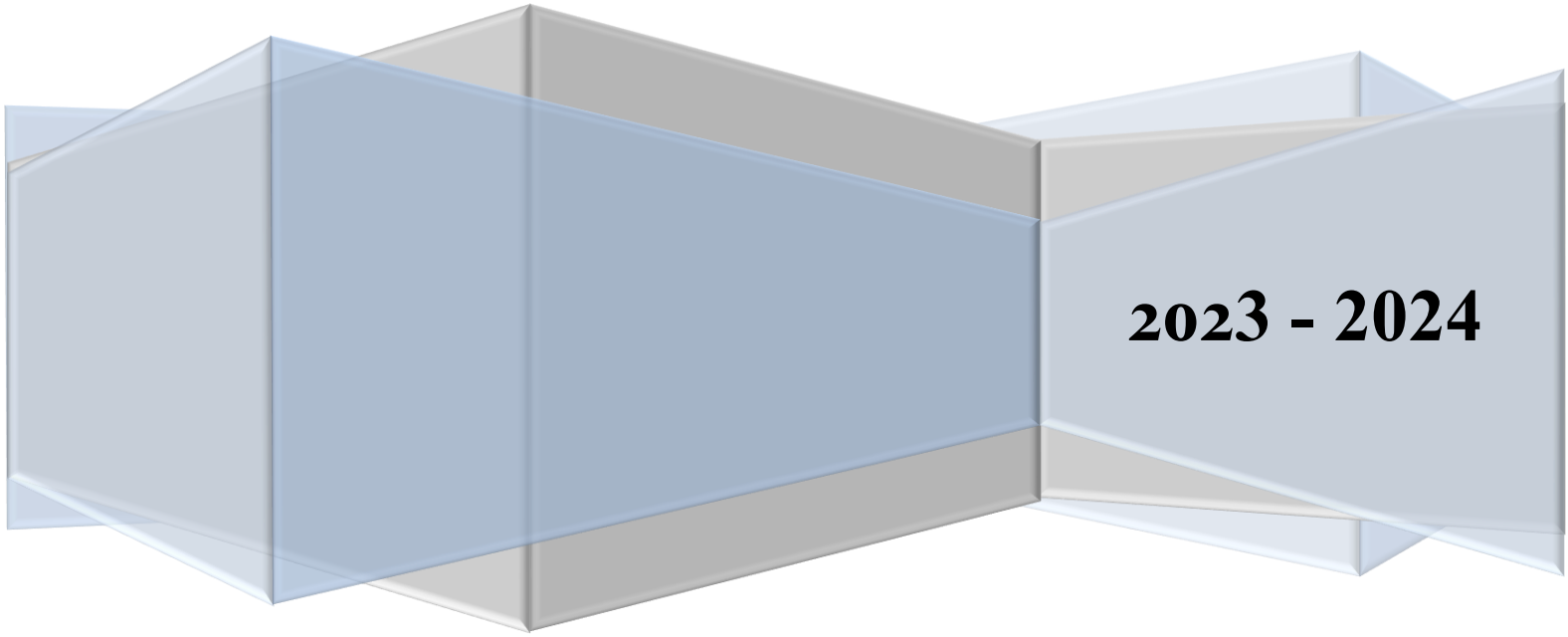
University of Baghdad

College of Science for Women

Department of Computer Science

Computer Mathematics

Ahmed J. Kadhim, M. Sc.



2023 - 2024

Arithmetic Modulo m

We can define arithmetic operations on $\boldsymbol{Z_m}$, the set of nonnegative integers less than m, that is, the set $\{0, 1, \ldots, m-1\}$. In particular, we define addition of these integers, denoted by $+_m$ by $a +_m b = (a + b) \bmod m$,

where the addition on the right-hand side of this equation is the ordinary addition of integers, and we define multiplication of these integers, denoted by $._m$ by

$a ._m b = (a . b) \bmod m$,

where the multiplication on the right-hand side of this equation is the ordinary multiplication of integers. The operations $+_m$ and $._m$ are called addition and multiplication modulo m and when we use these operations, we are said to be doing **arithmetic modulo** m.

Example: Use the definition of addition and multiplication in $\boldsymbol{Z_m}$ to find $7 +_{11} 9$ and $7 ._{11} 9$.

Using the definition of addition modulo 11, we find that

$7 +_{11} 9 = (7 + 9) \bmod 11 = 16 \bmod 11 = 5$,

and

$7 ._{11} 9 = (7 . 9) \bmod 11 = 63 \bmod 11 = 8$.

Hence $7 +_{11} 9 = 5$ and $7 ._{11} 9 = 8$.

Primes

Every integer greater than 1 is divisible by at least two integers, because a positive integer is divisible by 1 and by itself. Positive integers that have exactly two different positive integer factors are called **primes**.

Definition: An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

Example: The integer 7 is prime because its only positive factors are 1 and 7, whereas the integer 9 is composite because it is divisible by 3.

Greatest Common Divisors and Least Common Multiples

Definition: Let a *and* b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a *and* b. The greatest common divisor of a and b is denoted by $gcd(a, b)$.

Example: What is the greatest common divisor of 24 and 36?

The positive common divisors of $24\ and\ 36$ are $1, 2, 3, 4, 6, and\ 12$. Hence, $gcd(24, 36) = 12$.

Definition: The integers $a\ and\ b$ are *relatively prime* if their greatest common divisor is 1.

Example: What is the greatest common divisor of $17\ and\ 22$?

The integers $17\ and\ 22$ have no positive common divisors other than 1, it follows that the integers 17 and 22 are relatively prime, because $gcd(17, 22) = 1$.

Definition: The integers $a_1,\ a_2, \ldots,\ a_n$ are *pairwise relatively prime* if $gcd(a_i,\ a_j) = 1$ whenever $1 \leq i < j \leq n$.

Example: Determine whether the integers 10, 17, and 21 are pairwise relatively prime and whether the integers 10, 19, and 24 are pairwise relatively prime.

Because $gcd(10, 17) = 1,\ gcd(10, 21) = 1,\ and\ gcd(17, 21) = 1$, we conclude that 10, 17, and 21 are pairwise relatively prime.

Because $gcd(10, 24) = 2 > 1$, we see that 10, 19, and 24 are not pairwise relatively prime.

Prime Factorizations

Another way to find the greatest common divisor of two positive integers is to use the prime factorizations of these integers. Suppose that the prime factorizations of the positive integers $a\ and\ b$ are

$$a = p_1^{a_1}.p_2^{a_2} \ldots p_n^{a_n},\ b = p_1^{b_1}.p_2^{b_2} \ldots p_n^{b_n}$$

where each exponent is a nonnegative integer, and where all primes occurring in the prime factorization of either $a\ or\ b$ are included in both factorizations, with zero exponents if necessary. Then $gcd(a, b)$ is given by

$$gcd(a, b) = p_1^{\min(a_1, b_1)}.p_2^{\min(a_2, b_2)} \ldots p_n^{\min(a_n, b_n)}$$

Example: Because the prime factorizations of 120 and 500 are $120 = 2^3 . 3 . 5$ and $500 = 2^2 . 5^3$, the greatest common divisor is

$$gcd(120, 500) = 2^{\min(3,2)}.3^{\min(1,0)}.5^{\min(1,3)} = 2^2.3^0.5^1 = 20$$

Definition: The *least common multiple* of the positive integers $a\ and\ b$ is the smallest positive integer that is divisible by both $a\ and\ b$. The least common multiple of $a\ and\ b$ is denoted by $lcm(a, b)$.

The least common multiple exists because the set of integers divisible by both $a\ and\ b$ is nonempty and every nonempty set of positive integers has a least element so the least common multiple of $a\ and\ b$ is given by

$$lcm(a,b) = p_1^{\max(a_1,b_1)}.p_2^{\max(a_2,b_2)} \dots p_n^{\max(a_n,b_n)}$$

Example: What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

We have

$$lcm(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3,4)}.3^{\max(5,3)}.7^{\max(2,0)} = 2^4.3^5.7^2$$

Theorem: Let $a\ and\ b$ be positive integers. Then $ab = gcd(a,b).lcm(a,b)$

Example: Find $gcd(1000,625)$ and $lcm(1000,625)$ and verify that $gcd(1000,625).lcm(1000,625) = 1000.625.$

We have

$1000 = 5^3.2^3\ and\ 625 = 5^4$

since, $gcd(1000,625) = 2^{\min(3,0)}.5^{\min(3,4)} = 2^0.5^3 = 125,$

$$lcm(1000,625) = 2^{\max(3,0)}.5^{\max(3,4)} = 2^3.5^4 = 5000,$$

Then, $1000\,.625 = gcd(1000,625).lcm(1000,625) = 125\,.5000 = 625000$

The Euclidean Algorithm

Computing the greatest common divisor of two integers directly from the prime factorizations of these integers is inefficient. The reason is that it is time-consuming to find prime factorizations. We will give a more efficient method of finding the greatest common divisor, called the **Euclidean algorithm**.

We will use successive divisions to reduce the problem of finding the greatest common divisor of two positive integers to the same problem with smaller integers, until one of the integers is zero. The Euclidean algorithm is based on the following result about greatest common divisors and the division algorithm.

Theorem: Let $a = bq + r$, where a, b, q, and r are integers. Then $gcd(a,b) = gcd(b,r)$.

Example: Find the greatest common divisor of $414\ and\ 662$ using the Euclidean algorithm.

Successive uses of the division algorithm give:

$$662 = 414\,.1 + 248$$

$$414 = 248\,.1 + 166$$

$248 = 166 . 1 + 82$

$166 = 82 . 2 + 2$

$82 = 2 . 41.$

Hence, $gcd(414, 662) = 2$, because 2 is the last nonzero remainder.

Problems:

1. Answer of the following with true or false:
   - The prime factorization of 126 is $2 . 3^3 . 7$.
   - The greatest common divisors of $17, 17^{17}$ is 17.
   - The quotient and remainder when 44 is divided by 8 is $44 = 8.4 + 4$.
   - The quotient of -17 is divided by 2 is $-9 = -17\ div\ 2$ and the remainder is $1 = -17\ mod\ 2$
2. Determine whether the integers in each of these sets are pairwise relatively prime.
   - $14, 15, 21$
   - $12, 17, 31, 37$
3. What are the greatest common divisors and the least common multiple of these pairs of integers?
   - $3^7 . 5^3 . 7^3$, $2^{11} . 3^5 . 5^9$
   - $11 . 13 . 17$, $2^9 . 3^7 . 5^5 . 7^3$
4. Find $gcd(144, 88)$ and $lcm(144, 88)$ and verify that $gcd(144, 88). lcm(144, 88) = 144. 88.$
5. If the product of two integers is $2^7 . 3^8 . 5^2 . 7^{11}$ and their greatest common divisor is $2^3 . 3^4 . 5$, what is their least common multiple?
6. Use the Euclidean algorithm to find:
   - $gcd(123, 277)$.
   - $gcd(1001, 1331)$.
7. Suppose that $a\ and\ b$ are integers, $a \equiv 4\ (mod\ 13)$, and $b \equiv 9\ (mod\ 13)$. Find the integer c with $0 \leq c \leq 12$ such that
   - $c \equiv 9a\ (mod\ 13)$.
   - $c \equiv a + b\ (mod\ 13)$.
   - $c \equiv 2a + 3b\ (mod\ 13)$.

$(a + b) mod\ m = \big((a\ mod\ m) + (b\ mod\ m)\big) mod\ m$

and

$a.b\ mod\ m = \big((a\ mod\ m)(b\ mod\ m)\big) mod\ m$

- $c \equiv a^2 + b^2\ (mod\ 13)$.
- $c \equiv a^3 - b^3\ (mod\ 13)$.

$$a^3 - b^3\ (mod\ 13) = (4\ mod\ 13)^3 - (9\ mod\ 13)^3\ mod 13$$
$$= (64 - 729) mod\ 13$$
$$= -665\ mod\ 13$$
$$= -665 - 13(-52)$$
$$= 11$$

Note: $mod(x, y) = x - y * n$

$n = floor(\frac{x}{y})$

$= floor\left(\frac{-665}{13}\right)$

$= floor(-51{,}1538)$

$= -52$

So,

$mod(x, y) = x - y * n$

$= -665 - 13(-52)$

$= -665 + 676 = 11$