Chapter 3: Number Theory and Algorithm

Learning Objectives

After studying this topic, you should be able to:

1. Describe the concept of divisibility and modular arithmetic.
2. Explain about the primes of integers and prime factorization.
3. Find the greatest common divisors (gcd) and least common multiples (lcm).
4. Apply Euclidean Algorithm in finding gcd.
5. Express number theory in pseudocode and flowchart.

$\frac{b}{a} \Rightarrow a/b \Rightarrow a$ divides b

$4 \div 2 = \frac{4}{2} \rightarrow 2 = 2$ divides 4 (integer)

3.1 Divisibility and Modular Arithmetic

Divisibility

> 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 b is a multiple of a.
- The notation $a \mid b$ denotes a divides b.
- When an integer is divided by a positive integer, there is a quotient and a remainder, and this is can be called as **division algorithm**.

> Let a be an integer and d a positive integer, Then there are unique integers q and r, with $0 \leq r \leq d$, such that $a = dq + r$ (dividend, divisor, quotient, remainder)

- 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.
- The notation is used to express the quotient and remainder:

$$q = a \textbf{ div } d \text{ [a/d]}, \qquad r = a \textbf{ mod } d \text{ (a – d)}$$

$0 \leq r < d$

Example:

Given that 101 is divided by 11. Determine the quotient and remainder.

$11 \overline{)101}$ quotient $= 9$, -99, remainder $= 2$

$0 \leq 2 < d$

$101 = 11 \cdot 9 + 2$ (division algorithm)

$\therefore$ quotient $= q = 101$ div 11

remainder $= 2 = 101$ mod 11

Example:

-11 is divided by 3.

Wrong:

$$3\overline{)-11}\quad -3$$
$$-(-9)$$
$$-2$$

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

* remainder cannot be negative, does not satisfy $0 \le r \le 3$ (d)

Ans:

$$3\overline{)-11}\quad -4$$
$$-(-12)$$
$$1$$

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

$\therefore$ quotient $= -4 = -11 \text{ div } 3$

remainder $= 1 = -11 \bmod 3$

Example:

$$
\begin{array}{r}
-5 \\
5\overline{)-24} \\
-(-25) \\
\hline
1
\end{array}
$$

$$-24 = 5(-5) + 1$$

Modular Arithmetic

- If a and b are integers and m is a positive integer, then a is congruent to b modulo m if m divides $a - b$.
- The notation used is $a \equiv b(\text{mod})m$ to indicate that a is congruent to b modulo m.
- So $a \equiv b(\text{mod})m = m \mid (a-b)$

Example:

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

1. $6\overline{)17}\ 2$, -12, 5; $6\overline{)5}\ 0$, 5. $17 - 5 = 12$; $6 \mid 12 \checkmark$. $\therefore$ 17 is congruent to 5 modulo 6 $= 6 \mid (17-5)$ $\therefore 17 \equiv 5 \pmod 6$

2. $6\overline{)24}\ 4$, -24, 0; $6\overline{)14}\ 2$, -12, 2. $24 - 14 = 10$; $6 \mid 10 = 6\overline{)10}\ 1$, 6, 4. $\therefore$ 24 − 14 = 10 is not divisible by 6, hence 24 is not congruent to 14 modulo 6. $\therefore 24 \not\equiv 14 \pmod 6$

3.2 Primes

- A prime is an integer greater than 1 that is not divisible by positive integers other than 1 and itself
- An integer p is greater than 1 is called prime if the only positive factors of p are 1 and p.
-

Prime factorization

- Every integer greater than 1 can be written uniquely as a prime or as the product of two/more primes where the prime factors are written in order of non-decreasing size.

Example:

State prime factorization of 100, 641, 999 and 1024.

method of repeated division

$2\overline{)100}\ 50$, $2\overline{)50}\ 25$, $5\overline{)25}\ 5$, $5\overline{)5}\ 1$

$100 = 2 \times 2 \times 5 \times 5$ ← prime factorization

3.3 Greatest Common Divisor

- The largest integer that divides both of two integers is called the greatest common divisor of these integers.
- Let a and b be integers, not both zero. The largest integers 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 $gcd(a, b)$.
- One way to find the greatest common divisor of two integers is to find all the positive common divisors of both integers and then take the largest divisor.

Examples:

1. What is the greatest common divisor of 24 and 36?
2. What is the greatest common divisor of 17 and 22?

- Another way to find the greatest common divisor of two positive integers is to use the prime factorization of these integers.

Example:

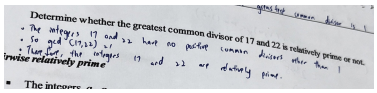
Given that the prime factorization of 120 and 500 = $2^3 \cdot 3 \cdot 5$ and 500 = $2^2 \cdot 5^3$. Find the greatest common divisor.

Relatively prime

- The integers a and b are relatively prime if their greatest common divider is 1.

Example:

Determine whether the greatest common divisor of 17 and 22 is relatively prime or not.



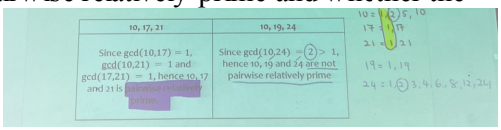
Pairwise relatively prime

- The integers $a_1, a_2, ..., a_n$ are pairwise relatively prime if $\gcd(a_i, a_j) = 1$ whenever $1 \le i \le j \le n$.

when the integer > 2

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.



3.4 Least Common multiple (Lcm)

- Prime factorizations can also be used to find the least common multiple of two integers.
- 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 $lcm(a, b)$.

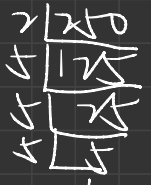
Example:

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

Example:

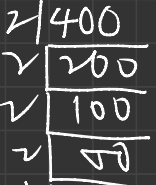
Given two integers 250 and 400.

a) Find the prime factorization for both integers



$250 = 2 \times 5 \times 5 \times 5$

$250 = 2 \cdot 5^3$



$400 = 2 \times 2 \times 2 \times 2 \times 5 \times 5$

$400 = 2^4 \cdot 5^2$

b) Hence, determine the greatest common divisor for the integers.

$$\text{Gcd}(250, 400) = 2^{\min(1,4)} 5^{\min(3,2)}$$
$$= 2^1 \cdot 5^2$$
$$= 50$$

3.5 The Euclidean Algorithm

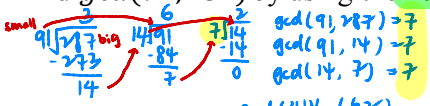
- A technique for quickly finding the GCD of two integers.
- The Euclidean Algorithm for finding $gcd(a,b)$ is as follows:

$gcd(0,2) = 2$
$gcd(4,0) = 4$

1. If $A = 0$, then $gcd(A,B) = B$. Since the $gcd(0,B) = B$, and we can stop.
2. If $B = 0$, then $gcd(A,B) = A$. Since the $gcd(A,0) = A$, and we can stop.
3. Write A in quotient remainder form $(A = B \cdot Q + R)$ ← division algorithm
4. Find $gcd(B,R)$ using the Euclidean Algorithm since $gcd(A,B) = gcd(B,R)$.
5. The algorithm stops when we find remainder 0.

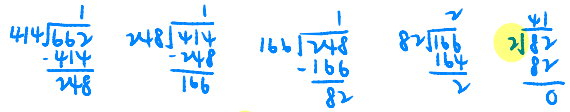
Example:

1. Find $gcd(91,287)$ by using the Euclidean Algorithm.



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

gcd(414, 662)



$\therefore gcd(414, 662) = 2$

3.6 Pseudocode and Flowchart

Pseudocode

- Pseudocode specifies the steps required to accomplish the task.
- It is a type of structured English that is use to specify an algorithm.

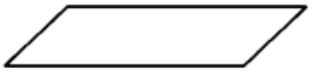
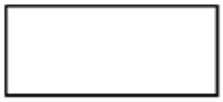
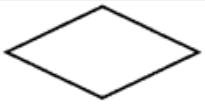
Example:

Write the pseudocode for finding average of any three numbers.

Step 1 Start
Step 2 Read values of X, Y, Z
Step 3 sum S = X+Y+Z
Step 4 average A = S/3
Step 5 Write value of A → output/result
Step 6 Stop

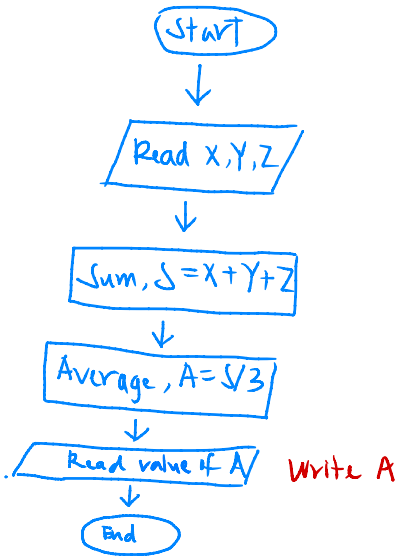
Flowchart

- Flowchart are used to illustrate algorithms in order to aid in the visualisation of a program.
- Flowcharts are used to be read top to bottom and left to right in order to follow an algorithms logic from start to finish.
- Symbols are used in flowchart.

Name	Symbol	Function
Start/End		Used to markup the starting and ending point
Arrows		Used for connection
Input/Output		Used for input and output information
Process		Used to represent single step
Decision		Used for branching or decision making

Example:

Construct the flowchart for finding average of any three numbers.



Tutorial Questions.

1. What are the quotient and remainder when

   a) 19 is divided by 7?
   b) -111 is divided by 11?
   c) 789 is divided by 23?
   d) 1001 is divided by 13?
   e) 0 is divided by19?
   f) 3 is divided by 5?
   g) -1 is divided by 3?
   h) 4 is divided by 1?

2. Find a div m and a mod m when

   a) a = 228, m = 119
   b) a = 9009, m = 223
   c) a = -10101, m = 333
   d) a = -765432, m = 38271

3. Decide whether each of these integers is congruent to 3 modulo 7.

   a) 80
   b) 103
   c) -29
   d) -122

4. Find the prime factorization of each of these integers.

   a) 88
   b) 126
   c) 729
   d) 1001
   e) 1111
   f) 909090

5. Find the prime factorization of 10!.

6. Which positive integers less than 30 are relatively prime to 30?

7. Determine whether the integers in each of these sets are pairwise relatively prime.

   a) 11, 15, 19
   b) 14, 15, 21
   c) 12, 17, 31, 37
   d) 7, 8, 9, 11

8. What are the greatest common divisor and least common multiple of these pairs of integers?

   a) $2^2 \cdot 3^3 \cdot 5^5, 2^5 \cdot 3^3 \cdot 5^2$
   b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$
   c) $17, 17^{17}$
   d) $2^2 \cdot 7, 5^3 \cdot 13$
   e) $0, 5$
   f) $2 \cdot 3 \cdot 5 \cdot 7, 2 \cdot 3 \cdot 5 \cdot 7$

9. Use the Euclidean algorithm to find

a) $gcd(12,18)$
b) $gcd(111,201)$
c) $gcd(1001,1331)$
d) $gcd(12345,54321)$
e) $gcd(1000,5040)$
f) $gcd(9888,6060)$

10. Construct the algorithm by using pseudocode and flowcharts for each question.

a) Finding average of five numbers.
b) Finding the maximum element in a finite sequence.
c) Finding the sum of three integers.
d) Area of circle (πr^2)

1. b)
$$\begin{array}{r} -11 \\ 11\overline{)-111} \\ -(-121) \\ \hline 10 \end{array}$$

$-111 = 11(-11) + 10$

∴ quotient $= -11 = -111$ div 11
remainder $= 10 = -111$ mod 11

d)
$$\begin{array}{r} 77 \\ 13\overline{)1001} \\ 1001 \\ \hline 0 \end{array}$$

$1001 = 13(77)$

∴ quotient $= 77 = 1001$ div 13
remainder $= 77 = 1001$ mod 13

3. a)
$$\begin{array}{r} 11 \\ 7\overline{)80} \\ 77 \\ \hline 3 \end{array}$$

$$\begin{array}{r} 0 \\ 7\overline{)3} \\ 0 \\ \hline 3 \end{array}$$

> 80 is congruent to 3 modulo 7 = 7|(80-3)
∴ $80 \equiv 3 \pmod 7$

b)
$$\begin{array}{r} 14 \\ 7\overline{)103} \\ 98 \\ \hline 5 \end{array}$$

$$\begin{array}{r} 0 \\ 7\overline{)3} \\ 0 \\ \hline 3 \end{array}$$

$103 - 3 = 100$

$$\begin{array}{r} 14 \\ 7\overline{)100} \\ 98 \\ \hline 2 \end{array}$$

> $103 - 3 = 100$ is not divisible by 7, hence 103 is not congruent to 3 modulo 7
∴ $103 \not\equiv 3 \pmod 7$

4. b)

2	126
3	63
3	21
7	7
	1

$\therefore 126 = 2 \times 3 \times 3 \times 7$

c)

3	729
3	243
3	81
3	27
3	9
3	3
	1

$\therefore 729 = 3 \times 3 \times 3 \times 3 \times 3 \times 3$

8. a) $Gcd = 2^{\min(2,5)} 3^{\min(3,3)} 5^{\min(5,2)}$

$= 2^2 3^3 5^2$

$= 2700$

$Lcm = 2^{\max(2,5)} 3^{\max(3,3)} 5^{\max(5,2)}$

$= 2^5 3^3 5^5$

$= 2700000$

b) $Gcd = 2^{\min(1,11)} 3^{\min(1,9)} 5^{\min(1,0)} 7^{\min(1,0)} 11^{\min(1,1)} 13^{\min(1,0)} 17^{\min(0,14)}$

$= 2^1 3^1 5^0 7^0 11^1 13^0 17^0$

$= 66$

$Lcm = 2^{\max(1,11)} 3^{\max(1,9)} 5^{\max(1,0)} 7^{\max(1,0)} 11^{\max(1,1)} 13^{\max(1,0)} 17^{\max(0,14)}$

$= 2^{11} 3^9 5^1 7^1 11^1 13^1 17^{14}$

9. e) gcd(1000, 5040)

$1000 \overline{)5040}$ 5, 5000, 40

$40 \overline{)1000}$ 25, 1000, 0

$\therefore gcd(1000, 5040) = 40$

f)

$6060 \overline{)9888}$ 1, 6060, 3828

$3828 \overline{)6060}$ 1, 3828, 2232

$2232 \overline{)3828}$ 1, 2232, 1596

$1596 \overline{)2232}$ 1, 1596, 636

$$
\begin{array}{r|l}
 & 2 \\
636 & 1596 \\
 & 1272 \\
\hline
 & 324
\end{array}
\qquad
\begin{array}{r|l}
 & 1 \\
324 & 636 \\
 & 324 \\
\hline
 & 312
\end{array}
\qquad
\begin{array}{r|l}
 & 1 \\
312 & 324 \\
 & 312 \\
\hline
 & 12
\end{array}
\qquad
\begin{array}{r|l}
 & 26 \\
12 & 312 \\
 & 312 \\
\hline
 & 0
\end{array}
$$

$\therefore \gcd(9888, 6060) = 12$