**NATIONAL INSTITUTE OF TECHNOLOGY DELHI**

A blue and white logo

Description automatically generated

**Department of Computer Science & Engineering**

**CSB 451**

**Network Security & Cryptography**

***Assignment – 7***

**Submitted By:**

**Himanshu Verma**

**201210023**

**Submitted To: Dr. Karan Verma**

**Question 1**

**Solution:**

For n = 41,

n^2+n+41 = 1681 +41 +41 = 1763

now 1763 is not a prime number, however for n=1 to 40, the polynomial gives all prime numbers. This is an example of Euler's polynomial that generates prime numbers for consecutive values of n. However, it does not generate a prime number for all n as demonstrated by n=41.

This is a consequence of the fact that polynomials are algebraic expressions, and prime numbers are generally produced by number-theoretic properties. For any given polynomial, there will always be some integer values for which the polynomial doesn't produce prime numbers. This is because prime numbers are a fundamentally different kind of mathematical object from polynomials.

A notebook with writing on it

Description automatically generated

For the sum of the series (1+1/2+1/3+...+1/n+...),

The sum approaches infinity as n approaches infinity as it is a harmonic series with the proof attached above.

Now, The prime number theorem states that the number of primes less than or equal to x is approximately equal to x/ln(x) for large x. From this, we can infer that as n gets larger, the density of primes among integers decreases. This is because the ratio of primes to integers as n gets large approaches 1/ln(n). As we know that ln(n) grows much slower than n, so the density of primes among integers diminishes as n increases. However, the Prime Number Theorem does not predict the exact location of prime numbers but gives a statistical distribution, which means there can still be large gaps between consecutive primes.

**Question 2:**

**Solution:**

**A:** In modular arithmetic, we select an integer, n, as our “modulus”. Then our system of numbers only includes the numbers 0, 1, 2, 3, ..., n-1. To make arithmetic sense, we have the numbers “wrap around” once they reach n. Modular arithmetic is typically denoted by a ≡ b (mod m), which reads as "a is congruent to b modulo m". It means that a and b have the same remainder when divided by m.

**B:** 2+1 = 3 (mod 5) = 3

2+2 = 4 (mod 5) = 4

2+3 = 5 (mod 5) = 0

2+4 = 6 (mod 5) = 1

134 ÷ 5 = 26 with a remainder of 4. So, 134 (mod5) = 4

**Question 3:**

**Solution:**

First, we need to check whether 3 is divisible by 7. Since it's not, we can apply Fermat's Little Theorem:

37−1 ≡ 36 ≡ 1mod 7

Now, we need to find 331 in terms of 36:

331=36×5+1

Using modular arithmetic rules:

331 ≡ (36)5×31 mod 7

From Fermat's Little Theorem, we know that 36 ≡ 1mod 7, so:

331 ≡ 15×31mod 7

331 ≡ 3 mod 7

So, 331 is congruent to 3 modulo 7. Therefore, 331 mod 7 = 3.

**Question 4:**

**Solution:**

Since both 29 and 13 are prime numbers, gcd(29, 13) = 1.

Hence, we can apply Euler’s theorem to get

29(φ(13)) ≡ 1 (mod 13) , φ(13) = 12

In this case, 2912 ≡ 1 (mod 13) as 13 is prime.

202 = 12(16) + 10

29202 = (2912)26\*2910 = 126\*2910 = 2910(mod 13)

29 = 3 mod 13,

2910 = 310 = 3(mod 13)2

**Hence, Remainder = 3**

**Question 5:**

**Solution:**

To find the greatest common divisor (gcd) of two numbers 7544 and 115 using the Euclidean Algorithm, we repeatedly apply the following steps:

1. Divide the larger number by the smaller number.
2. Replace the larger number with the remainder of the division.
3. Repeat the process until the remainder is zero.

Step 1:7544=65×115+69

Step 2:115=1×69+46

Step 3:69=1×46+23

Step 4:46=2\*23+0

At this point, we have reached a remainder of 0, so 23 is the gcd of 754and 115. Therefore, gcd(7544,115)=23.