有限の算術と
秘密分散の数理技術

角皆 宏 (つのがい ひろし)

上智大学オープンキャンパス
情報理工学科体験授業
2011-07-24

「数理技術」とは

物理技術 (17 世紀以来) :

基礎数理 $\Longrightarrow$ 物理現象 $\Longrightarrow$ 実用技術

理論的裏付け　　仕組みの構成

情報技術 (20 世紀以来) :

数理現象 $\Longrightarrow$ 数理技術 $\Longrightarrow$ 実用技術

仕組みの構成　　物理的実現

数理の探求・解明が直接に技術発展に繋がる

計算機で扱えるもの

計算機では本質的に

有限・離散

のものしか扱えない

- 無限・連続のものの近似
- 有限・離散であることの積極的活用

有限の算術 (剰余系)

m : 1 以上の整数を一つ取って固定

m で割った余りのみに注目して計算する

a と b とが m を法として合同
(congruent modulo m)

$$a \equiv b \pmod{m}$$

$\overleftrightarrow{\Longleftrightarrow}$ a と b とを m で割った余りが等しい

$\Longleftrightarrow$ $m \mid (a-b)$ ($a-b$ が m で割切れる)

$\longrightarrow$ 整数全体が有限個 (m 個) の類に分けられる

有限の算術 (剰余系)

m を法とした剰余のみに着目して
(well-defined に) 足し算・掛け算が出来る

足し算はほぼ当たり前

右は $\mathrm{m} = 5$

$3+4 = 7 \equiv 2 \pmod 5$

$+$	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

剰余系の足し算・引き算

m を法として (mod m で) 考えたとき、
どんな a, b に対しても、その a, b について

$$a + x \equiv b \pmod{m}$$

となる x が必ず丁度 1 つ見付かる

$\longrightarrow$ mod m の世界での引き算：“$x = b - a$”

右は $m = 5$

$3+4 = 7 \equiv 2 \pmod{5}$

mod 5 の世界で

“$3 + 4 = 2$”

“$4 = 2 - 3$”

$+$	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

実習：剰余系の掛け算

$\mathrm{m} = 3, 4, 5, 6, 7$ について、

配布ワークシートの掛け算表を埋めてみよう

掛け算は当たり前？

右は $\mathrm{m} = 5$

$2 \times 3 = 6 \equiv 1 \pmod 5$

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(配布ワークシートの表には 0 の行・列はない)

実習：剰余系の掛け算

$\mathrm{m} = 3, 4, 5, 6, 7$ **について、**

配布ワークシートの掛け算表を埋めてみよう

m **の値による様子の違いは？**

剰余系の掛け算・割り算

$m = 4$:

$\times$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

$m = 6$:

$\times$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

$ax \equiv b \pmod{m}$ **となる** x **は**

($a \not\equiv 0 \pmod{m}$ **でも) 見付かるとは限らない**

$\longrightarrow \bmod m$ **の世界で割り算が出来るとは限らない**

剰余系の掛け算・割り算

$m = 5$:

$\times$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$m = 7$:

$\times$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

$m = 3, 5, 7$ **の場合には、** $a \not\equiv 0 \pmod{m}$ **であれば、**

$$ax \equiv b \pmod{m}$$

となる x **が必ず丁度** 1 **つ見付かる**

$\longrightarrow \mod m$ **の世界で (**0 **以外での) 割り算が出来る**

素数を法とする剰余系での割り算

一般の m **では**
$\mod m$ **の世界で割り算が出来るとは限らないが、**

法 m **が素数であるときは、**

$a \not\equiv 0 \pmod{m}$ **であれば、**

$ax \equiv b \pmod{m}$ **となる** x **が**
必ず丁度 1 **つ見付かる**

$\longrightarrow \mod m$ **の世界で (**0 **以外での) 割り算が出来る**
“$x = b/a$”

有限体

体 (field) : 四則演算 (加減乗除) が出来る集合

例 : 有理数体 $\mathbb{Q}$ ・実数体 $\mathbb{R}$ ・複素数体 $\mathbb{C}$

素数 p に対して、

p で割った余りの集合 $\overset{1:1}{\longleftrightarrow} \{0, 1, \ldots, \mathrm{p}-1\}$

この中で (0 で割る以外の) 四則演算が出来る

$\ldots$ **有限体** (finite field) ・p 元体 $\mathbb{F}_{\mathrm{p}}$, $\mathbb{Z}/\mathrm{p}\mathbb{Z}$

四則演算しか使わない計算なら、

有限体 $\mathbb{F}_{\mathrm{p}}$ 上でも実数や複素数と同様に行なえる

物理技術を利用した理工学においては、
その基礎となる微分積分 (解析学) が
理工学に携わる者の必須教養であったが、

有限・離散な世界である計算機上の
情報・数理技術を利用した理工学においては、
その基礎となる抽象代数学が
理工学に携わる者の必須教養となっている

- 基礎理学はすぐには役に立たない
- けれども不思議といつか役に立つ
- それがいつかは判らない

$\longrightarrow$ “良いもの” を追い求めるのが大切

数理技術としての応用例

有限体の算術を利用した、
ちょっと不思議な応用例を紹介しよう

秘密分散

(秘密情報の安全な管理の一方法)

秘密分散

殿様が隠し財宝の在処を子供達に伝える
(会社の社長が超重要機密を重役達に伝える)

伝える相手は 3 人としよう

それぞれに異なる手掛かりを教える

但し、

- どの 1 人も自分だけでは何も判らない
- どの 2 人でも教え合えば判る

ようにするにはどうしたら良いか ？

秘密分散

アナログ技術で実現するのは中々難しそうだ

$\longrightarrow$ ディジタル技術・数理技術の利用

$\longrightarrow$ 秘密情報を数値化・符号化して処理
(有限・離散の世界の積極的活用)

秘密分散

駄目な例１：秘密情報を 3 桁の数字列として
各人に 1 桁づつ教える

- 2 人がつるんでも判らない
- 各人は何も知らないよりも情報がある

駄目な例２：秘密情報を 3 桁の数字列として
各人に 2 桁づつ教える

- 2 人がつるめば判るが、
- 各人は何も知らないよりも情報がある

秘密分散

そこで、

有限体の性質を活用した

数理技術の出番だ !!

秘密分散

- 素数 p を固定 (これは公開)
- 秘密情報は有限体 $\mathbb{F}_p$ の元 b とする
- ランダムに $\mathbb{F}_p$ の元 a を選ぶ (これも秘密)
- $\mathbb{F}_p$ 上の "直線" $y = ax + b$ を考える
- 伝える相手それぞれに対して
  - ⋆ 異なる $\mathbb{F}_p$ の元 $x_i (\neq 0)$ を選び
    $y_i = ax_i + b$ を計算する
  - ⋆ "直線上の点" (x_i, y_i) を教える

秘密分散

2 人つるむと判る理由：

2 点を通る “直線” $y = ax + b$ は唯一に定まる

2 点 $(x_i, y_i), (x_j, y_j)$ を通る直線は

$$a = \frac{y_i - y_j}{x_i - x_j}, \qquad b = y_i - \frac{y_i - y_j}{x_i - x_j} x_i$$

$\longrightarrow$ 秘密情報 b が判明した

秘密分散

1 人では判らない理由：

2 点を通る “直線” $y = ax + b$ は必ず存在する

2 点 $(x_i, y_i), (0, b)$ を通る直線の傾きは

$$a = \frac{y_i - b}{x_i}$$

どの値 b も同様に可能性がある

$\longrightarrow$ 何も知らないのと同じ

実習： 秘密分散

みなさんに配った“秘密情報の一部”(鍵)

$$(x, y)$$

$p = 7$ を法として、
1 次式 $y \equiv ax + b \pmod 7$ を用いて
秘密情報 b を分散して伝えたもの

近くの人の鍵を見せてもらって
秘密情報 b を復元しよう
(鍵が同じ値だったら他の人に)

実習：秘密分散

- **自分の鍵** $(x_0, y_0) = (\quad , \quad)$
- **もう一人の鍵** $(x_1, y_1) = (\quad , \quad)$
- **直線の傾き (ランダムに選んだ秘密のパラメタ)**

$$a = \frac{y_1 - y_0}{x_1 - x_0} = \frac{\square - \square}{\square - \square} = \frac{\square}{\square} = \square$$

- **秘密情報**

$$b = y_0 - ax_0 = \square - \square \cdot \square = \boxed{\square}$$

7 を法とした足し算・掛け算の表

$+$	1	2	3	4	5	6
1	2	3	4	5	6	0
2	3	4	5	6	0	1
3	4	5	6	0	1	2
4	5	6	0	1	2	3
5	6	0	1	2	3	4
6	0	1	2	3	4	5

$\times$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

「割り算」って何さ？ — 定義に立ち戻ること

有限体での $\frac{b}{a}$ とは何か？

「割り算」とは何だったか？

$\frac{b}{a}$ とは、$ax = b$ となる (ただ一つの) x のこと

定義に立ち戻る (定義から出発する) ことで、
何であるかがはっきりする

代数と幾何 — 数と図形 — の共働

- 2 点 $(x_i, y_i), (x_j, y_j)$ を通る直線 $y = ax + b$ が
  ただ一つに決まる (**幾何**)
- $\begin{cases} y_i = ax_i + b \\ y_j = ax_j + b \end{cases}$ を満たす a, b が
  ただ一つに決まる (**代数**)

- $a = \dfrac{y_i - y_j}{x_i - x_j},\ b = y_i - \dfrac{y_i - y_j}{x_i - x_j} x_i$
  これなら有限体でも考えられる (代数の利点)
- 有限体でも直観的に考察できる (幾何の利点)

実際に使うには

- もっと多い人数で秘密を分散したい
  $\longrightarrow$ 人数より大きな素数 p を用いれば良い

- あてずっぽうでも確率 $\frac{1}{p}$ で当たってしまう
  $\longrightarrow$ 実際には大きな素数 p を使う
  (100 桁とか 200 桁とか)

- 今は割り算を表に頼ったので効率が悪い
  $\longrightarrow$ Euclid の互除法を用いると効率良く行なえる

今回の方式の一般化

今は 1 次式 (“直線”) を使ったので、
2 人が見せ合えば判ったが、

3 人の協力で判るようにするには、
2 次式 (“放物線”) を使えば良い

一般に、

k 人の協力で判るようにするには、
$(k-1)$ 次式を使って仕組みを設計すればよい

(“n 人中 k 人” で出来る)

数理技術とその応用

基礎数理・数理現象
(有限体・線型代数・代数幾何など)

$\longrightarrow$ 基本的な数理技術
(秘密分散・公開鍵暗号・鍵共有
・誤り訂正符号など)

$\longrightarrow$ 様々な応用
(バーコード・電子署名・電子投票など)

情報理工学科で触れられること

- 基盤となる数学そのものの探求・解明
- その数理技術・情報技術としての応用
- それを用いた人間活動の支援の実現
- そのための人間の情報処理の探求・解明

$\longrightarrow$ 様々な興味を持った人が刺激し合って学ぶ

おしまい

数学図書室公開

4 号館 5 階 4-595A

- 旧数学科からの伝統ある私学随一の専門図書室
- 専門書・論文雑誌の他、初年級の参考書も豊富
  (図書 3 万冊以上・論文雑誌約 200 タイトル)

$\longrightarrow$ 見学ツアー希望者は集まってください

情報理工学科 教員・在校生相談コーナー

1 号館 1 階 1-103