Lecture 4: The Integers

Moldir Toleubek
moldir.toleubek@astanait.edu.kz

Astana IT University

October,2025

Overview

- Divisibility and Modular Arithmetic
- Integer Representation
- Primes and Greatest Common Divisors
- Solving Congruences

Division

Definition

If a and b are integers with $a \neq 0$, we say that a **divides** b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When a divides b we say that a is a factor or divisor of b,and that b is a multiple of a.The notation $a|b$ denotes that a divides b.We write $a \not| b$ when a does not divide b.

Example. Determine whether $3|7$ and whether $3|12$.

Division

Definition

If a and b are integers with $a \neq 0$, we say that a **divides** b if there is an integer c such that $b = ac$, or equivalently, if $\frac{b}{a}$ is an integer. When a divides b we say that a is a factor or divisor of b,and that b is a multiple of a.The notation $a|b$ denotes that a divides b.We write $a \not| b$ when a does not divide b.

Example. Determine whether $3|7$ and whether $3|12$.
Solution. We see that $3 \not| 7$, because $7/3$ is not an integer. On the other hand, $3|12$ because $12/3 = 4$.

Division

Theorem

Let a, b, and c be integers, where $a \neq 0$. Then
(i) if $a|b$ and $a|c$, then $a|(b+c)$
(ii) if $a|b$, then $a|bc$ for all integers c
(iii) if $a|b$ and $b|c$, then $a|c$

Division Algorithm

Theorem

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Example. Division of 58 by 17:

Division Algorithm

Theorem

Let a be an integer and d a positive integer. Then there are unique integers q and r, with $0 \leq r < d$, such that $a = dq + r$.

Example. Division of 58 by 17:

$$58 = 3(17) + 7$$

Why we don't consider $58 = 2(17) + 24$?

Division Algorithm

Definition

In the equality given in the division algorithm, d is called the **divisor**, a is called the **dividend**, q is called the **quotient**, and r is called the **remainder**. This notation is used to express the quotient and remainder:

$q = a \textbf{ div } d$, $r = a \textbf{ mod } d$

Example. What are the quotient and remainder when 101 is divided by 11?

Division Algorithm

Definition

In the equality given in the division algorithm, d is called the **divisor**, a is called the **dividend**, q is called the **quotient**, and r is called the **remainder**. This notation is used to express the quotient and remainder:
$q = a \textbf{ div } d$, $r = a \textbf{ mod } d$

Example. What are the quotient and remainder when 101 is divided by 11?
Solution.

$$101 = 11 \cdot 9 + 2$$

Hence, the quotient when 101 is divided by 11 is $9 = 101 \textbf{ div } 11$, and the remainder is $2 = 101 \textbf{ mod } 11$.

ASTANA IT UNIVERSITY

Division Algorithm

Example

What are the quotient and remainder when -11 is divided by 3?

Division Algorithm

Example

What are the quotient and remainder when -11 is divided by 3?

Solution.

$$-11 = 3(-4) + 1$$

Hence, the quotient when -11 is divided by 3 is -4 = -11 **div** 3, and the remainder is 1 = -11 **mod** 3.

Modular Arithmetic

Definition

If a and b are integers and m is a positive integer, then **a is congruent to b modulo m** if *m divides a-b*. We use the notation $a \equiv b(\mathbf{mod}\ m)$ to indicate that a is congruent to b modulo m. We say that $a \equiv b(\mathbf{mod}\ m)$ is a congruence and that m is its modulus (plural moduli). If a and b are not congruent modulo m, we write $a \not\equiv b(\mathbf{mod} m)$.

Theorem

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if a $\mathbf{mod}$ $m \equiv b$ $\mathbf{mod}$ m.

Examlpe. Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6

Modular Arithmetic

Theorem

Let a and b be integers, and let m be a positive integer. Then $a \equiv b \pmod{m}$ if and only if $a \mathbf{\ mod\ } m \equiv b \mathbf{\ mod\ } m$.

Examlpe. Determine whether 17 is congruent to 5 modulo 6 and whether 24 and 14 are congruent modulo 6

Solution. Because 6 divides 17-5 = 12, we see that $17 \equiv 5(mod 6)$. However, because 24-14 = 10 is not divisible by 6, we see that $24 \not\equiv 14(mod 6)$.

Modular Arithmetic

Theorem

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \text{ and } ac \equiv bd \pmod{m}$$

.

Example. $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$
Apply here the Theorem above

Modular Arithmetic

Theorem

Let m be a positive integer. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, then

$$a + c \equiv b + d \pmod{m} \text{ and } ac \equiv bd \pmod{m}$$

.

Example. $7 \equiv 2 \pmod{5}$ and $11 \equiv 1 \pmod{5}$
Solution.

$$18 \equiv 3 \pmod{5}$$

$$77 \equiv 2 \pmod{5}$$

Modular Arithmetic

Corollary

Let m be a positive integer and let a and b be integers. Then

$$(a+b)\textbf{mod } m = ((a \textbf{ mod } m) + (b \textbf{ mod } m)) \textbf{ mod } m$$

$$ab \textbf{ mod } m = ((a \textbf{ mod } m)(b \textbf{ mod } m)) \textbf{ mod } m$$

Example. Find the value of the given expression

$$(177 \textbf{ mod } 31 + 270 \textbf{ mod } 31) \textbf{ mod } 31$$

Greatest common divisors and Least Common Multiples

Example. What is the greatest common divisor of 24 and 36?
Example. What is the least common multiple of $2^3 3^5 7^2$ and $2^4 3^3$?

Greatest common divisors and Least Common Multiples

Definition

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

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).**

ASTANA IT UNIVERSITY

Greatest common divisors and Least Common Multiples

Theorem

Let a and b be positive integers. Then

$$ab = gcd(a, b) \cdot lcm(a, b).$$

Definition

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

The Euclidean Algorithm

The **Euclidean Algorithm** is a technique for quickly finding the GCD of two integers.

Lemma

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

Euclidean Algorithm	
Calculate	**Which satisfies**
$r_1 = a \bmod b$	$a = q_1 b + r_1$
$r_2 = b \bmod r_1$	$b = q_2 r_1 + r_2$
$r_3 = r_1 \bmod r_2$	$r_1 = q_3 r_2 + r_3$
• • •	• • •
$r_n = r_{n-2} \bmod r_{n-1}$	$r_{n-2} = q_n r_{n-1} + r_n$
$r_{n+1} = r_{n-1} \bmod r_n = 0$	$r_{n-1} = q_{n+1} r_n + 0$ $d = \gcd(a, b) = r_n$

The Euclidean Algorithm

Example

Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

$$662 = 414 \cdot 1 + 248$$
$$414 = 248 \cdot 1 + 166$$
$$248 = 166 \cdot 1 + 82$$
$$166 = 82 \cdot 2 + 2$$
$$82 = 2 \cdot 41$$

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

Greatest common divisors and Least Common Multiples

Theorem

BÉZOUT'S THEOREM If a and b are positive integers, then there exist integers s and t such that gcd(a,b)= sa+tb.

Definition

If a and b are positive integers, then integers s and t such that gcd(a,b) = sa+tb are called **Bézout coefficients** of a and b.

ASTANA IT UNIVERSITY

Greatest common divisors and Least Common Multiples

Example

Express gcd(252, 198)=18 as a linear combination of 252 and 198.

Greatest common divisors and Least Common Multiples

Example

Express gcd(252, 198)=18 as a linear combination of 252 and 198.

Solution. To show that gcd(252, 198)=18, the Euclidean algorithm uses these divisions:

$$252 = 1 \cdot 198 + 54$$

$$198 = 3 \cdot 54 + 36$$

$$54 = 1 \cdot 36 + 18$$

$$36 = 2 \cdot 18$$

Our aim is to express 18 as a linear combination of 252 and 198.

So, what is a next step?

Greatest common divisors and Least Common Multiples

Solution. Our aim is to express 18 as a linear combination of 252 and 198.

$$18 = 54 - 1 \cdot 36$$

$$36 = 198 - 3 \cdot 54$$

Then,

$$18 = 54 - 1 \cdot 36 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198$$

$$54 = 252 - 1 \cdot 198$$

$$18 = 4 \cdot (252 - 1 \cdot 198) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198$$

Integer Representation

Theorem

Let b be an integer greater than 1. Then if n is a positive integer, it can be expressed uniquely in the form

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

where k is a nonnegative integer, $a_0, a_1, \ldots, a_k$ are nonnegative integers less than b, and $a_k \neq 0$.

Theorem above is called the **base b expansion of n.**

Among the most important bases in computer science are base 2, base 8, and base 16. Base 8 expansions are called **octal** expansions and base 16 expansions are **hexadecimal** expansions.

Integer Representation

Choosing 2 as the base gives **binary expansions** of integers.

Example

What is the decimal expansion of the integer that has $(101011111)_2$ as its binary expansion?

Integer Representation

Example

What is the decimal expansion of the integer that has $(101011111)_2$ as its binary expansion?

Solution.

$(101011111)_2 = 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2_6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1$

$+ 1 \cdot 2^0 = 351.$

ASTANA IT UNIVERSITY

Integer Representation

Example

What is the decimal expansion of the number with octal expansion $(7016)_8$?

Example

What is the decimal expansion of the number with hexadecimal expansion $(2AE0B)_{16}$?

Integer Representation

TABLE 1 **Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.**

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

Integer Representation

Example

Find the octal expansion of $(12345)_{10}$

Integer Representation

We will now describe an algorithm for constructing the base b expansion of an integer n.

$$n = bq_0 + a_0, \quad 0 \leq a_0 < b.$$

The remainder, a_0, is the rightmost digit in the base b expansion of n. Next, divide q_0 by b to obtain

$$q_0 = bq_1 + a_1, \quad 0 \leq a_1 < b.$$

The second digit from the right in the base b expansion of n. Continue this process, until q = 0

ASTANA IT UNIVERSITY

Example

Find the octal expansion of $(12345)_{10}$

Solution.

$$12345 = 8 \cdot 1543 + 1.$$

$$1543 = 8 \cdot 192 + 7,$$

$$192 = 8 \cdot 24 + 0,$$

$$24 = 8 \cdot 3 + 0,$$

$$3 = 8 \cdot 0 + 3$$

The successive remainders that we have found, 1, 7, 0, 0, and 3, are the digits from the right to the left of 12345 in base 8. Hence,

$$(12345)_{10} = (30071)_8.$$

Example

Find the hexadecimal expansion of $(177130)_{10}$

Algorithm

ALGORITHM 1 Constructing Base b Expansions.

procedure *base b expansion*(n, b: positive integers with $b > 1$)
$q := n$
$k := 0$
while $q \neq 0$
    $a_k := q$ **mod** b
    $q := q$ **div** b
    $k := k + 1$
return $(a_{k-1}, \ldots, a_1, a_0)$ $\{(a_{k-1} \ldots a_1 a_0)_b$ is the base b expansion of $n\}$

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.

Primes

Theorem

THE FUNDAMENTAL THEOREM OF ARITHMETIC Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Primes

Example

Find the prime factorizations of 100, 641, 999, and 1024.

Example

Find the prime factorizations of 100, 641, 999, and 1024.

Solution.

$$100 = 2 \cdot 2 \cdot 5 \cdot 5 = 2^2 5^2$$

$$641 = 641$$

$$999 = 3 \cdot 3 \cdot 3 \cdot 37 = 3^3 \cdot 37$$

$$1024 = 2^{10}$$

Primes

Example

Find the prime factorization of 7007.

Example

Find the prime factorization of 7007.

Solution. The prime factorization of 7007 is $7 \cdot 7 \cdot 11 \cdot 13 = 7^2 \cdot 11 \cdot 13$.

Primes

Theorem

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

Example. Show that 101 is prime.

Primes

Theorem

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

Example. Show that 101 is prime.

Solution. The only primes not exceeding $\sqrt{101}$ are 2, 3, 5, and 7. Because 101 is not divisible by 2, 3, 5, or 7 (the quotient of 101 and each of these integers is not an integer), it follows that 101 is prime.

ASTANA IT UNIVERSITY

Solving Congruence

Definition

A congruence of the form

$$ax \equiv b \pmod{m}$$

where m is a positive integer, a and b are integers, and x is a variable, is called a **linear congruence.**

Frame Title

Chinese Remainder Theorem ...