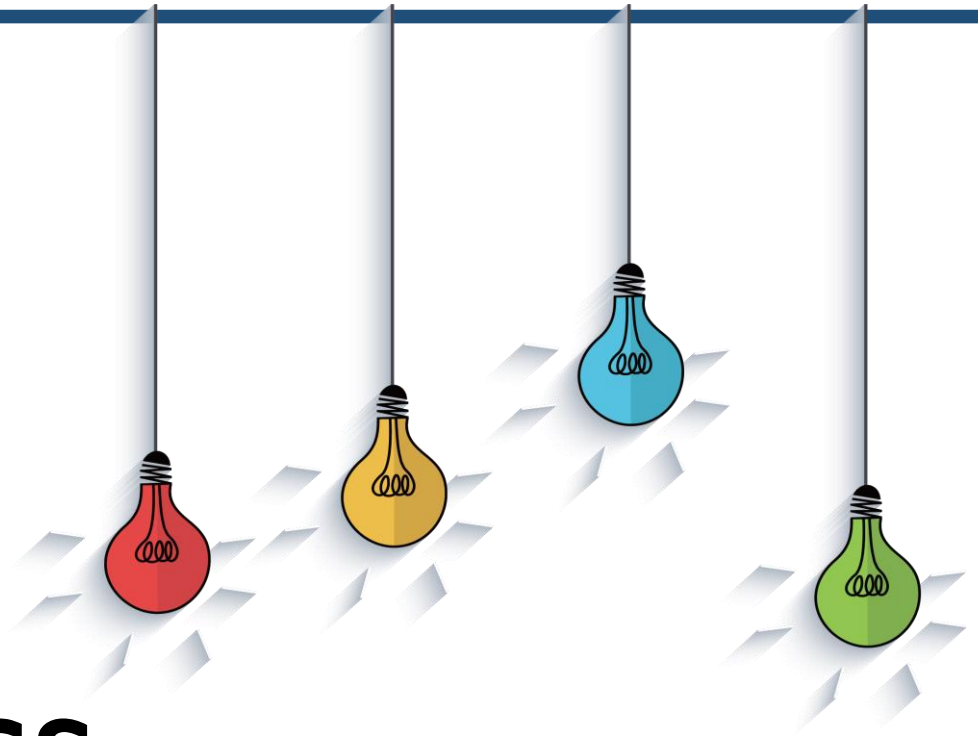
UMN
UNIVERSITAS
MULTIMEDIA
NUSANTARA



IF120
Discrete Mathematics

06 Number Theory

Angga Aditya Permana, Januar Wahjudi, Yaya Suryana, Meriske, Muhammad Fahrury Romdendine

REVIEW

- Relations
- Equivalence Relations
- Matrices of Relations

OUTLINE

- Number Theory
- Binary, Octal, and Hexadecimal System Numbers
- Euclid Algorithm

Number Theory

- **Number theory** is the branch of mathematics concerned with the integers.
- Traditionally, number theory was a *pure* branch of mathematics—known for its abstract nature rather than its applications.
- The great English mathematician, G. H. Hardy (1877–1947), used number theory as an example of a beautiful, but impractical, branch of mathematics.
- However, in the late 1900s, number theory became extremely useful in cryptosystems—systems used for secure communications.

Divisors

- *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 $d \nmid n$.

❑ Since $21 = 3 \cdot 7$, 3 divides 21 and we write $3 \mid 21$. The quotient is 7. We call 3 a divisor or factor of 21.

- We note that if *n* and *d* are positive integers and $d \mid n$, then $d \leq n$. (If $d \mid n$, there exists an integer *q* such that $n = dq$. Since *n* and *d* are positive integers, $1 \leq q$. Therefore, $d \leq dq = n$.)
- Whether an integer $d > 0$ divides an integer *n* or not, we obtain a unique quotient *q* and remainder *r* as given by the Quotient-Remainder Theorem: There exist unique integers *q* (**quotient**) and *r* (**remainder**) satisfying $n = dq + r$, $0 \leq r < d$. The remainder *r* equals zero if and only if *d* divides *n*.

Divisors

- Some additional properties of divisors are given in the following theorem
- Theorem 6.1:

  Let m, n, and d be integers.

a) *If d | m and d | n, then*

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

b) *If d | m and d | n, then*

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

c) *If d | m, then d | mn.*

- *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**.

❑ 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.

Prime and Composite

- Theorem 6.2:

  A positive integer n greater than 1 is composite if and only if n has a divisor d satisfying $2 \leq d \leq \sqrt{n}$.

- Algorithm 6.1: **Testing Whether an Integer is Prime**

```
Input: n
Output: d
is prime(n) {
        for d = 2 to √n
                if (n mod d == 0)
                        return d
        return 0
}
```

Prime and Composite

- To determine whether 43 is prime, Algorithm 6.1 checks whether any of

$$2, 3, 4, 5, 6 = \lfloor \sqrt{43} \rfloor$$

divides 43. Since none of these numbers divides 43, the condition

$$n \bmod d == 0$$

is always false. Therefore, the algorithm returns 0 to indicate that 43 is prime.

- To determine whether 451 is prime, Algorithm 6.1 checks whether any of

$$2, 3, \ldots, 21 = \lfloor \sqrt{451} \rfloor$$

divides 451. For $d = 2, 3, \ldots, 10$, d does not divide 451 and the condition

$$n \bmod d == 0$$

is false. However, when $d = 11$, d does divide 451 and the condition

$$n \bmod d == 0$$

is true. Therefore, the algorithm returns 11 to indicate that 451 is composite and 11 divides 451.

Prime and Composite

- Notice that if a composite integer *n* is input to Algorithm 6.1, the divisor returned is prime; that is, Algorithm 6.1 returns a prime factor of a composite integer.

❑ If the input to Algorithm 6.1 is $n = 1274$, the algorithm returns the prime 2 because 2 divides 1274, specifically

$$1274 = 2 \cdot 637.$$

If we now input $n = 637$ to Algorithm 6.1, the algorithm returns the prime 7 because 7 divides 637, specifically

$$637 = 7 \cdot 91.$$

If we now input $n = 91$ to Algorithm 6.1, the algorithm returns the prime 7 because 7 divides 91, specifically

$$91 = 7 \cdot 13.$$

If we now input $n = 13$ to Algorithm 6.1, the algorithm returns 0 because 13 is prime.

Combining the previous equations gives 1274 as a product of primes

$$1274 = 2 \cdot 637 = 2 \cdot 7 \cdot 91 = 2 \cdot 7 \cdot 7 \cdot 13.$$

GCD

- *Definition*: Let *m* and *n* be integers with not both *m* and *n* zero. A **common divisor** of *m* and *n* is an integer that divides both *m* and *n*. The **greatest common divisor**, written

$$\gcd(m, n),$$

  is the **largest** common divisor of *m* and *n*.

- The positive divisors 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, $\gcd(30, 105)$, is 15.

LCM

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

$$lcm(m, n),$$

  is the **smallest** positive common multiple of *m* and *n*.

- The least common multiple of 30 and 105, $lcm(30, 105)$, is 210 because 210 is divisible by both 30 and 105 and, by inspection, no positive integer smaller than 210 is divisible by both 30 and 105.

GCD & LCM

- We find the greatest common divisor of 30 and 105 by looking at their prime factorizations

$$30 = 2 \cdot 3 \cdot 5 \qquad 105 = 3 \cdot 5 \cdot 7.$$

Notice that 3 is a common divisor of 30 and 105 since it occurs in the prime factorization of both numbers. For the same reason, 5 is also a common divisor of 30 and 105. Also, $3 \cdot 5 = 15$ is also a common divisor of 30 and 105. Since no larger product of primes is common to both 30 and 105, we conclude that 15 is the greatest common divisor of 30 and 105.

- Similarly, we can find the least common multiple of 30 and 105.

The prime factorization of $lcm(30, 105)$ must contain 2, 3, and 5 as factors [so that 30 divides $lcm(30, 105)$]. It must also contain 3, 5, and 7 [so that 105 divides $lcm(30, 105)$]. The smallest number with this property is

$$2 \cdot 3 \cdot 5 \cdot 7 = 210.$$

Therefore, $lcm(30, 105) = 210$.

GCD & LCM

- Theorem 6.3:

  For any positive integers m and n,

$$\gcd(m,n) \cdot lcm(m,n) = mn.$$

- In previous Examples, we found that

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

  and

$$lcm(30,105) = 210.$$

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

$$\gcd(30,105) \cdot lcm(30,105) = 15 \cdot 210 = 3150 = 30 \cdot 105.$$

- If we have an algorithm to compute the greatest common divisor, we can compute the least common multiple by using Theorem 6.3:

$$lcm(m,n) = \frac{mn}{\gcd(m,n)}.$$

Binary, Octal, and Hexadecimal System Numbers

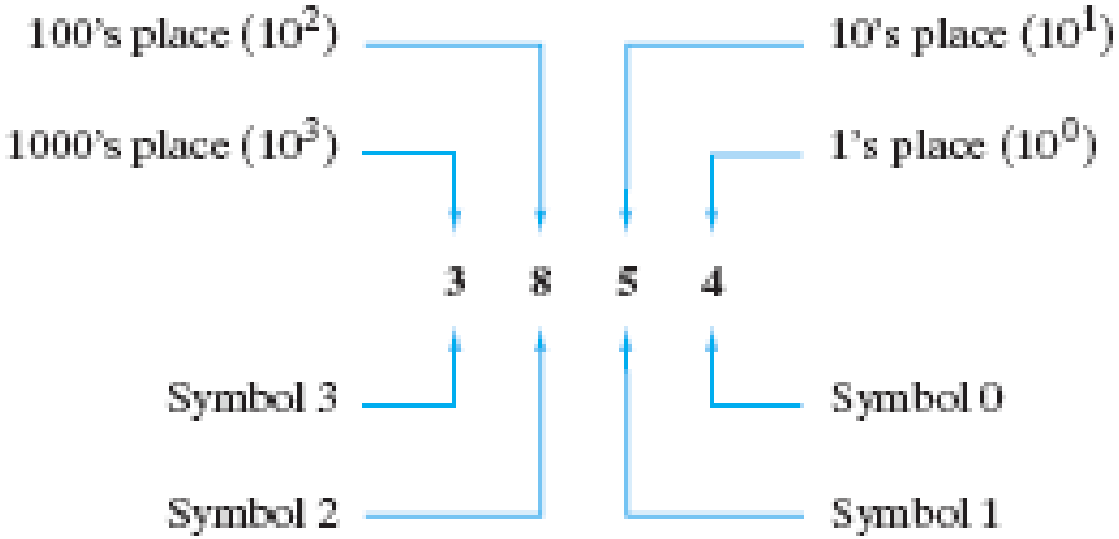
- A **bit** is a *b*inary dig*it*, that is, a 0 or a 1.
- In a digital computer, data and instructions are encoded as bits. (The term *digital* refers to the use of the digits 0 and 1.)
- Technology determines how the bits are physically represented within a computer system.
- Today's hardware relies on the state of an electronic circuit to represent a bit.
- The circuit must be capable of being in two states—one representing 1, the other 0.
- In this section we discuss the **binary number system,** which represents integers using bits, the **octal number system,** which represents integers using eight symbols, and the **hexadecimal number system,** which represents integers using 16 symbols.

Decimal Number System

- In the **decimal** number system, to represent integers we use the 10 symbols 0, 1, 2, 3, 4, 5, 6, 7, 8, and 9.

❑For example,

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



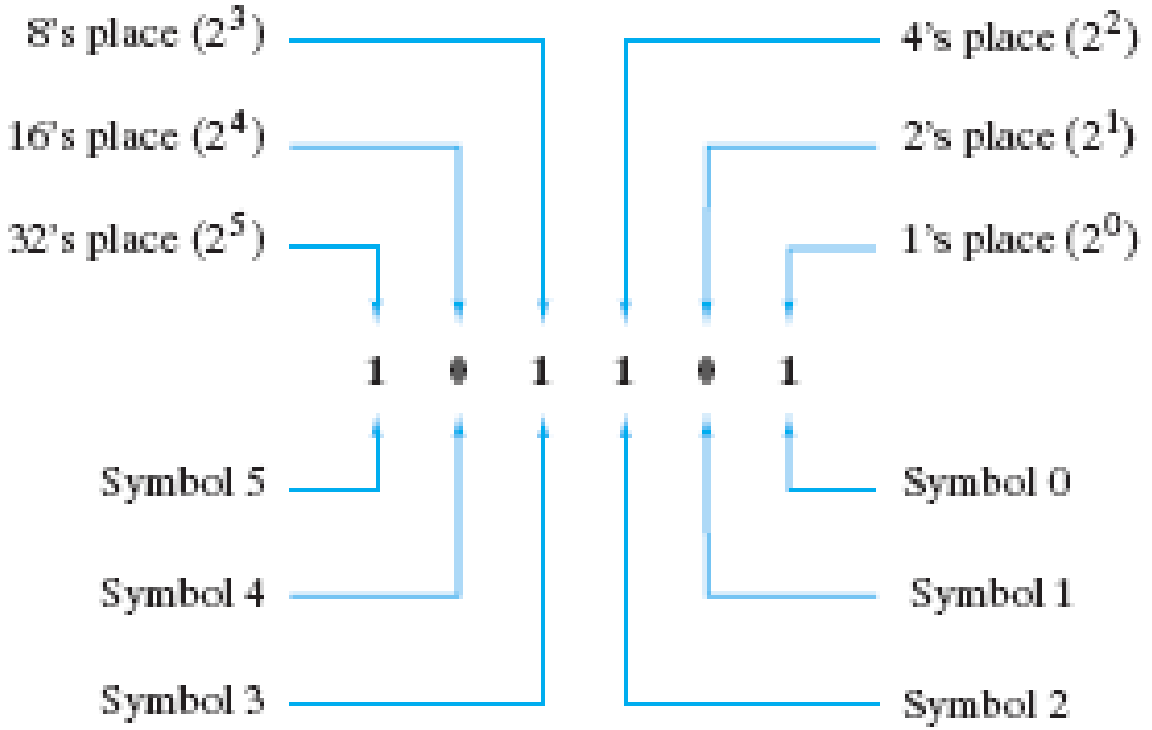
- We call the value on which the system is based (10 in the case of the decimal system) the **base** of the number system.

Binary Number System

- In the **binary** (base 2) number system, to represent integers we need only two symbols, 0 and 1.

❑For example, in base 2,

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



Binary Number System

- The binary number 101101_2 represents the number consisting of one 1, no 2's, one 4, one 8, no 16's, and one 32 (see previous Figure). This representation may be expressed

$$101101_2 = 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0$$

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

$$\begin{aligned} 101101_2 &= 1 \cdot 32 + 0 \cdot 16 + 1 \cdot 8 + 1 \cdot 4 + 0 \cdot 2 + 1 \cdot 1 \\ &= 32 + 8 + 4 + 1 = 45_{10}. \end{aligned}$$

Binary Number System

- Algorithm 6.2: **Converting an Integer from Base *b* to Decimal**

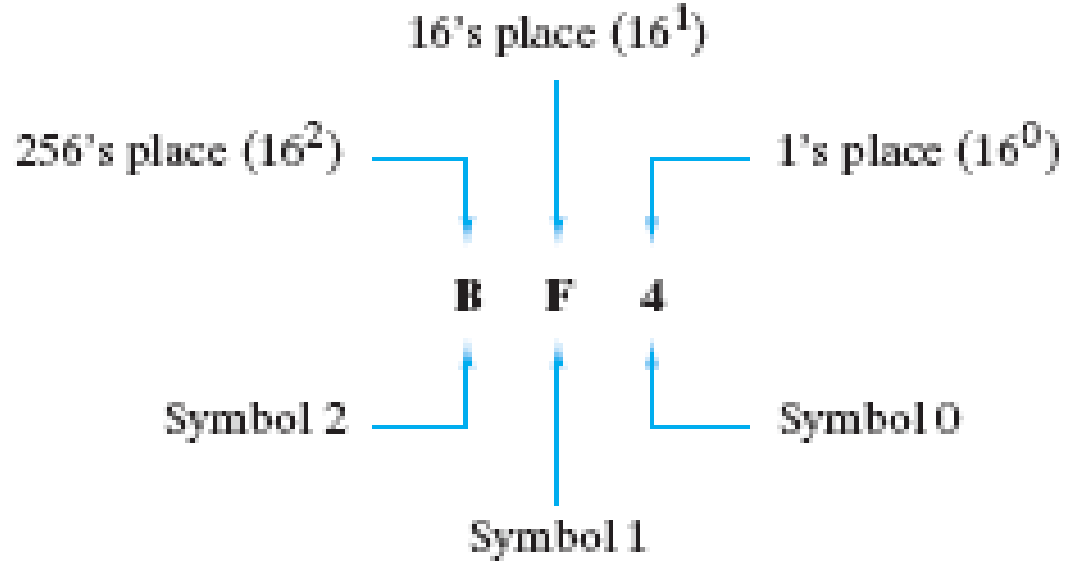
```
Input: c, n, b
Output: dec_val
base_b_to_dec (c, n, b) {
        dec_val = 0
        power = 1
        for i = 0 to n {
                dec_val = dec_val + c_i * power
                power = power * b
        }
        return dec_val
}
```

Hexadecimal Number System

- Other important bases for number systems in computer science are base 8 or **octal** and base 16 or **hexadecimal** (sometimes shortened to **hex**).
- We will discuss the hexadecimal system and leave the octal system for your exercises.
- 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.

❑For example, in base 16,

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



Hexadecimal Number System

- Convert the hexadecimal number B4F to decimal.

  We obtain

$$B4F_{16} = 11 \cdot 16^2 + 4 \cdot 16^1 + 15 \cdot 16^0$$
$$= 11 \cdot 256 + 4 \cdot 16 + 15 \cdot 1 = 2816 + 64 + 15 = 2895_{10}.$$

Converting Decimal to Binary

- Write the decimal number 130 in binary.

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

$2)\underline{130}$	remainder $= 0$	1's bit
$2)\underline{65}$	remainder $= 1$	2's bit
$2)\underline{32}$	remainder $= 0$	4's bit
$2)\underline{16}$	remainder $= 0$	8's bit
$2)\underline{8}$	remainder $= 0$	16's bit
$2)\underline{4}$	remainder $= 0$	32's bit
$2)\underline{2}$	remainder $= 0$	64's bit
$2)\underline{1}$	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

$$130_{10} = 10000010_2.$$

Converting Decimal to Hex

- Convert the decimal number 20385 to hexadecimal.

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

$16\overline{)20385}$	remainder = 1	1's place
$16\overline{)1274}$	remainder = 10	16's place
$16\overline{)79}$	remainder = 15	16^2's place
$16\overline{)4}$	remainder = 4	16^3's place
0		

We may stop when the quotient is 0. The first remainder gives the number of 1's, the second remainder gives the number of 16's, and so on; thus we obtain

$$20385_{10} = 4FA1_{16}.$$

Addition Operation in Binary

- Add the binary numbers 10011011 and 1011011.

  We write the problem as

$$\begin{array}{rr} & 10011011 \\ + & 1011011 \\ \hline \end{array}$$

  As in decimal addition, 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

$$\begin{array}{rr} & 1 \\ & 10011011 \\ + & 1011011 \\ \hline & 0 \end{array}$$

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

$$\begin{array}{rr} & 1 \\ & 10011011 \\ + & 1011011 \\ \hline & 10 \end{array}$$

  Continuing in this way, we obtain

$$\begin{array}{rr} & 10011011 \\ + & 1011011 \\ \hline & 11110110 \end{array}$$

Addition Operation in Hex

- Add the hexadecimal numbers 84F and 42EA.

  The problem may be written

```
  84F
+ 42EA
```

  We begin in the rightmost column by adding F and A. Since F is 15_{10} and A is 10_{10}, F + A = 15_{10} + 10_{10} = 25_{10} = 19_{16}. We write 9 and carry 1:

```
   1
  84F
+ 42EA
   9
```

  Next, we add 1, 4, and E, obtaining 13_{16}. We write 3 and carry 1:

```
   1
  84F
+ 42EA
  39
```

  Continuing in this way, we obtain

```
  84F
+ 42EA
 4B39
```

Euclidean Algorithm

- The **Euclidean algorithm** is an old, famous, and *efficient* algorithm for finding the greatest common divisor of two integers.
- Theorem 6.4:

  If a is a nonnegative integer, b is a positive integer, and r = a mod *b, then*

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

❑ Since 105 mod 30 = 15, by Theorem 6.4

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

Since 30 mod 15 = 0, by Theorem 6.4

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

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

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

Euclidean Algorithm

- Algorithm 6.3: **Euclidean Algorithm**

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

  Output: Greatest common divisor of *a* and *b*

```
1.  gcd(a, b) {
2.          if (a < b)
3.                  swap(a, b)
4.          while (b ¬=0) {
5.                  r = a mod b
6.                  a = b
7.                  b = r
8.          }
9.          return a
10. }
```

Euclidean Algorithm

- We show how Algorithm 6.3 finds gcd(504, 396).

  Let a = 504 and b = 396. Since $a > b$, we move to line 4. Since b = 0, we proceed to line 5, where we set r to

  $$a \bmod b = 504 \bmod 396 = 108.$$

  We then move to lines 6 and 7, where we set a to 396 and b to 108. We then return to line 4. Since $b \neq 0$, we proceed to line 5, where we set r to

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

  We then move to lines 6 and 7, where we set a to 108 and b to 72. We then return to line 4. Since $b \neq 0$, we proceed to line 5, where we set r to

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

  We then move to lines 6 and 7, where we set a to 72 and b to 36. We then return to line 4. Since $b \neq 0$, we proceed to line 5, where we set r to

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

  We then move to lines 6 and 7, where we set a to 36 and b to 0. We then return to line 4. This time b = 0, so we skip to line 9, where we return a (36), the greatest common divisor of 396 and 504.

Special Result

- Theorem 6.5:

  If a and b are nonnegative integers, not both zero, there exist integers s and t such that

$$\gcd(a, b) = sa + tb.$$

- Consider how the Euclidean algorithm computes gcd(273, 110). We begin with a = 273 and b = 110. The Euclidean algorithm first computes

$$r = 273 \, mod \, 110 = 53. \qquad \textbf{(6.1)}$$

It then sets a = 110 and b = 53. The Euclidean algorithm next computes

$$r = 110 \, mod \, 53 = 4. \qquad \textbf{(6.2)}$$

It then sets a = 53 and b = 4. The Euclidean algorithm next computes

$$r = 53 \, mod \, 4 = 1. \qquad \textbf{(6.3)}$$

It then sets a = 4 and b = 1. The Euclidean algorithm next computes

$$r = 4 \, mod \, 1 = 0.$$

Since r = 0, the algorithm terminates, having found the greatest common divisor of 273 and 110 to be 1.

Special Result

To find *s* and *t*, we work back, beginning with the last equation [equation (6.3)] in which $r \neq 0$. Equation (6.3) may be rewritten as

$$1 = 53 - 4 \cdot 13 \qquad \textbf{(6.4)}$$

since the quotient when 53 is divided by 4 is 13. Equation (6.2) may be rewritten as

$$4 = 110 - 53 \cdot 2.$$

We then substitute this formula for 4 into equation (6.4) to obtain

$$1 = 53 - 4 \cdot 13 = 53 - (110 - 53 \cdot 2)13 = 27 \cdot 53 - 13 \cdot 110. \textbf{(6.5)}$$

Equation (6.1) may be rewritten as

$$53 = 273 - 110 \cdot 2.$$

We then substitute this formula for 53 into equation (6.5) to obtain

$$1 = 27 \cdot 53 - 13 \cdot 110 = 27(273 - 110 \cdot 2) - 13 \cdot 110$$
$$= 27 \cdot 273 - 67 \cdot 110.$$

Thus, if we take $s = 27$ and $t = -67$, we obtain

$$\gcd(273, 110) = 1 = s \cdot 273 + t \cdot 110.$$

PRACTICE

PRACTICE 1

- In Exercises below, trace Algorithm 6.1 for the given input. Which of the integers are prime? Find the prime factorization of each integer!

1. $n = 9$
2. $n = 47$
3. $n = 209$
4. $n = 637$

PRACTICE 2

- Find the greatest common divisor and least common multiple of each pair of integers. Verify that $\gcd(m,n) \cdot lcm(m,n) = mn$.

1. 0, 17
2. 5, 25
3. 60, 90
4. 110, 273
5. 220, 1400

PRACTICE 3

- In Exercises below, express each binary number (1-3), hex number (4-6), and octal number (7-8) in decimal.

1. 1001
2. 11011
3. 11011011
4. 3A
5. 1E9
6. 3E7C
7. 63
8. 7643

PRACTICE 4

- In Exercises below, add the binary numbers (1-3) and hex numbers (4-6).

1. 1001 + 1111
2. 11011 + 1101
3. 110110 + 101101
4. 4A + B4
5. 195 + 76E
6. 49F7 + C66

PRACTICE 5

- Use the Euclidean algorithm to find the greatest common divisor of each pair of integers below. For each number pair a, b, find integers s and t such that $sa + tb = \gcd(a, b)$.

1. 60, 90
2. 110, 273
3. 220, 1400

NEXT WEEK'S OUTLINE

- Counting Method Principle
- Permutation and Combination

REFERENCES

- Johnsonbaugh, R., 2005, *Discrete Mathematics*, New Jersey: Pearson Education, Inc.
- Rosen, Kenneth H., 2005, *Discrete Mathematics and Its Applications*, 6th edition, McGraw-Hill.
- Hansun, S., 2021, *Matematika Diskret Teknik*, Deepublish.
- Lipschutz, Seymour, Lipson, Marc Lars, *Schaum's Outline of Theory and Problems of Discrete Mathematics*, McGraw-Hill.
- Liu, C.L., 1995, *Dasar-Dasar Matematika Diskret*, Jakarta: Gramedia Pustaka Utama.
- Other offline and online resources.

Visi

Menjadi Program Studi Strata Satu Informatika **unggulan** yang menghasilkan lulusan **berwawasan internasional** yang **kompeten** di bidang Ilmu Komputer (*Computer Science*), **berjiwa wirausaha** dan **berbudi pekerti luhur**.

INFORMATIKA
UMN
UNIVERSITAS MULTIMEDIA NUSANTARA

Misi

1. Menyelenggarakan pembelajaran dengan teknologi dan kurikulum terbaik serta didukung tenaga pengajar profesional.
2. Melaksanakan kegiatan penelitian di bidang Informatika untuk memajukan ilmu dan teknologi Informatika.
3. Melaksanakan kegiatan pengabdian kepada masyarakat berbasis ilmu dan teknologi Informatika dalam rangka mengamalkan ilmu dan teknologi Informatika.