENTIAL SOLUTION

lt is Named after the ancient Greek Mathematician Euclid, who first described it his elements (300 B.C).Euclid Algorithm is an efficient method computing the Greatest Common Divisor(GCD).

Formally calculating GCD(a,b) : Suppose $(a > b)$

1. divide b into a :

$$a = q_1 b + r_1$$

2. if $r_1 == 0$ then

b/a and $GCD(a, b) = b$

else

represent b by $b = q_2 r_1 + r_2$

3.continue in this way until reminder is Zero, the GCD is last non Zero reminder.

$$a = q_1 b + r_1$$
$$b = q_2 r_1 + r_2$$
$$r1 = q_3 r_2 + r_3$$
$$.$$
$$.$$
$$.$$
$$r_k - 2 = q_k r_k - 1 + r_1 k$$
$$b_k - 1 = q_k + 1 r_k + 0$$
$$GCD(a, b) = r_k$$

4 RECURSIVE VERSION

GCD(a,b)

r = a mod b

if $r == 0$

return b;

else

return GCD(a,b);

5 Real life application of Euclid

1.House foundation construction
2.cryptography and RSA

1.House foundation construction

[2] Suppose there is a need for cost estimation on the total number of block (119 ft ,width doesn't matters) required for the above house foundation construction of $(544ft * 356ft)$ dimension with 230ft height.

Known parameters :-

Land:

$$Length(x) = 544ft$$
$$Breadth(y) = 356ft$$
$$Foundation_height = 176ft$$

Block:

$$Length(r) = 119ft$$

Width (doesn't really matters)

Step 1 : Euclid of land length (544) by Block length (119)

Greatest Common Divisor = 17

$$Nos.ofblocks(1ft) = (544/119) * 17 = 77.71ft$$

Total no of blocks in 230 ft $tall = 77.714 * 230 = 17874.28$ blocks to raise the building foundation on single horizontal (length) level

For the two horizontal$sides = 17874.28 * 2 = 35748.56blocks$

If one block of 119 ft cost 20, it means we will $need = 20 * 17874.28 = 500,480$ to raise the building foundation on single horizontal (length) level

2.cryptography and RSA [3]

$$RSA$$

1.Generate two large unique Prime Numbers p and q.
2.compute $n = p * q$ and $Q = (p-1) * (q-1)$
3.select a random Number $1 < e < Q$ such that $GCD(e, Q) = 1$
4.compute the unique integer $1 < d < Q$ such that

$$ed \equiv 1 \mod Q$$

5.(d,n) is the Privet Key.
6.(e,n) Public Key.

$$Encryption$$

Represent a message as an integer M in the interval $[0, n-1]$ send out the encrypt data

$$c \equiv m^e \mod Q$$

$$Decryption$$

Decrypt the key

$$m \equiv c^d \mod n$$

6 APPLICATIONS

Euclid Algorithm is use to find GCD of any two numbers.when GCD values is equal to 1 Menes it is co-prime numbers it is use to RSA cryptography.this is very important of GCD is to find inverse of the numbers. this is very important use of Euclid Algorithm.

References

[1] Euclidean algorithm. https://en.wikipedia.org/wiki/Euclidean$_algorithm$.

[2] Euclidean algorithm in daily life. https://www.quora.com/What-are-the-use-of-Euclidean-algorithm-in-daily-life.

[3] RSA Algorithm. https://www.di-mgt.com.au/rsa$_alg.html$.