MATH221
Mathematics for Computer Science

Unit 8
Elementary Number Theory

OBJECTIVES

- Understand the definition of divisibility.
- Understand apply the Quotient-Remainder Theorem.
- Understand and be able to find the Greatest Common Divisor.
- Understand and apply the Euclidean Algorithm.
- Understand the concept of the Fundamental Theorem of Arithmetic.

Divisibility

If n and d are integers and $d \neq 0$, then *n is divisible by d* if and only if

$$n = d \times k \quad \text{for some } k \in \mathbb{Z}.$$

We write ***$d \mid n$*** and say that ***d divides n (n is divisible by d)***.

In logic notation, the definition of divisibility is written

$$d \mid n \Leftrightarrow \quad \exists k \in \mathbb{Z},\ n = dk.$$

Divisibility

Alternatively, if

$$d \mid n \Leftrightarrow \quad \exists k \in \mathbb{Z},\ n = dk.$$

We say that

n is a multiple of d, or
d is a factor of n, or
d is a divisor of n, or
d divides n.

Discussion:

1. Is -16 a divisor of 32?
   Yes.
   $32 = -16 \times -2$.

2. If $l \in \mathbb{Z}$ and $l \neq 0$, does $l \mid 0$?
   Yes.
   $0 = l \times k$ for some $k \in \mathbb{Z}$.

Discussion:

3. Find all values of $a \in \mathbb{Z}$ such that $a \mid 1$.

   $a \mid 1 \Leftrightarrow \exists k \in \mathbb{Z}, 1 = ak$.
   For $a = 1$ and $k = 1$, $ak = 1$.
   For $a = -1$ and $k = -1$, $ak = 1$.
   Therefore, $a = -1$ or 1.

Discussion:

4. What is the relationship between a and b if $a \mid b$, and $b \mid a$, $a, b \in \mathbb{Z}$?
   Now, $a \mid b \Leftrightarrow \exists k \in \mathbb{Z}, b = ak$ (1)
   $b \mid a \Leftrightarrow \exists l \in \mathbb{Z}, a = bl$ (2)
   Substitute (2) into (1),
   $b = (bl)k$
   Divide both sides by b,
   $1 = lk$
   Since $l, k \in \mathbb{Z}$, $\Rightarrow$ $l = k = 1$. or $l = k = -1$.
   Hence, $a = \pm b$.

Discussion:

5. If $a, b \in \mathbb{Z}$, is $3a + 3b$ divisible by 3?

   Now, $3a + 3b = 3(a + b)$
   $= 3s$
   where $s = a + b$ and $s \in \mathbb{Z}$.
   Hence, $3 \mid 3a + 3b$, that is, $3a + 3b$ is divisible by 3.

Discussion:

6. If $a, b, c, x, y \in \mathbb{Z}$. If $b \mid a$ and $b \mid c$, does $b \mid (ax + cy)$? Why?

Now, $b \mid a \Leftrightarrow \exists k \in \mathbb{Z}, a = bk$ (1)

$b \mid c \Leftrightarrow \exists l \in \mathbb{Z}, c = bl$ (2)

(1) $\times x$, $ax = bkx$ (3)

(2) $\times y$, $cy = bly$ (4)

(3) + (4), $ax + cy = bkx + bly$

$= b(kx + ly)$

$= bm$ where $m = kx + ly$, $m \in \mathbb{Z}$.

Hence, $b \mid (ax + cy)$.

Discussion:

7. If $a, b \in \mathbb{N}$, is it true that $a \mid b$ implies $a \leq b$?

Now, $a \mid b \Rightarrow \exists k \in \mathbb{Z}, b = ak$.

Since $a, b \geq 1$, so $k \geq 1$.

Multiply both sides of the inequality by a,

$ka \geq 1a$.

Hence, $b \geq a$.

That is, $a \leq b$

Therefore, if $a, b \in \mathbb{N}$, it is true that $a \mid b$ implies $a \leq b$.

Theorem - Transitivity of Divisibility

For all integers a, b and c, if $a \mid b$ and $b \mid c$, then $a \mid c$.

Note: After going through the details of the proof for this theorem, for the remaining theorems, lemma, etc., we shall focus on the application. For their proofs, please refer to the supplementary notes.

Transitivity of Divisibility: Proof

We know that

$a \mid b \Rightarrow \exists k \in \mathbb{Z}, b = ak$ (1)

$b \mid c \Rightarrow \exists l \in \mathbb{Z}, c = bl$ (2)

Show that $a \mid c$, that is, find $m \in \mathbb{Z}$ such that $c = ma$.

Now, $c = bl$ by (2)

$= (ak)l$ by (1)

$= (kl)a$ by associativity and commutativity

Let $m = kl$, then $m \in \mathbb{Z}$ (since $\times$ is a closed operation on $\mathbb{Z}$).
Therefore, $c = ma$ and so $a \mid c$.

Theorem - Divisible by a Prime

Theorem:
Every integer $n \geq 2$ is divisible by some prime number.

Theorem – Infinite Primes

Theorem:
There are infinitely many primes.

The Quotient-Remainder Theorem

If $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, then there exist unique integers q and r such that

$$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$

The theorem says that when we divide any integer n by any positive integer d, there will be a **unique quotient *q*** and **remainder *r*** satisfying $0 \leq r < d$.

The Quotient-Remainder Theorem: Note

Note that the theorem makes two assertions:

1. Existence: There exists $q, r \in \mathbb{Z}$ such that
   $$n = dq + r \quad \text{and} \quad 0 \leq r < d.$$
2. Uniqueness: There is only one pair of values of q and r with these properties.

The Quotient-Remainder Theorem: Note

The Quotient-Remainder Theorem says that when we divide any integer n by any positive integer d, there will be a quotient q and a remainder r, where $0 \leq r < d$.

Example.

Let $n = 11$, $d = 4$.

Then we have $11 = 4 \times 2 + 3$;

That is, $q = 2$ and $r = 3$.

Exercise:

Find values for $q, r \in \mathbb{Z}$ such that $n = d \times q + r$, $0 \leq r < d$, for the following.

(i) $n = 54$, $d = 4$

For positive n, a positive quotient q is multiplied to the divisor d to obtain a number slightly smaller than n.

Then the nonnegative integer r is then added to the product $(d \times q)$ to make it equal to n.

That is,

$$54 = 4 \times 13 + 2.$$

Hence, $q = 13$, $r = 2$.

Exercise:

(ii) $n = -54$, $d = 4$

For negative n, a negative quotient q is multiplied to the divisor d to obtain a number slightly smaller than n (ie. more negative than n).

Then the nonnegative integer r is then added to the product $(d \times q)$ to make it equal to n.

That is,

$$-54 = 4 \times -14 + 2.$$

Hence, $q = -14$, $r = 2$.

Exercise:

(iii) $n = 54$, $d = 70$

Now, $54 = 70 \times 0 + 54$.

Hence, $q = 0$, $r = 54$.

Can you find a second set of q and r ($r < d$)?

No. The Quotient-Remainder Theorem says that q and r are unique, that is, there is only one solution for q and r in the previous exercise.

Theorem – Classification of Integer

Theorem:
Every Integer is either Odd or Even.

Greatest Common Divisor

Let $a, b \in \mathbb{Z}$ with $a \neq 0$ or $b \neq 0$. A natural number c is said to be the greatest common divisor (gcd) of a and b if and only if

(i) $c \mid a$ and $c \mid b$; and

(ii) if $d \mid a$ and $d \mid b$ for some $d \in \mathbb{N}$, then $d \mid c$.

We write $\gcd(a, b) = c$.

Exercise:

1. Evaluate gcd(18, 12), gcd(18, -12), gcd(-18, 12) and gcd(-18, -12).
   Common divisors: -6, -3, -2, -1, 1, 2, 3, 6
   For all the above the greatest common divisor is 6.

2. What can you say about gcd(a, b); gcd (a, $-b$); gcd($-a$, b); gcd($-a$, $-b$)?
   All have the same value.

3. Evaluate gcd(7, 11).
   1.

Exercise:

4. For $a, b \in \mathbb{Z}$ where not both are zero, does gcd(a, b) always exist? Is it unique?
   Yes, it will always exist.
   Yes.
   For example, gcd(4, 0) = 4 and gcd(0, -3) = 3.

5. gcd(0, 0) is not allowed. Why? What would it be if it were found in the same way as for other pairs of numbers?
   Every integer divides 0 and there is no largest integer.
   So there is no largest common divisor. Hence, the definition of GCD excludes this case.

Exercise:

6. Evaluate gcd(2772, 2310).

   Use the Euclidean Algorithm that we will learn later in this unit.

Lemmas

Lemma 1:

If r is a positive integer, then $\gcd(r, 0) = r$.

Lemma 2:

If $a, b \in \mathbb{Z}$ with $b \geq 1$, and if q and r are integers such that $a = b \times q + r$, then

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

The Euclidean Algorithm

The Euclidean Algorithm is a process for finding the greatest common divisor between two integers.

It is described as follows:

1. Let A and B be integers with $A > B \geq 0$.
2. If $B = 0$, then $\gcd(A, B) = A$.

   If $B > 0$, then the quotient-remainder theorem can be used to divide A by B to obtain a quotient q and a remainder r:

   $$A = Bq + r \quad \text{where } 0 \leq r < B.$$

   Hence, $\gcd(A, B) = \gcd(B, r)$.
3. Repeat the process starting at (2), but use B instead of A and r instead of B.

   The repetitions are guaranteed to terminate eventually with $r = 0$.

The Euclidean Algorithm: Example

Evaluate gcd(2772, 2310).

Step 1: Divide 2772 by 2310:

$$2772 = 2310 \times 1 + 462$$

$$\gcd(2772, 2310) = \gcd(2310, 462)$$

Step 2: Divide 2310 by 462:

$$2310 = 462 \times 5 + 0$$

$$\gcd(2310, 462) = \gcd(462, 0)$$

Since gcd(462, 0) = 462, hence, gcd(2772, 2310) = 462.

Note for Answering QUIZ Questions: Expressing Steps in Applying Euclidean Algorithm

In using Euclidean Algorithm to find gcd(x, y), we will express gcd(x, y) = gcd(x_1, y_1) = gcd(x_2, y_2) =….=gcd(x_n, 0), what is the value of n for gcd(2772, 2310)?

Evaluate gcd(2772, 2310).

Step 1: Divide 2772 by 2310:

$2772 = 2310 \times 1 + 462$

gcd(2772, 2310) = gcd(2310, 462)

Step 2: Divide 2310 by 462:

$2310 = 462 \times 5 + 0$

gcd(2310, 462) = gcd(462, 0)

Since gcd(462, 0) = 462, hence, gcd(2772, 2310) = 462

Hence, gcd(2772, 2310) = gcd(2310, 462) = gcd(462, 0).

In this calculation, x_1 = 2310, y_1 =462; x_2 = 462, y_2 = 0

Hence, n =2

Relatively Prime

If $a, b \in \mathbb{Z}$ and gcd(a, b) = 1, then a and b are ***relatively prime***.

Example:

Since gcd(17, 9) = 1.

Hence, we say that 17 and 9 are *relatively prime*.

Theorem on Linear Combination of gcd

If $a, b \in \mathbb{Z}$ and not both equal zero, then gcd(a, b) exists and there exist $m, n \in \mathbb{Z}$ such that gcd(a, b) = $ma + nb$.

Theorem on Linear Combination of gcd: Notes

1. The theorem says two things.
   (i) gcd(a, b) always exists as long as both a and b are not both zero; and
   (ii) gcd(a, b) can be written as a *linear combination* of a and b.

2. The proof to this theorem is similar to that of the Quotient-Remainder Theorem. The proof is not examinable.

How to find Linear Combination of gcd?

1. Use Euclidean Algorithm to find the gcd step-by-step and write down the expression resulted from applying quotient-remainder theorem in each step.

2. Work backwards systematically as shown in the next slide to get the linear combination of gcd.

Find Linear Combination of gcd: Example

Finding linear combination of gcd for 7854 and 2772.

Using Euclidean Algo, we compute gcd(7854, 2772) as follows:

$7854 = 2772 \times 2 + 2310$ ------- (1)

$2772 = 2310 \times 1 + 462$ -------(2)

$2310 = 462 \times 5 + 0$

Hence, gcd(7854, 2772) = gcd(462, 0) = 462

(1) $\Rightarrow$ $2310 = 7854 - 2772 \times 2$ --------(3)

(2) $\Rightarrow$ $462 = 2772 - 2310 \times 1$ --------(4)

Work backwards from (4), we get:

$462 = 2772 - 2310 \times 1$ (from (4))

$= 2772 - (7854 - 2772 \times 2) \times 1$ (from (3))

$= (-1) \times 7854 + 3 \times 2772$

Hence, the linear combination of gcd for 7854 and 2772 is:

$462 = (-1) \times 7854 + 3 \times 2772$

Corollaries

Corollary 1:

If a, b are relatively prime, then $\exists m, n \in \mathbb{Z}$ such that

$$1 = ma + nb.$$

Corollary 2:

Let $a, b, c \in \mathbb{Z}$.

If gcd(a, b) = 1 and $a \mid bc$, then $a \mid c$.

Euclid's Lemma

Let p be a prime and $a, b \in$ N. *If* $p \mid ab$, then p | a or p | b.

Exercise:

1. Write the following numbers in terms of their prime factors.

   32
   $= 16 \times 2$
   $= 8 \times 2 \times 2$
   $= 4 \times 2 \times 2 \times 2$
   $= 2 \times 2 \times 2 \times 2 \times 2$

Exercise:

2. Write the following numbers in terms of their prime factors.

   924
   $= 462 \times 2$
   $= 231 \times 2 \times 2$
   $= 77 \times 3 \times 2 \times 2$
   $= 11 \times 7 \times 3 \times 2 \times 2$

Exercise:

3. Are these factorization unique? How do you know?

   Yes.

   The Fundamental Theorem of Arithmetic states that each integer **greater than 1** can be decomposed into prime factors – and this decomposition is the **only one**.

4. Can you express EVERY natural number as a product of primes?

   No, since 1 is not prime.

The Fundamental Theorem of Arithmetic

If $a \in \mathbb{Z}$ and $a > 1$, then a can be factorized in a *unique way* in the form

$$a = p_1^{\alpha^1} \; p_2^{\alpha^2} \ldots\ldots\ldots p_k^{\alpha^k}$$

where $p_1, p_2, \ldots, p_k$, are prime numbers and $\alpha_i \in \mathbb{N}$ for each $i = 1, 2, \ldots, k$.

Example:

$924 = 11 \times 7 \times 3 \times 2 \times 2 = 11 \times 7 \times 3 \times 2^2$

Finding Prime Numbers

The easiest method to find prime numbers up to *n* is to use the *Sieve of Eratosthenes algorithm*.

Sieve of Eratosthenes Algorithm

The *Sieve of Eratosthenes* is a method of finding primes up to *n* as follows:

(i) Write down all integers from 1 to *n*.

(ii) Delete all multiples (not the number) of primes up to $(\sqrt{n}+1)$, that is, all multiples of 2, 3, 5, 7, …

(iii) The remaining values are the primes numbers up to *n*.

Exercise: Find all primes between 1 and 100.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Least Common Multiples

Let a, b ∈ Z be two nonzero integers. The **least common multiple** of a and b, denoted lcm(a, b), is the positive number c with the properties:

(1) c is a common multiple of a and b; that is, a | c and b | c .

(2) If d is a common multiple of a and b, then c ≤ d .

Examples: lcm(18, 12) = 36

lcm(18, 15) = 90

Least Common Multiples

We can use prime factorisations to calculate the lcm. Suppose

$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$

Then

$\text{lcm}(a, b) = a = p_1^{\gamma_1} p_2^{\gamma_2} \ldots p_k^{\gamma_k}$ *where*

where $\gamma_i = \alpha_i$, *if* $\alpha_i \geq \beta_i$

$\gamma_i = \beta_i$, *otherwise*

Calculating Least Common Multiples: Examples

Given that $3220 = 2^2 \times 5 \times 7 \times 23$ and $1155 = 3 \times 5 \times 7 \times 11$, we have

$\text{lcm}(3220, 1155) = 2^2 \times 3 \times 5 \times 7 \times 11 \times 23$

Given that $35100 = 2^2 \times 3^3 \times 5^2 \times 13$ and $6975 = 3^2 \times 5^2 \times 31$, we have

$\text{lcm}(35100, 6975) = 2^2 \times 3^3 \times 5^2 \times 13 \times 31$

End of Unit 8