UNIVERSITY OF MICHIGAN-DEARBORN

Chapter 5 : Introduction to Number Theory

Introduction

What is Number Theory?

DEARBORN

- **Number theory** or **"arithmetic"** is the branch of pure mathematics devoted primarily to the study of the natural numbers and the integers.
- In this chapter, we used some basic number theory definitions such as "*divides*" and "*prime number*". We must cover three sections in this chapter, which are :

  ① We will start by reviewing these basic definitions and extend the discussion to unique *factorization*, *greatest common divisors* and *least common multiples*.

  ② Then, we discuss *representations of integers* and some algorithms for integer arithmetic.

  ③ Finally, *The Euclidean algorithm* for computing the greatest common divisor is the subject of the last section. This is surely one of the oldest algorithms.

Divisors

Introduction to Number Theory

- **Definition :** Let n and d be integers, $d \neq 0$. We say that *d divides n* if there exists an integer q satisfying $n = dq$.

  We call *q the quotient* and *d a divisor or factor of n*.

  - If *d divides n*, we write $d \mid n$.
  - If *d does not divide n* , we write $d \nmid n$.

- **Example:**

Since $21 = 3 \times 7$, we can see that 3 divides 21, we write **3 | 21**. The quotient is 7.

We call 3 a *divisor or factor* of 21.

Introduction to Number Theory

- **Theorem:** Let m, n and d be integers.

a) If $d \mid m$ and $d \mid n$, then

$$d \mid (m + n)$$

b) If $d \mid m$ and $d \mid n$, then

$$d \mid (m - n)$$

c) If $d \mid m$, then

$$d \mid mn$$

- ***Proof:*** Suppose that $d \mid m$ and $d \mid n$. By definition :

$$m = dq1$$

For some integer q1 and

$$n = dq2$$

For some integer q2. If we add the equations of m and n, we obtain

$$\mathbf{m + n = dq1 + dq2 = d\,(q1 + q2)}$$

Introduction to Number Theory

- **Definition :**
  - ❖ An integer greater than 1 whose only positive divisors are itself and 1 is called *prime*.
  - ❖ An integer greater than 1 that is not prime is called *composite.*

- **Example:**
  - ✓ The integer 23 is *prime* because its only divisors are itself and 1.
  - ✓ The integer 34 is *composite* because it is divisible by 17, which is neither 1 nor 34.

Introduction to Number Theory

- **Theorem 1:** Any integer greater than 1 can be written as a problem of primes. Moreover, if the primes are written in nondecreasing order, the factorization is unique. In symbols, if

$$n = p1\ p2\ \dots\ pi$$

Where the pk are primes and $p1 \leq p2 \leq \dots \leq pi$, and

$$n = p'1\ p'2\ \dots\ p'j$$

Where the p'k are primes and $p'1 \leq p'2 \leq \dots \leq p'j$, then $i = j$ and

pk = p'k for all k = 1, …, I

- **Theorem 2:** *The number of primes if infinite*. If p is a prime, there is a prime large than p.

Let consider all of the distinct primes less than or equal to p :

$$p1\ p2\ \dots\ pn$$

Consider the integer : m = [p1 p2 … pn] + 1

We consider m is a prime, if m is divided by pi (equal to [p1 p2 … pn]), the remainder is 1 :

m = pi + 1

Introduction to Number Theory

- **Definition :** Let m and n be integers with n and m different to zero. A *common divisor* of m and n is an integer that divides both m and n. The *greatest common divisor*, written

gcd(m, n)

gcd(m, n) is the largest common divisor of m and n.

- **Example:**

The positive divisor of 30 are

1, 2, 3, 5, 6, 10, 15, 30

And the positive divisors of 105 are

1, 3, 5, 7, 15, 21, 35, 105

Thus the positive common divisors of 30 and 105 are : 1, 3, 5, 15

It follows that the greatest common divisor of 30 and 105:

gcd(30, 105) = 15

Introduction to Number Theory

- **Theorem :** Let m and n be integers, m > 1, n > 1, with prime factorizations (or prime decomposition). The **Prime factorization** or integer **factorization** of a number is the determination of the set of **prime** numbers which multiply together to give the original integer.

$$m = p^{a1}_1 \ p^{a2}_2 \dots p^{ak}_k$$

And

$$n = p^{b1}_1 \ p^{b2}_2 \dots p^{bk}_k$$

[If the prime pi is not a factor of m, we let $a_i = 0$. Similarly, if the prime pi is not a factor of n, we let $b_i = 0$].

Then

$$\mathbf{gcd(m, n) = p^{min(a1,b1)}_1 \ p^{min(a2,b2)}_2 \dots \ p^{min(ak,bk)}_k}$$

- **Example :** We have $82320 = 2^4 \times 3^1 \times 5^1 \times 7^3 \times 11^0$

and $950796 = 2^2 \times 3^2 \times 5^0 \times 7^4 \times 11^1$

$$\gcd(82320, 950796) = 2^{\min(4,2)} \times 3^{\min(1,2)} \times 5^{\min(1,0)} \times 7^{\min(3,4)} \times 11^{\min(0,1)}$$

$$= 2^2 \times 3^1 \times 5^0 \times 7^3 \times 11^0$$

$$= 4116$$

Introduction to Number Theory

- **Definition :** Let m and n be positive integers. A *common multiple* of m and n is an integer that divides by both m and n. The *least common divisor*, written

lcm(m, n)

lcd(m, n) is the smallest common multiple of m and n.

- **Example 1:** The least common multiple of 30 and 105:

$$\text{lcm}(30, 105) = 210$$

Because 210 is divisible by 30 and 105 and by inspection, no positive integer smaller than 210 is divisible by both 30 and 105.

- **Example 2:** We can find the least common multiple of 30 and 105 by looking at their

prime factorizations : $30 = 2 \times 3 \times 5$ $105 = 3 \times 5 \times 7$

The prime factorization of lcm(30, 105) must contain 2, 3 and 5 as factors, it must also contain 3, 5 and 7. The smallest number with the property is

$$2 \times 3 \times 5 \times 7 = 210$$

Therefore, lcm(30, 105) = 210.

Introduction to Number Theory

- **Theorem :** Let m and n be integers, m > 1, n > 1, with prime factorizations

$$m = p^{a1}_1 \; p^{a2}_2 \ldots p^{ak}_k$$

And

$$n = p^{b1}_1 \; p^{b2}_2 \ldots p^{bk}_k$$

[If the prime pi is not a factor of m, we let $a_i = 0$. Similarly, if the prime pi is not a factor of n, we let $b_i = 0$].

Then $\mathbf{gcd(m, n) = p^{max(a1,b1)}_1 \; p^{max(a2,b2)}_2 \ldots p^{max(ak,bk)}_k}$

- **Example :** We have $82320 = 2^4 \times 3^1 \times 5^1 \times 7^3 \times 11^0$

and $950796 = 2^2 \times 3^2 \times 5^0 \times 7^4 \times 11^1$

$$gcd(82320, 950796) = 2^{max(4,2)} \times 3^{max(1,2)} \times 5^{max(1,0)} \times 7^{max(3,4)} \times 11^{max(0,1)}$$

$$= 2^4 \times 3^2 \times 5^1 \times 7^4 \times 11^1$$

$$= 19015920$$

Introduction to Number Theory

- **Theorem :** For any positive integers m and n,

$$\gcd(m, n) \times \mathrm{lcm}(m, n) = mn$$

- **Example :** In the previous example, we found that

$$\gcd(30, 105) = 15$$

and

$$\mathrm{lcm}(30, 105) = 210$$

Notice that the product of the gcd and lcm is equal to the product of the pair of numbers; that is,

$$\begin{aligned}\gcd(30, 105) \times \mathrm{lcm}(30, 105) &= 15 \times 210\\ &= 3150 = 30 \times 105\end{aligned}$$

Exercises

Exercise 1 : Find the greatest common divisor of each pair of integers :

a) 0, 17

b) 110, 273

c) 20, 40

d) $3^2 \times 7^3 \times 11$, $3^2 \times 7^3 \times 11$

Exercise 2 : Find the least common multiple of each pair of integers :

a) 5, 25

b) 60, 90

c) 20, 40

Exercise 3 : Let m, n and d be integers. Show that if d | m, then d | mn.

Exercise 4 : Let a, b and c be integers. Show that if a | b and b | c, then a | c.

Representation of integers and some algorithms for integer arithmetic

Introduction to Number Theory

- In this section, we discuss :
  - *the decimal number system:* it represents integers using 10 symbols.
  - *the binary number system :* it represents integers using bits (a bit is a binary digit, that is a 0 or a 1).
  - *The hexadecimal number system :* it represents integers using 16 symbols.
  - *The octal number system :* it represents integers using 8 symbols.

Introduction to Number Theory

DEARBORN

- In the *decimal number system*, to represent integers we use the 10 symbols:

  0, 1, 2, 3, 4, 5, 6, 7, 8, and 9.

- In representing an integer, the symbol's position is significant: reading from the right, the first symbol represents the number of 1's, the next symbol the number of 10's, the next symbol the number of 100's, and so on.

- ***Example of The decimal number system in base 10:***

$$3854 = 3 \times 10^3 + 8 \times 10^2 + 5 \times 10^1 + 4 \times 10^0$$

We call the value on which the system is based (10 in the case of the decimal system) the *base* of the number system

100's place (10^2) 10's place (10^1)

1000's place (10^3) 1's place (10^0)

3 8 5 4

symbol 3 symbol 0

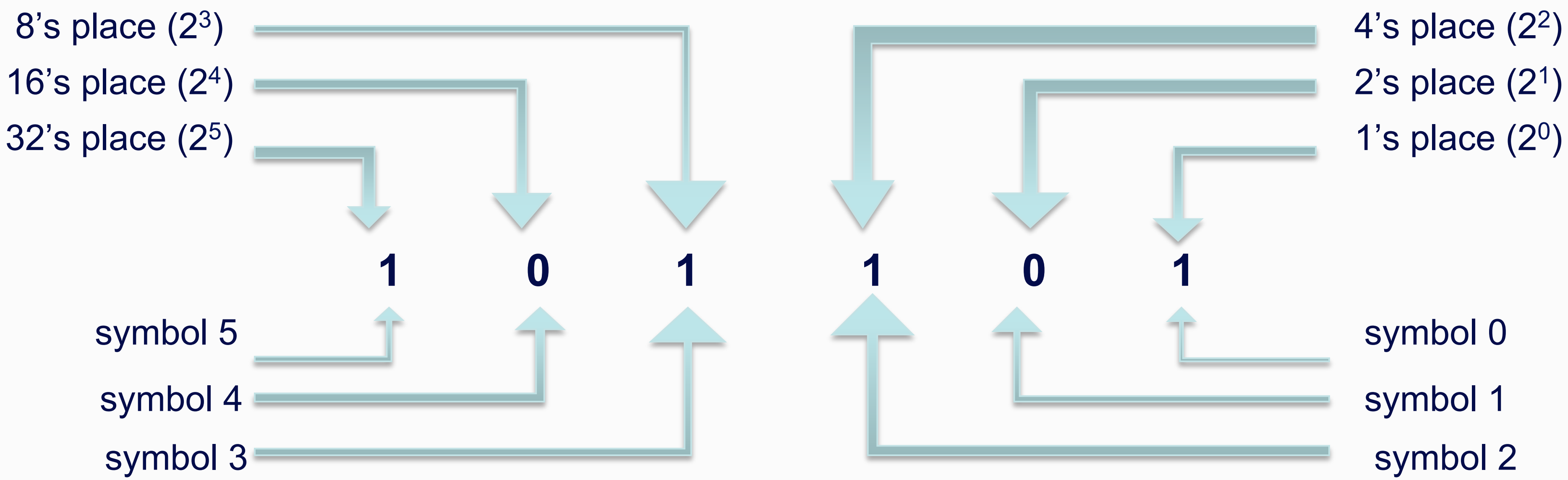
symbol 2 symbol 1

Introduction to Number Theory

DEARBORN

- In the *binary number system*, to represent integers we need only two symbols, 0 and 1.
- In representing an integer, reading from the right, the first symbol represents the number of 1's, the next symbol the number of 2's, the next symbol the number of 4's, the next symbol the number of 8'sand so on.
- ***Example of The binary number system in base 2:***

$$101101 = 1 \times 2^5 + 0 \times 2^4 + 1 \times 2^3 + 1 \times 2^2 + 0 \times 2^1 + 1 \times 2^0$$



Introduction to Number Theory

- <u>*binary to decimal number system*:</u>

<u>Example</u> : The binary number $10101_2 = 1*2^5 + 0*2^4 + 1*2^3 + 1*2^2 + 0*2^1 + 1*2^0$

Computing the right-hand side in decimal, we find that

$$10101_2 = 1 \times 32 + 0 \times 16 + 1 \times 8 + 1 \times 4 + 0 \times 2 + 1 \times 1 = 32 + 8 + 4 + 1 = 45_{10}$$

<u>Algorithm</u> : Converting an integer from Base b to decimal

This algorithm returns the decimal value of the base b integer Cn Cn-1 … C1C0.

Input : c, n, b

Output : dec_val

```
Base_b_to_dec(c, n, b) {
    dec_val = 0
    power = 1
    for i =0 to n {
        dec_val = dec_val + ci * power
        power = power*b
    }
    return dec_val
}
```

Introduction to Number Theory

- **Example :** Express a binary number 1011 by decimal (base 2).

1 0 1 1

$1 \times 2^0 = 1$

$1 \times 2^1 = 2$

$0 \times 2^2 = 0$

$1 \times 2^3 = 8$

The decimal number : **1 + 2 + 0 + 8 = 11**

Introduction to Number Theory

- Other important bases for number systems in computer science are base 8 or *octal* and base 16 or *hexadecimal* (sometimes shortened to *hex*).
- In the hexadecimal number system, to represent integers we use the symbols 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E and F. The symbols A-F are interpreted as decimal 10-15.
- In representing an integer, reading from the right, the first symbol represents the number of 1's, the next symbol the number of16's, the next symbol the number of 16^2's, and so on. For example, in base 16,

$$B4F = 11 \times 16^2 + 4 \times 16^1 + 15 \times 16^0$$

In general, the symbol in position n (with the right most symbol being in position 0) represents the number of 16^n's.

256' place (16^2) 16's place (16^1) 1's place (16^0)

B **4** **F**

symbol 2 symbol 1 symbol 0

DEARBORN

Introduction to Number Theory

Hexadecimal to Decimal Conversion Chart

Hexadecimal	Decimal
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8
9	9
A	10
B	11
C	12
D	13
E	14
F	15

Introduction to Number Theory

- ***Hexadecimal to decimal number system***:

Convert the hexadecimal number B4F to decimal

$$B4F_{16} = 11 \times 16^2 + 4 \times 16^1 + 15 \times 16^0$$

$$= 11 \times 256 + 4 \times 16 + 15 \times 1$$

$$= 2816 + 64 + 15$$

$$= 2895_{10}$$

Introduction to Number Theory

- ***Decimal to binary number system:***

Write the decimal number 130 in binary

The computation shows that the successive divisions by 2 with the remainders recorded at the right

2) 130	quotient = 65	remainder = 0	1's bit
2) 65	quotient = 32	remainder = 1	2's bit
2) 32	quotient = 16	remainder = 0	4's bit
2) 16	quotient = 8	remainder = 0	8's bit
2) 8	quotient = 4	remainder = 0	16's bit
2) 4	quotient = 2	remainder = 0	32's bit
2) 2	quotient = 1	remainder = 0	64's bit
2) 1	quotient = 0	remainder = 1	128's bit
0			

We may stop when the quotient is 0. Remembering that the first remainder gives the number of 1's, the second remainder gives the number of 2's, and so on, we obtain $130_{10} = 10000010_2$

Introduction to Number Theory

DEARBORN

- ***Decimal to Hexadecimal number system:***

Write the decimal number 20385 to hexadecimal.

The computation shows that the successive divisions by 16 with the remainders recorded at the right

16) 20385	quotient = 1274	remainder = 1	1's place
16) 1274	quotient = 79	remainder = 10	16's place
16) 79	quotient = 4	remainder = 15	16^2's place
16) 4	quotient = 0	remainder = 4	16^3's place
0			

We may stop when the quotient is 0. Remembering that the first remainder gives the number of 1's, the second remainder gives the number of 16's, and so on, we obtain $20385_{10} = 4FA1_{16}$

- *Binary addition:*

Add the binary numbers 10011011 and 1011011. We write the problem as

$$\begin{array}{r} 10011011 \\ +\ \underline{\ \ 1011011} \end{array}$$

As in decimal addiction, we begin from the right, adding 1 and 1. This sum is 10_2; thus we write 0 and carry 1. At this point the computation is

$$\begin{array}{r} 1 \\ 10011011 \\ +\ \underline{\ \ 1011011} \\ 0 \end{array}$$

Next, we add 1 and 1 and 1, which is 11_2. We write 1 and carry 1. At this point, the computation is

$$\begin{array}{r} 1 \\ 10011011 \\ +\ \underline{\ \ 1011011} \\ 10 \end{array}$$

Continuing in this way, we obtain

$$\begin{array}{r} 10011011 \\ +\ \underline{\ \ 1011011} \\ 11110110 \end{array}$$

Introduction to Number Theory

- ***Hexadecimal addition:***

Add the hexadecimal numbers $F0BA_{16}$ and $E9AD_{16}$ with base 16. We write the problem as

$$
\begin{array}{ccccc}
 & & 1 & 1 & \\
 & F & 0 & B & A_{16} \\
+ & E & 9 & A & D_{16} \\
\hline
\mathbf{1} & \mathbf{D} & \mathbf{A} & \mathbf{6} & \mathbf{7_{16}}
\end{array}
$$

$A + D = 10 + 13 = 23 = 16 + 7 = 17_{16}$

$1 + B + A = 1 + 11 + 10 = 22 = 16 + 6 = 16_{16}$

$1 + 0 + 9 = 10 = A$

$F + E = 15 + 14 = 29 = 16 + 13 = 1D_{16}$

Hexadecimal addition = $\mathbf{1DA67_{16}}$

Introduction to Number Theory

- **Theorem :** If a, b and z are positive integers, we define

$$ab \bmod z = [(a \bmod z)\ (b \bmod z)] \bmod z$$

- **Example :** To compute $a^{29} \bmod z$, we successively compute

$a^2 \bmod z$, $a^5 \bmod z$ $a^{13} \bmod z$ $a^{29} \bmod z$

$$a^2 \bmod z = a\ a \bmod z = [(a \bmod z)\ (a \bmod z)] \bmod z$$

$$a^5 \bmod z = a^1\ a^4 \bmod z = [(a \bmod z)\ (a^4 \bmod z)] \bmod z$$

$$a^{13} \bmod z = a^5\ a^8 \bmod z = [(a^5 \bmod z)\ (a^8 \bmod z)] \bmod z$$

$$a^{29} \bmod z = a^{13}\ a^{16} \bmod z = [(a^{13} \bmod z)\ (a^{16} \bmod z)] \bmod z$$

Exercises

DEARBORN

Exercise 1 : Express each binary number in decimal.

a) 1001
b) 100000

Exercise 2 : Express each decimal number in binary.

a) 43
b) 400

Exercise 3 : Add the binary numbers.

a) 1001 + 1111
b) 101101 + 11011

Exercise 4 : Express each hexadecimal number in decimal

a) 3A
b) A03

UNIVERSITY OF MICHIGAN-DEARBORN

The Euclidean algorithm

Introduction to Number Theory

DEARBORN

- In the first section, we discussed some methods of computing the greatest common divisor of two integers.
- The *Euclidean algorithm* is an odd, famous, and efficient algorithm for finding the greatest common divisor of two integers,
- The Euclidean algorithm is based on the fact that if $r = a \bmod b$, then

$$\gcd(a, b) = \gcd(b, r)$$

- **Example :**
  - ❖ Since 105 mod 30 = 15, we can write

$$\gcd(105, 30) = \gcd(30, 15)$$

  - ❖ Since 30 mod 15 = 0, we can write

$$\gcd(30, 15) = \gcd(15, 0)$$

By inspection, gcd(15, 0) = 15. Therefore,

$$\gcd(105, 30) = \gcd(30, 15) = \gcd(15, 0) = 15$$

Introduction to Number Theory

- **Algorithm :** Euclidean Algorithm

This algorithm finds the greatest common divisor of the nonnegative integers a and b, where a and b are both different to zero.

Input: a and b (nonnegative integers, not both zero)

Output : Greatest common divisor of a and b

```
gcd(a, b) {
    // make a largest
    if (a < b)
        swap(a, b)
    while (b ≠ 0) {
        r = a mod b
        a = b
        b = r
    }
    return a
}
```

Introduction to Number Theory

- **<u>Example :</u>** We show how the Euclidean algorithm finds gcd(504, 396)
  - ❖ Let a = 504 and b = 396. Since a > b, we move to line 5. Since b ≠ 0, we proceed to line 6, where we set r to

$$a \bmod b = 505 \bmod 396 = 108$$

We then move to lines 7 and 8, where we set a to 396 and b to 108. We then return to line 5.

❖ Since b ≠ 0, We proceed to line 6, where we set r to

$$a \bmod b = 396 \bmod 108 = 72$$

We then move to line 7 and 8, where we set a to 108 and b to 72. We then return to line 5.

❖ Since b ≠ 0, We proceed to line 6, where we set r to

$$a \bmod b = 108 \bmod 72 = 36$$

We then move to line 7 and 8, where we set a to 72 and b to 36. We then return to line 5.

❖ Since b ≠ 0, We proceed to line 6, where we set r to

$$a \bmod b = 72 \bmod 36 = 0$$

We then move to line 7 and 8, where we set a to 36 and b to 0. We then return to line 5.

This time b = 0, so we skip the line 10, where we **return a (36), the greatest common divisor of 396 and 504.**

Exercises

DEARBORN

<u>Exercise 1 :</u> Use the Euclidean algorithm to find the greatest common divisor of each pair of integers.

a) 60, 90

b) 315, 825

c) 2091, 4807

<u>Exercise 2 :</u>

Let consider $\{fn\}$ a Fibonacci sequence. Show by the mathematical induction that

$$gcd(fn, fn+1) = 1, \qquad n \geq 1.$$