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 6

Asst. Lect. Mohammed Jabbar
mohammed.jabbar.obaid@uomus.edu.iq

الرياضيات :المرحلة السادسة

نظرية الاعداد

المحاضرة الاولى

استاذ المادة: م.م محمد جبار

Cybersecurity Department
قسم الأمن السيبراني

Contents

1 Mersenne Primes

Mersenne Primes

Definition 1.1. A number $M_p = 2^p - 1$ is called a Mersenne number. If M_p is prime, then it is called a Mersenne prime.

For example:

$M_2 = 2^2 - 1 = 3, \quad M_3 = 2^3 - 1 = 7, \quad M_5 = 2^5 - 1 = 31, \quad M_7 = 2^7 - 1 = 127$

Remark 1.1. **Necessary Condition:** If M_p is prime, then p must be prime. (However, the converse is not true; e.g., when $p = 11$, $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ is composite.)

Example 1.1. – For $p = 2$:

$$M_2 = 2^2 - 1 = 3 \quad \text{(prime)}.$$

– For $p = 3$:

$$M_3 = 2^3 - 1 = 7 \quad \text{(prime)}.$$

– For $p = 5$:

$$M_5 = 2^5 - 1 = 31 \quad \text{(prime)}.$$

– For $p = 7$:

$$M_7 = 2^7 - 1 = 127 \quad \text{(prime)}.$$

– For $p = 11$:

$$M_{11} = 2^{11} - 1 = 2047 \quad \text{(composite, since } 2047 = 23 \times 89\text{)}.$$

Theorem 1.1. *If n is a positive composite number, then $2^n - 1$ is a composite number.*

Example 1.2. The numbers 4, 6, and 9 are composite. Accordingly, $2^4 - 1 = 15$, $2^6 - 1 = 63$, and $2^9 - 1 = 511 = 7 \times 73$ are composite.

Lemma 1.1. For any integer $n \geq 1$, we have the factorization

$$x^n - 1 = (x-1)\left(x^{n-1} + x^{n-2} + \cdots + x + 1\right).$$

Lemma 1.2. Let $a > 1$ and $n > 1$. If $a^n + 1$ is prime, then a is even and $n = 2^k$ for some $k \geq 1$.

Proof. We first prove that n must be even.

Step 1: Suppose n is odd.

Assume that n is odd:

Since

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1).$$

Now, we replace a with $-a$:

$$(-a)^n - 1 = (-a-1)((-a)^n + (-a)^{n-1} + (-a)^{n-2} + \cdots + (-a) + 1).$$

$$\Rightarrow (-a)^n = -a^n, (-a)^{n-1} = a^{n-1}, (-a)^{n-2} = -a^{n-2}, \ldots.$$

$$\Rightarrow -(a^n + 1) = -(a+1)(a^{n-1} - a^{n-2} + \cdots - a + 1).$$

$$\Rightarrow a^n + 1 = (a+1)(a^{n-1} - a^{n-2} + \cdots - a + 1).$$

For $n \geq 2$, we have: $1 < a + 1 < a^n + 1$.

Thus, if n is odd, the number $a^n + 1$ is divisible by $a + 1$, and it is not prime. Hence, n cannot be odd, then n even.

Now, since n even, let $n = 2^s \cdot t$, where t is odd. If $a^n + 1$ is prime, then:

$$a^n + 1 = a^{2^s \cdot t} + 1.$$

But $a^n + 1$ cannot be prime if $t \geq 2$ and t is odd. Therefore, $t = 1$, which gives $n = 2^s$.

Thus, $n = 2^k$ for some integer $k \geq 1$. □