DISCRETE MATHEMATICS AND APPLICATIONS

Number Theory 1

Intan Sabariah Sabri (intansabariah@ump.edu.my)
Siti Zanariah Satari (zanariah@ump.edu.my)
Adam Shariff Adli Aminuddin (adamshariff@ump.edu.my)

Faculty of Industrial Sciences & Technology

Chapter Description

- Chapter outline

  1.1 Factorability

  1.2 Primes

  1.3 The Division Algorithm

- Aims
  - Able to determine the divisibility of integers
  - Able to determine the prime factorization of an integer
  - Able to find the quotient and remainder from a division of integers

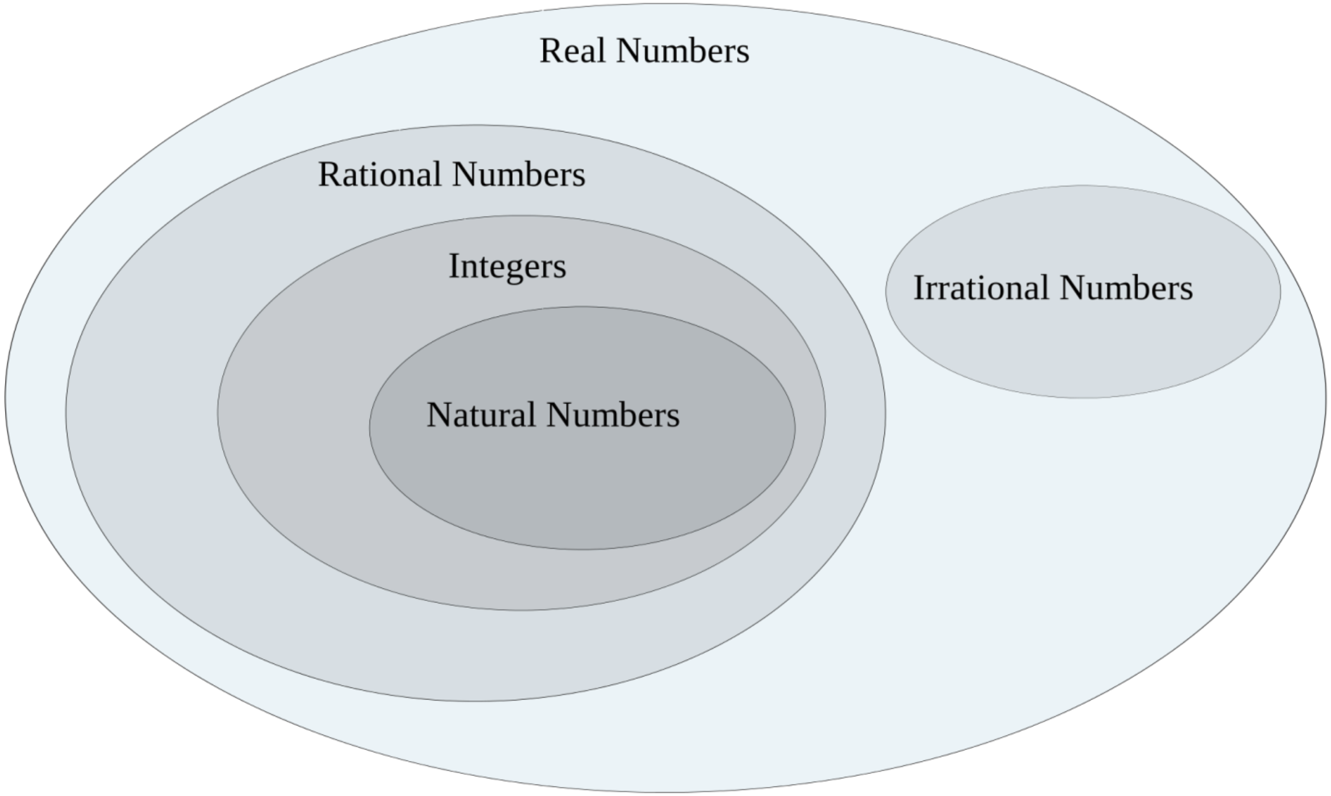
References

- Rosen K.H., Discrete Mathematics & Its Applications, (Seventh Edition), McGraw-Hill, 2011
- Epp S.S, Discrete Mathematics with Applications, (Fourth Edition), Thomson Learning, 2011
- Ram Rabu, Discrete Mathematics, Pearson, 2012
- Walls W.D., A beginner's guide to Discrete Mathematics, Springer, 2013
- Chandrasekaren, N. & Umaparvathi, M., Discrete Mathematics, PHI Learning Private Limited, Delhi, 2015

Introduction

- Number theory is a field of mathematics which focuses on integer properties, characteristics and its applications.
- It is fundamental importance for computer science students to improve the basic understanding of numbers properties
- Some of interesting applications includes
  - Cryptography (Encryption and decryption)
  - Random number generation
  - Arithmetic operations in software development

Number System



Number System (True or False)

1. An integer is also a rational number.

True. Since any integer can be formatted as a fraction by putting it over 1.

2. A rational number is also an integer.

False. The integer 4 is also rational number. But for the rational number 3/4 is not an integer.

3. A number is either a rational number or an irrational number, but not both.

True. In decimal form, a number is either non-terminating and non-repeating (so it's an irrational) or else it's not (so it's a rational); there is no overlap between these two number types.

Divisibility of Integers (i)

If an integer is divided by another integer (except 0), the quotient produced maybe an integer or not integer

$$\frac{10}{2} = 5$$

5 is integer

$$\frac{10}{4} = 2.5$$

2.5 is not integer

Extra: Do you ever wonder why an integer can't be divided by 0?

Divisibility of Integers (ii)

Definition 1.1 : Divisibility

- Let *a*, *b* and *c* be integers where *a ≠ 0*

a divides *b,* if there exist *c* such that b=ac

$$a|b \text{ if } \exists c, b = ac$$

a do not divide *b,* if there is no *c* such that b=ac

$$a \nmid \text{b if } \nexists c, b = ac$$

- *a* and *c* is a factor of *b*, and *b* is a multiple of *a*

Divisibility of Integers : Example

1. $8 \nmid 20$ because $20=(8)(2.5)$, 2.5 is not integer
2. $8 \nmid 24$ because $24=(8)(3)$, 3 is integer
3. $15 \nmid 0$ because $0=(15)(0)$, 0 is integer

Now you should be able to answer why any integer can’t be divided by 0

Divisibility of Integers : Theorem

- Let a, b and c be integers. Then,

1. If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$
2. If $a \mid b$, then $a \mid bc$ for all integers c
3. If $a \mid b$ and $b \mid c$, then $a \mid c$

Try to prove this theorems after Chapter 4: Proving methods

Prime

All positive integer larger than 1 is divisible by at least two integers

Definition 1.2 : Prime number

- A positive integer p greater than 1 is prime if it has exactly two factors which are 1 and p (itself)

Definition 1.3: Composite number

- A positive integer c greater than 1 is composite if it has more than two factors. Composite number is not prime

List of Primes <100

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43,

47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97

- The only even prime numbers is 2
- Two prime numbers with a gap of a number is known as twin primes etc. (3, 5), (5, 7), (11, 13), (41, 43), (59, 61), (71, 73), (101, 103), (107, 109), (137, 139)
- There are more properties of primes which remains to be unsolved

Prime : Theorems

Theorem 1: Fundamental theorem of arithmetic

- Every positive integer greater than 1 can be represented uniquely as the product of primes.

Theorem 2: Simple primality test

- If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$

Theorem 3: Distribution of primes

- There are infinitely many primes.

Prime factorization

All positive integer larger than 1 is divisible by at least two integers, then we can determine its prime factors

Step 1: Divide the integer c with the smallest divisible prime less than c in non-decreasing order

Step 2: Determine the remainder and it will be the new c

Step 3: Repeat step 1 until remainder is 0

Step 4: All the divisible prime is the prime factors of c

Prime factorization: Example (i)

Prime factors of 30

2	30
3	15
5	5
	1

$30 = 2 \times 3 \times 5$

30 has three prime factors 2, 3 and 5.

Thus, it is definitely composite

Prime factorization: Example (ii)

Prime factorization of 19

$$\begin{array}{r|l} 19 & 19 \\ \hline & 1 \end{array}$$

$19 = 19$

19 has only one prime factors : 19

19 has exactly two factors 1 and 19

Thus, it is prime

Prime factorization: Example (ii)

Prime factorization of 68

2	68
2	34
17	17
	1

$68 = 2 \times 2 \times 17$

$68 = 2^2 \times 17$

68 has two prime factors : 2 and 17

68 has other prime factor: 2

Thus, it is composite. It is not prime

Division algorithm

Case 1: If $m > 0$,

If $m, n \in \mathbb{Z}$, and $n > 0$, we can write $m = qn + r$ where $q, r \in \mathbb{Z}, 0 \le r \le n$.

Case 2 : If $m < 0$,

If $m, n \in \mathbb{Z}$, and $n > 0$, then $r = r + n$ and $q = q - 1$.

m- dividend, *n*- divisor, *q* - quotient, *r* - remainder

$q = m$ **div** n $r = m$ **mod** n

If $r = 0$ $\longrightarrow$ m is multiple of n

$\longrightarrow$ $n \mid m$, "n divides m"

$\longrightarrow$ $m = qn$ and $n \le m$

If not $\longrightarrow$ $n \nmid m$, "n does not divide m"

Division algorithm : Examples

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

Solution: $101 = 11 \cdot 9 + 2$,
the quotient is 9 = 101 **div** 11 and
the remainder is 2 = 101 **mod** 11

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

Solution: $-11 = 3(-4) + 1$,
the quotient is -4 = -11 **div** 3 and
the remainder is 1 = -11 **mod** 3

3) Find the quotient and remainder when $m = 17$ and $n = 3$

Solution: $17 = 5(3) + 2$ so $q = 5$ and $r = 2$

Adam Shariff Adli Aminuddin