**Number Theory in Cryptography**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Dhiraj Jayswal

Dhirajjayswal0123@gmail.com

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Abstract:**

Number theory is a branch of pure mathematics that is devoted to the study of the integers, integer-valued functions as well as the properties of mathematical objects made out of integers. Cryptography is the practice and study of techniques used for constructing and analyzing protocols that prevent third parties or the public from reading private messages. Here number theory is used in the process of encryption and decryption to make the channel more secure.

**Introduction:**

This research paper is dedicated to exploring the use of number theory in the process of cryptography. In this modern world of technologies, we have most of our communication over the internet. Be it our day-to-day calls via apps like Messenger and WhatsApp or our messages via platforms like Instagram, Facebook, or Twitter. Not only that but everything we browse over the internet such as mail or a shopping website uses some kind of data. These data may include details ranging from bank account details, home address to your communication. The use of the internet would not be preferable if these data could be accessed and read by anyone and everyone over the internet. Thus comes the concept of Cryptography. WhatsApp and other similar platforms use end-to-end encryption over their channel which makes sure that even if someone gets access to your data unless they have the decryption key they won't be able to read it as it will be an encrypted format.

**Let's take an example:**

Two friends Ravi and Thrupthi are classmates and study together. During college hours they communicate with each other by passing paper with the message written on it. Now the condition is that they don't want someone else to read their message. So to tackle this problem they came up with a solution. They decided that everything they write will be written by changing the 1st letter to the next letter and the 2nd letter to the letter that comes before it. and that will be repeated for every letter in the sentence. So "Hello" will be written as "Idmkp". This made sure that even when someone else had the paper they were not able to make sense of it. For them, it was something gibberish or meaningless.

Here Ravi and Thrupthi used the concept of Cryptography. The paper with the text was the message. The pattern as per which the letters were changed was the key. The process of changing the normal text to these coded formats is called encryption and the process of changing the text back from coded format to the readable format is called decryption.

**Observation:**

Now in the above case, we can see that the 1st letters were being replaced by the one coming after and for 2nd the letter by the one coming before. However it might have worked in a small-scale environment like a classroom we cant use it to decrypt our data over the internet, as unlike the classroom internet is filled with hackers and there are various data leaks. In those case scenarios, it is not long before they can figure out the pattern and decrypt all our data. So to secure us against those cases we need a better key which is nearly impossible to decrypt and this is where mathematical techniques and number theory come.

**Divisibility and Greatest Common Divisor:**

The greatest common divisor (GCD) of two or more numbers is the greatest common factor number that exactly divides both of them. For example, the greatest common factor of 25 and 15 is 5, since both the numbers can be divided by 5 with the remainder 0. GCD is one of the key components in number theory(Euclid's algorithm). Let's take two integers a & b such that a = qb + r , where q is the quotient and r is the remainder. Now for the case where the remainder left is 0. We can use the below formula

gcd (a,b) = gcd (b, a%b)

Let a = 42 & b = 18. Now lets try to implement above equation.

gcd (42 , 18) = gcd (42 - 18 , 18)

=> gcd (22 , 18) = gcd (22 - 18 , 18)

=> gcd (22 , 18) = gcd (22 - 18 , 18)

=> gcd (6 , 18) = gcd (18 - 6 , 6)

=> gcd (12 , 6) = gcd (12 - 6 , 6)

=> gcd (6 , 6)

So, gcd (42, 18) is 6. Now lets take 2 integers x and y such that: gcd (a, b) = ax + by

Here, irrelevant of the value of x and y the equation is valid indicating that u and v are not unique.

**Euclidean Algorithm:**

Euclidean algorithm is a powerful technique that helps us quickly calculate the greatest common divisor of two integers. The algorithm is as follows:

If a = 0 then gcd (a,b) = b

If b = 0 then gcd (a,b) = a

Write a in quotient remainder form (a = qb+ r )

Find gcd (b,r) using the Euclidean algorithm since gcd(a,b) = gcd(b,r)

Let a and b be defined as two integers either greater or less than 0. The sequence of integers taking the remainder into account as r0, r1, r2,…..,rn will be defines:

r0 = a, r1 = b, for i ≥ 1, if ri ƒ = 0, then ri + 1 = ri -1 % ri

The variable, n is the integer-defined attribute to the fact that rn−1 ≠ 0 and rn = 0. This sequence helps us supply an algorithm to compute the gcd of two numbers. Given below is the code in the Python programming language.

def gcd (a , b) :

if (b==0):

return a

else:

return gcd (b, a % b)

For example, gcd(20, 15) is 5. This program returns the gcd by recursively looping the function until variable b becomes 0. Which will be the stopping point.

**Primes & Prime Factorization:**

An integer is said to be a prime number if p > 1 and has only two divisors 1 and itself (here p). For example, 7 is a prime number because it can be only divided by 1 and 7 which is p here. But 15 is not a prime number as it can be divided by 1, 3, 5, and 15.

**Congruence:**

Let a and b be integers such that a-b is integrally divisible by a number m. Here m is called modulus and the statement can be read as a and b are congruent to modulo m. It can be written in mathematical form as below:

a ≡ b (mod m)

For example, 32 is congruent to 2 modulus 15. Here a = 32, b = 2 and modulus = 15. Now putting it in the equation, we get:

32 ≡ 2 (mod 15)

So it should follow the rule of a - b / m. Substituting the values we get:

=> 32 - 2 / 15

=> 30 / 15

=> 2

Here as we can see 30 was divisible by 15 with the remainder 0. So the equation was correct. From the same equation, we can derive that addition and multiplication of the same numbers to both a and b will also return an equation that will be congruent.

For example: Multiplication

a ≡ b (mod m) => ax ≡ bx (mod m)

Let x be 2

=> 32 \* 2 ≡ 2 \* 2 (mod 15)

=> 64 ≡ 4 (mod 15)

=> 64 - 4 / 15

=> 60 / 15

=> 4 (remainder is 0, hence equation is valid)

For example: Addition

a ≡ b (mod m) => a + x ≡ b + x (mod m)

Let x be 2

=> 32 + 2 ≡ 2 + 2 (mod 15)

=> 34 ≡ 4 (mod 15)

=> 34 - 4 / 15

=> 30 / 15

=> 2 (remainder is 0, hence equation is valid)

**Solving ax ≡ c(mod m) for x:**

Consider a and b be integers and m a positive integer, for ax ≡ b (mod m) and 1≤ x < m. The objective here is to solve the value of x. Now, have d = gcd(a, m) such that d divides b. Let u and v be integers such that ua + vm = d and x = uc % m. And the reason because of which this fact is valid is that the result from a string of congruence ie.

ax = a (ub/d % m) ≡ a.ub/d ≡ (a \* ub/d + v \* mb/d) ≡ b/d \* d ≡ b (mod m).

Using the above theorem we can take parameters a, b, and m called axbm and create a python function such that gcd (a, m) divides c and returns x as a solution that satisfies the above equation.

def axbm (a, b, m):

g, u, v = gcd (a, m)

x = (( u \* c ) // g) % m

return x

Here, for input 4, 2 , 15 for function axbm we will get 8 as the value of x. ie. 4(8) - 2 = 15(2). where 4(8) - 2 is divisible by 15.

**Euler's Formula:**

Euler's Formula counts all the positive integers up to a given integer n that are relatively prime to it. It is represented using ϕ(n). In mathematical terms, it can be written as 1≤ k ≤ n, where k is the number of integers in range and for which the gcd (n, k) = 1.

**Solving Euler's Formula: xk ≡ b (mod m) for x:**

The integers k,b, and m should satisfy the following three conditions.

m = pq where p and q are prime numbers.

gcd(b,m) = 1

gcd(k,(p-1)(q-1)) = 1

We are going to get two integers number u and v for which the following equation is satisfied:

uk + v(p - 1)(q - 1) = 1 ( i )

to get the solution of the equation : xk ≡ b(mod m)

Finally,

x = ( bu ) % m where 1 ≤ x < m ( ii )

To check the validity of the value of x, we need to keep the value in the given equation.

xk = (( bu ) % m)k ≡ ( bu )k (mod m) ≡ ( buk )(mod m)

xk = buk(mod m) (iii)

As we know that gcd(b,m)=1,

So we can write:

b(p - 1)(q - 1) ≡ 1(mod m)

1 ≡ 1v ≡ (b(p - 1)(q - 1))v ≡ bv(p - 1)(q - 1)(mod m)

Hence,

1 ≡ bv(p - 1)(q - 1)(mod m) (iv)

Multiplying LHS of equation (iii) with LHS of equation (iv) and RHS of equation (iii) with RHS of equation (iv), we get :

xk ≡ buk bv (p-1 )(q-1)(mod m)

xk ≡ buk + v (p-1)(q-1)(mod m)

xk ≡ b1(mod m) from ( i )

which proves the value obtained for x from (ii) is correct.

Example:-

Let k = 5, b = 3, p = 7, q = 2

then, m = pq = 14

(p-1)(q-1) = (7-1)(2-1) = 6

Now, let's check the three conditions before finding the value of x.

m = pq = 14 where p7 and 2 are prime numbers.

gcd(3,14) = 1

gcd(5,6) = 1

Using equation.(i)

u5 + u6 = 1

5 \* 5 + ( - 4 ) \* 6 = 1

Therefore, u = 5 and v = - 4.

From equation. (ii)

x = (35) % 14 = 5

Let's verify the value of x:

x5 ≡ 3 (mod 14)

Keeping value of x as 5, x5 (mod 14) = 55 (mod 14) = 3, which verifies our value of x is valid.

**Application of Cryptography:**

Let's look back into the scenario of Ravi and Thrupthi. Ravi will again send a message to Thrupthi, but now that he has knowledge of Number Theory this time he will send the message in the form of numbers. Here both Ravi and Thrupthi will follow the below process.

Step 1: Both of them will select big prime numbers, p, and q.

Step 2 : They let m = pq and use k such that gcd (k, (p - 1)(q - 1)) = 1 in his process. They make k and m public. ie. Its value will be accessible to everyone.

Step 3: Now Ravi wants to send the message "c" to Thrupthi, so he will compute c = bk % m, and send b instead, where b will range between 1 and m-1. ie. 1 ≤ b <m.

Step 4: As Thrupthi knows the values of k, p and q and gcd (k, (p - 1)(q - 1)) = 1, she can easily find the value of x by solving the equation xk = b (mod m) where 1 ≤ x < m. however, ak ≡ b(mod m) and 1 ≤ a < m. Here because x's solution is unparalleled, they will have x = a hence, Thrupthi can decode the message sent by Ravi.

Step 5: Here no one except Ravi and Thrupthi will be able to decrypt the message. Since to decrypt the message they will need to solve the value of xk ≡ b (mod m) where 1 ≤ x < m, which requires the value of p and q, which are only known to Ravi and Thrupthi. Here p and q serve as a secret key for Ravi and Thrupthi which helps them decrypt the message. This method that Ravi and Thrupthi are using is called RSA. Here a simple Python function can be used to encrypt and decrypt the message:

Encrypt:

def encrypt ( b, k, m ) :

return ( b\*\*k) % m

Decrypt:

def decrypt ( k , c ) :

p , q = key[0], key[1]

return xtokeqb ( k, c, p, q )

Here c is used in the function xtokeqb as it serves as the second argument derived from the function encrypt. Here the function serves a very beneficial use for both Ravi and Thrupthi as they can now send messages to each other without the worry of a third party being able to read their messages.

**Discussion:**

In this paper, we have looked into the algorithms that are powered by number theory and are used for cryptography and RSA(Rivest, Shamir, Adleman). We also learned how we can design effective and efficient algorithms, using Python to help us better understand the use of Number theory in Cryptography. It also provides us with a glimpse of the use of applied mathematics and Number theory in today's digital era.

**References:**

1. Nguyen, K. Cryptography and Number Theory. rn, 55, 7.
2. Prof. Selvakumar R - Number Theory, Mat5002
3. Weisstein, Eric W. "Number." From MathWorld--A Wolfram Web Resource