1+1+・・・+1=0?

（1 をいくつか足しても０？）

吉村浩 著

山口数理科学出版会

はじめに[†]

カレンダーは「$1+1+1+1+1+1+1=0$ の世界」?

次の問題を考えてみましょう.

問題 1 2003 年 10 月 8 日は水曜日です. 1 年後の 10 月 8 日は何曜日でしょうか. ただし, 2004 年はうるう年[1] であることに注意してください.

この問題を考えるために, 2003 年 10 月のカレンダーを見てみましょう.

2003 年 10 月

日	月	火	水	木	金	土
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

このカレンダーの数 (日にち) の配列で気づくことは何でしょう? ここで問題となっている水曜日にあたる日にちを書き上げると, 次のようになります.

$$1,\ 8,\ 15,\ 22,\ 29.$$

これらの数にはどういう規則があるのでしょう? すぐわかるように, 最初の数 1 に 7 ずつ足していった数が並んでいます. つまり, 1, 8, 15, 22, 29 に共通するのは

7 で割ると余りが 1

になるということです. あるいは, 1, 8, 15, 22, 29 の

どの 2 つの数の差も 7 で割り切れる

ということもできます. 他の曜日についても同様です. 実際に, 日にちを 7 で割った余りをカレンダーの下に書いていくと, 次のようになります.

[†]本稿は, 「総合演習」(理学部 2 年共通講義, 2003 年 10 月 8 日, 15 日) での講義ノートをもとにしたものです.

[1]**知っていましたか?** 夏季オリンピックやアメリカ大統領選挙の年を, 'うるう年' と覚えている人もいるでしょう. そもそも 'うるう年' は, 次のように決められています.

「西暦年が 4 で割り切れる年を 'うるう年' とする. 例外として, 西暦年が 100 で割り切れ, さらに 400 で割り切れない年は平年 (365 日) とする.」

ですから 2004 年は 'うるう年' です. また, 2000 年は例外条件をくぐり抜け, 'うるう年' でした.

日	月	火	水	木	金	土
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	
5	**6**	**0**	**1**	**2**	**3**	**4**

各列のどの数も 7 で割ったときの余りが等しい.

このようにカレンダーは, 日にちを 7 で割って余りが等しいものを**同一視**して, それぞれ日, 月, 火, ... とよぶわけですね. カレンダーは 31 日までしかありませんが, わたしたちが日常使う**自然数**[2] を 7 で割った余りを表にしてみましょう.

自然数	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	⋯
7 で割った余り	0	1	2	3	4	5	6	0	1	2	3	4	5	6	0	1	2	⋯

このように, 自然数を “7 で割った余りの数 (剰余) の世界” から見たとき

$$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6$$

という 7 つの数が順次繰り返し現れます. したがって, 上の表の 2 行目の任意の数とそれから右側に 7 つ進んだ数は同じです. このように “7 で割った剰余の世界” は,

7 つ増えると振り出しに戻る数の世界

といえます. このことはまさに「曜日」の性質をいい換えたものに過ぎません (今日とその 7 日後の曜日は同じですね).

それでは, ここで問題 1 を考えてみましょう. わかっていることは次の 2 つです.

- 2003 年 10 月 8 日は水曜日.
- 2004 年 10 月 8 日は 366 日後.

そこで, 366 を 7 で割り算してみましょう. すると

$$366 = 52 \times 7 + 2$$

となります. これを “7 で割った剰余の世界” から見れば

「366 は 52 回振り出しに戻って, それから 2 つ進んだ数である」

といえます. したがって, 問題 1 の答えは水曜日から 2 つ進んだ金曜日となります.

[2] 普通 1, 2, 3, ... を自然数といいますが, ここでは 0 も含めることにします.

どうでしょうか. このようにカレンダーは, “7で割った剰余” に基づいていることがわかりました. また, “7で割った剰余の世界” は, “7つ増えると振り出しに戻る数の世界” であるといいました. これを数式で書くとすれば, 次のようになるでしょうか.

$$\mathbf{1+1+1+1+1+1+1=0}\quad \textbf{(1の7個の和が0).}$$

この「7」という数は曜日の数に対応したものでしたが, これを任意の自然数に置き換えてみましょう. すなわち, n を任意に選んだ1つの自然数 (ただし, $n \geqq 2$) とし, 次を考えます.

$$\underbrace{\mathbf{1+1+\cdots+1}}_{\boldsymbol{n}\textbf{個}} = \mathbf{0}\quad \textbf{(1の}\boldsymbol{n}\textbf{個の和が0).}$$

それにしても, “1の n 個の和が0” になるなんてナンセンスでしょうか? 実際, 普通

$$\underbrace{1+1+\cdots+1}_{n\text{個}} = n\quad (1\text{の}n\text{個の和は}n)$$

となるわけですから. また, 自然数 0, 1, 2, ... やそのマイナスの数 -1, -2, ... は無限にあるわけですが, “1の n 個の和が0となる数の世界” では,

数は有限個しかない

ことが示されます. ならばなおのこと「そんなのあり?」と思われるでしょうか. ところが, 実はそのような数の世界 (体系) を考えることができ, しかもそれはナンセンスどころか, 様々な数理現象に現れる重要な体系で, さらにわたしたちの日常生活の中でも意外なところに応用されています. その様子の一端をこれから見ていきましょう.

“1の n 個の和が0となる数の体系”

- $\underbrace{1+1+\cdots+1}_{n\text{個}} = 0$
- 数は有限個しかない.

目 次

1　代数系 $\mathbb{Z}$

これから, “1 の n 個の和が 0 となる数の体系” を考えていくわけですが, このときの “数の体系” という言葉の意味を明確にしておきましょう.

ここでは, わたしたちにとって最も身近な数である, 自然数 0, 1, 2, 3, ... とそのマイナスの数 -1, -2, -3, ..., すなわち **整数** をモデルにして, “数の体系” というものを考えます. そのために, 整数の集合ではどのようなことが成り立っているか見てみましょう. 以降, 整数全体を $\mathbb{Z}$ という記号で表すことにします[3].

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

整数に関して最も重要なことは, 整数どうしは足し算と掛け算ができるという事実です. 実際, わたしたちが生まれて初めて数を覚え, その次に習うのが数の足し算と掛け算です. この足し算と掛け算について, $\mathbb{Z}$ は次の法則を満たしていることがわかります (以下, a, b, c, ... という文字で整数を表すことにします).

法則 1.1 (整数全体 $\mathbb{Z}$ が満たす法則)

(I) 和 (足し算) $a+b$ と 積 (掛け算) $a \times b$ ができる *.

(II) 和に関する法則.

(1) $a+b=b+a$ (交換法則).

(2) $(a+b)+c=a+(b+c)$ (結合法則).

(3) 任意の a に対し, $a+0=a$ を満たす.

(4) 任意の a に対し, ある b が存在し $a+b=0$ を満たす.
(b は ‘a のマイナス’ $-a$ である).

(III) 積に関する法則.

(1) $ab=ba$ (交換法則).

(2) $(ab)c=a(bc)$ (結合法則).

(3) $a(b+c)=ab+ac$ (分配法則).

(4) 任意の a に対し, $a \cdot 1=a$ を満たす.

* a と b の積 $a \times b$ を, $a \cdot b$ または単に ab で表したりします.

このように法則として書くと, 一見, なにやら難しいことをいっているようにもみえます. しかし, よく見れば, わたしたちが小学校で初めて数の足し算と掛け算を習い, 以来ごく当たり前のように使っている性質ばかりです. わたしたちが数を

[3] $\mathbb{Z}$ はドイツ語で数を表す Zahl に由来します.

計算するとき, あまり意識されませんが, 実はこの法則に基づいて行っています. この法則は, 数の和や積の根底にある最も基本的な法則なのです[4].

注意 1.2 一般に, 集合の 2 つの**元**[5] に対して 1 つの元を定める規則を, **演算**とよびます. この言葉を使えば, 法則 (1.1) の (I) は次のようにいえます.

集合 $\mathbb{Z}$ には, 和と積の 2 つの演算が定まっている.

ここで重要なことは, $\mathbb{Z}$ は和と積に関して**閉じている**こと, すなわち 2 つの整数の和と積はまた整数になるということです. 一方, 整数どうしの割り算の結果は一般に整数ではないので (例 $1 \div 2 = \frac{1}{2}$), $\mathbb{Z}$ は割り算に関して閉じていません. したがって, 割り算は法則 (1.1) には含まれていないのです. 「それなら引き算はどうしたの ?」と思われるかもしれません. 確かに, $\mathbb{Z}$ は引き算に関して閉じています (整数から整数を引くとまた整数ですね). 実は, a から b を引くというのは,

$$a - b = a + (-b)$$

です. すなわち, 引き算は, 和とマイナスの数 (法則 (1.1) の II(4)) によって定められるので, 引き算も法則 (1.1) に含まれているといえます.

このように, 整数の集合 $\mathbb{Z}$ は, 和と積の 2 つの演算が定められ, 法則 (1.1) を満たす "数の体系" です. そこで一般に, この $\mathbb{Z}$ のように, 2 つの演算 (和と積) が定められた集合で, その元 a, b, c に対して, 法則 (1.1) の (II)(III) を満たすものを, "数の体系" とよぶことにします (このとき, (II)(3)(4) と (III)(4) にある '0' と '1' とは何なのか, 気になるかもしれません. その詳しい意味は, 次節で考えることにします). これを数学の用語を使って, 法則 (1.1) を満たす**代数系**[6] とよぶことにしましょう. したがって, $\mathbb{Z}$ は法則 (1.1) を満たす代数系といえます. また "1 の n 個の和が 0 となる数の体系" とは,

"1 の n 個の和が 0" となるような, 法則 (1.1) を満たす代数系

ということになります. 以降, これを単に "1 の n 個の和が 0" の代数系 とよぶことにします. そのような代数系を次節で考えます.

整数全体 $\mathbb{Z}$ は法則 (1.1) を満たす代数系である.

[4]例えば, 法則 (1.1) を使って, 整数に関する次のような事実を示すことができます.

(1) $-(-a) = a$ (2) $0 \times a = 0$ (3) $(-1) \times (-1) = 1$ (4) $(-a) \times (-b) = ab$.

[5]集合は, いくつかの 'もの' をひとまとめにした 'ものの集まり' です. その集合を構成している個々の 'もの' を**元**といいます. 例えば, 「整数 3 は集合 $\mathbb{Z}$ の元である」といういい方をします.

[6]一般に, 演算が定められた集合を代数系とよびますが, 中でも重要な法則を満たす代数系には固有の名称が付いています. 例えば, 法則 (1.1) を満たす代数系は, **環 (ring)** とよばれます.

2　代数系 $\mathbb{Z}_n$ (“1 の n 個の和が 0” の代数系)

n を任意の整数 (ただし, $n \geqq 2$) とします. この節で “1 の n 個の和が 0” の代数系を構成しましょう. これを以降, $\mathbb{Z}$ の下に n を付けて, $\mathbb{Z}_n$ で表すことにします. 注意として, n は 2 以上の整数であれば何でも構いませんが, n の取り方によって構成される代数系 $\mathbb{Z}_n$ は全く異なったものになります. つまり, 異なる整数 n ($\geqq 2$) ごとに, 異なる代数系 $\mathbb{Z}_n$ が存在するわけです.

整数 n	$\Longrightarrow$	**代数系** $\mathbb{Z}_n$	
整数 2	$\longrightarrow$	代数系 $\mathbb{Z}_2$	(“1 の 2 個の和が 0” の代数系)
整数 3	$\longrightarrow$	代数系 $\mathbb{Z}_3$	(“1 の 3 個の和が 0” の代数系)
	$\vdots$		
整数 100	$\longrightarrow$	代数系 $\mathbb{Z}_{100}$	(“1 の 100 個の和が 0” の代数系)
	$\vdots$		

それでは, いまから代数系 $\mathbb{Z}_n$ を次の手順で構成していきます.

(1) $\mathbb{Z}_n$ を構成する元を定める.

(2) $\mathbb{Z}_n$ の演算 (和と積) を定める.

(3) $\mathbb{Z}_n$ は法則 (1.1) を満たし, さらに “1 の n 個の和が 0” となることを示す.

2.1　$\mathbb{Z}_n$ の元

これから構成する代数系 $\mathbb{Z}_n$ は, もちろん代数系 $\mathbb{Z}$ とは性質の異なるものですが, 実は $\mathbb{Z}$ を基に構成されます.

わたしたちは, 代数系 $\mathbb{Z}$ の元 (すなわち整数) を表すために, $0, 1, 2, \ldots, -1, -2, \ldots$ という記号 (アラビア数字) を使います. この記号の上にバー (¯) を付けたものを, $\mathbb{Z}_n$ の元とします[7]. したがって, $\mathbb{Z}_n$ を構成する元は次の通りです.

$$\ldots,\ \overline{\mathbf{-3}},\ \overline{\mathbf{-2}},\ \overline{\mathbf{-1}},\ \overline{\mathbf{0}},\ \overline{\mathbf{1}},\ \overline{\mathbf{2}},\ \overline{\mathbf{3}},\ \ldots$$

ここで, これら個々の元が何を意味しているのかは考慮しません. というのも, 代数系というは, それを構成する個々の元が何であるかは問題ではなく, 演算という ‘2 つの元の間の関係性’ (演算構造) に関して定義される概念だからです. したがって, 整数 a の上にバーの付いた単なる記号 $\bar{a}$ 全てからなる集合を $\mathbb{Z}_n$ とし, そこに和と積の演算を定めていくわけです.

[7] 整数 n ごとに, $\mathbb{Z}_n$ は異なる代数系であると注意しました. したがって, 厳密にいえば, $\mathbb{Z}_n$ の元を表すために, 整数 n に応じて異なる記号を導入する必要があります. しかし, そこで考えている n がどういう整数かを明確に意識しておけば, 同じ記号 $\bar{a}$ を使っても混乱は起きないでしょう.

このように, $\mathbb{Z}_n$ の元を $\overline{a}$ (a は整数) として定めたわけですが, 例えば $5 \neq 19$ (整数 5 と整数 19 は異なる) となることから, $\mathbb{Z}_n$ においても $\overline{5} \neq \overline{19}$ と思われるかもしれません. しかし, $\overline{5} \neq \overline{19}$ あるいは $\overline{5} = \overline{19}$ のいずれになるかはわかりません. というのも, $\mathbb{Z}_n$ のいかなる元が等しいのか, すなわち $\mathbb{Z}_n$ の 2 つの元 $\overline{a}$ と $\overline{b}$ に対し,

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

となるための条件について, まだ何も述べていないからです. では, これを次のように定義しましょう.

定義 2.1 ($\mathbb{Z}_n$ の元の相等)

整数 a と b を n で割ったときの余りが等しいとき, $\overline{a} = \overline{b}$ と定義する.

a と b を n で割ったときの余りが等しいということは, $a - b$ が n で割り切れることに他なりません. したがって, 次のようにいい換えても構いません.

定義 2.2 ($\mathbb{Z}_n$ の元の相等)

整数 $a - b$ が n で割り切れるとき, $\overline{a} = \overline{b}$ と定義する.

例 2.3 先ほどの $\mathbb{Z}_n$ の 2 つの元 $\overline{5}$ と $\overline{19}$ の相等を考えてみましょう. 定義 (2.2) によれば, 5 と 19 との差の数

$$5 - 19 = -14$$

が, n で割り切れるかそうでないかが問題となります. 例えば $n = 2$ のとき, -14 は 2 で割り切れますから

$$\mathbb{Z}_2 \text{ において}, \overline{5} = \overline{19}$$

となります. 一方, 例えば $n = 3$ のとき, -14 は 3 で割り切れませんから

$$\mathbb{Z}_3 \text{ において}, \overline{5} \neq \overline{19}$$

となります. このように, 2 つの元の $\mathbb{Z}_n$ における相等は, 整数 n の取り方によって異なるわけです. いま, 整数 -14 を割り切る 2 以上の整数を全て書き上げると

$$2,\ 7,\ 14$$

の 3 つです. したがって, $\overline{5}$ と $\overline{19}$ の相等は次のようになります.

$$\begin{cases} \mathbb{Z}_2,\ \mathbb{Z}_7 \text{ または } \mathbb{Z}_{14} \text{ において}, & \overline{5} = \overline{19} \\ \mathbb{Z}_n\ (n \neq 2, 7, 14) \text{ において}, & \overline{5} \neq \overline{19}. \end{cases}$$

例 2.4 $n=3$ のときの $\mathbb{Z}_3$ を考えます. 例えば, $6-(-6)=12$ は 3 で割り切れるので, $\overline{6}=\overline{-6}$ です. 一方, $8-13=-5$ は 3 で割り切れないので, $\overline{8}\neq\overline{13}$ となります. ところで, 任意の整数を 3 で割ると, その余りは 0 か 1 か 2 のいずれかです. したがって, $\mathbb{Z}_3$ は見かけ上, 無限個の元

$$\ldots,\overline{-100},\ldots,\overline{-3},\overline{-2},\overline{-1},\overline{0},\overline{1},\overline{2},\overline{3},\ldots,\overline{100},\ldots$$

からなっていますが, 実は各々の元は $\overline{0}$, $\overline{1}$, $\overline{2}$ のいずれかに等しいわけです. 等しいものどうし並べてみると, 次のようになります.

$$\begin{aligned}
\cdots &= \overline{-6} = \overline{-3} = \mathbf{\overline{0}} = \overline{3} = \overline{6} = \cdots \quad (3\text{で割って余りが}0)\\
\cdots &= \overline{-5} = \overline{-2} = \mathbf{\overline{1}} = \overline{4} = \overline{7} = \cdots \quad (3\text{で割って余りが}1)\\
\cdots &= \overline{-4} = \overline{-1} = \mathbf{\overline{2}} = \overline{5} = \overline{8} = \cdots \quad (3\text{で割って余りが}2).
\end{aligned}$$

したがって, 次のようになります.

$$\mathbb{Z}_3=\{\overline{0},\ \overline{1},\ \overline{2}\}\quad(\mathbb{Z}_3\text{ は }3\text{ つの元からなる}).$$

例 2.5 $n=2$ のときの $\mathbb{Z}_2$ は, もっとも簡単な代数系です. 前の例と同様に, $\mathbb{Z}_2$ において等しい元を並べてみると, 次のようになります.

$$\begin{aligned}
\cdots &= \overline{-4} = \overline{-2} = \mathbf{\overline{0}} = \overline{2} = \overline{4} = \cdots \quad (2\text{で割って余りが}0,\text{すなわち偶数})\\
\cdots &= \overline{-3} = \overline{-1} = \mathbf{\overline{1}} = \overline{3} = \overline{5} = \cdots \quad (2\text{で割って余りが}1,\text{すなわち奇数}).
\end{aligned}$$

したがって, 次のようになります.

$$\mathbb{Z}_2=\{\overline{0},\ \overline{1}\}\quad(\mathbb{Z}_2\text{ は }2\text{ つの元からなる}).$$

例 (2.4) と例 (2.5) で述べたことは, 一般の $\mathbb{Z}_n$ においても成り立ちます. つまり, 任意の整数を n で割った余りは 0, 1, ..., $n-1$ のいずれかです. したがって

$\mathbb{Z}_n$ は n 個の元からなる.

$$\mathbb{Z}_n=\{\overline{0},\ \overline{1},\ \overline{2},\ \ldots,\ \overline{n-1}\}.$$

注意 2.6 $\mathbb{Z}_n$ では, n で割った余りが等しい整数全てを同一視して, 1 つの元と見なすわけです. したがって, $\mathbb{Z}_n$ は "整数を n で割った余りの数 (剰余) の体系 " ともいえます.

$$\begin{aligned}
\mathbf{\overline{0}}&:\ n\text{で割って余りが}0\text{の整数全体の代表}\\
\mathbf{\overline{1}}&:\ n\text{で割って余りが}1\text{の整数全体の代表}\\
\mathbf{\overline{2}}&:\ n\text{で割って余りが}2\text{の整数全体の代表}\\
&\vdots\\
\mathbf{\overline{n-1}}&:\ n\text{で割って余りが}n-1\text{の整数全体の代表}.
\end{aligned}$$

ここで, 次の問題を, いま述べた $\mathbb{Z}_n$ の性質を使って考えてみましょう.

問題 2 あるマラソン大会で $n+1$ 人 $(n \geqq 2)$ が完走したとします. このとき, タイムを秒で計時したとして, タイム差が n の倍数であるような完走者が 2 人いることを示してください. (例えば, 完走者が 112 人の場合, そのタイム差が 111 の倍数, すなわち 0 秒 (同着), 111 秒, 222 秒, ... のいずれかであるような 2 人が存在する).

解答. 完走者 $n+1$ 人のタイムを $a_1, a_2, \ldots, a_n, a_{n+1}$ (秒) とします. いま, $\mathbb{Z}_n$ において, $\overline{a_1}, \overline{a_2}, \ldots, \overline{a_n}, \overline{a_{n+1}}$ を考えると, $\mathbb{Z}_n$ は n 個の元からなるので, これら見かけ上 $n+1$ 個の $\mathbb{Z}_n$ の元のうち, 少なくとも 2 つは等しいはずです. その 2 つを $\overline{a_i}$ と $\overline{a_j}$ とすると,

$$\mathbb{Z}_n \text{ において, } \overline{a_i} = \overline{a_j}$$

すなわち, $a_i - a_j$ が n で割り切れます. したがって, タイムがそれぞれ a_i と a_j となる 2 人のタイム差 $a_i - a_j$ は, n の倍数です. ■

2.2 $\mathbb{Z}_n$ の和と積

代数系における和や積などの演算というのは, 2 つの元に対して 1 つの元を定める規則のことでした. それでは, $\mathbb{Z}_n$ における和と積の記号をそれぞれ, $\oplus$, $\otimes$ と表すことにして[8], それらを次のように定義しましょう.

定義 2.7 ($\mathbb{Z}_n$ の和と積)

和： $\overline{a} \oplus \overline{b} = \overline{a+b}$

積： $\overline{a} \otimes \overline{b} = \overline{a \cdot b}$

(※ 右辺の $+$ と $\cdot$ は整数の和と積).

この定義を少し詳しく書けば, 次のようになります.

和： $\overline{a} \oplus \overline{b} = \overline{r}$, ただし, r は整数 a と b の和 $a+b$ を n で割った余り.

積： $\overline{a} \otimes \overline{b} = \overline{s}$, ただし, s は整数 a と b 積の $a \cdot b$ を n で割った余り.

このように演算を定義したとき, まず確認しなければいけないことは, この演算に矛盾がないことです. つまり,

等しいものどうしの和や積はまた等しい

[8] この $\mathbb{Z}_n$ における演算記号 $\oplus$ と $\otimes$ は, 整数の場合と同様に $+$ と $\times$ を用いても構いません. 実際, 記号の節約のためにもそうするのが普通です. ただし, その場合注意しないといけないのは, 考えている代数系における $+$ と $\times$ の意味 (定義) を明確にしておくということです.

ということ, すなわち

$$\left.\begin{array}{l}\overline{a}=\overline{c}\\ \overline{b}=\overline{d}\end{array}\right\} \Longrightarrow \left\{\begin{array}{l}\overline{a}\oplus\overline{b}=\overline{c}\oplus\overline{d}\\ \overline{a}\otimes\overline{b}=\overline{c}\otimes\overline{d}\end{array}\right.$$

が成り立つということです. 「こんなのあたりまえじゃないの」という人も, 次の例を見てください.

例 2.8 $\mathbb{Z}_3$ において, $\overline{5}=\overline{8}$, $\overline{-2}=\overline{13}$ です. これら等しいものどうしを辺々足すと,

$$\begin{array}{lll}\overline{5}\oplus\overline{-2} & =\overline{5+(-2)} & = \overline{3}\\ \overline{8}\oplus\overline{13} & =\overline{8+13} & = \overline{21}\end{array}$$

となります. ここで, 「等しいものどうしの和はまた等しい」とすれば, $\overline{3}=\overline{21}$ となるはずです. 実際, $3-21=-18$ は 3 で割り切れるので, $\overline{3}=\overline{21}$ となっています. したがって,

$$\overline{5}\oplus\overline{-2}=\overline{8}\oplus\overline{13}$$

が成り立ちます. 同様に, 積の場合は

$$\begin{array}{lll}\overline{5}\otimes\overline{-2} & = \overline{5\cdot(-2)} & = \overline{-10}\\ \overline{8}\otimes\overline{13} & = \overline{8\cdot 13} & = \overline{104}.\end{array}$$

ここで, $(-10)-104=-114$ は 3 で割り切れるので, $\overline{-10}=\overline{104}$ となっています. したがって, 積の場合も

$$\overline{5}\otimes\overline{-2}=\overline{8}\otimes\overline{13}$$

が成り立ちます.

これがどんな場合にも成り立つことが, 次のように示されます.

定理 2.9 $\mathbb{Z}_n$ の元 $\overline{a}$, $\overline{b}$, $\overline{c}$, $\overline{d}$ が,

$$\overline{a}=\overline{c},\quad \overline{b}=\overline{d}$$

を満たしているとする. このとき, 次が成り立つ.

$$\overline{a}\oplus\overline{b}\ =\ \overline{c}\oplus\overline{d},\quad \overline{a}\otimes\overline{b}\ =\ \overline{c}\otimes\overline{d}.$$

証明. $\overline{a}=\overline{c}$ より, $a-c$ は n で割り切れるので, $a-c=np$ (p はある整数) と書けます. 同様に, $\overline{b}=\overline{d}$ より, $b-d=nq$ (q はある整数) と書けます. よって,

$$a=c+np,\quad b=d+nq.$$

このとき,

$$a+b=(c+np)+(d+nq)=(c+d)+n(p+q).$$

これより,

$$(a+b)-(c+d)=n(p+q).$$

したがって, $(a+b)-(c+d)$ は n で割り切れるので, $\overline{a+b}=\overline{c+d}$, すなわち $\overline{a}\oplus\overline{b}=\overline{c}\oplus\overline{d}$ が成り立ちます. 同様に,

$$ab=(c+np)(d+nq)=cd+n(cq+dp+npq)$$

となります. これより

$$ab-cd=n(cq+dp+npq).$$

したがって, $ab-cd$ は n で割り切れるので, $\overline{ab}=\overline{cd}$, すなわち $\overline{a}\otimes\overline{b}=\overline{c}\otimes\overline{d}$ が成り立ちます. ■

2.3 $\mathbb{Z}_n$ は“1 の n 個の和が 0”の代数系

ではこの節の目標である, $\mathbb{Z}_n$ は法則 (1.1) を満たし, “1 の n 個の和が 0” の代数系であることを示していきましょう.

考えている $\mathbb{Z}_n$ における和と積は, 定義 (2.7) で定められた $\oplus$ と $\otimes$ です. したがって, $\mathbb{Z}_n$ が法則 (1.1) を満たすということは, 法則 (1.1) にある和・積 $(+,\cdot)$ と a, b, c を, それぞれ $\mathbb{Z}_n$ の和・積 $(\oplus,\otimes)$ と $\mathbb{Z}_n$ の元 $\overline{a}$, $\overline{b}$, $\overline{c}$ に置き換えたものを $\mathbb{Z}_n$ が満たす, ということを意味します. では, 実際にそれを示しましょう.

定理 2.10 $\mathbb{Z}_n$ は法則 (1.1) を満たす代数系である.

証明. まず, 法則 (1.1) の (I) は, $\mathbb{Z}_n$ の和と積の定義 (2.7) と定理 (2.9) によります.

次に, 法則 (1.1) の (II)(1)(2) と (III)(1)(2)(3) をよく見てください. これらは代数系 $\mathbb{Z}$ が満たす法則でした. 一方, $\mathbb{Z}_n$ の和 $\oplus$ と積 $\otimes$ の定義では, 整数の和 $+$ と積 $\cdot$ を使っています (定義 (2.7) の 2 つの定義式のそれぞれの右辺). したがって, $\mathbb{Z}_n$ が (II)(1)(2) と (III)(1)(2)(3) を満たすのは当然 (?). といっても念のために 1 つ, (III)(3) だけ示してみます (残りも同様にできますので, 示してみてください).

$$\begin{aligned}
\overline{a}\otimes(\overline{b}\oplus\overline{c}) &= \overline{a}\otimes(\overline{b+c}) && (\mathbb{Z}_n\text{の和の定義より})\\
&= \overline{a(b+c)} && (\mathbb{Z}_n\text{の積の定義より})\\
&= \overline{ab+ac} && (\mathbb{Z}\text{が (III)(3) を満たすことより})\\
&= \overline{ab}\oplus\overline{ac} && (\mathbb{Z}_n\text{の和の定義より})\\
&= (\overline{a}\otimes\overline{b})\oplus(\overline{a}\otimes\overline{c}) && (\mathbb{Z}_n\text{の積の定義より}).
\end{aligned}$$

したがって, $\overline{a}\otimes(\overline{b}\oplus\overline{c})=(\overline{a}\otimes\overline{b})\oplus(\overline{a}\otimes\overline{c})$ が成り立つことが示されました.

最後に, (II)(3)(4) と (III)(4) が成り立つことは, 次を見ればわかるでしょう.

- $\overline{a} \oplus \overline{0} = \overline{a+0} = \overline{a}$
- $\overline{a} \oplus \overline{-a} = \overline{a+(-a)} = \overline{0}$
- $\overline{a} \otimes \overline{1} = \overline{a \cdot 1} = \overline{a}$.

つまり, 代数系 $\mathbb{Z}$ の 0, 1, $-a$ に相当するのが, $\mathbb{Z}_n$ においては $\overline{0}$, $\overline{1}$, $\overline{-a}$ となるわけです. 以上より, $\mathbb{Z}_n$ は法則 (1.1) を満たす代数系であることが示されました. ■

上の定理の証明の最後に述べたことを, 少し詳しく見てみましょう.

代数系 $\mathbb{Z}$ において 0 と 1 は, 法則 (1.1) のそれぞれ (II)(3) と (III)(4) を満たす整数に他なりません. 一般に, 和と積が定められた代数系において, このように

- **任意の元 a に対し, $a + x = a$ を満たすような元 x**
- **任意の元 a に対し, $a \cdot y = a$ を満たすような元 y**

が, それぞれただ 1 つ存在します. この x と y をその代数系のそれぞれ, **零元**と**単位元**とよびます[9]. したがって, 代数系 $\mathbb{Z}$ の零元は整数 0, 単位元は整数 1 となります. 一方, 代数系 $\mathbb{Z}_n$ の零元は $\overline{0}$, 単位元は $\overline{1}$ となるわけです.

	代数系 $\mathbb{Z}$	代数系 $\mathbb{Z}_n$
零元	0	$\overline{0}$
単位元	1	$\overline{1}$

これまで, "1 の n 個の和が 0" となる代数系, という表現を使ってきましたが, 実は正確には, **"単位元の n 個の和が零元" となる代数系**, という意味で使っていたわけです. 代数系 $\mathbb{Z}$ においては, もちろん

$$\underbrace{1+1+\cdots+1}_{n\text{個}} = n$$

すなわち, $\mathbb{Z}$ は "1 の n 個の和が n" となる代数系です. 一方, 代数系 $\mathbb{Z}_n$ においては

$$\underbrace{\overline{1} \oplus \overline{1} \oplus \cdots \oplus \overline{1}}_{n\text{個}} = \underbrace{\overline{1+1+\cdots+1}}_{n\text{個}} = \overline{n} = \overline{0}$$

となります. すなわち, 次のことがいえたわけです.

$\mathbb{Z}_n$ は, "1 の n 個の和が 0" となる代数系である.

$$\underbrace{\overline{1} \oplus \overline{1} \oplus \cdots \oplus \overline{1}}_{n\text{個}} = \overline{0}.$$

[9] 代数系の零元と単位元を, 整数の場合と同様の記号 0 と 1 で表すのが一般です.

2.4 代数系 $\mathbb{Z}_n$ の演算表

代数系の 2 つの元の和と積を定める, 次のような表を**演算表**といいます.

$+$	a	b	c	$\cdots$
a	$*$	$*$	$*$	$\cdots$
b	$*$	$*$	x	$\cdots$
c	$*$	$*$	$*$	$\cdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\ddots$

これは, 和に関する演算表で (左上隅に和の記号 $+$ がある), 第 1 列 (一番左の列) と第 1 行 (一番上の行) には, 代数系の元を順番に対応するように並べます. そして, 第 1 列に並んでいる 1 つの元と, 第 1 行に並んでいる 1 つの元とが交差する欄に, それらの和の値を記入します. 例えばこの表では, 第 3 行にある b と第 4 列にある c の和が x である, すなわち $b + c = x$ であることを示しています. このように, 代数系の全ての元の演算関係を表にすることによって, 演算構造を一目でとらえることができるわけです.

次の例で, いくつかの n に対して, 代数系 $\mathbb{Z}_n$ の演算表を見てみましょう.

例 2.11 以下の表では, $\mathbb{Z}_n$ の元 $\overline{a}$ を簡単のために, 単に a で表すことにします. したがって, $\mathbb{Z}_n$ の演算表を作るには, 第 1 行と第 1 列に並べたそれぞれの数の和または積を普通に計算して, それを n で割った余りを所定の位置に書き込んでいけばよいわけです. では, 実際に $n = 2, 3, 4$ の場合の演算表を見てみましょう.

(1) $n = 2$ のとき.

$\oplus$	0	1
0	0	1
1	1	0

$\otimes$	0	1
0	0	0
1	0	1

$\mathbb{Z}_2$ の演算表

(2) $n = 3$ のとき.

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_3$ の演算表

(3) $n = 4$ のとき.

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

$\otimes$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_4$ の演算表

注意 2.12 一般に, 代数系において割り算が可能であるということは, 0 (零元) でない任意の元 a に対し, $a \cdot b = 1$ (単位元) となる元 b (すなわち, a の**逆元** $\frac{1}{a}$) が, その代数系の中に存在することに他なりません. 代数系 $\mathbb{Z}$ は割り算ができない代数系です (なぜなら, 例えば, 整数 2 の逆元 $\frac{1}{2}$ は整数ではないから).

例 (2.11) の積に関する演算表をよく見ると, 代数系 $\mathbb{Z}_2$ と $\mathbb{Z}_3$ においては, 0 でない各々の元は逆元をもつことがわかります. したがって, $\mathbb{Z}_2$ と $\mathbb{Z}_3$ は割り算が可能な代数系です. 一方, 代数系 $\mathbb{Z}_4$ においては, 1 と 3 は逆元をもちますが ($1 \times 1 = 1$, $3 \times 3 = 1$), 2 は逆元をもちません. したがって, $\mathbb{Z}_4$ は割り算ができない代数系です.

では, どのような $\mathbb{Z}_n$ が割り算可能な代数系なのでしょうか? 実は, 次のことが知られています.

定理 2.13 整数 n ($\geqq 2$) が素数[10] のとき, 代数系 $\mathbb{Z}_n$ は割り算可能な代数系である.

割り算可能な代数系を**体 (field)** といいます. したがって, n が素数のとき, 代数系 $\mathbb{Z}_n$ は有限個の元からなる**有限体**です. 次の節で簡単な例を見ますが, 代数系の中でも特にこの有限体は, 現代のデジタル情報の通信技術を支える理論において, とても重要な役割を果たします.

注意 2.14 これまで, n は 2 以上の整数として, "1 の n 個の和が 0 " となる代数系 $\mathbb{Z}_n$ を見てきました. では, $n = 1$ のときの代数系, すなわち

$$1 \ = \ 0$$

となる代数系というのは考えられるのでしょうか? 実は, この節で述べた代数系 $\mathbb{Z}_n$ についての議論は, $n = 1$ としてもそのまま成り立ちます. ただし, そのときの代数系 $\mathbb{Z}_1$ は, ただ 1 つの元からなる代数系になることがわかります. このような特殊というか 'つまらない' 代数系は除外して考えるのが普通です.

[10] 2 以上の整数 n は, 1 とそれ自身の他に約数 (n を割り切る数) をもたないとき, **素数**といいます. いま, 20 までの素数を順番にあげていくと, 2, 3, 5, 7, 11, 13, 17, 19 となります. 最初の 2 以外の素数は全て奇数です.

代数系 $\mathbb{Z}_n$ について, これまでのことをまとめてみましょう. 以降簡単のために, $\mathbb{Z}_n$ の和 $\oplus$ と 積 $\otimes$ を, 整数の場合と同様の記号 $+$ と $\cdot$ で表します.

代数系 $\mathbb{Z}_n$ のまとめ： 整数 n $(\geqq 2)$ に対し, 代数系

$$\begin{aligned} \mathbb{Z}_n &= \{\overline{0},\ \overline{1},\ \overline{2},\ \ldots,\ \overline{n-1}\} \\ \text{和} \quad \overline{a}+\overline{b} &= \overline{a+b} \\ \text{積} \quad \overline{a}\cdot\overline{b} &= \overline{a\cdot b} \end{aligned}$$

は, 代数系 $\mathbb{Z}$ と同様に, 法則 (1.1) を満たしている. また, 次が成り立つ.

$$\underbrace{\overline{1}+\overline{1}+\cdots+\overline{1}}_{n\text{個}} = \overline{0}.$$

代数系 $\mathbb{Z}$ と代数系 $\mathbb{Z}_n$ との間には, 次の関係がある.

代数系 $\mathbb{Z}$		**代数系 $\mathbb{Z}_n$**
a を n で割った余りが r	$\Longleftrightarrow$	$\overline{a}=\overline{r}$
a が n で割り切れる	$\Longleftrightarrow$	$\overline{a}=\overline{0}$
$a-b$ が n で割り切れる	$\Longleftrightarrow$	$\overline{a}=\overline{b}$

代数系 $\mathbb{Z}_n$ は, **標数 n の有限環**とよばれます.

3　代数系 $\mathbb{Z}_n$ の応用

最後に, 代数系 $\mathbb{Z}_n$ のいくつかの応用を見てみましょう. その前に, 代数系 $\mathbb{Z}_n$ の元の累乗に関する注意を 1 つしておきます.

いま, $\overline{a}$ を代数系 $\mathbb{Z}_n$ の元, k を自然数とします. このとき, 定義 (2.7) による $\mathbb{Z}_n$ の積を繰り返し行えば, $\mathbb{Z}_n$ において次の等式が成り立つことがわかります.

$$\underbrace{\overline{a} \times \overline{a} \times \cdots \times \overline{a}}_{k\text{ 個}} \;=\; \overline{\underbrace{a \times a \times \cdots \times a}_{k\text{ 個}}}.$$

ここで, 念のために, この等式の左辺と右辺にある積の記号 $\times$ は, それぞれ代数系 $\mathbb{Z}_n$ と代数系 $\mathbb{Z}$ における積を表すことに注意しておきます. そこで, 整数 a の k 乗の表記 a^k と同様に, $\overline{a}^k$ は $\overline{a}$ の k 個の積を表すとします. すなわち

$$\overline{a}^{\,k} \;=\; \underbrace{\overline{a} \times \overline{a} \times \cdots \times \overline{a}}_{k\text{ 個}}.$$

このように $\overline{a}$ の k 乗 $\overline{a}^k$ を定めると, 最初にあげた等式は次のようになります.

$$\boldsymbol{\overline{a}^{\,k} \;=\; \overline{a^k}}.$$

これはとても簡単な等式ですが, 以下の問題からもわかるように, 整数の剰余の計算においてとても有効です.

3.1　いくつかの問題への応用

「はじめに」で述べたカレンダーの曜日は, 代数系 $\mathbb{Z}_7$ に基づいているといえます. では, $\mathbb{Z}_7$ を使って, 次の問題を考えてみましょう.

問題 3　今日 (水曜日) から 1000 日後は何曜日でしょうか.

解答.　$1000 = 10^3$ であることと, 代数系 $\mathbb{Z}_7$ において $\overline{10} = \overline{3}$ であることに注意すれば,

$$\overline{1000} = \overline{10^3} = \overline{10}^{\,3} = \overline{3}^{\,3} = \overline{3^3} = \overline{27}$$

となります. ここで, $\mathbb{Z}_7$ において $\overline{27} = \overline{6}$ より,

$$\overline{1000} = \overline{6}.$$

したがって, 答えは水曜日の 6 日後の火曜日です. あるいは, $\mathbb{Z}_7$ において $\overline{27} = \overline{-1}$ より, $\overline{1000} = \overline{-1}$ なので, 水曜日の 1 日前の火曜日ともいえます. ■

次の様な問題を見れば, 代数系 $\mathbb{Z}_n$ の威力を実感できるでしょうか.

問題 4 次の余りを求めてください.

(1) 9^{134} を 8 で割った余り[11].

(2) 9^{134} を 7 で割った余り.

解答. (1) 代数系 $\mathbb{Z}_8$ において $\overline{9} = \overline{1}$ より,

$$\overline{9^{134}} = \overline{9}^{134} = \overline{1}^{134} = \overline{1^{134}} = \overline{1}.$$

したがって, 余りは 1 です.

(2) 代数系 $\mathbb{Z}_7$ において $\overline{9} = \overline{2}$ より,

$$\overline{9^{134}} = \overline{9}^{134} = \overline{2}^{134} = \overline{2^{134}}.$$

ここで, $134 = 44 \times 3 + 2$ と, $\mathbb{Z}_7$ において $\overline{8} = \overline{1}$ に注意して

$$\overline{2^{134}} = \overline{2^{44\times 3+2}} = \overline{(2^3)^{44} \times 2^2} = \overline{(2^3)^{44}} \times \overline{2^2} = \overline{2^3}^{44} \times \overline{2^2} = \overline{8}^{44} \times \overline{4} = \overline{1}^{44} \times \overline{4} = \overline{4}.$$

したがって, 余りは 4 です. ■

問題 5 自然数 n に対して, $n^3 + 2n$ は 3 で割り切れることを示してください.

解答. 代数系 $\mathbb{Z}_3$ において $\overline{2} = \overline{-1}$ より, $\overline{n^2+2} = \overline{n^2-1}$ となります. よって,

$$\overline{n^3+2n} = \overline{n(n^2+2)} = \overline{n(n^2-1)} = \overline{n(n-1)(n+1)} = \overline{n-1} \times \overline{n} \times \overline{n+1}.$$

ここで, $n-1$, n, $n+1$ は 3 つの連続する整数ですから, いずれか 1 つは 3 で割り切れます. すなわち, $\mathbb{Z}_3$ において $\overline{n-1}$, $\overline{n}$, $\overline{n+1}$ のいずれか 1 つは $\overline{0}$ です. よって,

$$\overline{n^3+2n} = \overline{n-1} \times \overline{n} \times \overline{n+1} = \overline{0}.$$

したがって, $n^3 + 2n$ は 3 で割り切れます. ■

問題 6 次の等式を満たす整数 a, b は存在するでしょうか.

$$a^2 + b^2 = 2003.$$

解答. a と b を任意の整数とすると, 代数系 $\mathbb{Z}_4$ において $\overline{a}$ と $\overline{b}$ は, $\overline{0}$, $\overline{1}$, $\overline{2}$, $\overline{3}$ のいずれかです. よって, $\overline{a}^2$ と $\overline{b}^2$ がとり得る値は

$$\overline{0}^2 = \overline{0},\ \overline{1}^2 = \overline{1},\ \overline{2}^2 = \overline{4} = \overline{0},\ \overline{3}^2 = \overline{9} = \overline{1}$$

[11] 実は, $9^{134} = 7387479093976217392533236523128439258832358029253553362339645949992280047443570448292192120102916499388111334653484766491271576 1$ です. さてこの数字は何桁？

すなわち, $\overline{0}$ か $\overline{1}$ のいずれかです. よって, $\overline{a}^2+\overline{b}^2$ $(=\overline{a^2+b^2})$ がとり得る値は,

$$\overline{0}\ (=\overline{0}+\overline{0}),\ \ \overline{1}\ (=\overline{0}+\overline{1}=\overline{1}+\overline{0}),\ \ \overline{2}\ (=\overline{1}+\overline{1})$$

の 3 つのうちのいずれかです. 一方, $\mathbb{Z}_4$ において, $\overline{2003}=\overline{3}$ です. 以上より,

$$\text{代数系 } \mathbb{Z}_4 \text{ において, } \overline{a^2+b^2}\ =\ \overline{2003}$$

となることはあり得ません. ここで, もし整数 a, b に対して, $a^2+b^2=2003$ が成り立つとすると, 上の等式が成り立つので, そのような整数 a, b は存在しません. ■

上の問題の整数 2003 は素数です (確認できますか?). 実は, 一般に素数に関して次のことが知られています.

定理 3.1 素数 p $(\neq 2)$ が $p=a^2+b^2$ $(a,b$ は整数) と書けるための必要十分条件は

$$\text{代数系 } \mathbb{Z}_4 \text{ において, } \overline{p}=\overline{1}$$

すなわち, p を 4 で割った余りが 1 となることである (付録 A 参照).

代数系 $\mathbb{Z}_9$ を使えば, 次のようなこともわかります.

例 3.2 与えられた整数 a が 9 で割り切れるかどうかを考えます. もちろん, 割り算を行えばわかるわけですが, ここではもっと簡単な方法を考えてみましょう.

例えば, 整数 $a=8512$ は, $8512=2+1\times 10+5\times 10^2+8\times 10^3$ と書けます. そこで, 一般に整数 a を, 次のように十進法で表すことにします.

$$a=a_0+a_1\times 10+a_2\times 10^2+\cdots+a_n\times 10^n$$
ただし, $a_0,a_1,a_2,\ldots,a_n$ は 0 から 9 までの整数.

このとき, 代数系 $\mathbb{Z}_9$ において, $\overline{10}=\overline{10^2}=\cdots=\overline{10^n}=\overline{1}$ より,

$$\begin{aligned}\overline{a} &= \overline{a_0+a_1\times 10+a_2\times 10^2+\cdots+a_n\times 10^n}\\ &= \overline{a_0}+\overline{a_1}\times\overline{10}+\overline{a_2}\times\overline{10^2}+\cdots+\overline{a_n}\times\overline{10^n}\\ &= \overline{a_0}+\overline{a_1}+\overline{a_2}+\cdots+\overline{a_n}\\ &= \overline{a_0+a_1+a_2+\cdots+a_n}\end{aligned}$$

となります. したがって, $\overline{a}=\overline{0}$ であるためには, $\overline{a_0+a_1+a_2+\cdots+a_n}=\overline{0}$ であることが必要十分です. すなわち, 次のことが示されました.

a が 9 で割り切れる $\Leftrightarrow$ $a_0+a_1+a_2+\cdots+a_n$ が 9 で割り切れる.

例えば, 整数 $a=37521$ に対し, $3+7+5+2+1=18$ は 9 で割り切れるので, 37521 も 9 で割り切れます. また, 整数 $a=568417$ に対し, $5+6+8+4+1+7=31$ は 9 で割り切れないので, 568417 も 9 で割り切れません (実際に割り算を行ってみてください). 代数系 $\mathbb{Z}_{11}$ を使って同様に考えれば, 次のことも示されます.

a が 11 で割り切れる $\Leftrightarrow$ $a_0-a_1+a_2-a_3+\cdots$ が 11 で割り切れる.

3.2　符号理論への応用

「符号理論」や「暗号理論」といった言葉を耳にしたことがあるでしょうか？普段の日常生活でもあまり聞く言葉ではありませんので, 意識されないかもしれません. しかし, これらの理論は, この情報化社会における情報の通信に, 今や欠くことのできない技術を支えるものです[12]. 例えば, みなさんがコンビニエンス・ストアなどで購入した商品パッケージの裏には, 次の様な**バーコード**とよばれる白黒のシマシマ模様が印刷されています.

これに読み取り装置 (バーコードリーダー) を当てるだけで, 商品名や金額などの情報がレジに入力されるわけです. バーコードは符号理論を応用した 1 例です. 実は, 代数系 $\mathbb{Z}_n$ はこの符号理論や暗号理論の数学的な基礎となるものです. ここでは, 代数系 $\mathbb{Z}_n$ の符号理論へのもう 1 つの簡単な応用例として, **ISBN コード**を見てみましょう.

ここに 1 冊の本「無限からの光芒」(志賀浩二著) があります. その裏表紙を見ると, 次のような記号が書かれています.

$$\text{ISBN}\,4-535-78161-3 \quad \text{C3041} \quad ¥3600\text{E}$$

みなさんが書店で購入した本にも, このような記号が書かれていることでしょう. この記号の後半の C3041 は本の分類番号で，¥3600E は価格を表しています．ここで問題にするのは, 前半の

$$\textbf{ISBN 4 – 535 – 78161 – 3}$$

です． 先頭の ISBN は, 書籍に関する国際的規格である International Standard Book Number (国際標準図書番号) の略で, それ以降の数字がこの本の書籍番号となります. 世界中で流通している各々の書籍には, 2 つとないその書籍固有の ISBN が付いており, したがって ISBN がわかれば, その書籍を特定できるわけです．この番号が表しているのは, 次の通りです.

4	–	535	–	78161	–	3
↑		↑		↑		↑
国番号		**出版社コード**		**書籍コード**		**チェックコード**.

[12]符号理論 (coding theory) は, デジタル化された情報が誤って通信されても, それを正しく復元する技術の基礎となる理論です. 衛星通信や音楽 CD などの実用化は, この理論が裏付けになっています. 一方, 暗号理論 (cryptography theory) は, インターネットなどによってやりとりする文書や画像などの情報を, 通信途中で第三者に盗み見られたり, 改ざんされたりしないように変換するための技術の基礎となる理論です.

最初から 3 つの「国番号」,「出版社コード」,「書籍コード」の桁数は, 一定ではありません. 例えば, 日本の国番号は 4 で, スペインの国番号は 84 です. しかし, 最後の「チェックコード」の桁数は必ず 1 桁で, 全部で 10 個の数字からなります[13]. また, 途中にある 3 つのハイフン (−) は省略されていることもあります.

さて, この ISBN と代数系 $\mathbb{Z}_n$ との関係ですが, 実は

ISBN は 代数系 $\mathbb{Z}_{11}$ に基づいている

のです[14]. この様子を簡単に見てみましょう.

いま, ISBN の 10 個の数字を順に $a_1, a_2, \ldots, a_{10}$ とし,

$$\text{ISBN } a_1 - a_2a_3a_4 - a_5a_6a_7a_8a_9 - a_{10}$$

とします. このとき, 次の 2 つの規則があります.

規則 1. $a_1 \sim a_9$ までは $0 \sim 9$ までの数字とる.

規則 2. 最後の a_{10} は $0 \sim 10$ までの数字で[15], 次の等式を満たすようにとる.

代数系 $\mathbb{Z}_{11}$ において, $a_1 + 2a_2 + 3a_3 + \cdots + 10a_{10} = 0$.
(すなわち, 整数 $a_1 + 2a_2 + 3a_3 + \cdots + 10a_{10}$ は 11 で割り切れる).

この規則により, 特に最後の数字 a_{10} は, $a_1 \sim a_9$ までの数字でただ 1 つに決まってしまうことがわかります. したがって, ISBN は, 実際には 9 桁の番号で書籍を識別していることになります. この ISBN は, 次のような利点をもちます.

(1) **ISBN の 10 桁の数字のうち 1 つが誤って伝えられても, その情報が誤っていることがわかる.**

(2) **ISBN の 10 桁の数字のうち 2 つが誤って入れ換わって伝えられても, その情報が誤っていることがわかる.**

例えば 1 冊の本 (ISBN $4-535-78161-3$) を, この番号によって注文するとします. このとき, 何らかの理由で誤って, 例えば 3 番目の数字「3」が「2」になったり, あるいは 5 番目と 6 番目の数字「7」と「8」が入れ換わって注文されたとします. ところが, 注文を受けた側は, これらの情報が誤っていることがわかるのです. 何か手品のようにも見えますが, 代数系 $\mathbb{Z}_{11}$ の性質を使えば, このからくりがわかります (付録 B 参照).

---

[13]ただし, 近年の書籍出版数の増加に対応するため, 2005 年より 10 桁から 13 桁の ISBN に移行される予定です.

[14]代数系 $\mathbb{Z}_{11}$ が使われる理由は, 11 が 10 以上の素数のうち最小であるからだと思われます. したがって, 定理 2.13 より, $\mathbb{Z}_{11}$ は割り算可能な代数系です.

[15]ただし, a_{10} が 10 の場合, ISBN の桁数が 11 桁になるので, 10 の代わりに X (ギリシャ文字の 10) を使います.

4　付録

4.1　$p = a^2 + b^2$ と書ける素数 p

以下は, 1000 までの素数の一覧表です. そのうち太字は, $p = a^2 + b^2$ (a, b は整数) と書ける素数 p を表します (実際にそのような素数 p を, $p = a^2 + b^2$ と表してみては ?).

1000 **までの素数表**

2	3	**5**	7	11	**13**	**17**	19	23	**29**	31	**37**	**41**	43	47
53	59	**61**	67	71	**73**	79	83	**89**	**97**	**101**	103	107	**109**	**113**
127	131	**137**	139	**149**	151	**157**	163	167	**173**	179	**181**	191	**193**	**197**
199	211	223	227	**229**	**233**	239	**241**	251	**257**	263	**269**	271	**277**	**281**
283	**293**	307	311	**313**	**317**	331	**337**	347	**349**	**353**	359	367	**373**	379
383	**389**	**397**	**401**	**409**	419	**421**	431	**433**	439	443	**449**	**457**	**461**	463
467	479	487	491	499	503	**509**	**521**	523	**541**	547	**557**	563	**569**	571
577	587	**593**	599	**601**	607	**613**	**617**	619	631	**641**	643	647	**653**	659
661	**673**	**677**	683	691	**701**	**709**	719	727	**733**	739	743	751	**757**	**761**
769	**773**	787	**797**	**809**	811	**821**	823	827	**829**	839	**853**	**857**	859	863
877	**881**	883	887	907	911	919	**929**	**937**	**941**	947	**953**	967	971	**977**
983	991	**997**												

4.2　3.2 節の (1)(2) の証明

いま,

$$\text{ISBN } a_1 - a_2a_3a_4 - a_5a_6a_7a_8a_9 - a_{10}$$

とします. 規則 2 により, 代数系 $\mathbb{Z}_{11}$ において,

$$a_1 + 2a_2 + 3a_3 + \cdots + 10a_{10} = 0 \quad \cdots (*)$$

です. この i 番目 ($1 \leqq i \leqq 10$) の数字 a_i が, 誤って a_i' になったとします. この誤った番号は, 規則 2 に従っていないことがわかります. 実際に, 代数系 $\mathbb{Z}_{11}$ において,

$$\begin{aligned}
&a_1 + 2a_2 + \cdots + ia_i' + \cdots + 10a_{10} && (※\ a_i'\text{は間違った数字}) \\
&= a_1 + 2a_2 + \cdots + ia_i + \cdots + 10a_{10} + i(a_i' - a_i) \\
&= i(a_i' - a_i) && (※\ \text{等式 } (*) \text{ より}) \\
&\neq 0 && (※\ i \neq 0, a_i' - a_i \neq 0 \text{ より}).
\end{aligned}$$

すなわち, 誤った番号は規則 2 に従っていないことが示されました.

次に, i 番目の数字 a_i と j 番目の数字 a_j ($1 \leqq i < j \leqq 10$) が, 誤って入れ換わったとします. ここで, $a_i = a_j$ ならば, 入れ換わっていても問題はありませんので, $a_i \neq a_j$ とします. このとき, 代数系 $\mathbb{Z}_{11}$ において,

$$\begin{aligned}
&a_1 + 2a_2 + \cdots + ia_j + \cdots + ja_i + \cdots + 10a_{10} && (※\ a_i\text{と } a_j\text{は入れ換わった数字}) \\
&= \{(a_1 + 2a_2 + \cdots + ia_i + \cdots + ja_j + \cdots + 10a_{10}) - (ia_i + ja_j)\} + \{ia_j + ja_i\} \\
&= -(ia_i + ja_j) + (ia_j + ja_i) && (※\ \text{等式 } (*) \text{ より}) \\
&= (j - i)(a_i - a_j) \\
&\neq 0 && (※\ j - i \neq 0, a_i - a_j \neq 0 \text{ より}).
\end{aligned}$$

すなわち, 誤って入れ換わった番号は, 規則 2 に従っていないことが示されました.

$1+1+\cdots+1=0$？ (1 をいくつか足しても 0？)

2004 年 4 月　第 1 版　発行

著者　吉村　浩

発行　山口数理科学出版会