Modular Arithmetic: The Key to Unbreakable Secrets in Cipher

WOMANIUM GLOBAL ONLINE QUANTUM MEDIA PROJECT #Quantum30 Challenge Day 2

Listen

Introduction:

In today's interconnected world, the security of sensitive information is of utmost importance. Cryptography, the art of securing data through mathematical techniques, plays a pivotal role in ensuring confidentiality and integrity. At the core of modern cryptography lies ***modular arithmetic***, a fascinating branch of mathematics that deals with numbers wrapping around a fixed value called the modulus. In this comprehensive article, we will delve into the intricacies of modular arithmetic and explore its indispensable role in cryptography. We will also examine two classic cryptographic algorithms — the Shift Cipher and the Affine Cipher — to witness the practical applications of this mathematical marvel.

. . .

Understanding Modular Arithmetic and the Modulo Operator:

Modular arithmetic involves performing arithmetic operations on numbers that "wrap around" once a fixed value (the modulus) is reached. The modulo operator (denoted by '%' or 'mod') is employed to find the remainder when one number is divided by another.

Let $a,r,m \in Z$ and $m > 0$,

then, $a \equiv r \bmod m$ if m divides (a-r) i.e. $m|(a-b)$.

For instance, consider $a = 17$, $b = 5$, then $17 \equiv r \bmod 5 \Rightarrow r = 2$.

Here, r = 2 is the remainder if we divide 17 by 5. Therefore, (a-r) = (17–2) = 15 is divisible by 5. But this r can be any integer not just 2 rather depending on the value of m and here comes the use of modular operator in cryptography. For instance, r may be r = 7, and for it (17–7) = 10 which is also divisible by 5. You can check with different values of r by adding or subtracting 5 (as m = 5 in this example) to it. Therefore we conclude that the remainder is not unique.

There comes the concept of the equivalence class.

Equivalence Classes and Modular Congruence:

In modular arithmetic, we classify numbers that yield the same remainder when divided by a modulus into equivalence classes. For example, in modulo 6, the equivalence class of 9 comprises all integers of the form (6n + 9), where n is an integer. So, the equivalence class of 9 includes {..., -9, -3, 3, 9, 15, ...}.

Now comes another important concept in cryptography as well as in Abstract Algebra which is 'Rings' and some essential ciphers.

Rings — A Versatile Algebraic Structure:

Rings are algebraic structures that form the backbone of modular arithmetic. A ring consists of a set equipped with two binary operations: addition and multiplication. For a set to be considered a ring, it must satisfy properties like closure under addition and multiplication, associativity, distributivity, and the existence of additive and multiplicative identities.

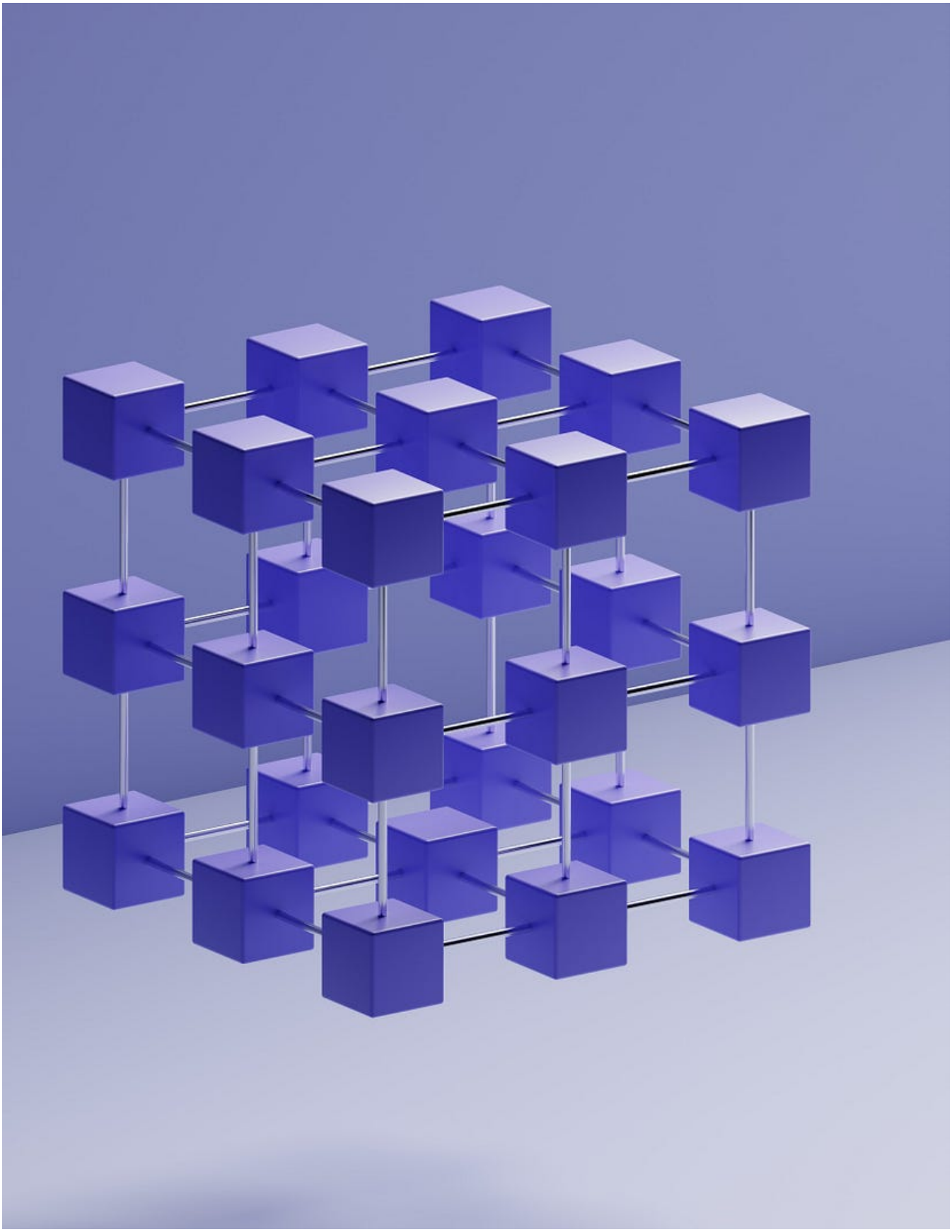


Photo by Shubham's Web3 on Unsplash

Shift Cipher:

The Shift Cipher, also known as the Caesar Cipher, is a classic encryption method that shifts each letter of the plaintext by a fixed number of positions in the alphabet.

For example, with a shift of 5, “HELLO” becomes “MJQQT.”

Affine Cipher:

The Affine Cipher takes encryption a step further by combining multiplication and addition in modular arithmetic. It employs two keys: ‘a’ (the multiplier) and ‘b’ (the shift). The encryption formula is E(x) = (ax + b) % m, where ‘m’ is the size of the alphabet. For example, with a=3 and b=7, the plaintext “CRYPTOGRAPHY” becomes “NMDARZMVKSY.”

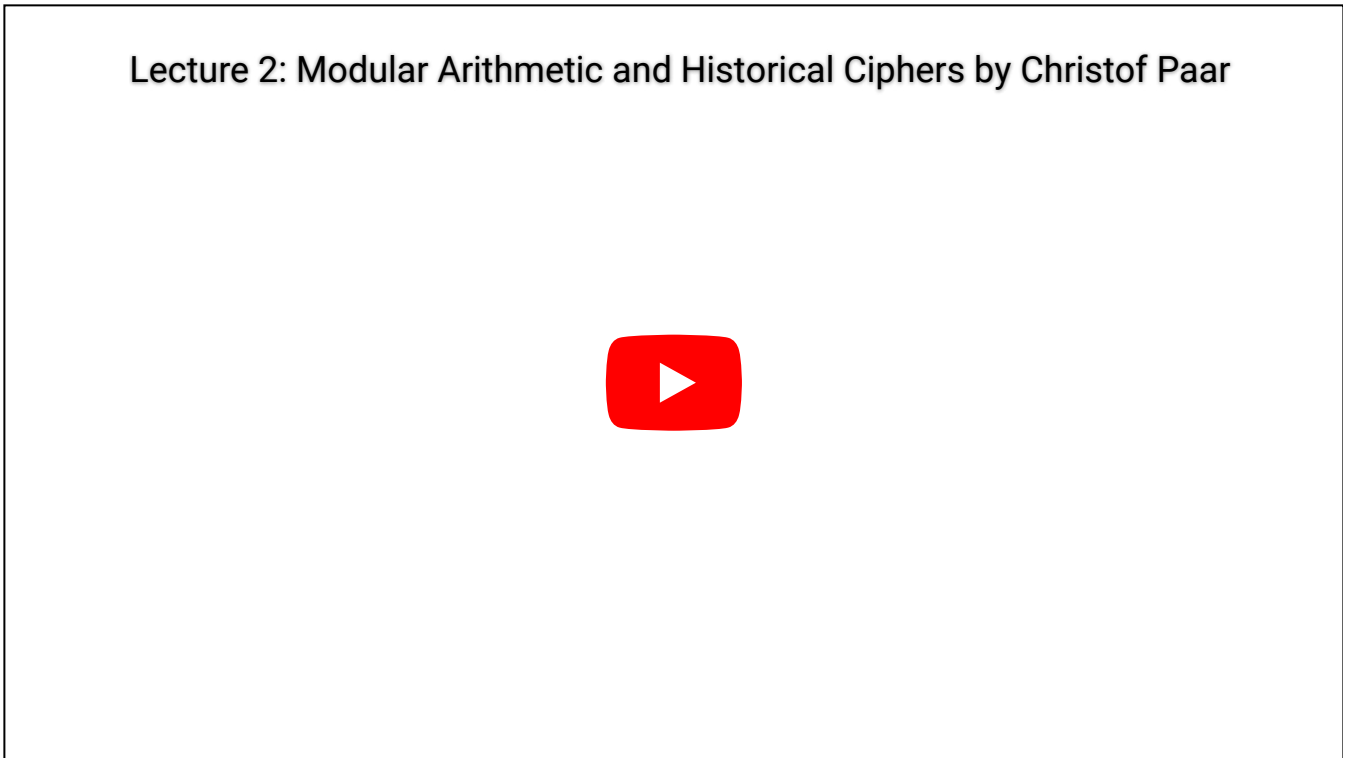
Conclusion:

Modular arithmetic serves as the backbone of modern cryptography, ensuring secure data transmission in various domains such as communications, e-commerce, and financial transactions. Its ability to handle remainders and establish equivalence classes is at the heart of many cryptographic algorithms. The Shift Cipher and the Affine Cipher exemplify the practical applications of modular arithmetic, showcasing how seemingly simple mathematical operations can create powerful encryption techniques.

As technology continues to advance, the study of modular arithmetic and cryptography will remain at the forefront of information security, safeguarding our digital world against potential threats and ensuring the confidentiality of sensitive data.

. . .

This article is written based on the below video lecture.



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

For the sake of simplicity, I try not to include all the mathematical derivation and concepts. Otherwise, this article will be long and might be boring also. This article is written for general purposes and an overview of this field. This field is really interesting and as a math guy, I really enjoy the whole topic. However, Interested people find those concepts in the video lecture if they want to deep dive into this field.

I am 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

Written by Murshed SK

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