CS 0441
Lecture 8: Introduction to number theory

KP. Wang

Overview

- In this lecture, we will introduce basics about the number theory, in particular, with emphasis on the integers.
- An integer is a whole number (not a fractional number) that can be positive, negative, or zero.

Divisibility

- Given an integer, the division of it by a positive integer produces a quotient and a remainder.
- Some division only involves the quotients. Hence, we introduce the concept of the divisibility.

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 $a \mid b$ denotes that a divides b. We write $a \nmid b$ when a does not divide b.

Example 1

Example

Determine whether $3 \mid 7$ and whether $3 \mid 12$.

Solution: We see that $3 \nmid 7$, because $7/3$ is not an integer. On the other hand, $3 \mid 12$ because $12/3 = 4$.

Example 2

Example

Let n and d be positive integers. How many positive integers not exceeding n are divisible by d ?

Solution

The positive integers divisible by d are all the integers of the form dk, where k is a positive integer. Hence, the number of positive integers divisible by d that do not exceed n equals the number of integers k with $0 < dk \leqslant n$, or with $0 < k \leqslant n/d$. Therefore, there are $\lfloor n/d \rfloor$ positive integers not exceeding n that are divisible by d.

Properties of divisibility

- We introduce the property of divisibility as follows.

Theorem

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

- We will prove the property (i).

Proof.

Suppose that $a \mid b$ and $a \mid c$. Then, from the definition of divisibility, it follows that there are integers s and t with $b = as$ and $c = at$. Hence,

$$b + c = as + at = a(s + t).$$

Therefore, a divides $b + c$. ∎

- An important corollary following the above theorem is

Corollary

If a, b, and c are integers, where $a \neq 0$, such that $a \mid b$ and $a \mid c$, then $a \mid mb + nc$ whenever m and n are integers.

The division theorem

- Also, some integers may not be divisible by a positive integer. Then we may obtain a quotient and a remainder, for which we present the following

Theorem

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

- 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:

$$q = a \operatorname{div} d, \quad r = a \bmod d.$$

Remark

- Normally we choose the remainder r in $[0, d)$.
- Note that the integer a is divisible by the integer d if and only if the remainder is zero when a is divided by d.

Example 3

Example

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

Solution

We have

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

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

Example 4

Example

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

Solution

We have

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

Hence, the quotient when -11 is divided by 3 is $-4 = -11 \operatorname{div} 3$*, and the remainder is* $1 = -11 \bmod 3$*.*
Note that the remainder cannot be negative. Consequently, the remainder is not -2 , even though

$$-11 = 3(-3) - 2$$

because $r = -2$ *does not satisfy* $0 \leqslant r < 3$*.*

Modular arithmetic

- We have seen the notation $a \bmod d$. Now let us further discuss the 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 $a \equiv b \pmod{m}$ to indicate that a is **congruent** to b **modulo** m. We say that $a \equiv b \pmod{m}$ is a congruence and that m is its modulus (plural moduli). If a and b are not congruent modulo m, we write $a \not\equiv b \pmod{m}$.

Remark

- Note there lies a fundamental difference between the notations $a \equiv b (\bmod m)$ and $a \bmod m = b$ include "mod".
- The first represents a relation on the set of integers, whereas the second represents a function.

- We present the following

Theorem

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

Proof.

Let us prove from both directions. Suppose that $a \equiv b \pmod{m}$. Note $a \equiv b \pmod{m}$ implies $m \mid (a-b)$, which by definition implies that $a - b = km$ for some integer k. Therefore $a = b + km$. Taking both sides modulo m we get

$$a \bmod m = (b + km) \bmod m = b \bmod m.$$

■

Proof.

Suppose that $a \bmod m = b \bmod m$. By the division theorem, $a = mq + (a \bmod m)$ and $b = ms + (b \bmod m)$ for some integers q and s.

$$\begin{aligned} a - b &= (mq + (a \bmod m)) - (ms + (b \bmod m)) \\ &= m(q - s) + (a \bmod m - b \bmod m) \\ &= m(q - s) \text{ (since } a \bmod m = b \bmod m) \end{aligned}$$

Therefore $m \mid (a - b)$ and $a \equiv b \pmod{m}$. ■

Example 5

Example

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* $17 \equiv 5 (\text{mod} 6)$.
However, because $24 - 14 = 10$ *is not divisible by 6 , we see that* $24 \not\equiv 14 (\text{mod} 6)$.

- We can further discuss the congruence with the following

Theorem

Let m be a positive integer. The integers a and b are congruent modulo m if and only if there is an integer k such that $a = b + km$.

Proof.

Proof: If $a \equiv b \pmod m$, by the definition of congruence (Definition 3), we know that $m \mid (a - b)$. This means that there is an integer k such that $a - b = km$, so that $a = b + km$. Conversely, if there is an integer k such that $a = b + km$, then $km = a - b$. Hence, m divides $a - b$, so that $a \equiv b \pmod m$. ■

Remark

- The set of all integers congruent to an integer a modulo m is called the congruence class of a modulo m. For example, $\mathbb{Z} = [0] \cup [1] \cup [2]$.

- Now let us discuss the arithmetic of congruence.
- First we consider the following

Theorem

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

Proof.

We use a direct proof. Because $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, by the division theorem there are integers s and t with $b = a + sm$ and $d = c + tm$. Hence,

$$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$$

and

$$bd = (a + sm)(c + tm) = ac + m(at + cs + stm).$$

Hence,

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

$\blacksquare$

Example 6

Example

Because $7 \equiv 2 \pmod 5$ and $11 \equiv 1 \pmod 5$, it follows from the theorem that

$$18 = 7 + 11 \equiv 2 + 1 = 3 \pmod 5$$

and that

$$77 = 7 \cdot 11 \equiv 2 \cdot 1 = 2 \pmod 5.$$

Remark

- We must be careful working with congruences. Some properties we may expect to be true are not valid. For example, if $ac \equiv bc \pmod{m}$, the congruence $a \equiv b \pmod{m}$ may be false.
- Similarly, if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, the congruence $a^c \equiv b^d \pmod{m}$ may be false.

- The following corollary is also of importance.

Corollary

Let m be a positive integer and let a and b be integers. Then $(a+b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$ and $ab \bmod m = ((a \bmod m)(b \bmod m)) \bmod m$.

Proof.

By the definitions of $\bmod m$ and of congruence modulo m, we know that $a \equiv (a \bmod m) \pmod m$ and $b \equiv (b \bmod m) \pmod m$. Hence, Theorem 5 tells us that

$$a + b \equiv (a \bmod m) + (b \bmod m) \pmod m$$

and

$$ab \equiv (a \bmod m)(b \bmod m) \pmod m.$$

■

Arithmetic modulo m

- We can define arithmetic operations on $\mathbb{Z}_m$, 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 $\cdot_m$ by
$$a \cdot_m b = (a \cdot b) \bmod m,$$
where the multiplication on the right-hand side of this equation is the ordinary multiplication of integers.

- The operations $+_m$ and $\cdot_m$ are called addition and multiplication modulo m and when we use these operations, we are said to be doing arithmetic modulo m.

Example 7

Example

Use the definition of addition and multiplication in $\mathbb{Z}_m$ to find $7 +_{11} 9$ and $7 \cdot_{11} 9$.

Solution

Using the definition of addition modulo 11*, we find that*

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

and

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

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

Properties of modulo addition and modulo product

The operations $+_m$ and $\cdot_m$ satisfy many of the same properties of ordinary addition and multiplication of integers. In particular, they satisfy these properties:

- **Closure:** If a and b belong to $\mathbf{Z}_m$, then $a +_m b$ and $a \cdot_m b$ belong to $\mathbb{Z}_m$.
- **Associativity:** If a, b, and c belong to $\mathbb{Z}_m$, then $(a + {}_m b) + {}_m c = a + {}_m (b + {}_m c)$ and $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
- **Commutativity:** If a and b belong to $\mathbb{Z}_m$, then $a + {}_m b = b + {}_m a$ and $a \cdot {}_m b = b \cdot {}_m a$. Identity elements The elements 0 and 1 are identity elements for addition and multiplication modulo m, respectively. That is, if a belongs to $\mathbb{Z}_m$, then $a + {}_m 0 = 0 +_m a = a$ and $a \cdot {}_m 1 = 1 \cdot_m a = a$.

- **Additive inverses:** If $a \neq 0$ belongs to $\mathbb{Z}_m$, then $m - a$ is an additive inverse of a modulo m and 0 is its own additive inverse. That is $a +_m (m - a) = 0$ and $0 +_m 0 = 0$.
- **Distributivity:** If a, b, and c belong to $\mathbb{Z}_m$, then $a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ and $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.

Representations of integers

- In everyday life we use decimal notation to express integers. For example, 965 is used to denote $9 \cdot 10^2 + 6 \cdot 10 + 5$. In particular, computers usually use binary notation (with 2 as the base) when carrying out arithmetic, and octal (base 8) or hexadecimal (base 16) notation.
- In general, we present the following

Theorem

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

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

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

- The representation of n given in the above theorem is called the base $\boldsymbol{b}$ expansion of $\boldsymbol{n}$. The base b expansion of n is denoted by $(a_k a_{k-1} \ldots a_1 a_0)_b$.

Binary representations

- Choosing the number 2 as the base gives binary expansions of integers. In binary notation each digit is either a 0 or a 1 . In other words, the binary expansion of an integer is just a bit string.

Example 8

Example

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

Solution

We have

$$\begin{aligned}(101011111)_2 =& 1 \cdot 2^8 + 0 \cdot 2^7 + 1 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 \\ &+ 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 351\end{aligned}$$

Octal and hexadecimal representations

- We can also represent a number with base 8 expansions, which is called octal expansions. The octal digits are $0, 1, 2, 3, 4, 5, 6, 7$.
- In the hexadecimal system , we represent a number with base 16 expansions, called hexadecimal expansions. The hexadecimal digits are $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E$ and F, where the letters A through F represent the digits corresponding to the numbers 10 through 15 (in decimal notation).

Example 9

Example

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

Solution

Using the definition of a base b expansion with $b = 8$ tells us that

$$(7016)_8 = 7 \cdot 8^3 + 0 \cdot 8^2 + 1 \cdot 8 + 6 = 3598$$

Example 10

Example

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

Solution

Using the definition of a base b expansion with $b = 16$ tells us that

$$(2AE0B)_{16} = 2 \cdot 16^4 + 10 \cdot 16^3 + 14 \cdot 16^2 + 0 \cdot 16 + 11 = 175627.$$

*Each hexadecimal digit can be represented using four bits. For instance, we see that $(11100101)_2 = (E5)_{16}$ because $(1110)_2 = (E)_{16}$ and $(0101)_2 = (5)_{16}$. **Bytes**, which are bit strings of length eight, can be represented by two hexadecimal digits.*

Base conversion

- We will now describe an algorithm for constructing the base b expansion of an integer n. First, divide n by b to obtain a quotient and remainder, that is,

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

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

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

- We see that a_1 is the second digit from the right in the base b expansion of n. Continue this process, successively dividing the quotients by b, obtaining additional base b digits as the remainders.
- This process terminates when we obtain a quotient equal to zero. It produces the base b digits of n from the right to the left given by, for example, $(a_k a_{k-1} \cdots a_1 a_0)_b$, where $k \in \mathbb{N}$.

Example 11

Example

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

Solution

First, divide 12345 by 8 to obtain

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

Successively dividing quotients by 8 gives

$$\begin{aligned} 1543 &= 8 \cdot 192 + 7, \\ 192 &= 8 \cdot 24 + 0, \\ 24 &= 8 \cdot 3 + 0, \\ 3 &= 8 \cdot 0 + 3. \end{aligned}$$

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 12

Example

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

Solution

First divide 177130 by 16 to obtain

$$177130 = 16 \cdot 11070 + 10$$

Successively dividing quotients by 16 gives

$$\begin{aligned} 11070 &= 16 \cdot 691 + 14, \\ 691 &= 16 \cdot 43 + 3, \\ 43 &= 16 \cdot 2 + 11, \\ 2 &= 16 \cdot 0 + 2. \end{aligned}$$

The successive remainders that we have found, 10, 14,3,11, 2, give us the digits from the right to the left of 177130 in the hexadecimal (base 16) expansion of $(177130)_{10}$*. It follows that*

$$(177130)_{10} = (2B3EA)_{16}.$$

Conversion between binary, octal and hexadecimal expansions

- Afterwards, we can also discuss the conversion of numbers in all different bases.
- When we conduct the conversions, it is always handy to use the following table

Decimal	0	1	2	3	4	5	6	7	8
Hexadecimal	0	1	2	3	4	5	6	7	8
Octal	0	1	2	3	4	5	6	7	10
Binary	0	1	10	11	100	101	110	111	1000

Decimal	9	10	11	12	13	14	15
Hexadecimal	9	A	B	C	D	E	F
Octal	11	12	13	14	15	16	17
Binary	1001	1010	1011	1100	1101	1110	1111

Example 13

Example

Find the octal and hexadecimal expansions of $\left(\;11\quad 111011\quad 1100\;\right)_2$ and the binary expansions of $(765)_8$ and $(A8D)_{16}$.

Solution

First we convert the given binary number to octal and hexadecimal bases.

To convert $\left(\ 11\quad 1110\quad 1011\quad 1100\ \right)_2$ *into octal notation we group the binary digits into blocks of three, adding initial zeros at the start of* ***the leftmost block*** *if necessary. These blocks, from left to right, are* $011, 111, 010, 111,$ *and* 100*, corresponding to 3, 7, 2, 7 and 4, respectively. Consequently,*
$(11111010111100)_2 = (37274)_8$.

To convert $(1111\ 101011\ 1100)_2$ *into hexadecimal notation we group the binary digits into blocks of four, adding initial zeros at the start of* ***the leftmost block*** *if necessary. These blocks, from left to right, are 0011, 1110, 1011 and 1100, corresponding to the hexadecimal digits* $3, E, B$ *and* C*, respectively. Consequently,*
$(11111010111100)_2 = (3EBC)_{16}$.

Solution

On the other way around, to convert $(765)_8$ *into binary notation, we replace each octal digit by a block of three binary digits. These blocks are 111, 110, and 101. Hence,* $(765)_8 = (111110101)_2$*. To convert* $(A8D)_{16}$ *into binary notation, we replace each hexadecimal digit by a block of four binary digits. These blocks are 1010, 1000, and 1101. Hence,* $(A8D)_{16} = (101010001101)_2$*.*

Binary arithmetic

- In what follows, we will emphasis on the arithmetic between binary numbers.
- Suppose the binary expansions of a and b are

$$a = (a_{n-1}a_{n-2}\dots a_1 a_0)_2\,, b = (b_{n-1}b_{n-2}\dots b_1 b_0)_2\,,$$

  such that a and b each have n bits (putting bits equal to 0 at the beginning of one of these expansions if necessary).
- Let us introduce the binary addition and multiplication .

Binary addition

- To add the above given a and b, first add their rightmost bits. This gives

$$a_0 + b_0 = c_0 \cdot 2 + s_0,$$

where s_0 is the rightmost bit in the binary expansion of $a + b$ and c_0 is the **carry**, which is either 0 or 1.

- Then add the next pair of bits and the carry,

$$a_1 + b_1 + c_0 = c_1 \cdot 2 + s_1,$$

where s_1 is the next bit (from the right) in the binary expansion of $a + b$, and c_1 is the carry.

- Continue this process, adding the corresponding bits in the two binary expansions and the carry, to determine the next bit from the right in the binary expansion of $a + b$.
- At the last stage, add a_{n-1}, b_{n-1}, and c_{n-2} to obtain $c_{n-1} \cdot 2 + s_{n-1}$. The **leading bit** of the sum is $s_n = c_{n-1}$.
- This procedure produces the binary expansion of the sum, namely, $a + b = (s_n s_{n-1} s_{n-2} \dots s_1 s_0)_2$.

Example 14

Example

Add $a = (1110)_2$ and $b = (1011)_2$.

Solution

Following the procedure specified in the algorithm, first note that

$$a_0 + b_0 = 0 + 1 = 0 \cdot 2 + 1,$$

so that $c_0 = 0$ *and* $s_0 = 1$*. Then, because*

$$a_1 + b_1 + c_0 = 1 + 1 + 0 = 1 \cdot 2 + 0,$$

it follows that $c_1 = 1$ *and* $s_1 = 0$*. Continuing,*

$$a_2 + b_2 + c_1 = 1 + 0 + 1 = 1 \cdot 2 + 0$$

so that $c_2 = 1$ *and* $s_2 = 0$*. Finally, because*

$$a_3 + b_3 + c_2 = 1 + 1 + 1 = 1 \cdot 2 + 1,$$

follows that $c_3 = 1$ *and* $s_3 = 1$*. This means that* $s_4 = c_3 = 1$*. Therefore,* $s = a + b = (11001)_2$*.*

Remark

- Equivalently, you can also perform the addition in the columnar form as follows

$$\begin{array}{r} 1110 \\ +1011 \\ \hline 11001 \end{array}.$$

- The above columnar addition can be very handy in calculations, which you can use extensively. But when a question asks you to perform the binary addition in detailed steps, make sure you can follow the steps shown in Example 14.

Binary multiplication

- Next, consider the multiplication of two n-bit integers a and b. Using the distributive law, we see that

$$\begin{aligned} ab &= a\left(b_0 2^0 + b_1 2^1 + \cdots + b_{n-1} 2^{n-1}\right) \\ &= a\left(b_0 2^0\right) + a\left(b_1 2^1\right) + \cdots + a\left(b_{n-1} 2^{n-1}\right). \end{aligned}$$

  We can compute ab using this equation.

- We first note that $ab_j = a$ if $b_j = 1$ and $ab_j = 0$ if $b_j = 0$. Each time we multiply a term by 2 , we **shift** its binary expansion one place to the left and add a zero at the tail end of the expansion.

- Consequently, we can obtain $(ab_j)\,2^j$ by shifting the binary expansion of $ab_j j$ places to the left, adding j zero bits at the tail end of this binary expansion. Finally, we obtain ab by adding the n integers $ab_j 2^j, j = 0, 1, 2, \ldots, n-1$.

Example 15

Example

Find the product of $a = (110)_2$ and $b = (101)_2$.

Solution

Solution: First note that

$$ab_0 \cdot 2^0 = (110)_2 \cdot 1 \cdot 2^0 = (110)_2,$$
$$ab_1 \cdot 2^1 = (110)_2 \cdot 0 \cdot 2^1 = (0000)_2,$$

and

$$ab_2 \cdot 2^2 = (110)_2 \cdot 1 \cdot 2^2 = (11000)_2.$$

To find the product, add $(110)_2, (0000)_2$*, and* $(11000)_2$*. Carrying out these additions (using the binary addition, including initial zero bits when necessary) shows that* $ab = (11110)_2$*.*

Remark

- An equivalent columnar form is

$$\begin{array}{r} 1\ 1\ 0 \\ \times \quad 1\ 0\ 1 \\ \hline 1\ 1\ 0 \\ 1\ 1\ 0\ \cdot\ \ \\ \hline 1\ 1\ 1\ 1\ 0 \end{array}$$

- Similarly, you can apply the handy long multiplication. But also make sure you can follow steps in Example 15.