



Republic of Iraq Ministry of Higher Education and Scientific Research Al- Mustaqbal University Collage of science - Department of Cyber Security



1st class

2024-2025

Number Theory

Lecture 5

Asst. Lect. Mohammed Jabbar

mohammed.jabbar.obaid@uomus.edu.iq

الرياضيات :المرحلة الاولى نظرية الاعداد

المحاضرة الخامسة

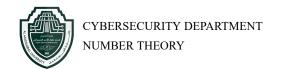
استاذ المادة: م.م محمد جبار



Cybersecurity Department قسم الأمن السيبراني

Contents

1	Prime Numbers		
	1.1	Lists of primes by type	3
	1.2	Exercises of Prime Numbers	5



1 Prime Numbers

We have previously been introduced to prime numbers. In this section, we will explore these numbers in greater depth and study their special Sequences.

Number of primes infinite

Theorem 1.1. *There are infinitely many prime numbers.*

Proof. Let the number of primes is finite

$$p_1, p_2, p_3, \ldots, p_n.$$

and let

$$N = p_1 p_2 p_3 \dots p_n + 1.$$

There are two cases: either N is a prime number or a composite number.

Case 1: If N prime C! with (the number of primes is finite).

Case 2: If N composite, then $p \mid N$.

But $p_1, p_2, \ldots, p_n \nmid N$, because leaves a remainder of 1 C! with N composite.

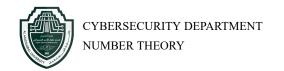
 \Rightarrow N is prime C! with (the number of primes is finite).

Therefore, there are infinitely many prime numbers.

Sequence of $N_n = (p_1 p_2 p_3 \dots p_n) + 1$

3 = 2 + 1 $7 = 2 \cdot 3 + 1$ $31 = 2 \cdot 3 \cdot 5 + 1$ $211 = 2 \cdot 3 \cdot 5 \cdot 7 + 1$ $2311 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1$

where p_i represents the first n prime numbers.



Example 1.1. From $N_n = (p_1 p_2 p_3 \dots p_n) + 1$, find N_4, N_7 and N_9 .

Sol.

$$N_4 = (2 \cdot 3 \cdot 5 \cdot 7) + 1 \qquad N_7 = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17) + 1$$

= 210 + 1 = 211 = 510510 + 1 = 510511

The Fundamental Theorem of Arithmetic

Theorem 1.2. Every integer n > 1 can be written uniquely in the form

$$n = p_1 p_2 \cdots p_s$$

where p_1, p_2, \ldots, p_s are primes such that $p_1 \leq p_2 \leq \cdots \leq p_s$.

Remark 1.1. If $n = p_1 p_2 \cdots p_s$ where each p_i is prime, we call this the prime factorization of n.

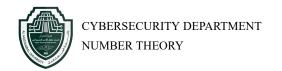
The number 1 is neither prime nor composite.

Ans. 1 is not composite because there are no integers a, b > 1 such that 1 = ab.

Now, let 1 is prime number and n composite $\ni n = pq, p, q$ primes. Then

 $n = p \times q$ $n = 1 \times p \times q$ $n = 1 \times 1 \times p \times q$ $n = 1 \times 1 \times 1 \times p \times q$ \vdots $n = 1 \times 1 \times \dots \times 1 \times p \times q \mathbb{C}! \text{ with unique product of primes}$ $\therefore 1 \text{ is not prime number.}$

Theorem 1.3. Let p be a prime and $a, b \in \mathbb{N}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.



Proof. If $p \mid a$ we are done.

If
$$p \nmid a \Rightarrow \gcd(p, a) = 1 \Rightarrow \gcd(bp, ab) = b$$
.
Since $p \mid pb, p \mid ab$, then $p \mid \gcd(bp, ab) \Rightarrow p \mid b \gcd(p, a) \Rightarrow p \mid b \cdot 1 \Rightarrow p \mid b$.

Prime Divisor

Lemma 1.1. If n > 1 is composite, then n has a prime divisor $p \le \sqrt{n}$.

Example 1.2. n = 97. Note that $\sqrt{97} < \sqrt{100} = 10$. The primes less than 10 are 2, 3, 5, and 7.

1.1 Lists of primes by type

Cousin Primes

Cousin Primes are pairs of prime numbers that differ by 4. In other words, two primes p and q are cousin primes if:

q = p + 4 and both p and q are primes.

Examples:

1. For p = 3:

$$q = 3 + 4 = 7$$

Both 3 and 7 are prime numbers. So, (3, 7) is a pair of **Cousin Primes**.

2. For p = 7:

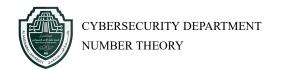
$$q = 7 + 4 = 11$$

Both 7 and 11 are prime numbers. So, (7, 11) is a pair of Cousin Primes.

3. For p = 13:

$$q = 13 + 4 = 17$$

Both 13 and 17 are prime numbers. So, (13, 17) is a pair of Cousin Primes.



Cullen Primes

A Cullen Prime is a prime number of the form:

$$C_n = n \cdot 2^n + 1$$

where n is a positive integer and C_n is prime.

Examples:

1. For n = 1:

$$C_1 = 1 \cdot 2^1 + 1 = 3$$

Since 3 is prime, $C_1 = 3$ is a **Cullen Prime**.

2. For n = 2:

$$C_2 = 2 \cdot 2^2 + 1 = 9$$

Since 9 is not prime, $C_2 = 9$ is not a Cullen prime.

3. For n = 3:

$$C_3 = 3 \cdot 2^3 + 1 = 25$$

Since 25 is not prime, $C_3 = 25$ is not a Cullen prime.

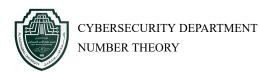
4. For n = 5:

$$C_5 = 5 \cdot 2^5 + 1 = 161$$

Since 161 is not prime, $C_5 = 161$ is not a Cullen prime.

5. A known large Cullen prime is:

$$C_{141} = 141 \cdot 2^{141} + 1$$



1.2 Exercises of Prime Numbers

Exercises

1. Let p and q be prime numbers. Suppose that the polynomial

 $x^2 - px + q = 0$

has an integer root. Find all possible values of p and q.

- 2. From $N_n = (p_1 p_2 p_3 \dots p_n) + 1$, find
 - (a) N_1 to N_3 .
 - (b) $N_1 * N_2 + 1$
- 3. Let p be a prime and a, k be positive integers. If $p \mid a^k$, then $p^k \mid a^k$.
- 4. Write prime between 72 and 111.

5. Let q_1, q_2, \ldots, q_m be prime numbers. If a prime p divides their product,

 $p \mid q_1 q_2 \cdots q_m,$

Then p must be equal to one of q_1, q_2, \ldots, q_m , i.e., $p = q_k$ for some k.