Exploring Number Theory: Euclidean Algorithm, Euler’s Phi Function, and Euler’s Theorem

WOMANIUM GLOBAL ONLINE QUANTUM MEDIA PROJECT #Quantum30 Challenge Day 8

Listen

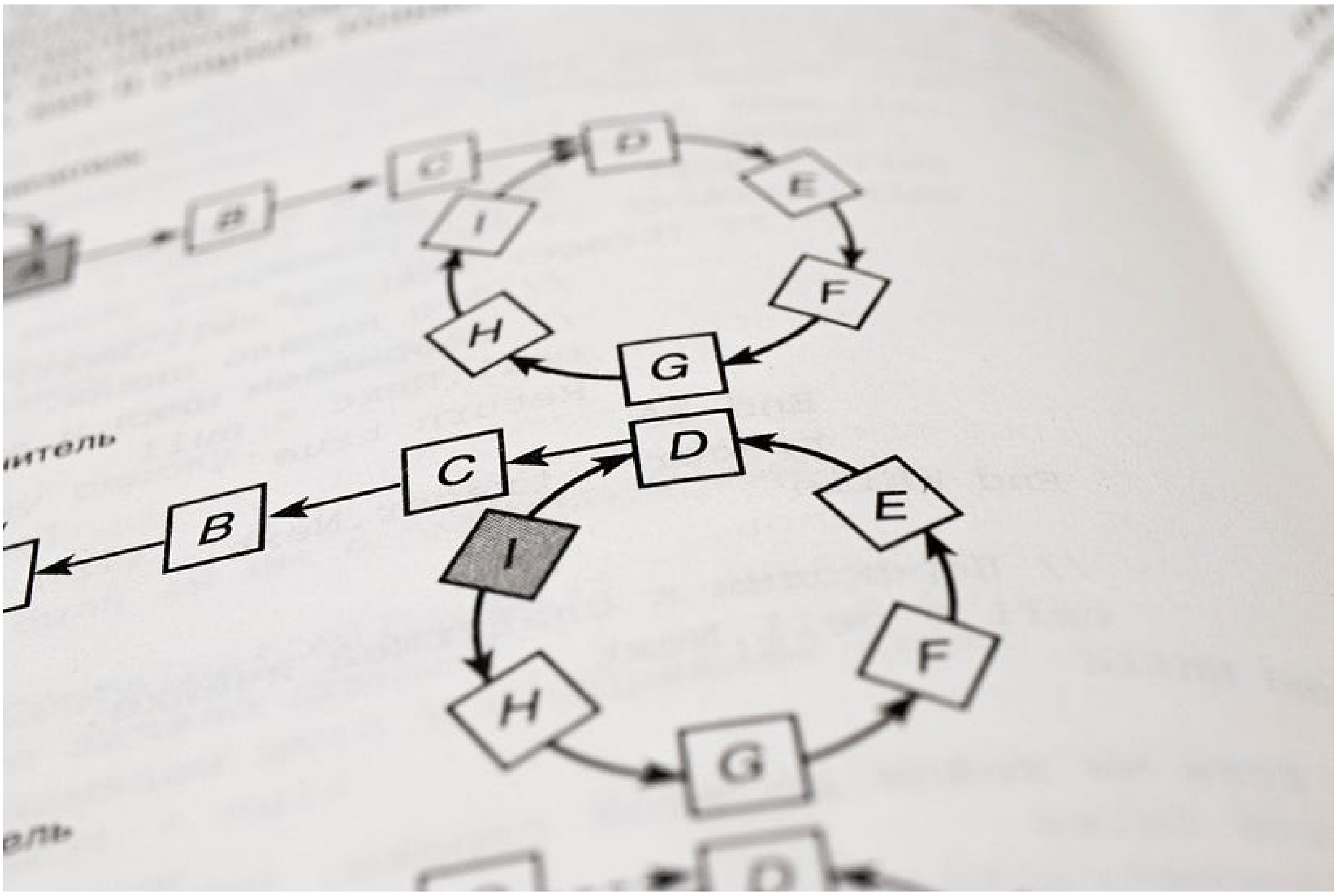


Photo by Андрей Сизов on Unsplash

Introduction to Number Theory and Its Significance:

Number theory, a branch of mathematics, delves into the properties and relationships of integers. This field holds great significance in various applications, including cryptography and coding theory. In the realm of Public Key Cryptography (PKC), understanding concepts like the Euclidean Algorithm, Euler’s Phi function, and Euler’s Theorem becomes crucial. These concepts lay the foundation for secure communication systems by enabling efficient encryption and decryption of messages.

The Euclidean Algorithm: Finding Greatest Common Divisors

At the core of modular arithmetic lies the Euclidean Algorithm. Its primary goal is to determine the greatest common divisor (GCD) of two integers. This algorithm plays a pivotal role in modular arithmetic, which involves working with remainders when dividing integers.

Consider an example where we wish to find the GCD of two numbers, say 48 and 18. We repeatedly apply the division algorithm:

$48 = 18 \cdot 2 + 12$

$18 = 12 \cdot 1 + 6$

$12 = 6 \cdot 2 + 0$

The last non-zero remainder, 6, is the GCD of 48 and 18. This algorithm can be extended to modular arithmetic by working with remainders in modulo operations.

Benefits of the Euclidean Algorithm:

The Euclidean Algorithm provides a more efficient approach to finding GCDs compared to exhaustive methods. In modular arithmetic, this efficiency becomes paramount when dealing with large numbers. Additionally, the algorithm can be extended to handle more complex scenarios, such as finding GCDs in the context of modular inverses.

. . .

Demonstrating the Euclidean Algorithm in Modular Arithmetic:

Consider the integers $r_0 = 973$ and $r_1 = 301$. To find their GCD using the Euclidean Algorithm, we perform the following steps:

$973 = 301 \cdot 3 + 70$

$301 = 70 \cdot 4 + 21$

$70 = 21 \cdot 3 + 7$

21 = 7·3 + 0

The last non-zero remainder is 7, which is the GCD of 973 and 301. Notably, 973 mod 301 = 70, and thus, we can observe that gcd(r_0, r_1) = gcd(r_0 mod r_1,r_1).

The Extended Euclidean Algorithm:

In some cases, we require not only the GCD but also the coefficients s and t that satisfy Bézout's identity: $s·r_0 + t·r_1$ = gcd(r_0, r_1). The Extended Euclidean Algorithm provides a method to find these coefficients.

For r_0 = 973 and r_1 = 301, we can compute s and t using the following recursive formula:

$$s = s_{prev} - q \cdot s_{curr}$$
$$t = t_{prev} - q \cdot t_{curr}$$

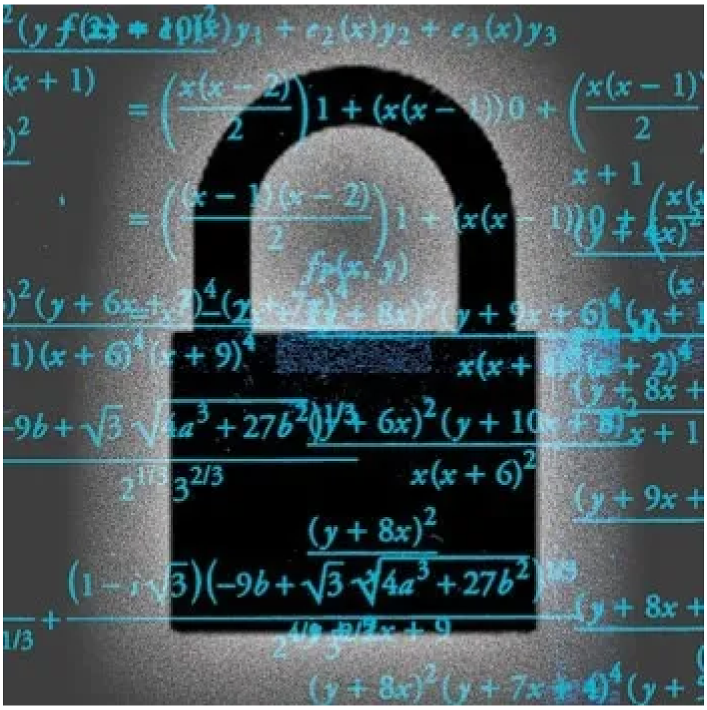
Starting with

$$s_{prev} = 1, s_{curr} = 0, t_{prev} = 0, and\ t_{curr} = 1$$

and updating them after each iteration with q as the quotient.

Applications of the Extended Euclidean Algorithm:

The Extended Euclidean Algorithm has various applications, with one notable use being in computing modular inverses. In PKC, modular inverses are crucial for operations like decryption. The Extended Euclidean Algorithm provides an efficient way to calculate these inverses.



Picture Credit: https://math.duke.edu/courses/cryptography-and-society

. . .

Euler’s Phi Function and Its Significance:

Euler’s Phi function, denoted as ϕ(n), is a vital tool in number theory. It counts the number of positive integers less than n that are coprime to n, i.e., share no common factors with n.

For example, let m = 240. We can find ϕ(n) by considering the prime factorization of 240, which is 2^4 * 3^1* 5^1. Applying the formula for ϕ(n) , we get:

$$\phi(240) = 240 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 64$$

Fermat’s Little Theorem and Euler’s Theorem:

Fermat’s Little Theorem and Euler’s Theorem establish crucial relationships between modular exponentiation and integer properties. Fermat’s Little Theorem states that if a is an integer and p is a prime number not dividing a, then

$$a^{p-1} \equiv 1 \pmod{p}$$

Euler’s Theorem extends this concept to non-prime moduli. If a and m are coprime integers, then

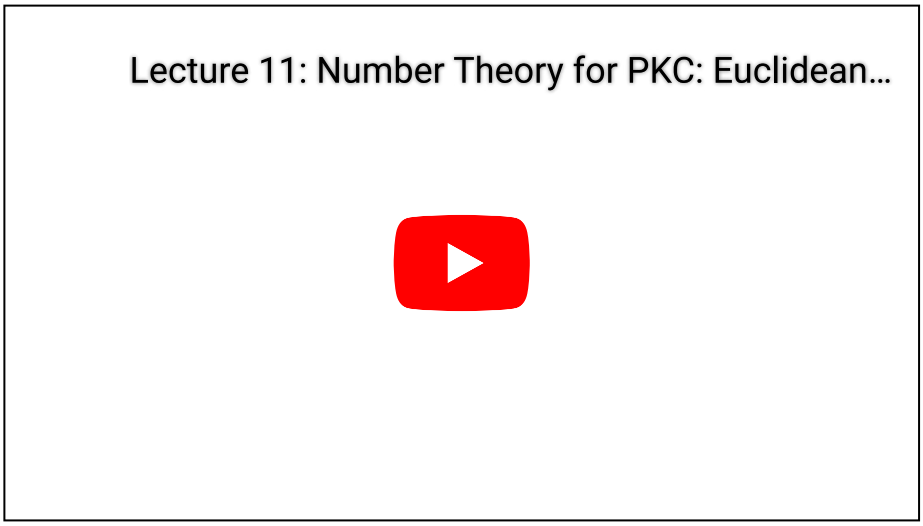
$$a^{\phi(m)} \equiv 1 \pmod{m}$$

Conclusion:

Number theory’s significance in PKC is undeniable. The Euclidean Algorithm, Euler’s Phi function, and Euler’s Theorem collectively contribute to the secure transmission of information through encryption and decryption. The modular arithmetic foundation established by these concepts enables cryptographic protocols that safeguard digital communication in today’s interconnected world.

· · ·

This article is written based on the below video lecture.



Lecture 11: Number Theory for PKC: Euclidean…

This video is provided by QuantumComputingIndia, as a part of the #Quantum30 learning challenge.

I have been exploring Cryptography since the start of this month and throughout this month I will gain in-depth knowledge of this field. Your suggestion will be really helpful for my future endeavor.

This is a part of **WOMANIUM GLOBAL ONLINE QUANTUM MEDIA PROJECT**. This project will help me to dive into the cryptographic world(From Classical to Quantum Approach). From onwards I shall share my learning log with others who are curious about this particular and promising field.

I want to take a moment to express my gratitude to **Marlou Slot** and **Dr. Manjula Gandhi** for this initiative and encouragement and sincere thanks to **Moses Sam Paul Johnraj** for providing the 30-day schedule.

#Quantum30 #QuantumComputing #QuantumJourney #QuantumEnthusiast #Womanium #Cryptography #QuantumCryptography #QuantumComputingIndia

Written by Murshed SK

Physics Undergrad | Quantum Information Science and Computation Enthusiast | Passionate about Quantum Machine Learning | <Womanium | Quantum> Scholar