JANKIDEVI
PUBLIC SCHOOL

Modular Arithmetic & Cryptography

Applied Mathematics (241)

Academic year 2023-24

Submitted by-

Kartavya Jharwal
XII-Commerce

Submitted to-

Mr. Shubham Nigam.
Applied Mathematics
Teacher

Certificate

This is to certify that Kartavya Jharwal of Grade XII has completed his Applied mathematics project titled *"Modular Arithmetic & Cryptography"* under the guidance of Mr. Shubham Nigam for the academic year 2023-24. The certified student has been dedicated throughout his research and completed his work before the given deadline without missing any important details for the project. It is also certified that this project is the individual work of the student and can be submitted for evaluation.

[redacted]

Mr. Shubham Nigam.
Applied
Mathematics
Teacher

[redacted]

Principal signature &
School stamp

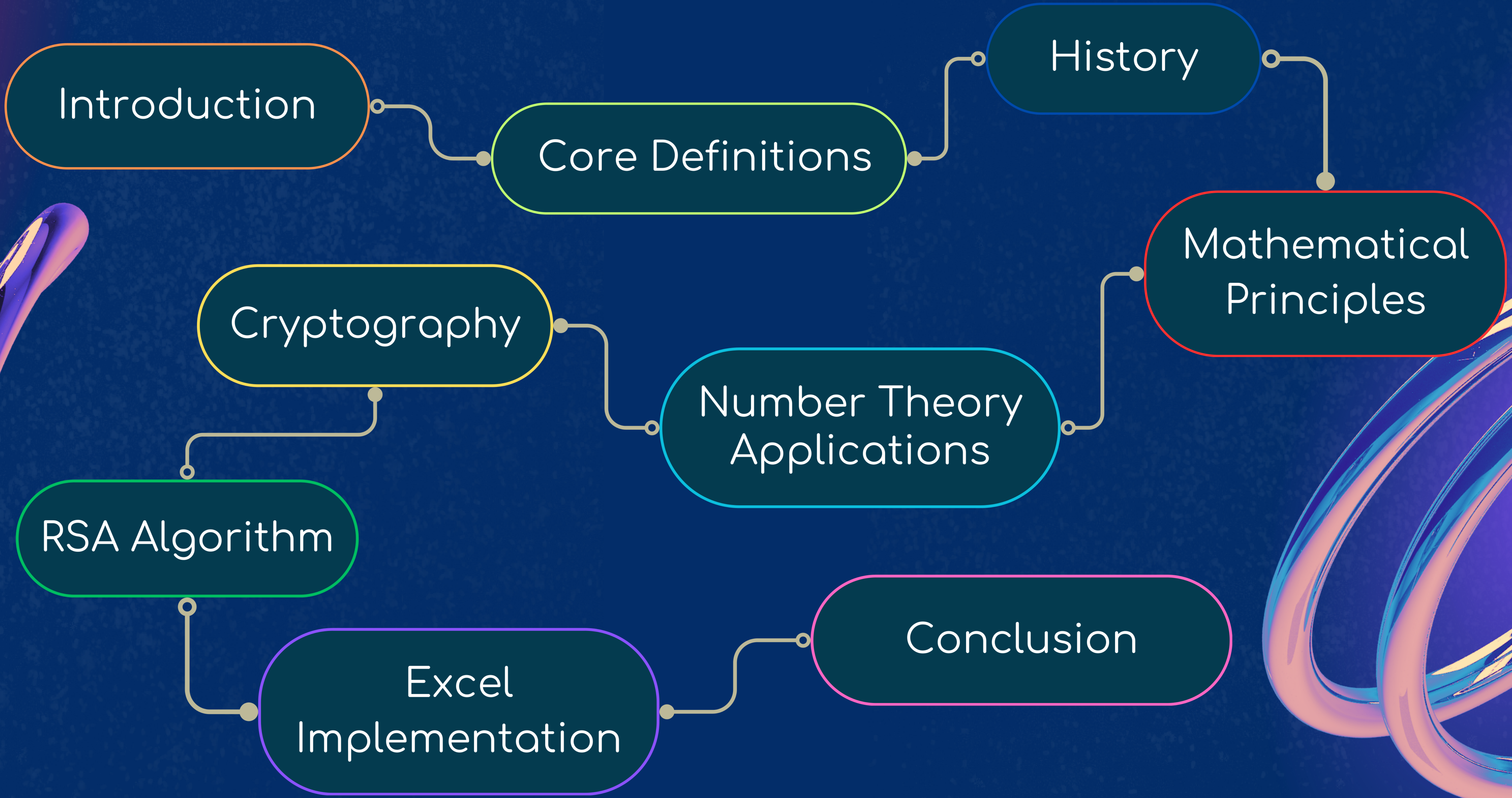
Acknowledgment

I extend my deepest gratitude to everyone who has played a role, directly or indirectly, in supporting me throughout the development of this project.

Special thanks to my Applied Mathematics mentor, Mr. Shubham Nigam, whose guidance and insights have been instrumental in shaping this work.

Lastly, heartfelt appreciation to my parents and friends for their unwavering support and coordination throughout this project.

Index



Introduction

Core Definitions

History

Mathematical Principles

Number Theory Applications

Cryptography

RSA Algorithm

Excel Implementation

Conclusion

Introduction

At its core, modular arithmetic is a unique form of arithmetic intricately connected to remainders. The arithmetic operations within this system are based on the residual values left when integers are divided by a fixed quantity, known as the modulus. In simpler terms, modular arithmetic encapsulates the essence of counting within a cyclic framework, where the remainder after division becomes a central focus.

The roots of modular arithmetic extend back to ancient civilizations, where early mathematicians grappled with the cyclical nature of time and numerical patterns. The development of modular arithmetic is marked by its application in solving real-world problems related to calendars, timekeeping, and divisibility.

Introduction

Carl Friedrich Gauss, a prominent mathematician, notably shaped the modern understanding of modular arithmetic. His seminal work, "Disquisitiones Arithmeticae," published in 1801, emphasized the arithmetic of remainders as a foundational aspect of this mathematical discipline. Today, modular arithmetic is an indispensable tool, seamlessly integrated into various branches of mathematics.

Beyond its historical significance, modular arithmetic emerges as a versatile tool with applications spanning cryptography, computer science, and beyond. Its distinctive arithmetic, centered around remainders, allows for the simplification of complex computations involving residual values. In subsequent sections, I will unravel the intricacies of modular arithmetic operations, exploring how it harmonizes with fundamental mathematical expressions involving addition, subtraction, multiplication, and division.

MODULUS *Properties*

01

if $A \equiv B \pmod{C}$ then $B \equiv A \pmod{C}$

02

if $A \equiv B \pmod{C}$ and $B \equiv D \pmod{C}$ then $A \equiv D \pmod{C}$

03

$(A + B) \bmod C = (A \bmod C + B \bmod C) \bmod C$

04

$(A - B) \bmod C = (A \bmod C - B \bmod C) \bmod C$

05

$(A * B) \bmod C = (A \bmod C * B \bmod C) \bmod C$

06

$A^B \bmod C = ((A \bmod C)^B) \bmod C$

Number Theory Applications

Explore practical applications of modular arithmetic in number theory, covering Fermat's Little Theorem, Euler's Totient Function, the Chinese Remainder Theorem, the Möbius Function, and the Divisor Sum Function. These applications showcase the versatility of modular arithmetic, from primality testing to cryptography.

01.

Fermat's Little Theorem, a cornerstone of number theory rooted in modular arithmetic, states that if p is a prime number and a is an integer not divisible by p, then $a*p-1\equiv 1(\text{mod } p)$. This theorem provides a powerful tool for verifying primality and plays a crucial role in modular exponentiation.

02.

Euler's Totient Function, denoted as $\phi(n)$, is intimately connected to modular arithmetic. It calculates the count of positive integers less than n that are coprime to n. Specifically, $\phi(n)$ is the order of the multiplicative group of integers modulo n, showcasing its inherent link to modular structures.

03.

The Möbius function, denoted as $\mu(n)$, is a number-theoretic function deeply rooted in modular arithmetic.
It is defined as follows: $\mu(n)=0$ if n has a squared prime factor, $\mu(n)=1$ if n is a product of an even number of distinct primes, and $\mu(n)=-1$ if n is a product of an odd number of distinct primes.

04.

The divisor sum function, often denoted as $\sigma(n)$, involves the summation of all positive divisors of n. Its relationship with modular arithmetic becomes apparent when considering the properties of divisors in the context of modular operations, illustrating how modular arithmetic interfaces with divisor-related functions.

05.

The Chinese Remainder Theorem efficiently solves systems of simultaneous modular congruences with pairwise coprime moduli. Ensuring a unique solution modulo the product of the moduli, it decomposes complex equations into simpler, independent components. This elegant theorem is fundamental in modular arithmetic, offering a concise method for handling intricate systems of equations.

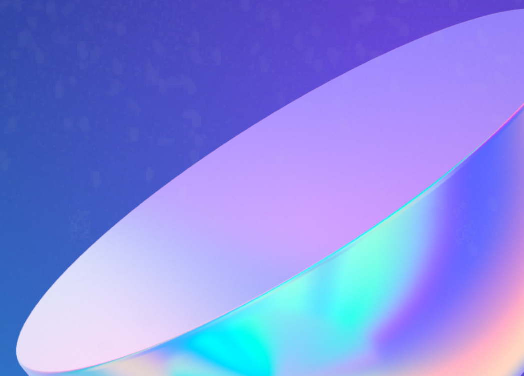
Cryptography and Modular Arithmetic

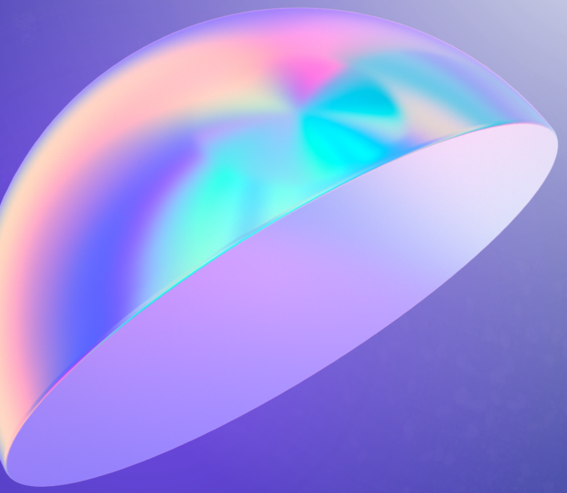
Introduction:

Cryptography, an essential aspect of secure communication, is deeply rooted in mathematical principles, with modular arithmetic serving as a cornerstone in various cryptographic algorithms. One such prominent algorithm is RSA, a widely used public-key cryptosystem known for its robust security features.

Modular Arithmetic in Cryptography:

1. Foundation of Cryptographic Operations:
    - Modular arithmetic lays the foundation for cryptographic operations by introducing the concept of remainders when dividing integers.
2. RSA Algorithm Overview:
    - RSA, a public-key cryptosystem, heavily relies on modular arithmetic for secure communication.





Cryptography and Modular Arithmetic

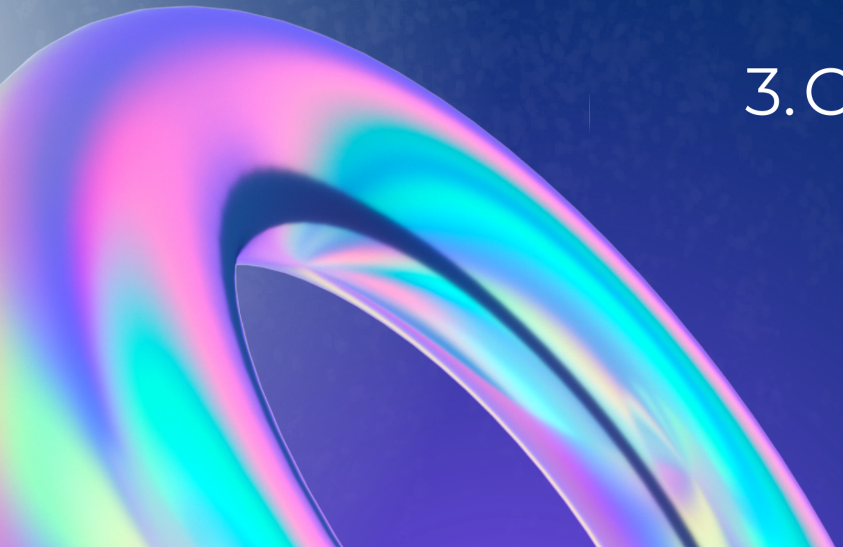
RSA Key Generation:

RSA key generation involves meticulous selection to ensure the security of the algorithm.

1. Public and Private Key Computation:
    - The totient function $\varphi(N) = (p-1)(q-1)$ is calculated.
    - A public exponent 'e' is chosen, often a small prime.
    - The private exponent 'd' is computed such that $(e * d) \equiv 1 \pmod{\varphi(N)}$.

Modular Arithmetic in RSA Encryption:

1. Plaintext to Numerical Value:
    - The plaintext is converted into a numerical value, M.
2. Encryption Process:
    - Cipher text (C) is computed using modular exponentiation: $C \equiv M*e\ (mod\ N)$.
3. Clarification in RSA Encryption:
    - Encryption involves raising the plaintext M to the power of the public exponent e and then taking the result modulo N: $C \equiv M*e\ (mod\ N)$.



RSA Algorithm and Modular Arithmetic

Detailing RSA Key Generation:

The RSA key generation involves the selection of two large prime numbers, p and q. The product N=p*q forms the modulus for both the public and private keys. Mathematically, this process is represented as:

$$N=p*q$$

The security of RSA relies on the complexity of factoring N. Larger prime numbers increase the difficulty of this factorization, thus enhancing security. The public key e and private key d are then computed using modular arithmetic:

$$e*d\equiv1(\mathrm{mod}\phi(N))$$

Here,)$\phi(N)$ is Euler's totient function, and $\equiv$ denotes congruence.

Clarification in RSA Encryption and Decryption:

RSA Encryption:

The encryption process involves raising the plaintext M to the power of the public exponent e and then taking the result modulo N:

$$C\equiv M*e(\mathrm{mod}N)$$

RSA Decryption:

Decryption uses the private exponent d to recover the original plaintext. The ciphertext C is raised to the power of d modulo N:

$$M\equiv C*d(\mathrm{mod}N)$$

Security and Applications of RSA:

RSA's security is deeply rooted in modular arithmetic, especially in the context of key length considerations and addressing challenges:

1. Key Length Considerations:
   - The length of N significantly impacts security. A longer N provides resistance against brute-force attacks.
2. Challenges Over Time:
   - Ongoing advancements in computing necessitate adjustments in key length to maintain security standards.
3. Vulnerabilities and Solutions:
   - Historical vulnerabilities, like insufficient randomness in key generation, have been addressed through continuous algorithmic evolution.

Linking Modular Exponentiation to RSA:

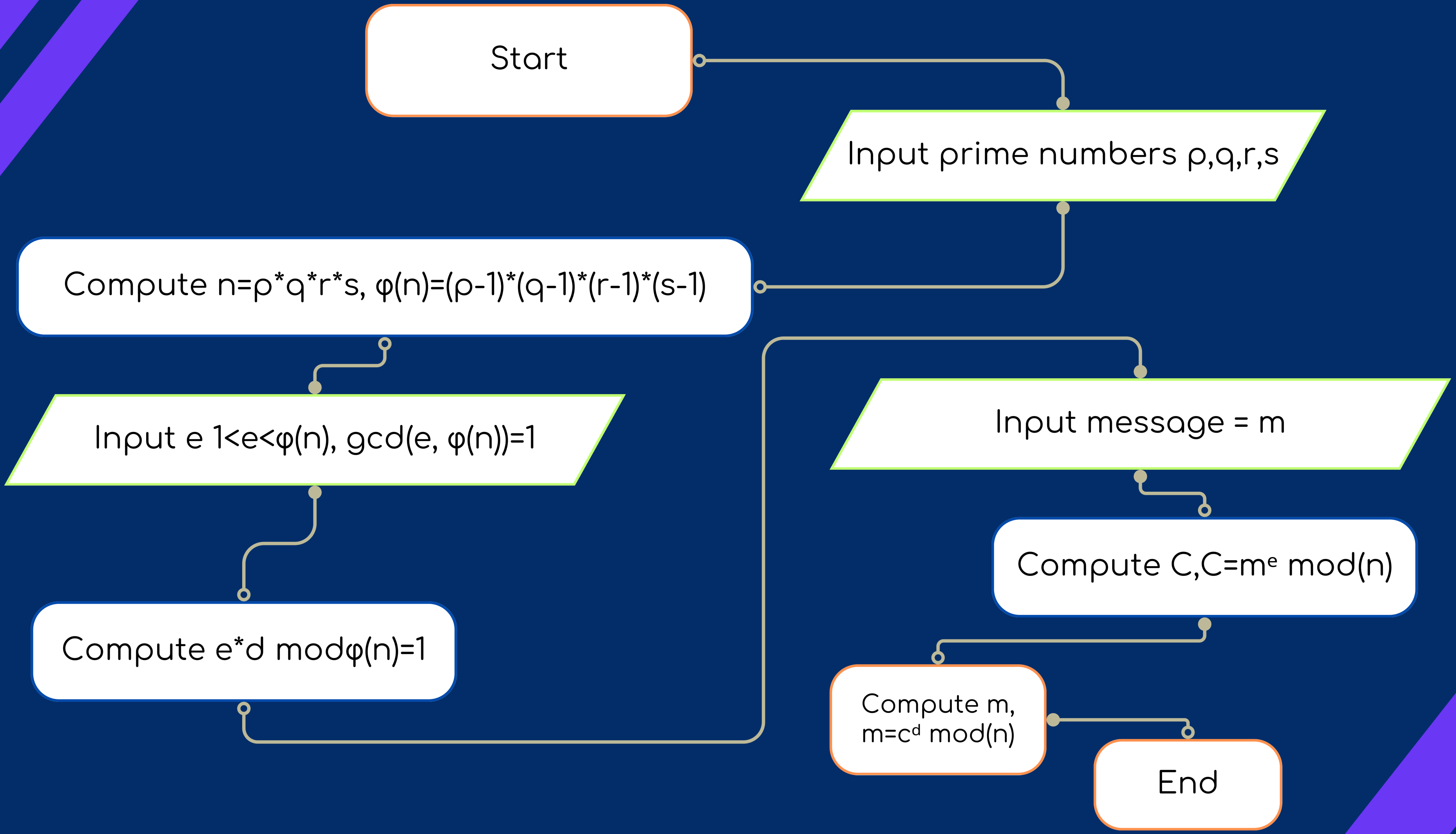
The core of RSA encryption and decryption lies in modular exponentiation. For encryption:

$$C \equiv M*e(modN)$$

And for decryption:

$$M \equiv C*d(modN)$$

This integration with modular arithmetic ensures the security of RSA, creating a formidable mathematical foundation against unauthorized access and information compromise.



Start

Input prime numbers p,q,r,s

Compute n=p*q*r*s, φ(n)=(p-1)*(q-1)*(r-1)*(s-1)

Input e 1<e<φ(n), gcd(e, φ(n))=1

Compute e*d modφ(n)=1

Input message = m

Compute C,C=m^e mod(n)

Compute m,
m=c^d mod(n)

End

Examples

Problem: If it's currently 3 o'clock, what time will it be in 14 hours using a 12-hour clock?
Solution: (3+14)mod 12 = 5.(3+14) mod 12=5.
So, it will be 5 o'clock.

Problem: If an event starts at 8:45 and lasts for 2 hours and 30 minutes, what time will it end?
Solution:(8×60+45+150)mod 720=375mod 720=375.
(8×60+45+150)mod720=375mod720=375.
Converting 375 back to hours and minutes, the event will end at 6:15.

Problem: If today is Tuesday, what day will it be 10 days from now?
Solution:(2+10)mod 7=5.(2+10)mod7=5.
So, it will be Sunday.

Problem: If today is Friday, and you want to know the day of the week 25 days from now, what day will it be?
Solution:(5+25)mod 7=2.(5+25)mod7=2.
So, it will be a Tuesday.

More Examples

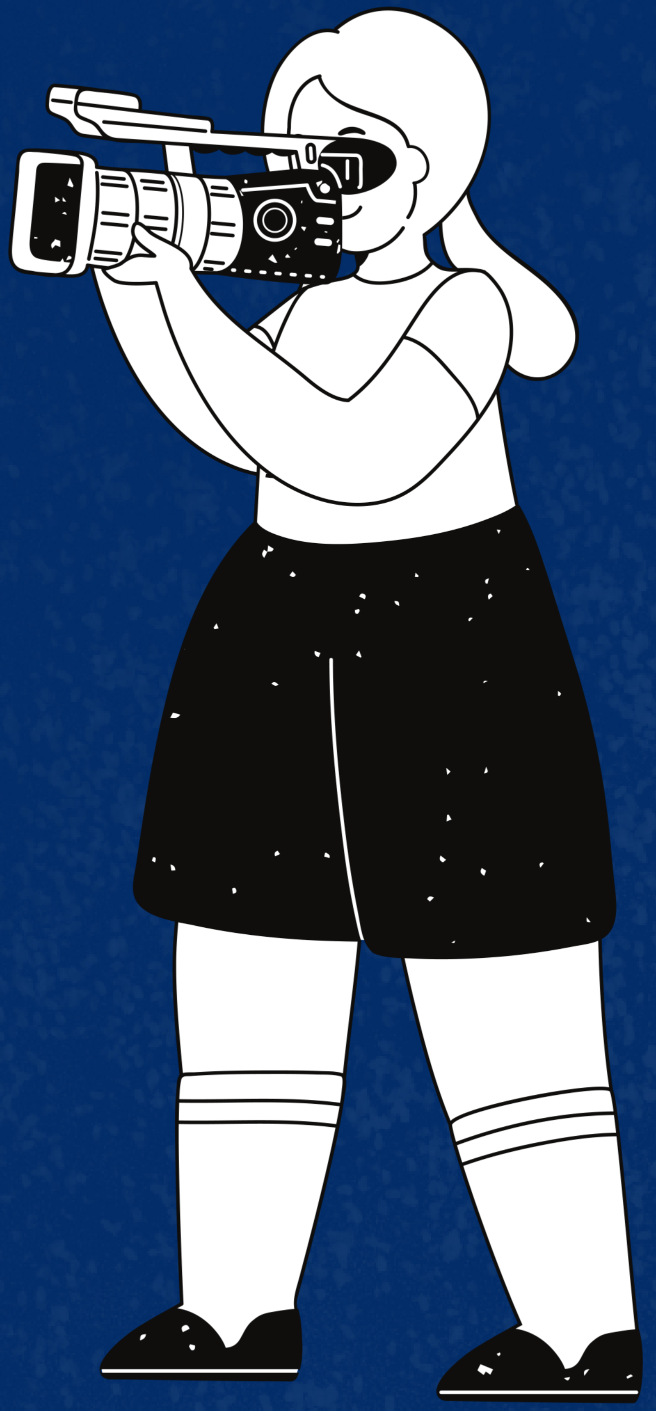
Problem: Calculate (210)mod 7.
Solution: (210)mod 7 = 1024 mod 7 = 3.

Problem: Find the modular inverse of 9 modulo 26, denoted as 9−1mod 26.
Solution:$9 \times 3 \equiv 1 (\text{mod} 26)$
So, 9−1mod 26=3.

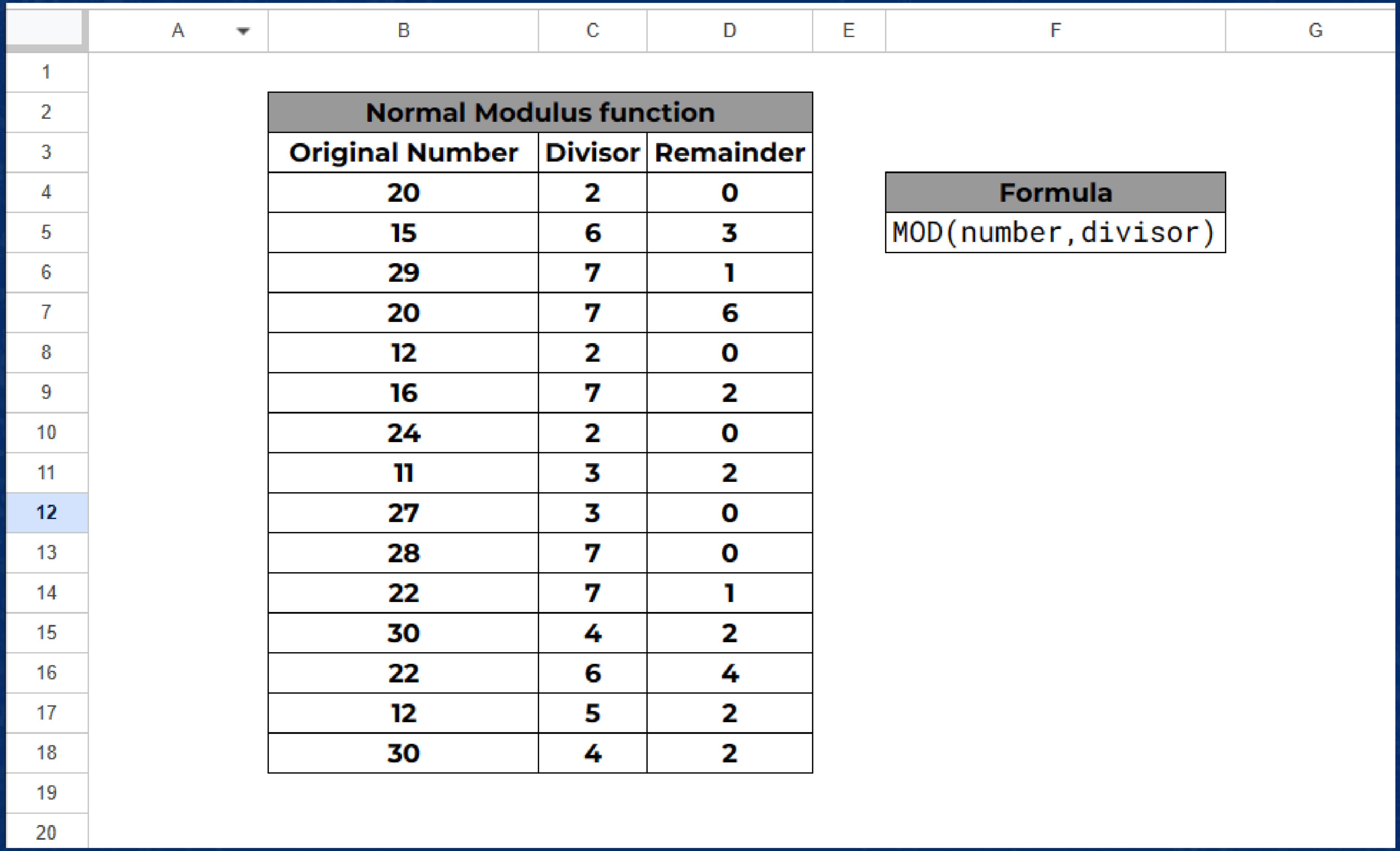
Problem: Solve the congruence $3x \equiv 4(\text{mod} 7)$.
Solution:$x \equiv 5(\text{mod} 7)$

Problem: Solve the system of simultaneous congruences:
$x \equiv 2(\text{mod} 3)$ $x \equiv 3(\text{mod} 5)$
Solution: $x \equiv 8(\text{mod} 15)$

Problem: In a simplified cryptographic scenario, encrypt a message M=15 using a public exponent e=3 and a modulus N=35.
Solution: $C \equiv M^e \text{ mod } N = 15^3 \text{ mod } 35 = 15$.



Excel Implementation



Normal Modulus function		
Original Number	Divisor	Remainder
20	2	0
15	6	3
29	7	1
20	7	6
12	2	0
16	7	2
24	2	0
11	3	2
27	3	0
28	7	0
22	7	1
30	4	2
22	6	4
12	5	2
30	4	2

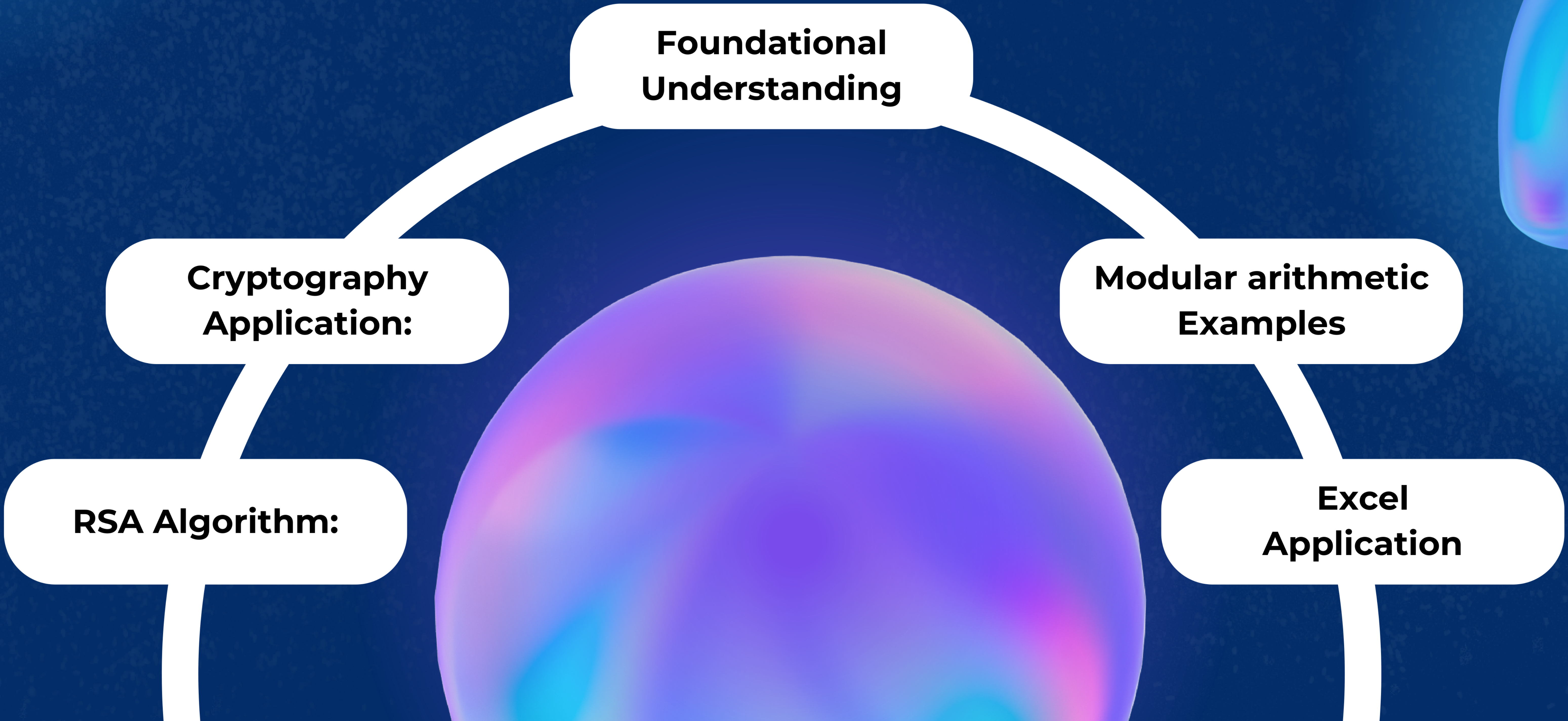
Formula
MOD(number,divisor)

Conclusion

In conclusion, this project has explored modular arithmetic as a fundamental concept and its crucial role in cryptography. The RSA algorithm served as a practical example, illustrating how modular arithmetic ensures secure communication through key processes.

This exploration highlights the essential nature of modular arithmetic in cryptography, emphasizing its role in securing digital information. The principles discussed lay a solid foundation for advancing and fortifying digital security practices.

Student’s Learnings



Foundational Understanding

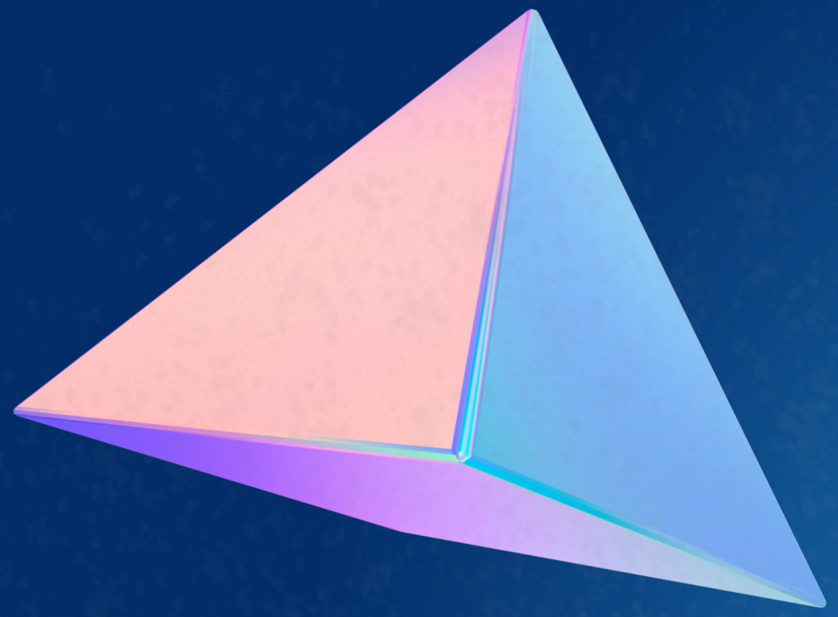
Cryptography Application:

Modular arithmetic Examples

RSA Algorithm:

Excel Application

BIBLIOGRAPHY



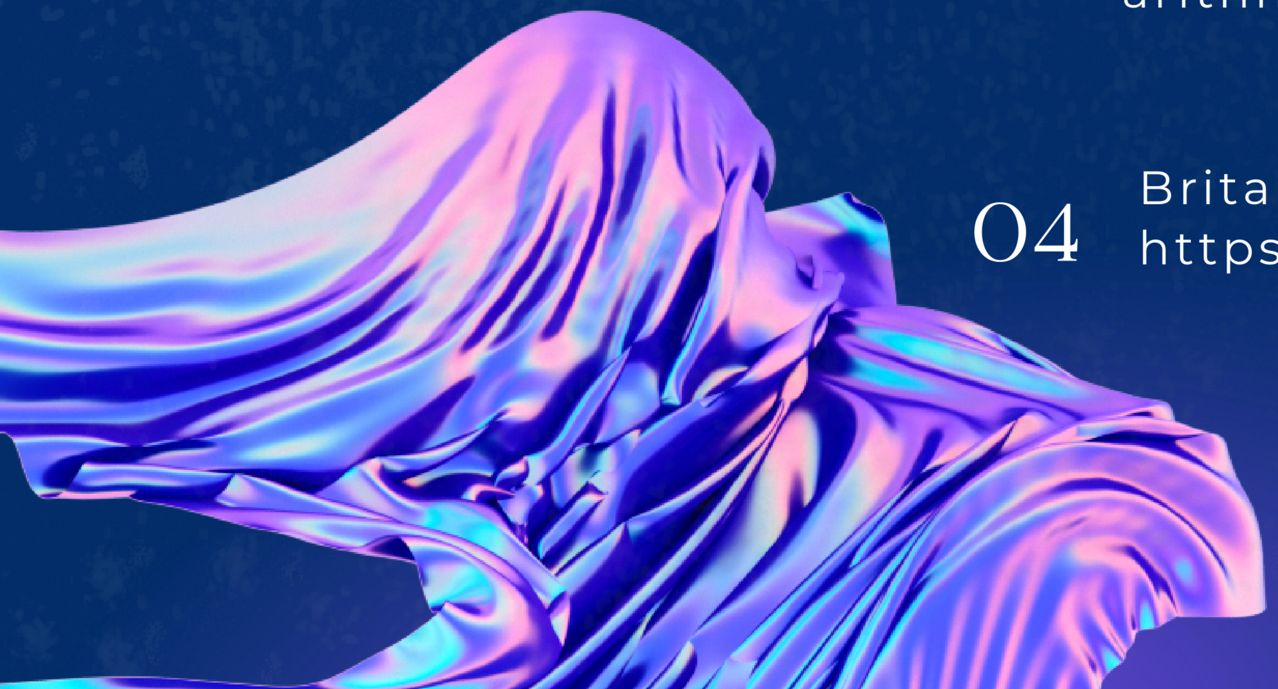
A LIST OF ALL OF THE SOURCES I HAVE USED IN THE PROCESS OF RESEARCHING FOR THIS ESSAY

01 Modular Arithmetic. (2022). Brilliant.org. Retrieved from https://brilliant.org/wiki/modular-arithmetic/

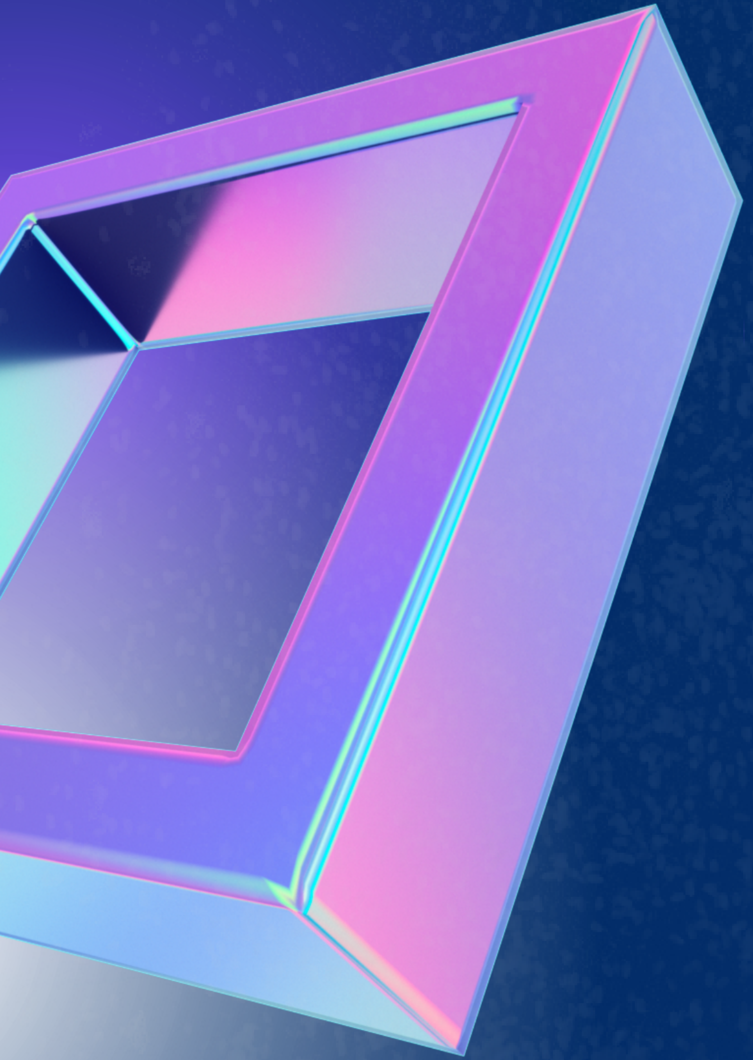
02 Modular arithmetic. In Wikipedia, The Free Encyclopedia. from https://en.wikipedia.org/w/index.php?title=Modular_arithmetic&oldid=1189364824

03 Khan Academy. Retrieved from https://www.khanacademy.org/computing/computer-science/cryptography/modarithmetic/a/what-is-modular-arithmetic

04 Britannica. Modular Arithmetic from https://www.britannica.com/science/modular-arithmetic



Thank You



EXPLORE

website