2110301 INTRODUCTION TO DISCRETE STRUCTURES

THEORY OF NUMBER FOR COMPUTING

ELEMENTARY & APPLIED NUMBER THEORY

Athasit Surarerks, *Dr. en Inf.*
FACULTY OF ENGINEERING
CHULALONGKORN UNIVERSITY

MATHEMATICS IS THE QUEEN OF THE SCIENCES, AND NUMBER THEORY IS THE QUEEN OF MATHEMATICS.

C.F.GAUSS (1777-1855)

OBJECTIVES

PROVIDE A SOLID FOUNDATION OF ELEMENTARY NUMBER THEORY FOR APPLIED NUMBER THEORY OF THE NEXT CHAPTERS.

PROVIDE INDEPENDENTLY A SELF-CONTAINED TEXT OF ELEMENTARY NUMBER THEORY FOR COMPUTING

Preliminaries

Let us recall two integral functions
That we use in this section.

Floor & Ceiling

Modulo

Floor & Ceiling

Floor function of a real number x, denoted by $\lfloor x \rfloor$, is a function from x to the maximum integer that is less than or equal to x.

$\lfloor x \rfloor = m$ where m is an integer, $x-1 < m \leq x$

Ceiling function of a real number x, denoted by $\lceil x \rceil$, is a function from x to the minimum integer that is greater than or equal to x.

$\lceil x \rceil = m$ where m is an integer, $x \leq m < x+1$

FLOOR & CEILING

Example

$\lfloor 3.33 \rfloor = 3$	$\lfloor -3.33 \rfloor = -4$	$\lfloor -5 \rfloor = -5$	$\lfloor 5 \rfloor = 5$
$\lceil 3.33 \rceil = 4$	$\lceil -3.33 \rceil = -3$	$\lceil -5 \rceil = 5$	$\lceil 5 \rceil = 5$

Find $\lfloor \log_2 10 \rfloor$

$\lfloor x \rfloor = m$ means that $m \leq x < m+1$.

$\lceil x \rceil = m$ means that $m-1 < x \leq m$.

Since $2^3 \leq 10 \leq 2^4$, we have that $3 \leq \log_2 10 \leq 4$.
Then $\lfloor \log_2 10 \rfloor = 3$.

FLOOR & CEILING

ALTERNATIVE DEFINITIONS

Floor function $\lfloor x \rfloor = m$ where m is an integer such that
$x = m + \theta$ with $0 \leq \theta < 1$.

Ceiling function $\lceil x \rceil = m$ where m is an integer such that
$x = m - \theta$ with $0 \leq \theta < 1$.

Some properties

For any integer x, $x = \lfloor x \rfloor = \lceil x \rceil$.

For a non integer x, $\lceil x \rceil - \lfloor x \rfloor = 1$.

For any real x, $\lfloor -x \rfloor = -\lceil x \rceil$ and
$\lceil -x \rceil = -\lfloor x \rfloor$.

FLOOR & CEILING

Example: Prove that $\lfloor x \rfloor + m = \lfloor x + m \rfloor$
for any real number x and integer m.

Proof: Let $x = n + \theta$ with $0 \leq \theta < 1$. Then $\lfloor x \rfloor = n$.

But $\lfloor x + m \rfloor = \lfloor n + \theta + m \rfloor$
$= n + m$
$= \lfloor x \rfloor + m$. Q.E.D.

FLOOR & CEILING

Example: Prove that $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$.

Proof: Let $x = n + \theta$ with $0 \leq \theta < 1$. Then $\lfloor x \rfloor = n$.
Let $y = m + \beta$ with $0 \leq \beta < 1$. Then $\lfloor y \rfloor = m$.
But $\lfloor x + y \rfloor = \lfloor (n + m) + (\theta + \beta) \rfloor$; $0 \leq (\theta + \beta) < 2$.
Case $0 \leq \varepsilon = (\theta + \beta) < 1$

$$\lfloor (n + m) + (\theta + \beta) \rfloor = \lfloor (n + m) + \varepsilon \rfloor = m + n.$$

Case $1 \leq (\theta + \beta) < 2$, Let $\varepsilon = (\theta + \beta) - 1$. Then $0 \leq \varepsilon < 1$.

$$\lfloor (n + m) + (\theta + \beta) \rfloor = \lfloor (n + m) + 1 + \varepsilon \rfloor = m + n + 1.$$

In both case, $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor$. Q.E.D.

FLOOR & CEILING

More general,
for any real number x, let n be an integer.

$x \leq n$ if and only if $\lfloor x \rfloor \leq n$
$n \leq x$ if and only if $n \leq \lfloor x \rfloor$
$x \leq n$ if and only if $\lceil x \rceil \leq n$
$n \leq x$ if and only if $n \leq \lceil x \rceil$

FLOOR & CEILING

Interesting result

Let f be a continuous & monotonically increasing function.
If f satisfies the following condition:

$$f(x) \text{ is an integer only if } x \text{ is an integer}$$

then $\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor$ and $\lceil f(x) \rceil = \lceil f(\lceil x \rceil) \rceil$.

Proof: Show that $\lfloor f(x) \rfloor = \lfloor f(\lfloor x \rfloor) \rfloor$.
Let f be a continuous & monotonically increasing function.
Since $\lfloor x \rfloor \leq x$, we have $f(\lfloor x \rfloor) \leq f(x)$ and $\lfloor f(\lfloor x \rfloor) \rfloor \leq \lfloor f(x) \rfloor$.

Let $y < x$. That is $\lfloor f(y) \rfloor < \lfloor f(x) \rfloor$.
Since f is continuous, there exists z such that $f(z) = \lfloor f(x) \rfloor$ with $y < z \leq x$. Then z is an integer (f satisfies the condition).
We also have that $z \leq \lfloor x \rfloor$. That is $\lfloor f(x) \rfloor = f(z) \leq f(\lfloor x \rfloor)$.
$\lfloor f(x) \rfloor = \lfloor \lfloor f(x) \rfloor \rfloor \leq \lfloor f(\lfloor x \rfloor) \rfloor$. Q.E.D.

FLOOR & CEILING

Example: Show that $\lfloor \sqrt{\lfloor x \rfloor} \rfloor = \lfloor \sqrt{x} \rfloor$.
Let n be an integer such that $n = \lfloor \sqrt{\lfloor x \rfloor} \rfloor$.

Proof: Since $\lfloor x \rfloor < x$, we have $\lfloor \sqrt{\lfloor x \rfloor} \rfloor \leq \lfloor \sqrt{x} \rfloor$.
if x is an integer, the proof is complete.
if x is not integer, let $\sqrt{n}$ be an integer that $\sqrt{n} = \lfloor \sqrt{x} \rfloor$.
It is obvious that n is an integer.
Clearly, $n \leq \lfloor x \rfloor$. We have $\sqrt{n} \leq \sqrt{\lfloor x \rfloor}$.
We obtain $\lfloor \sqrt{x} \rfloor \leq \lfloor \sqrt{\lfloor x \rfloor} \rfloor$.
This completes the proof. Q.E.D.

FLOOR & CEILING

Exercises

- Prove that $x \le n$ if and only if $\lfloor x \rfloor \le n$
  $n \le x$ if and only if $n \le \lfloor x \rfloor$
  $x \le n$ if and only if $\lceil x \rceil \le n$
  $n \le x$ if and only if $n \le \lceil x \rceil$
- Prove that $\lceil \sqrt{\lceil x \rceil} \rceil = \lceil \sqrt{x} \rceil$

Division

Definition

For any integers a, b with $a \neq 0$.
a *divides* b if there exists an integer c that $b = ac$.

a is said to be a *factor* of b
b is said to be a *multiple* of a
a *divides* b is denoted by $a \mid b$
a *does not divide* b is denoted by $a \nmid b$.

Modulo

Definition

For any integers a, b.

a mod b = a - $\lfloor a / b \rfloor \times$ b.

b is called *modulus*.

a mod b is an integer.

Note: Since $(a/b)-1 < \lfloor (a/b) \rfloor \leq (a/b)$

$a-b < \lfloor (a/b) \rfloor b \leq a$	multiply by b
$-a \leq -\lfloor (a/b) \rfloor b < -a+b$	multiply by -1
$0 \leq a - \lfloor (a/b) \rfloor b < b$	increasing by a
$0 \leq a \bmod b < b$	

Contents

- Introduction
- Theory of Divisibility
- Diophantine Equations
- Distribution of Prime Numbers
- Theory of Congruences
- Computer Systems Design
- Cryptography & Information Security

Introduction

Brief review of the fundamental ideas of number theory and then present some mathematical preliminaries of elementary number theory.

Introduction

Number theory : the theory of the properties of integers such as

Properties of numbers

- parity
- primality
- Multiplicativity
- additivity

Algebraic Preliminaries

PARITY

Some well-known results, actually already known to Euclid, about the parity property of integers are as follows:

$\text{even}_1 \pm \text{even}_2 \pm \text{even}_3 \pm \ldots \pm \text{even}_k$ = even, if any positive k.

$\text{odd}_1 \pm \text{odd}_2 \pm \text{odd}_3 \pm \ldots \pm \text{odd}_k$ = even, if k is even.

$\text{odd}_1 \pm \text{odd}_2 \pm \text{odd}_3 \pm \ldots \pm \text{odd}_k$ = odd, if k is odd.

$\text{odd}_1 \times \text{odd}_2 \times \text{odd}_3 \times \ldots \times \text{odd}_k$ = odd, for any positive k.

$\text{even} \times \text{odd}_1 \times \text{odd}_2 \times \ldots \times \text{odd}_k$ = even, if there is at least 1 even.

PARITY

Error detection and correction method (parity check)

One additional bit at the end of code is 1 if the number of 1's is odd, otherwise it is 0.

EXAMPLE

Let two codes be 1101001001 and 1001011011. Then the new codes will be

11010010011 and 10010110110.

For example, after transmission we know there is an error if transmitted code is

11010110011 and 10010110110.

PARITY CHECK

Error detection and correction method (parity check)

1	0	0	1	0	1	1	0	0
1	0	1	1	1	0	1	1	0
1	1	0	0	0	0	0	1	1
0	1	1	0	0	1	0	0	1
0	0	0	1	1	0	0	0	0
1	0	1	0	1	0	1	0	1
0	1	0	0	0	0	0	0	1
1	0	0	1	1	0	1	0	0
1	1	0	0	0	0	0	0	0

PARITY CHECK

Error detection and correction method (parity check)

1	0	0	1	0	1	1	0	0
1	0	1	1	1	0	1	1	0
1	1	0	0	0	0	0	1	1
0	1	1	0	0	1	0	0	1
0	0	0	1	1	0	0	0	0
1	0	1	0	1	0	1	0	1
0	1	0	0	0	0	0	0	1
1	0	0	1	1	0	1	0	0
1	1	0	0	0	0	0	0	0

PRIMALITY

A positive integer n > 1 that has only two distinct factors, 1 and n itself is called prime; otherwise, it is called composite.

SOME INTERESTING RESULTS

- There are infinitely many primes. [Euclid]
- Only one even prime: 2
- Two largest twin primes (p and p+2),[1995]
  $570918348 \times 10^{5120} \pm 1$ and
  $242206083 \times 2^{38880} \pm 1$. [11713 digits]
- It is not known : infinitely many twin primes?
- infinitely many pairs (p, p+2) with
  p is prime and
  p+2 a product of most two primes.
  [J.R.Chen]
- Prime triples (p, p+2, p+6) : (347, 349, 353)
- Prime triples (p, p+4, p+6) : (307, 311, 313)
- Only one prime triples (p, p+2, p+4) : (3, 5, 7)

SOME INTERESTING RESULTS

Ancient Chinese mathematicians,

If p is a prime number, then $p \mid 2^p - 2$.

Example: 5 is a prime number, and $5 \mid 30$.

But, there are some composites that satisfy this condition.

Example: $341 = 11 \times 31$ is not prime, $341 \mid 2^{341} - 2$.

SOME INTERESTING RESULTS

PROBLEM: IT IS NOT EASY TO TEST WHETHER OR NOT A LARGE NUMBER n IS PRIME.

NEEDS TO TEST UP TO $n^{1/2}$

THE CURRENT BEST ALGORITHM FOR PRIMALITY TESTING NEEDS AT MOST

$\beta^{c \log \log \beta}$ (BIT OPERATIONS)

WHERE β IS A NUMBER OF BITS NEEDED FOR n
C IS A REAL POSITIVE CONSTANT.

MULTIPLICATIVITY

Fundamental Theorem of Arithmetic [Euclid]
Any positive integer $n > 1$,

$$n = p_1^{\alpha 1} p_2^{\alpha 2} \ldots p_k^{\alpha k} \text{ (unique)}$$

where $p_1 < p_2 < \ldots < p_k$ are primes and
$\alpha_1, \alpha_2, \ldots, \alpha_k$ are all positive integers.
[Proved by Gauss, 1777-1855]

EXAMPLES

1999 = 1999	2000 = $2^4 \times 5^3$
2001 = $3 \times 23 \times 29$	2002 = $2 \times 7 \times 11 \times 13$
2003 = 2003	2004 = $22 \times 3 \times 167$
2005 = 5×401	2006 = $2 \times 17 \times 59$
2007 = $3^2 \times 223$	2008 = $2^3 \times 251$

MULTIPLICATIVITY

PROBLEM:
IT IS DIFFICULT TO FACTOR A LARGE POSITIVE INTEGER (MORE THAN 100 DIGITS AT PRESENT) INTO ITS PRIME FACTORIZATION.
THE FASTEST FACTORING METHOD OF n

$$\exp(\, c(\log n)^{1/3} (\log \log n)^{2/3} \,),$$ (BIT OPERATIONS)

WHERE $c = (64/9)^{1/3} \sim 1.9$

The 9th Fermat number $F9 = 2^{2^9}+1$ (155 digits) was completely factored in 1990.
The 12th Fermat number has still not completely been factored , even though its five smallest prime factors are known).

SOME INTERESTING RESULTS

THE MOST RECENT RECORD [HERMAN TE RIELE,1999]

RANDOM NUMBER 155 DIGITS (512 BITS)

WRITTEN AS THE PRODUCT OF TWO PRIMES (78 DIGIT PRIMES)

1026395928297411057720541965739916759007165678
08038066803341933521790711307779

AND

1066034883801684548209272203600128786792079585
7598929152227060823719306280 8643

ADDITIVITY

THE LITTLE GOLDBACH CONJECTURE
TERNARY GOLDBACH CONJECTURE

Ch. Goldbach 1690-1764, proposed two conjectures

Every odd integer > 7 is the sum of 3 odd primes.
Every even integer > 4 is the sum of 2 odd primes.

EXAMPLES:

	6 = 3+3
	8 = 3+5
9 = 3+3+3	10 = 3+7 = 5+5
11 = 3+3+5	12 = 5+7
13 = 3+3+7 = 3+5+5	14 = 3+11
15 = 3+5+7 = 5+5+5	16 = 3+13 = 5+11

(The second conjecture implies the first.)

ADDITIVITY

Some results:

If a certain hypothesis (Riemann's) is true,
then every sufficiently large odd integer is the
sum of three odd primes.

Hardy & Littlewood, 1923

THREE-PRIME THEOREM

Every sufficiently large odd integer
can be written as the sum of three odd primes.

I.M. Vinogradov, 1937

Every sufficiently large even integer can be written
as the sum of a prime and a product of at most
two primes.

J.R. Chen, 1933-1996

ADDITIVITY

Goldbach partition of integer n, denoted by G(n), is

$$n = p_1 + p_2, \text{ n even and } p_1 < p_2$$

or

$$n = p_1 + p_2 + p_3, \text{ n odd and } p_1 < p_2 < p_3.$$

Examples: $|G(100)| = 6$
$|G(101)| = 32$
$|G(1001)| > 1001.$

ADDITIVITY

HARDY-RAMANUJAN TAXI NUMBER

1729 is the smallest positive integer expressible as a sum of two positive cubes in exactly two different ways, namely,

$$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$

(1729 is also the third smallest Carmichael number).

Carmichael number, 1912 (CONJECTURED)
A composite number n that satisfies bn+1 ≡ 1 (mod n) for every positive integer b such that gcd(b,n) = 1.
There are infinite ly many Carmichael numbers.
Proved this conjecture in 1992, by W.Alford, G. Granville and C.Pomerance.

Examples: 561, 1105, 1729, 2465, 2821, ...

ADDITIVITY

HARDY-RAMANUJAN TAXI NUMBER

1729 is the smallest positive integer expressible as a sum of two positive cubes in exactly two different ways, namely,

$$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$

(1729 is also the third smallest Carmichael number).

Fourth powers, known to Euler (1707-1783),

$$635318657 = 59^4 + 158^4 = 133^4 + 134^4.$$

ALGEBRAIC

Some notations

$\mathcal{N}$	natural numbers { 1, 2, 3, ... }
$\mathcal{Z}$	integers { ...,-2, -1, 0, 1, 2, ... }
$\mathcal{Z}/n\mathcal{Z}$	all residue classes modulo n { 0, 1, ..., n-1 }
$\mathcal{Q}$	rational numbers $\{ a/b \mid a,b \in \mathcal{Z},\ b \neq 0 \}$
$\mathcal{R}$	real numbers : algebraic numbers transcendental numbers
C	complex numbers $\{ a+bi \mid a,b \in \mathcal{R},\ i=(-1)^{1/2} \}$.

Algebraic numbers :
the root of a polynomial equation with integer coefficients.
Some are rational numbers, some are irrational numbers.

ALGEBRAIC

GROUP

A group $(\mathcal{G},*)$ is a nonempty set $\mathcal{G}$ of elements together with a binary operation *, such that The following axioms are satisfied:

- Closure: $\forall a,b \in \mathcal{G},\ a*b \in \mathcal{G}$.
- Associativity: $\forall a,b,c \in \mathcal{G},\ (a*b)*c = a*(b*c)$.
- Existence of identity: $\exists e$ unique $\in \mathcal{G}$, $\forall a \in \mathcal{G}$, $a*e=e*a=a$.
- Existence of inverse: $\exists b$ unique $\in \mathcal{G}$, $\forall a \in \mathcal{G}$, $a*b=b*a=e$.

Commutative group (Abelian group: Niels Henrik Abel, 1802-1829)
if it satisfies commutativity: $\forall a,b \in \mathcal{G},\ a*b = b*a$.

ALGEBRAIC

SEMIGROUP

A semigroup ($\mathcal{G}$,*) with respect to the binary operation *, is a nonempty set $\mathcal{G}$ of elements together with a binary operation *, such that the following axioms are satisfied:

Closure: $\forall a,b \in \mathcal{G}$, $a*b \in \mathcal{G}$.

Associativity: $\forall a,b,c \in \mathcal{G}$, $(a*b)*c = a*(b*c)$.

It is said to be a monoid with respect to the binary operation * if it also satisfies

Existence of identity: $\exists e$ unique $\in \mathcal{G}$, $\forall a \in \mathcal{G}$, $a*e=e*a=a$.

ALGEBRAIC

Examples:

($\mathcal{Z}$, +) is an abelian group. (additive group)

(Q^+, $\times$), ($\mathcal{R}^+$, $\times$) are abelian groups. (multiplicative group)

Definitions

Finite group	finite number of elements
Infinite group	infinite number of elements
Order of group	the number of elements $\lvert \mathcal{G} \rvert$
Subgroup	A nonempty subset of group under the same operation

ALGEBRAIC
SUBGROUP

A multiplicative group ($\mathcal{G}$,*).

a is an element of $\mathcal{G}$.

The element a^r form a subgroup of $\mathcal{G}$, called the subgroup generated by a.

A group $\mathcal{G}$ is cyclic if $\exists a \in \mathcal{G}$ such that $\forall x \in G$, $x = a^r$ for some integer r.

ALGEBRAIC
RING

A ring ($\mathcal{A}$, ⊕, ⊗) is a set of at least two elements with two binary operations ⊕ and ⊗., which we call addition and multiplication, defined on $\mathcal{A}$ such that the following axioms are satisfied:

Closure under ⊕ : $\forall a,b \in \mathcal{A}$, $a \oplus b \in \mathcal{A}$.

Associativity under ⊕ : $\forall a,b,c \in \mathcal{A}$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.

Commutative under ⊕ : $\forall a,b \in \mathcal{A}$, $a \oplus b = b \oplus a$.

Zero: $\exists 0$ unique $\in \mathcal{A}$, $\forall a \in \mathcal{A}$, $a \oplus 0 = 0 \oplus a = a$.

Additive inverse –a : $\forall a \in \mathcal{A}$, $a \oplus (-a) = (-a) \oplus a = 0$.

Closure under ⊗ : $\forall a,b \in \mathcal{A}$, $a \otimes b \in \mathcal{A}$.

Associativity under ⊗ : $\forall a,b,c \in A$, $(a \otimes b) \otimes c = a \otimes (b \otimes c)$.

Distributivity under ⊗ : $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$, $\forall a,b,c \in \mathcal{A}$.

$(a \oplus b) \otimes c = (a \otimes c) \oplus (b \otimes c)$, $\forall a,b,c \in \mathcal{A}$.

ALGEBRAIC
RING

Examples:

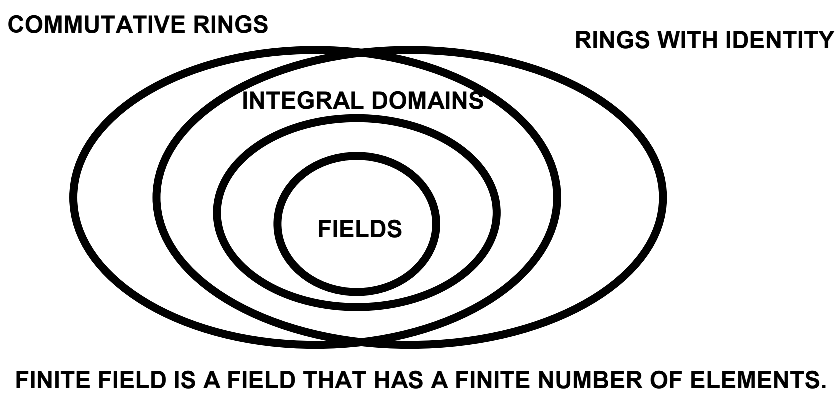
$(\mathcal{Z}, +, \times)$, $(\mathcal{Q}, +, \times)$, $(\mathcal{R}, +, \times)$, $(\mathcal{C}, +, \times)$ are rings.

Definitions

commutative ring	$\forall a,b \in A$, $a \otimes b = b \otimes a$.
ring with identity	$\forall a,1 \in A$, $a \otimes 1 = 1 \otimes a = a$.
integral domain	commutative ring and $ab = 0 \rightarrow a=0$ or $b=0$.
division ring	ring with identity $1 \neq 0$ and for each $a \neq 0$, $a \in \mathcal{A}$, $ax=1$ and $xa=1$ have solutions in $\mathcal{A}$.

ALGEBRAIC
FIELD

A field denoted by $(\mathcal{K}, \oplus, \otimes)$, is a division ring with commutative multiplication.



FINITE FIELD IS A FIELD THAT HAS A FINITE NUMBER OF ELEMENTS.

ALGEBRAIC

EVARISTE GALOIS (1811-1832)

Theorem GF

There exists a field of order q *if and only if* q is a prime power (*i.e.*, $q = p^r$) with p prime and $r \in \mathcal{N}$. Moreover, if q is a prime power, then there is, up to relabelling, only one field of that order.

ALGEBRAIC

EVARISTE GALOIS (1811-1832)

GF(5)

$\oplus$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\otimes$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1