

第73回数学教育実践研究会 レポート発表

余りものには『福』がある

北海道室蘭東翔高等学校教諭 長尾良平

平成22年6月12日 北海道大学情報教育館

1 始めに

昨年度は、3年生の看護・医療系の数学（数学課題探求）を担当しており、一通り調教演習を終えた後、トピック的な題材をいくつか扱った。その中から、「ISBNコード」についての実践について紹介したい。

ISBNコードは書籍に対して一意に決められる番号であり、**合同式**が応用されている。新課程では数学Aに初等整数論の内容が設定されることもあり、自身の学習の意味も込めて授業を行った。

2 授業の展開

授業では、まず合同式の定義を行い、具体例を挙げた。

—— 合同式とは . . . ——

整数 a, b について、 n で割った時の余りが等しい時、 a, b は「 n を法として**合同**」といい、

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

と表す。 $a \equiv b \pmod{n}$ は「 $a - b$ が n で割り切れること」と言い換えられる。

例1 定義の意味を具体例で確認。

(1) $17 \equiv 2 \pmod{5}$

☞ $17 \div 5 = 3 \cdots 2$

☞ $2 \div 5 = 0 \cdots 2$

☆ 17 を 5 で割った余りは 2

(2) $17 \not\equiv 4 \pmod{5}$

☞ $17 \div 5 = 3 \cdots 2$

☞ $4 \div 5 = 0 \cdots 4$

☆ 17 を 5 で割った余りは 4 ではない

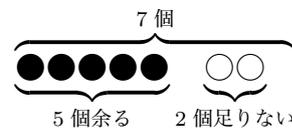
(3) $5 \equiv -2 \pmod{7}$

☞ $5 \div 7 = 0 \cdots 5$

☞ $-2 \div 7 = -1 \cdots 5$

☆ 「5 余る」 = 「2 足りない」

(3) については、



という理解も必要だと考え、図示することによって説明した。

これらの例を通して、（割り切れる部分はどうでもいいから）余りに注目していることを意識させた。

次に、合同式の性質を紹介し、余りを求める演習を通して、合同式に慣れてもらった。

—— 合同式の性質 ——

$a \equiv b \pmod{n}$, $c \equiv d \pmod{n}$ の時、次が成り立つ。

● $a + c \equiv b + d \pmod{n}$

● $a - c \equiv b - d \pmod{n}$

● $ac \equiv bd \pmod{n}$

● $a^k \equiv b^k \pmod{n}$ k は自然数

例2 $7 \equiv 2 \pmod{5}$, $9 \equiv 4 \pmod{5}$ より,

和 $16 \equiv 6 \pmod{5} \Rightarrow$ 余り 1

積 $63 \equiv 8 \pmod{5} \Rightarrow$ 余り 3

例3 7^{50} を 4 で割った時の余りを求めよ.

$$7 \equiv -1 \pmod{4}$$

の両辺を 50 乗して,

$$7^{50} \equiv (-1)^{50} \equiv 1 \pmod{4}$$

よって, 7^{50} を 4 で割った時の余りは 1 である.

ISBN コードって知ってる?

ISBN ○-●●-△△△△△△-☆

- 「○」の部分で地域を表す.
- 「●●」で出版社を表す.
- 「△△△△△△」の部分は出版物固有の番号である.
- 「☆」の部分は**チェックディジット**.
 \Rightarrow 入力時の誤りを確かめるためのもの.
 \Rightarrow 0~9, X (10の代わりに) を当てる.

チェックディジットの定め方

ISBN コードで現れる各桁の数字を右から, a_1, a_2, \dots, a_{10} とする時,

$$\sum_{k=1}^{10} a_k \cdot k \equiv 0 \pmod{11}$$

が成り立つように, チェックディジット a_1 の値を定める.

「JR全車両ハンドブック 2005」や「工場萌え」, 「Topology From The Differentiable Viewpoint」などの書籍を教室に持ち込み, ISBN コードについて説明した.

なお, 2007 年より規格が変わり, 現行の ISBN コードは 13 桁であり, チェックディジットの計算方法も変更になった.

例4 「ISBN4-00-021326-1」が誤りを含むか否かをチェックせよ.

ISBN	4	0	0	0	2	1	3	2	6	1
重み	10	9	8	7	6	5	4	3	2	1
×	40	0	0	0	12	5	12	6	12	1

$$40 + 12 + 5 + 12 + 6 + 12 + 1$$

$$\equiv -4 + 1 + 5 + 1 - 5 + 1 + 1 \pmod{11}$$

$$\equiv 0 \pmod{11}$$

となり, 誤りを含んでいないことが分かる.

例5 「ISBN4-00-005614-7」が誤りを含むか否かをチェックせよ.

ISBN	4	0	0	0	0	5	6	1	4	7
重み	10	9	8	7	6	5	4	3	2	1
×	40	0	0	0	0	25	24	3	8	7

$$40 + 25 + 24 + 3 + 8 + 7$$

$$\equiv -4 + 3 + 2 + 3 - 3 - 4 \pmod{11}$$

$$\equiv -3 \pmod{11}$$

となり, 誤りを含んでいることが分かる. なお, **誤りを検出できるが, 訂正はできない** (正しいコードは, 「ISBN4-00-005614-7」である).

例6 本に醤油をこぼしてしまって, ISBN コードの一部が見えなくなってしまった.

「ISBN4-00-02141 ●-6」であるとき, ●の部分の数字を答えよ.

●を a_2 で表すことにすると,

ISBN	4	0	0	0	2	1	4	1	a_2	6
重み	10	9	8	7	6	5	4	3	2	1
×	40	0	0	0	12	5	16	3	$2a_2$	6

$$40 + 12 + 5 + 16 + 3 + 2a_2 + 6$$

$$\equiv -4 + 1 + 5 + 5 + 3 + 2a_2 - 5 \pmod{11}$$

$$\equiv 2a_2 + 5 \pmod{11}$$

これより,

$$2a_2 + 5 \equiv 0 \pmod{11}$$

を満たす a_2 ($0 \leq a_2 \leq 9$) を考えると, $a_2 = 3$ が見つかる ($2 \times 3 + 5 = 11$ より).

3 授業を終えて

「大切なものは失って初めて気づく」のが世の常であるが、ISBNコードでは入力時の

- 任意の1箇所のミス
- 任意の2箇所の入れ替わり

を検出することができ（訂正はできない）,

- 任意の1箇所について**消失訂正**

まで行うことができる。

その理屈を初めて知った時、「上手いこと考える人があるもんだ!」と感心した記憶がある。自分が数学の教員を志したのは、「自分が面白いと感じたものを伝えたい!」という思いからであり、ISBNコードについてもどこかで扱いたいと考えていた。

授業時の生徒の反応は概ね良好で、面白がって問題に取り組んでくれた。「誰かに教えたい雑学になりました!」という感想もあった。

ISBNコードは題材として、

- 簡単すぎず、難しすぎない
- 意外性がある
- 身の回りにある

という点で、優れていると考える。また、生徒のレベルや扱う時間数、時期によって

- 性質を確認し、具体例で遊ぶ
- 理論的な考察を行う
- 他の例についても触れる

など、様々な取扱いが可能である。今回の実践では、整数論入門ということで、互除法・一次不定方程式（4時間）、合同式・ISBNコード（4時間）という配当で行った。

他の例については、最後に2つ挙げたので、参考にしていただきたい。何れも、コンピュータ関連で実際に使われているものである。

理論的な考察をするのであれば、ISBNの持つ性質を証明させてみるというのもよいだろう。その例を1つ挙げる。

定理 ISBNコードは、任意の2箇所の数字が入れ替わってしまった入力誤りを検出できる。

すなわち、

$$a_k = b_k \quad (k \neq i, j)$$

$$a_i = b_j, a_j = b_i \quad (i \neq j)$$

のとき、

$$\sum_{k=1}^{10} a_k \cdot k \not\equiv \sum_{k=1}^{10} b_k \cdot k \pmod{11}$$

が成り立つ。

証明 $a_k = b_k \quad (k \neq i, j)$ であることより、

$$\begin{aligned} & \sum_{k=1}^{10} a_k \cdot k - \sum_{k=1}^{10} b_k \cdot k \\ &= (a_i \cdot i + a_j \cdot j) - (b_i \cdot i + b_j \cdot j) \\ &= (a_i \cdot i + a_j \cdot j) - (a_j \cdot i + a_i \cdot j) \\ &= a_i(i - j) - a_j(i - j) \\ &= (a_i - a_j)(i - j) \end{aligned}$$

ここで、 $1 \leq i, j \leq 10, i \neq j$ より、

$$0 < |i - j| \leq 9 \quad (1)$$

が成り立ち、同様に、 $0 \leq a_i, a_j \leq 10, a_i \neq a_j$ より、

$$0 < |a_i - a_j| \leq 10 \quad (2)$$

が成り立つ。(1)(2)と、11が素数であることより、 $(a_i - a_j)(i - j)$ は11の倍数とはなり得ない。

よって、

$$\sum_{k=1}^{10} a_k \cdot k - \sum_{k=1}^{10} b_k \cdot k \not\equiv 0 \pmod{11}$$

すなわち

$$\sum_{k=1}^{10} a_k \cdot k \not\equiv \sum_{k=1}^{10} b_k \cdot k \pmod{11}$$

であることが示された。

Q.E.D

4 終わりに

データに情報を付け加え、安全性・正確性を向上させることを**冗長化**という。実例を2つ挙げるが、ともに、mod2で演算を行う。排他的論理和 (XOR: \oplus) を考えるととってもよい。

例7 (パリティ) サーバ等で用いられる RAID では、パリティを作成し冗長化を行うものがある。

Data1
0
0
1
1

 \oplus

Data2
0
1
0
1

 \Rightarrow

Parity
0
1
1
0

事故により、1台のデータが欠損してしまうと

Data1
☠
☠
☠
☠

Data2
0
1
0
1

Parity
0
1
1
0

となるが、残りの2台で排他的論理和を考えると

Data1
0
0
1
1

 \Leftarrow

Data2
0
1
0
1

 \oplus

Parity
0
1
1
0

となり、欠損したデータの復元ができる。

例8 (ハミング符号) 誤り検出能力と併せて、**誤り訂正能力**も持っている。

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

をそれぞれ、生成行列、パリティ検査行列という。 $u = [1\ 0\ 0\ 1]$ を $v = uG$ によって符号化する。

$$v = uG = [1\ 0\ 0\ 1\ 1\ 0\ 0]$$

となる。右側の $[1\ 0\ 0]$ の部分が、誤り訂正のために追加された情報である。

誤り検出・訂正は、 vH^T によって判断できる。 v が誤りを含まなければ、

$$vH^T = 0$$

が成り立つ。誤りを含んでいれば、 $vH^T \neq 0$ となり、誤りを検出し訂正することができる。

v の一部を改変した、 $v' = [1\ 0\ 1\ 1\ 1\ 0\ 0]$ で考えてみると、

$$v'H^T = [0\ 1\ 1]$$

となり、 H の3列目と一致している。このことは、 v' の3番目が誤りであることを示している。

現行の ISBN コードを紹介して、本稿を終える。

— 現行の ISBN コード —

ISBN □□□ - ○ - ●●-△△△△△△-☆

- 「□□□」は 978 または 979 のいずれかである。
- 残りの部分は、旧規格と同じである。

ISBN コードで現れる各桁の数字を右から、 a_1, a_2, \dots, a_{13} とする時、

$$\sum_{k=1}^7 a_{2k-1} + \sum_{k=1}^6 a_{2k} \cdot 3 \equiv 0 \pmod{10}$$

が成り立つように、チェックディジット a_1 の値を定める。

つまり、右から奇数番目の数字の和に、偶数番目の数字に3を乗じたものの和を加え、10の倍数になるように定める。

(注) ISBN の ○ - ●● - △△△△△△ の各部分の桁数は、地域や出版社によって変化する (現規格・旧規格ともに)。

参考文献

- [1] G.A. ジョーンズ, J.M. ジョーンズ
「情報理論と符号理論」シュプリンガー・ジャパン
- [2] 「数学セミナー 2004年6月号」日本評論社
- [3] 日本図書コード管理センター
<http://www.isbn-center.jp/>