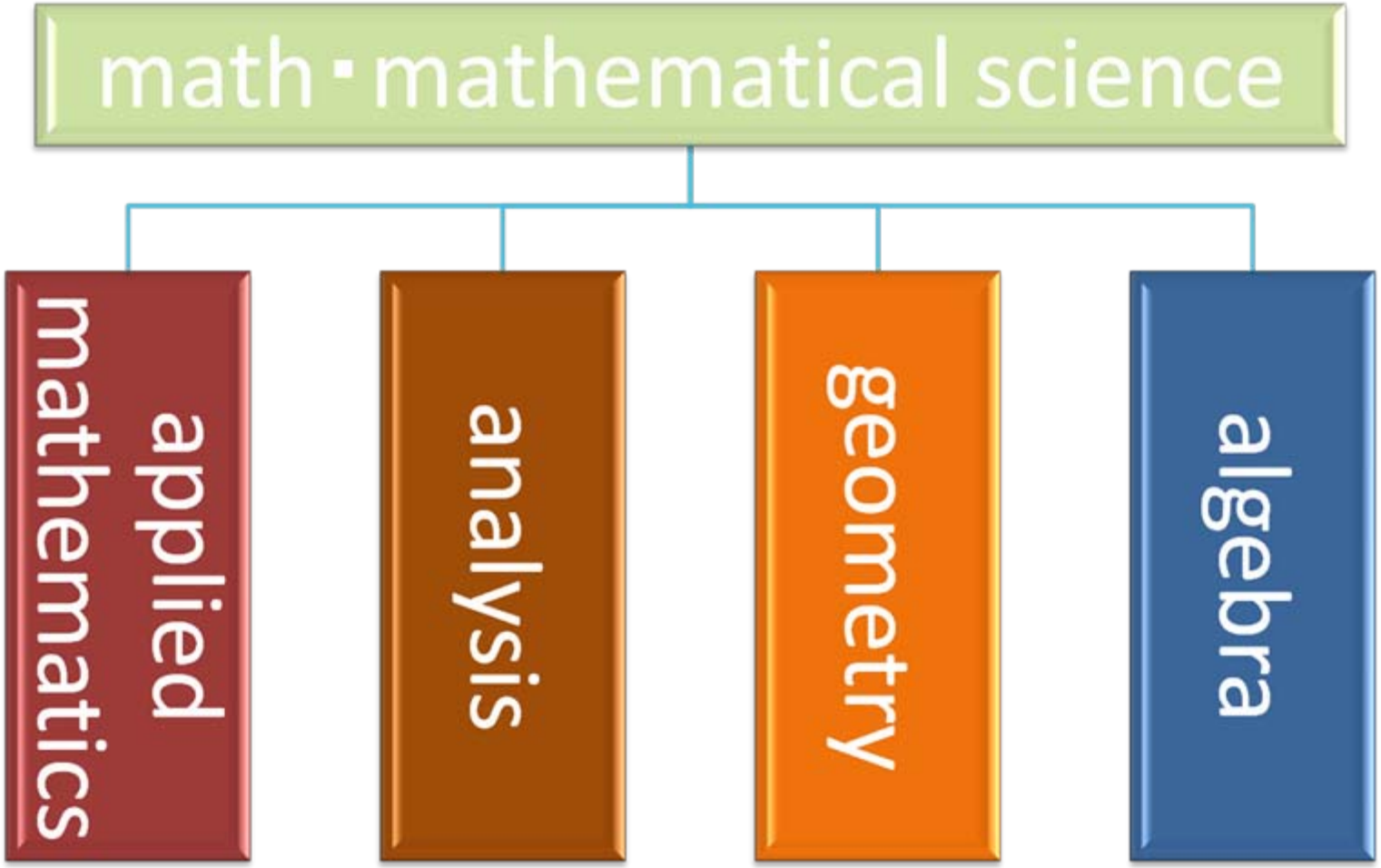
The World of Algebra
—Number Theory and Its Application—

#1 The World of Elementary Theory of Numbers and Finite Numbers

Graduate School of Mathematical Sciences,
the University of Tokyo

Toshiyuki Katsura

Fields of Mathematics



1. Numbers

Natural number $\mathbb{N} = \{1, 2, 3, 4, \cdots\}$

Integer $\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$

- may be called rational integer

Rational number $\mathbb{Q} = \{\cdots, 3, \frac{1}{2}, -\frac{5}{4}, \cdots\}$

Real number $\mathbb{R} = \{\cdots, 3, \frac{1}{2}, -\frac{5}{4}, \sqrt{2}, \pi, e, \cdots\}$

Complex number

$$\mathbb{C} = \{\cdots, 3, \frac{1}{2}, -\frac{5}{4}, \sqrt{2}, \pi, e, 2 + \sqrt{2}i, \cdots\}$$

$$i = \sqrt{-1}$$

$$\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Calculations are given to these groups.

addition $+$

multiplication $\times$ $\cdot$

ALGEBRAIC SYSTEM

Calculations of $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ Fulfill Below

definition When sum +, product・ are defined to a group K and fulfills conditions below, K is called a field.

$a, b, c \in K$

(I) (sum +)

(i) (association law) $(a+b)+c=a+(b+c)$

(ii) (existence of zero-dimension) for any $a \in K$, $0+a=a+0=a$

(iii) (existence of inverse concerning sum) for $a \in K$, there is $a' \in K$ that fulfills $a+a'=a'+a=0$

(iv) (commutative property) $a+b=b+a$

(II) (product・)

(i) (association law) $(a \cdot b) \cdot c=a \cdot (b \cdot c)$

(ii) (existence of multiplicative identity) for any $a \in K$, $1 \cdot a=a \cdot 1=a$

(iii) (existence of inverse concerning sum) for $b \in K, b \neq 0$, there is $b' \in K$ that fulfills $b \cdot b'=b' \cdot b=1$

(iv) (commutative property) $a \cdot b=b \cdot a$

(III) (distributive law)

(i) $(a+b) \cdot c=a \cdot c+b \cdot c$

(ii) $a \cdot (b+c)=a \cdot b+a \cdot c$

Marks for multiplication such as X and・ are often abbreviated, and for $a, b \in K$, a x b or a・b is often written as ab.

- Calculation of $\mathbb{Z}$ fulfills all except $(\mathrm{II})(\mathrm{iii})$

definition

When sum + and product・ is defined to a group R and all conditions except $(\mathrm{II})(\mathrm{iii})$ are fulfilled,

R is a commutative ring

$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ Have Infinitely Many Members.

Are there any fields that have finite members?

Finite field

É. Galois (1811-1832)

Sur la Théorie des Nombres.

(On the Theory of Numbers)

today

application to cryptology, code theory

Reprinted from “Iwanami’s Encyclopedia of

Math , the 3rd Edition”, Japan Math Society

The reprint from “Complete Works of Galois”

inserted here was omitted

according to copyright issues.

2. Integer $\mathbb{Z}$

Prime number

a natural number that is divisible only by 1 and itself

$$2, 3, 5, 7, 11, 13, 17, 19, 23, \cdots$$

theorem

There are infinitely many prime numbers

proof

proof by contradiction.

If number of primes is finite,

they could be written $p_1, p_2, \cdots, p_m$

and suppose $n = p_1 p_2 \cdots p_m + 1$

n can be divided by a prime

and cannot be divided by $p_1, \cdots, p_m$

repugnance

Largest Prime Known Now

$2^{32582657} - 1$ (Sept. 2006)

digit number **9808358**

$2^n - 1$ type prime Mersenne prime

Number of n that are prime numbers and now known is **44**.

Unsolved Problem

(1) Are **twin primes** infinite?

a prime number that differs from another prime number by 2

$$3\ \&\ 5,\ \ 5\ \&\ 7,\ \ 11\&\ \ 13,\ \ 17\&\ \ 19,\cdots$$

Largest twin prime known now

$$2003663613 \cdot 2^{195000} - 1$$

$$2003663613 \cdot 2^{195000} + 1$$

58711 digits (November, 2006)

(2) Goldbach's Conjecture

Every even integer greater than 4 can be written as the sum of two primes.

$$
\begin{aligned}
4 &= 2+2 \\
6 &= 3+3 \\
8 &= 3+5 \\
10 &= 5+5 \\
12 &= 5+7 \\
&\vdots
\end{aligned}
$$

a, b : integer

When q is an integer, and

$$b = aq$$

- b is divisible by a .
- a is aliquot of b
- b is multiple of a

This is written as $a \mid b$

Fundamental Properties of Integers

(1)（remainder theorem）

$$a, b \in \mathbb{Z},\ a \neq 0,\ b \neq 0$$

$$b = qa + r \qquad 0 \leq r < |a|$$

Only one combination of integers q, r exists.

(2) Natural numbers are factorized uniquely.

n : natural number

If numbers of primes are finite $p_1, \cdots, p_k$ $(i \neq j$ p_i

natural numbers $e_1, \cdots, e_k$

exist, and

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

is written uniquely regardless of order of products.

$a, b \in \mathbb{Z},\ a \neq 0,\ b \neq 0$

common divisor of a & b common factor

largest common divisor of a & b highest common factor

$\gcd(a, b)$

When greatest common divisor of a & b is 1,

a & b are coprimes.

3. Euclidean Algorithm

lemma

When a, b are 2 integers and not 0

and $a = qb + r$ （q, r : integer）

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

How to Calculate gcd of Integers a, b (not 0)

Use remainder theorem sequentially.

$$
\begin{aligned}
a &= m_1 b + r_1 \ , \ 0 \le r_1 \le |b| - 1 \\
b &= m_2 r_1 + r_2 \ , \ 0 \le r_2 \le r_1 - 1 \\
r_1 &= m_3 r_2 + r_3 \ , \ 0 \le r_3 \le r_2 - 1 \\
r_2 &= m_4 r_3 + r_4 \ , \ 0 \le r_4 \le r_3 - 1 \\
&\vdots
\end{aligned}
$$

Since $r_1 > r_2 > \cdots \ge 0$

There is a natural number n , that is $r_n \neq 0, \ r_{n+1} = 0$

Then $r_{n-1} = m_{n+1} \cdot r_n$

r_n is a greatest common factor of a, b

Example

$$
\begin{aligned}
54 &= 2 \times 20 + 14 \\
20 &= 1 \times 14 + 6 \\
14 &= 2 \times 6 + 2 \\
6 &= 3 \times 2
\end{aligned}
$$

gcd of 54 and 20 is 2

Reduction

$$r_1 = a - m_1 b$$

If $p_1 = 1,\ q_1 = -m_1\ ,\quad r_1 = p_1 a + q_1 b$

$$r_2 = b - m r_1 = b - m_2(p_1 a + q_1 b) = -m_2 p_1 a + (1 - m_2 q_1) b$$

If $p_2 = -m_2 p_1,\ q_2 = 1 - m_2 q_1 \qquad r_2 = p_2 a + q_2 b$

If r_1, r_2 are assigned into the third formula,

$$r_3 = p_3 a + q_3 b \qquad p_3, q_3 : \text{integer}$$

Inductively,

$$r_i = p_i a + q_i b \qquad p_i, q_i : \text{integer}$$

When $i = n,\ r_n$ is a gcd of a, b

$$\gcd(a, b) = r_n = p_n a + q_n b \qquad p_n, q_n : \text{integer}$$

Theorem

a, b are integers and not 0

greatest common factor of a, b : d

There are integers α, β , that fulfill

$$\alpha a + \beta b = d$$

System

a, b are coprime integers.

There are integers α, β , that fulfill

$$\alpha a + \beta b = 1$$

Example

If $a = 5,\ b = 7$

$x = 3,\ y = -2$, then

$$3 \times 5 + (-2) \times 7 = 1$$

4. Congruence

a, b, m integers

$b - a$ can be divided by $m \Leftrightarrow a \equiv b \pmod{m}$

congruence expression

properties

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

(i) $a \equiv a \pmod{m}$

(ii) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

(iii) $a \equiv b \pmod{m}$ **and** $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

Fix one integer, m

for $a \in \mathbb{Z}$

$$\overline{a} = \{x \in \mathbb{Z} \mid x \equiv a \pmod{m}\}$$

This is called **residue class** in the modulo m defined by a .

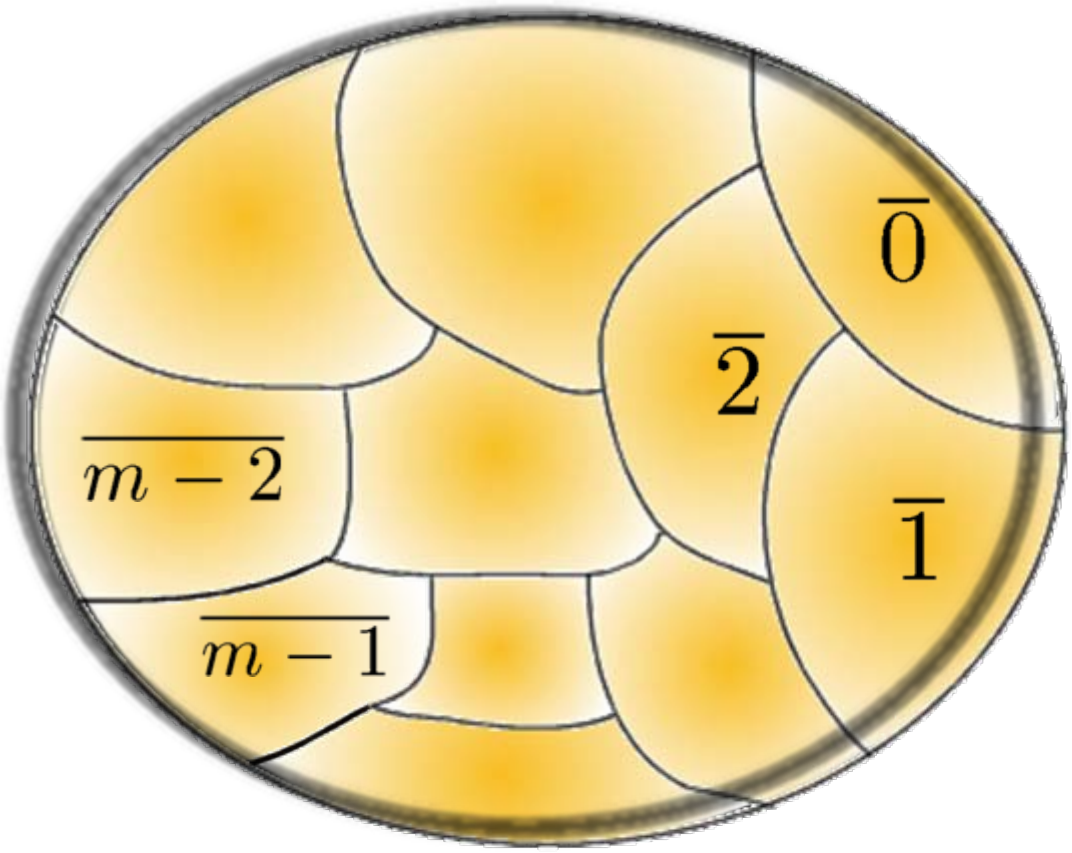
a is representative element of $\overline{a}$

notice. If $a \equiv b \pmod{m}$ then $\overline{a} = \overline{b}$

Set of whole residue classes related to mod m is written as

$$\mathbb{Z}/m\mathbb{Z}$$

$$\mathbb{Z}/m\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{m-2}, \overline{m-1}\}$$



Set of classes is $\mathbb{Z}/m\mathbb{Z}$

Addition and Multiplication on $\mathbb{Z}/m\mathbb{Z}$

lemma if $a_1 \equiv a_2 \pmod{m}$, $b_1 \equiv b_2 \pmod{m}$ then

$$a_1 \pm b_1 \equiv a_2 \pm b_2 \pmod{m}$$

$$a_1 b_1 \equiv a_2 b_2 \pmod{m}$$

- It is proved by this lemma that class does not change if a number in calculation is switched to another number of the same class.

Addition and Multiplication on $\mathbb{Z}/m\mathbb{Z}$

On $\overline{a}, \overline{b} \in \mathbb{Z}/m\mathbb{Z}$, we can define

addition : $\overline{a} + \overline{b} = \overline{a+b}$

multiplication : $\overline{a} \cdot \overline{b} = \overline{ab}$

zero element $\overline{0}$

$$\overline{a} + \overline{0} = \overline{0} + \overline{a} = \overline{a}$$

unit element $\overline{1}$

$$\overline{a} \cdot \overline{1} = \overline{1} \cdot \overline{a} = \overline{a}$$

ex

$$\mathbb{Z}/4\mathbb{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$$

for example, $\overline{1} + \overline{2} = \overline{3},\ \overline{2} + \overline{3} = \overline{5} = \overline{1}$

$$\overline{2} \cdot \overline{2} = \overline{4} = \overline{0},\ \overline{2} \cdot \overline{3} = \overline{6} = \overline{2}$$

- $\mathbb{Z}/m\mathbb{Z}$ is a **commutative ring**

It is not always a field.

ex

$\mathbb{Z}/4\mathbb{Z}$ **is not a field.**

$$\overline{2} \cdot \overline{2} = \overline{0}$$

If $\overline{2}$ has an inverse element, $\overline{x}$,

then $\overline{2} \cdot \overline{x} = \overline{1}$.

$$\overline{2} \cdot \overline{2} \cdot \overline{x} = \overline{0} \cdot \overline{x}$$

$$\overline{2} = \overline{2} \cdot \overline{1} \qquad \overline{0}$$

repugnance

A Lemma to Understand the Structure of $\mathbb{Z}/m\mathbb{Z}$

lemma

$a, b, c, m \in \mathbb{Z}$

Suppose m and c are coprime,

$$ac \equiv bc \pmod{m} \Rightarrow a \equiv b \pmod{m}$$

proof

The greatest common factor of m and c is 1, so integers x, y that satisfy $cx + my = 1$ exist.

$$a = acx + amy$$

$$b = bcx + bmy$$

Therefore,

$$a - b = (ac - bc)x + (ay - by)m$$

from the supposition, right member is divisible by m.

Therefore, $a - b$ is divisible by m.

5. Finite Field

$$\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$$

addition $\overline{0}+\overline{0}=\overline{0}\ ,\ \overline{0}+\overline{1}=\overline{1}$

$\overline{1}+\overline{0}=\overline{1}\ ,\ \overline{1}+\overline{1}=\overline{0}$

multiplication $\overline{0}\cdot\overline{0}=\overline{0}\ ,\ \overline{0}\cdot\overline{1}=\overline{0}$

$\overline{1}\cdot\overline{0}=\overline{0}\ ,\ \overline{1}\cdot\overline{1}=\overline{1}$

become fields.

Suppose p is a prime,

$$\mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$$

addition $\overline{a}+\overline{b}=\overline{a+b}$

multiplication $\overline{a}\cdot\overline{b}=\overline{ab}$

Theorem When p is a prime, $\mathbb{Z}/p\mathbb{Z}$ is a field.

proof

$\overline{0}$ zero element

$\overline{1}$ unit element

Inverse element for any element $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ that is not $\overline{0}$ should be indicated.

p is a prime, and $\overline{a} \neq \overline{0}$, so a & p are coprimes.

Integers x, y exist that satisfy

$$1 = xa + yp$$

In modulo p,

$$\overline{1} = \overline{xa + yp} = \overline{x}\,\overline{a} + \overline{y}\,\overline{p} = \overline{x}\,\overline{a} + \overline{y}\,\overline{0} = \overline{x}\,\overline{a}$$

$\overline{x}$ is an inverse element of $\overline{a}$!

Definition

p prime number

Suppose $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$

$\mathbb{F}_p$ is a finite field composed of p elements.

note1

$\mathbb{Z}/m\mathbb{Z}$ is a field $\Leftrightarrow$ m is a prime

note2

When n is a natural number, and p is a prime,
There is only 1 finite field $\mathbb{F}_{p^n}$
with p^n elements.
Also, a finite field is only $\mathbb{F}_{p^n}$
(n :natural number, p : prime)