平成２８年度教員免許状更新講習

整数

北海道教育大学中標津会場 平成２８年８月９日

目 次

1　はじめに

最近、高校数学Aに、ユークリッドの互除法などの整数に関する内容がいくつか盛り込まれました。これらは、少なくとも数十年の間、高校数学で大きくは取り上げられていなかったので、この講習では、これらの内容の背景や関連する話題を取り扱ってみます。予備知識はあまり仮定しませんが、証明に対する慣れは多少必要かも知れません。

はじめに自然数や整数の定義や、演算の定義を復習します。そして、これらの定義だけからいろいろな計算規則が導出されることを体験し、普段当然と思っていたり、証明に触れる機会のなかったことがらにも数学的な基礎付けがあることを見てみます。

素因数分解は自然数の性質の中でも非常に重要なものですが、素因数分解が可能であることに比べて分解の一意性はあまり意識されないかも知れません。一意性にも焦点を当てその応用を見てみます。

最古のアルゴリズムと言われるユークリッドの互除法は、2つの自然数の最大公約数を求める最速の方法です。応用範囲も非常に広く、その一端を見てみます。

最後に有理数や実数にも触れますが、代数系としての性質には深入りせず、無限集合としての性質を中心に見てみます。例えば、有理数と自然数の「濃度」が等しいことに2通りの証明を与えます。

この講習が、わずかでも日頃の教育活動のお役に立てばさいわいです。

2　整数の定義・基本的な性質

ここでは、自然数や整数の定義、演算の定義をし、その定義からいろいろな計算規則が導出されることを見ます。

2.1　自然数の定義 (ペアノの公理)

自然数は非常に基本的な数の集合ですが、19 世紀末まで数学的に厳密な定義は与えられていませんでした。数学者のクロネッカーも「整数は神の作ったものだが、他は人間の作ったものである」と言っており、自然数 (や整数) があり、諸性質を満たすことは当然のものとして盲目的に認めて、その先の議論は厳密に行うという立場だったようです。

現在では、同値な定義がいくつかありますが、みなさんが一番ご存知だと思われるのは、次のペアノの公理でしょう。

定義 1 (ペアノの公理 (1891))**.** 集合 S があり、$n \in S$ に対して「n の後者」n' があるとする。このような集合 S に対して次の公理を考える。

(P1) $1 \in S$ である。
(P2) $n \in S$ に対して、$n' \in S$ である。
(P3) $n \in S$ のとき、$n' \neq 1$ である。
(P4) $a, b \in S$ に対して、$a \neq b$ ならば $a' \neq b'$ である。
(P5) 「$n \in S$ に関する命題 Q が $n = 1$ のとき成立し、命題 Q が $n = k$ の時成立するならば $n = k'$ のときも成立する」ならば、命題 Q は任意の $n \in S$ に対して成立する。

この公理を満たす集合 S を**自然数**の集合と呼び $\mathbb{N}$ で表す。また、(P5) による証明方法を**数学的帰納法**と呼ぶ。

この定義にある、$a \in A$ という記号は、集合 A に要素 (元) a が属しているという意味です。また、自然数に 0 を含める流儀もあります。

ひとつ注意しておくと、自然数の定義というのは少し不正確で、正確には自然数とは何であるかの定義というべきかも知れません。つまり、(普段よく使っていてよく知っている) 自然数がペアノの公理を満たすことは明らかです。しかし、そういうことではなく、(今まで見たことも考えたこともない) ある集合がペアノの公理を満たしていれば、それを自然数の集合と呼ぼうということです。従って、ペアノの公理だけでは自然数の集合の存在は保証されません。

この公理の意義がどこにあるかと言うと、数学的に厳密な議論が可能になったこと、自然数のいろいろな性質がこれらの条件のみから得られること、逆にどれかが欠けると得られなくなることなどがあります。つまり、自然数を簡潔に整理された条件で定義したことにあると言えます。そこに数学的帰納法が入っていることは、それが自然数の本質に関わるということですから興味深くもあります。

2.2 自然数の定義 (ツェルメロの方法)

さて、ペアノの公理とは別の、同値な、自然数の定義もあります。以下に紹介するツェルメロの案を元にする自然数の定義は、ペアノの公理よりも直観的でわかりやすいと考える人も多いと思います。また、ツェルメロの方法は自然数を実際に構成しているので、自然数の集合の存在を保証しています。

例えば、4 個の要素を持つ集合というのは、無数に考えられますが、それらの総称を「4」と名付ける、というように、有限な n 個の要素を持つ集合の総称として自然数「n」を定めます。この定義だと、自然数 4 は無数の集合の総称ですから、それらを代表して、$\{0, 1, 2, 3\}$ という集合をとることができます。つまり、これと

1 対 1 対応の付く集合の総称を「4」と定めています。

しかし、自然数を定義している最中なので「3」などを用いるのは気を付けないと循環論法に陥ってしまいますから、正確には、

$$
\begin{aligned}
&0 = \emptyset \quad (\text{空集合}) \\
&1 = \{0\} = \{\emptyset\} \\
&2 = \{0, 1\} = \{\emptyset, \{\emptyset\}\} \\
&3 = \{0, 1, 2\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} \\
&\vdots
\end{aligned}
$$

というように、未定義の記号を使わないようにして帰納的に定義をします。

2.3 不完全性定理

物理好きの一般の方の興味を引く代表的話題は相対性理論だと思いますが、数学だとゲーデルの不完全性定理だと思います。せっかくですから、この機会に少しだけ触れます。

数学が矛盾を含めば大変なことになります。背理法を使えば、何でも証明できてしまうので、すべての主張が真 (かつ偽) になり、その体系は無意味なものになってしまいます。数を含まない数学 (正確には 1 階の述語論理と呼ばれる体系) は矛盾を含まないことが知られていましたが (これもゲーデルの定理)、自然数を含む数学の体系は矛盾を含むのかどうかが未解決だった時代があります。ゲーデルは、自然数を含めた数学の体系に矛盾があるのかないのかは証明できない、ということを証明しました。これが**不完全性定理**です。

この定理によれば、従来の数学が矛盾のない意味のある体系だと証明ができないわけですから一大事なのですが、「その体系の中では」証明できないというのが定理の正確な主張で、さらに別のものを体系に組み込めば無矛盾であることが証明できます。ですから、現在の数学が無意味であると思う数学者はいないといってよいでしょう。

2.4 自然数の和の定義

ペアノの公理を採用して、自然数に和や積を定義してみます。ここではまず和を定義します。ペアノの公理では、$1, 1', 1'', \ldots$ とダッシュが多数付いたものが自然数なのですが、これらを $1, 2, 3, \ldots$ と表すことにします[1]。

[1]騙されている感じがするかも知れませんが、ダッシュだらけの表記でも、以下の議論がすべて通用することが確認できますので、騙しているわけではなく、単に表記を簡単にしたということです。

定義 2 (自然数の和)**.** 自然数の和を次で帰納的に定める。

(i) $n \in \mathbb{N}$ に対して、$n+1 = n'$ と定める。
(ii) $m, n \in \mathbb{N}$ に対して、$m + n' = (m+n)'$ と定める。

(ii) を言い換えると、$m + (n+1) = (m+n) + 1$ となり、限定的な結合法則を表していることがわかります。

例 3. (1) $1 + 1 = 2$. これは ($1'$ の表記の) 定義によります。
(2) $2 + 1 = 3$. これも ($2' = 1''$ の表記の) 定義によります。
(3) $1 + 2 = 3$. 上の 2 つには「定義だ」とぶっきら棒に答え、この質問には目を輝かせて「それは良い質問だね」と答えるというジョークがあります。

$$1 + 2 \overset{\text{表記の定義}}{=} 1 + 1' \overset{\text{(ii)}}{=} (1+1)' \overset{\text{(i)}}{=} (1')' \overset{\text{表記の定義}}{=} 3$$

ここで、等号の上の (i) などは、定義 2 の (i) などを用いたという意味です。

問題 4. 定義に基いて計算せよ。
(1) $3 + 2$　(2) $2 + 3$

結合法則や交換法則が、和の定義から証明できますが、その準備として次の補題を証明します。

補題 5. 自然数 n に対して、$1 + n = n'$ が成立する[2]。つまり、$1 + n = n + 1$ が成立する。

(証明) n に関する数学的帰納法で証明します。
1. $n = 1$ の場合 は、(左辺) $= 1 + 1 \overset{\text{(i)}}{=} 1' =$ (右辺) だから補題は成立しています。
2. n まで補題が成立すると仮定すると、$n+1$ の場合 は、

$$(\text{左辺}) = 1 + (n+1) \overset{\text{(i)}}{=} 1 + n' \overset{\text{(ii)}}{=} (1+n)' \overset{\text{帰}}{=} (n')' \overset{\text{(i)}}{=} (n+1)' = (\text{右辺})$$

となり、$n+1$ の場合も補題は成立しています。ただし、途中の「帰」は帰納法の仮定を用いたという意味です。

以上より、すべての自然数 n に対して補題が証明されました。 □

この補題も活用して、和の結合法則と交換法則が証明できます。

[2] $n + 1 = n'$ ならば定義から直ちにわかりますが、和の交換法則が未証明なので、今のところ $1 + n = n'$ は直ちにはわかりません。

定理 6 (和の結合法則、交換法則)**.** 自然数 $l, m, n \in \mathbb{N}$ に対して、次が成り立つ。

(1) $(l+m)+n = l+(m+n)$
(2) $m+n = n+m$

(証明) (1) n に関する数学的帰納法で証明します。

1. $n=1$ の場合は、(左辺) $= (l+m)+1 \overset{\text{(i)}}{=} (l+m)' \overset{\text{(ii)}}{=} l+m' \overset{\text{(i)}}{=} l+(m+1) =$ (右辺) だから定理 (1) は成立しています。

2. n まで定理 (1) が成立すると仮定すると、$n+1$ の場合は、

$$\begin{aligned}
(\text{左辺}) &= (l+m)+(n+1) \\
&\overset{\text{(i)}}{=} (l+m)+n' \\
&\overset{\text{(ii)}}{=} ((l+m)+n)' \\
&\overset{\text{帰}}{=} (l+(m+n))' \\
&\overset{\text{(ii)}}{=} l+(m+n)' \\
&\overset{\text{(ii)}}{=} l+(m+n') \\
&\overset{\text{(i)}}{=} l+(m+(n+1)) = (\text{右辺})
\end{aligned}$$

となり、$n+1$ の場合も定理 (1) は成立しています。

以上より、すべての自然数 n に対して定理 (1) が証明されました。

(2) n に関する数学的帰納法で証明します。

1. $n=1$ の場合は、補題 5 より成立します。

2. n まで定理 (2) が成立すると仮定すると、$n+1$ の場合は、

$$\begin{aligned}
(\text{左辺}) &= m+(n+1) \\
&\overset{\text{(i)}}{=} m+n' \\
&\overset{\text{(ii)}}{=} (m+n)' \\
&\overset{\text{(帰)}}{=} (n+m)' \\
&\overset{\text{(ii)}}{=} n+m' \\
&\overset{\text{補題 5}}{=} n+(1+m) \\
&\overset{\text{(1)}}{=} (n+1)+m = (\text{右辺})
\end{aligned}$$

となり、$n+1$ の場合も定理 (2) は成立しています。ただし、途中の「帰」は帰納法の仮定を用いたという意味で、「(1)」は証明の済んでいる、この定理の (1) を用いたという意味です。

以上より、すべての自然数 n に対して定理 (2) が証明されました。 □

2.5 自然数の積の定義

次に自然数の積を定義します。

定義 7 (自然数の乗法)**.** 自然数の積を次で帰納的に定める。

(i) $n \in \mathbb{N}$ に対して、$n \cdot 1 = n$ と定める。
(ii) $m, n \in \mathbb{N}$ に対して、$m \cdot n' = m \cdot n + m$ と定める。

つまり、同数累加で定めているといえます。

例 8. 和の計算はわかっているものとして、積の計算をしてみます。

$$3 \cdot 2 \overset{\text{表記の定義}}{=} 3 \cdot 1' \overset{\text{(ii)}}{=} 3 \cdot 1 + 3 \overset{\text{(i)}}{=} 3 + 3 \overset{\text{和は既知}}{=} 6$$

ここで、等号の上の (i) などは、定義 7 の (i) などを用いたという意味です。

問題 9. 和の計算はわかっているものとして、積 $2 \cdot 3$ の計算をせよ。

補題 10. 自然数 $n \in \mathbb{N}$ に対して、$1 \cdot n = n$ が成立する。つまり、$1 \cdot n = n \cdot 1$ が成立する。

(証明) n に関する数学的帰納法で証明します。

1. $n = 1$ の場合 は、(左辺) $= 1 \cdot 1 \overset{\text{(i)}}{=} 1$ となり、補題は成立しています。
2. n まで補題が成立すると仮定すると、$n+1$ の場合 は、

$$\begin{aligned}
(\text{左辺}) &= 1 \cdot (n+1) \\
&= 1 \cdot n' \\
&\overset{\text{(ii)}}{=} 1 \cdot n + 1 \\
&\overset{\text{帰}}{=} n + 1 \\
&= n' \\
&= n + 1 = (\text{右辺})
\end{aligned}$$

となり、$n+1$ の場合も補題は成立しています。ただし、途中の「帰」は帰納法の仮定を用いたという意味です。

以上より、すべての自然数 n に対して補題が証明されました。 □

定理 11 (積の交換法則・結合法則、分配法則)**.** $l, m, n \in \mathbb{N}$ に対して、次が成り立つ。

(1) $l \cdot (m+n) = l \cdot m + l \cdot n$
(2) $(l+m) \cdot n = l \cdot n + m \cdot n$
(3) $(l \cdot m) \cdot n = l \cdot (n \cdot m)$
(4) $m \cdot n = n \cdot m$

(証明) (1) n に関する数学的帰納法で証明します。

1. $n = 1$ の場合 は、(左辺) $= l \cdot (m+1) = l \cdot m' \overset{\text{(ii)}}{=} l \cdot m + l \overset{\text{(i)}}{=} l \cdot m + l \cdot 1 =$ (右辺) となり、定理 (1) は成立しています。

2. n まで定理 (1) が成立すると仮定すると、$n+1$ の場合 は、

$$\begin{aligned}
(\text{左辺}) &= l \cdot (m + (n+1)) \\
&= l \cdot (m + n') \\
&= l \cdot (m+n)' \\
&\overset{\text{(ii)}}{=} l \cdot (m+n) + l \\
&\overset{\text{帰}}{=} l \cdot m + l \cdot n + l \\
&\overset{\text{(ii)}}{=} l \cdot m + l \cdot n' \\
&= l \cdot m + l \cdot (n+1) = (\text{右辺})
\end{aligned}$$

となり、$n+1$ の場合も定理 (1) は成立しています。ただし、途中の「帰」は帰納法の仮定を用いたという意味です。

以上より、すべての自然数 n に対して定理 (1) が証明されました。

(2) も n に関する数学的帰納法を用いて証明できますが、省略します (是非練習してみて下さい)。

(3) n に関する数学的帰納法で証明します。

1. $n = 1$ の場合 は、(左辺) $= (l \cdot m) \cdot 1 \overset{\text{(i)}}{=} l \cdot m \overset{\text{(i)}}{=} l \cdot (m \cdot 1) =$ (右辺) となり、定理 (3) は成立しています。

2. n まで定理 (3) が成立すると仮定すると、$n+1$ の場合 は、

$$
\begin{aligned}
(\text{左辺}) &= (l \cdot m) \cdot (n+1) \\
&= (l \cdot m) \cdot n' \\
&\overset{\text{(ii)}}{=} (l \cdot m) \cdot n + l \cdot m \\
&\overset{\text{帰}}{=} l \cdot (m \cdot n) + l \cdot m \\
&\overset{\text{(1)}}{=} l \cdot ((m \cdot n) + m) \\
&\overset{\text{(ii)}}{=} l \cdot (m \cdot n') \\
&= l \cdot (m \cdot (n+1)) = (\text{右辺})
\end{aligned}
$$

となり、$n+1$ の場合も定理 (3) は成立しています。ただし、途中の「帰」は帰納法の仮定を用いたという意味です。

以上より、すべての自然数 n に対して定理 (3) が証明されました。

(4) n に関する数学的帰納法で証明します。

1. $n=1$ の場合 は、$(\text{左辺}) = m \cdot 1 \overset{\text{補題}\,10}{=} 1 \cdot m = (\text{右辺})$ となり、定理 (4) は成立しています。

2. n まで定理 (4) が成立すると仮定すると、$n+1$ の場合 は、

$$
\begin{aligned}
(\text{左辺}) &= m \cdot (n+1) \\
&= m \cdot n' \\
&\overset{\text{(ii)}}{=} m \cdot n + m \\
&\overset{\text{帰}}{=} n \cdot m + m \\
&\overset{\text{補題}\,10}{=} n \cdot m + 1 \cdot m \\
&\overset{\text{(2)}}{=} (n+1) \cdot m = (\text{右辺})
\end{aligned}
$$

となり、$n+1$ の場合も定理 (4) は成立しています。ただし、途中の「帰」は帰納法の仮定を用いたという意味で、「(2)」は証明の済んでいる、この定理の (2) を用いたという意味です。

以上より、すべての自然数 n に対して定理 (4) が証明されました。 □

2.6 整数の定義

さて、自然数の定義や演算では、何やら苦行めいた数学に耐えてきましたが、もう自然数についてはわかったことにします。つまり、計算や計算規則は自在に使ってよいし、ダッシュの山からも開放されたということです。

次は整数の定義ですが、整数もみなさんは良く知っているものですので、今度は整数について何も知らないふりをして議論を進めることになります。

定義 12 (整数)**.** 整数の集合 $\mathbb{Z}$ を次のように定める。まず、

$$T = \{(a, b) \mid a, b \in \mathbb{N}\}$$

とおく。ただし、T の 2 つの元 (a, b) と (c, d) に対して、

$$a + d = b + c \quad \text{であるとき } (a, b) \text{ と } (c, d) \text{ を同一視する}$$

T を上の関係で同一視したものを $\mathbb{Z}$ と書き、$\mathbb{Z}$ の元を**整数**と呼ぶ。

まず種を明かしておくと、この定義は、(a, b) を $a - b$ と思うということで、そうすると同一視の意味がはっきりします。ではなぜそう定義しないかと言うと、負の数や差が未定義だからです。

同一視という見慣れない操作が出てきましたが、実はよく知っているものです。分数では、整数の対を $\frac{3}{2}$ のように書きますが、$\frac{6}{4}$ や $\frac{9}{6}$ も、表示は違うけれど同じ大きさの分数を表します。つまり、これらは同一の有理数であり、表記の違うものを同一視しているということになります。これと同じことを上では集合 T に対して行ったというわけです。

自然数は整数に含まれますが、自然数 n を、整数 $(n + 1, 1)$ と対応させることで (これは $(n + 1) - 1$ の意味に相当します)、$\mathbb{N} \subset \mathbb{Z}$ と考えます。

2.7 整数の演算の定義

$(a, b) \in T$ が $a - b$ の意味だとわかると、整数の和や積の定め方は自然に出てきます。また、差については「マイナス 1 倍」して加えればよいので、「マイナス 1 倍」を定義します。

定義 13 (0、和の逆元、和、積)**.** (1) $(1, 1) \in \mathbb{Z}$ を 0 と表す。
(2) 自然数 n に対して、$(1, n + 1) \in \mathbb{Z}$ を $-n$ と表す。
(3) $\mathbb{Z}$ における和と積を、

$$(a, b) + (c, d) = (a + c, b + d), \qquad (a, b) \cdot (c, d) = (ac + bd, ad + bc)$$

で定める。

この演算が、T の元の同一視と矛盾なく定義されていることを確かめる必要がありますが、詳細は省略します。

例 14. m を自然数とすると、次の計算ができます。
(1) $m + (-m) = (m + 1, 1) + (1, m + 1) = (m + 2, m + 2) \overset{\text{同}}{=} (1, 1) = 0.$

(2) $m \cdot 0 = (m+1,1)\cdot(1,1) = (m+2, m+2) \overset{\text{同}}{=} (1,1) = 0$ ただし、「同」は T における同一視をしたという意味です。

結合法則などの計算規則は、自然数の場合と比べて格段にわかりやすく証明できます。

定理 15 (和や積の計算規則)**.** $l, m, n \in \mathbb{Z}$ に対して、次が成り立つ。

(1) $m + n = n + m$
(2) $(l + m) + n = l + (m + n)$
(3) $m \cdot n = n \cdot m$
(4) $(l \cdot m) \cdot n = l \cdot (m \cdot n)$
(5) $l \cdot (m + n) = l \cdot m + l \cdot n$
(6) $(l + m) \cdot n = l \cdot n + m \cdot n$

(証明) 整数 n を自然数の組で表すと (n_1, n_2) となっているとします。同様に $l = (l_1, l_2)$, $m = (m_1, m_2)$ とします。
(1)

$$\begin{aligned}(\text{左辺}) = (m_1, m_2) + (n_1, n_2) &\overset{\text{和}}{=} (m_1 + n_1, m_2 + n_2) \overset{\text{自}}{=} (n_1 + m_1, n_2 + m_2)\\ &\overset{\text{和}}{=} (n_1, n_2) + (m_1, m_2) = (\text{右辺})\end{aligned}$$

となるので示されます。ただし、途中の「和」は整数の和の定義、「自」は自然数の和の交換法則を用いたという意味です。
(2)

$$\begin{aligned}(\text{左辺}) &= ((l_1, l_2) + (m_1, m_2)) + (n_1, n_2)\\ &\overset{\text{和}}{=} (l_1 + m_1, l_2 + m_2) + (n_1, n_2)\\ &\overset{\text{和}}{=} ((l_1 + m_1) + n_1, (l_2 + m_2) + n_2)\\ &\overset{\text{自}}{=} (l_1 + (m_1 + n_1), l_2 + (m_2 + n_2))\\ &\overset{\text{和}}{=} (l_1, l_2) + (n_1 + m_1, n_2 + m_2) = (\text{右辺})\end{aligned}$$

となるので示されます。ただし、途中の「和」は整数の和の定義、「自」は自然数の和の結合法則を用いたという意味です。
(3) から (6) も、自然数の交換法則や分配法則に帰着されますが、証明は省略します。
□

負の数どうしの積が正の数になるということは、中学校での導入段階では工夫をして説明しなくてはなりません。純粋に代数的な説明としては、以下のように、

負の数 (下の説明だと $-a$ や $-b$) が混じっていても分配法則が成り立つと仮定して説明するものがあります。

a と b を自然数とします。負の数が混じっていても分配法則が成立していれば、まず、

$$0 = 0 \cdot b = (a + (-a)) \cdot b \overset{分}{=} a \cdot b + (-a) \cdot b$$

だから、$(-a) \cdot b = -(a \cdot b)$ がわかります (*)。次に、

$$\begin{aligned} 0 &= (-a) \cdot 0 \\ &= (-a) \cdot (b + (-b)) \\ &\overset{分}{=} (-a) \cdot b + (-a) \cdot (-b) \\ &\overset{*}{=} -(a \cdot b) + (-a) \cdot (-b) \end{aligned}$$

だから、$(-a) \cdot (-b) = -(-a \cdot b) = a \cdot b$ がわかります。これは、負の数どうしの積が正になることを意味しています。ただし、途中の「分」は分配法則、「*」は上で証明した式を用いたという意味です。

しかし、我々の定義の下では、以下のように何の仮定も必要とせずに導くことができます。m, n を自然数としたとき、まず、

$$(-m) \cdot (-n) = (1, m+1) \cdot (1, n+1) = (2 + (m+1) \cdot (n+1), m+n+2)$$

となり、他方、

$$m \cdot n = (m+1, 1) \cdot (n+1, 1) = ((m+1) \cdot (n+1) + 2, m+n+2)$$

となります。両者が一致するので、$(-m) \cdot (-n) = m \cdot n$ となります。ただ、この証明は、定義も含めて無味乾燥すぎますから、負の数どうしの積が正であることの納得を得られやすい説明だというわけではありません。数学の厳密さと教育的効果の折合いも難しい所です[3]。

3 素数・素因数分解

ここでは、素数の定義をしてから、素数が無数にあることや、素因数分解が一意的に可能であることを証明します。次に素因数分解が一意的であることの応用として、$\sqrt{2}$ などの平方根が無理数であることを証明します。

[3]他にも「荒れる」話題としては、小学校での積の交換法則だとか、分数の割り算でなぜひっくり返して掛けるか、というものがあります。この講習では触れません。

3.1　素数

定義 16 (素数)**.** 2 以上の自然数で、1 と自分自身でしか割り切れないものを**素数**と呼ぶ。

素数が無数にあることは、紀元前から知られていました。

定理 17. 素数は無数にある

(証明) 有限個の素数があったとして、それらとは一致しない素数を作ることができれば、素数が無数にあることになります。以下でこのことを示します。

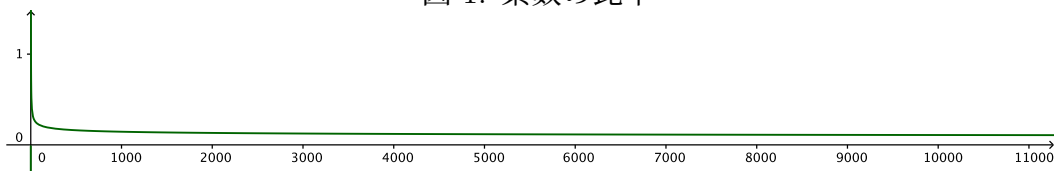
$p_1, p_2, \ldots, p_n$ を素数とします。自然数 $n = p_1 p_2 \cdots p_n + 1$ を考えると、n は $p_1, \ldots, p_n$ のどれで割っても 1 余ります。もし n に 1 と n 以外の約数がなければ、n は新しい素数です。反対に、n に 1 と n 以外の約数があったとすると、そのうち最小のものは新しい素数です。 □

素数は無数にありますが、大きくなればなるほどまばらになることが知られています。結果だけ述べると、1 から n までの素数の個数を $\pi(n)$ で表すと、

$$\frac{\pi(n)}{n} \sim \frac{1}{\log n} \qquad (n \text{ が限りなく大きくなると、両者は限りなく近づく})$$

です。

図 1: 素数の比率



例えば、100 までには 25 個の素数がありますから、$\pi(100)/100 = 0.25$ ですが、10^{10} までには 455,052,511 個の素数があるので、素数の比率は、$\pi(10^{10})/10^{10} \fallingdotseq 0.04550\cdots$ と大きく減少します。$1/\log 10^{10} = 0.04342\cdots$ なので、大体この比率と合っています。

3.2　エラトステネスのふるい

1 からある数までの範囲の素数を効率的に求める方法として、エラトステネスのふるいがあります。

まず、1 から n までの整数を表に書き、以下の手順を実行します。

(1) 1 を消します
(2) 消されていない最小の数 m (初回なら 2) に丸を付けます。
(3) いま丸を付けた数 m の倍数、$2m, 3m, 4m, \ldots$ を消します。
(4) すべての数が消されるか丸が付けば終了で、残っている数があるならば、(2) に戻ります。

手順が終了した後に、丸の付いた数が素数です。

1 から n までの範囲でエラトステネスのふるいを実行する場合、m の倍数を消す作業は、m が $\sqrt{n}$ を越えない範囲まで行えば、あとは、消されずに残っている数がすべて素数になります。

図 2: エラトステネスのふるい

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	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150
151	152	153	154	155	156	157	158	159	160
161	162	163	164	165	166	167	168	169	170
171	172	173	174	175	176	177	178	179	180
181	182	183	184	185	186	187	188	189	190
191	192	193	194	195	196	197	198	199	200

3.3 素因数分解とその一意性

自然数の素因数分解が可能であることと、分解が一意的であることが証明できます。

定理 18 (素因数分解とその一意性)**.** 自然数は素数の積に分解できる。また、その分解は順序を除いて一意的である。

(証明) [分解の存在] 自然数 n が素数ならば、すでに素数 1 個の積で表されているから、定理は成り立ちます。素数でなければ、2 以上 n 未満の約数が存在するので、$n = n_1 n_2$ $(n_1, n_2 < n)$ と分解できます。このように素数でなければ分解していくと、数が小さくなっていき、最後には素数の積に分解できます。

[分解の一意性] 自然数 n が、

$$n = p_1 p_2 \cdots p_k,$$
$$n = q_1 q_2 \cdots q_l$$

と、素数 $p_1, \ldots, p_k, q_1, \ldots, q_l$ (重複も許す) の積に、2 通りに表されているとします。すると、$q_1 q_2 \cdots q_l$ は p_1 で割り切れますから、$q_1, \ldots, q_l$ のどれかが p_1 と等しくなくてはなりません[4]。番号を付けかえて $p_1 = q_1$ とします。すると、$p_2 \cdots p_k = q_2 \cdots q_l$ となるので、同じことを繰り返すと、両辺の先頭から順番に一致してゆきます。すると、$k = l$ かつ $p_i = q_i$ $(1 \leqq i \leqq k)$ となり、分解が一意的であることがわかります。 □

素因数分解が一意的であることの応用として、$\sqrt{2}$ が無理数であることを示してみます。

例 19. $\sqrt{2}$ が無理数であることを背理法で証明します。$\sqrt{2} = m/n$ (m と n は自然数) と表せたと仮定します。整理すると、$2n^2 = m^2$ です。ここで、m と n の素因数分解を、

$$n = p_1 p_2 \cdots p_k,$$
$$m = q_1 q_2 \cdots q_l$$

とすると、

$$2p_1^2 p_2^2 \cdots p_k^2 = q_1^2 q_2^2 \cdots q_l^2$$

となります。ここで、両辺で素数が何個掛け合わされているか数えると、左辺が $2k+1$ 個、右辺が $2l$ 個となり、奇数と偶数なので一致しません。これは素因数分解の一意性に反するので矛盾です。従って最初の仮定が誤りで、$\sqrt{2}$ は無理数とわかります。

$\sqrt{2}$ が無理数であることの証明は、高校の教科書では、m と n を互いに素に取り、$2n^2 = m^2$ から m も n も偶数であることを示し矛盾を導く方法をとります。上の証明の優れている点は、n が平方数でない場合 $\sqrt{n}$ が無理数であることを、同じ方法で示せる所です。

[4]本当はこの部分はもう少し厳密な議論が必要ですが、省略しています。

定理 20. 自然数 n が自然数の平方ではないとき、$\sqrt{n}$ は無理数である。

(証明) n が自然数の平方でないので、n の素因数分解 $n = r_1 r_2 \cdots r_t$ に現れる素数 $r_1, r_2, \ldots, r_t$ の中には、奇数回現れるものが存在します。それを r とします。

$\sqrt{n} = a/b$ (a, b は自然数) と表せたと仮定します。整理すると、$nb^2 = a^2$ です。ここで、a と b の素因数分解を、

$$a = p_1 p_2 \cdots p_k,$$
$$b = q_1 q_2 \cdots q_l$$

とすると、

$$r_1 r_2 \cdots r_t \cdot p_1^2 p_2^2 \cdots p_k^2 = q_1^2 q_2^2 \cdots q_l^2$$

となります。ここで、両辺で素数 r が何回登場するか数えると、左辺は、$r_1 \cdots r_t$ の部分に奇数回、$p_1^2 p_2^2 \cdots p_k^2$ の部分に偶数回なので、合わせて奇数回ですが、右辺は偶数回なので一致せず、素因数分解の一意性に反するので矛盾です。従って最初の仮定が誤りで、$\sqrt{n}$ は無理数とわかります。 □

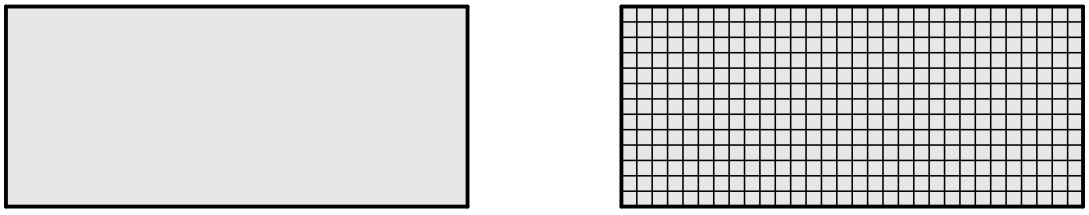
4 ユークリッドの互除法

ここでは、まず長方形を合同なタイルで敷き詰めることを考え、それがユークリッドの互除法の考え方に通じていることを見ます。次に、ユークリッドの互除法が、2元1次不定方程式や、合同式の連立方程式の解法に利用できることを見ます。

4.1 長方形の敷き詰め

例として、縦 26、横 60 の長方形を合同な正方形で敷き詰めることを考えます。敷き詰めが可能な最大の正方形の 1 辺の長さは、26 と 60 の最大公約数ですが、これを敷き詰めで考えます。

図 3: 縦 26 横 60 の長方形を正方形で敷き詰める



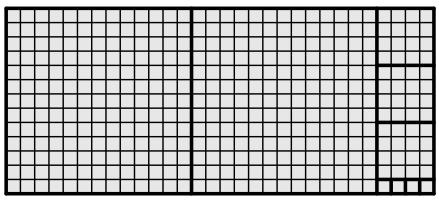
ユークリッドの互除法に関連するのは、以下のような敷き詰め方です。

まず、長方形に収まる最大の正方形で敷き詰めてみます。この場合は 1 辺 26 の正方形です。しかし、ぴったり敷き詰められず、縦 26、横 8 の長方形が残ります。これを再び長方形に収まる最大の正方形、つまり、1 辺 8 の正方形で敷き詰めます。すると、縦 2、横 8 の長方形が残ります。同様に今度は 1 辺 2 の正方形で敷き詰めるとぴったり敷き詰めが完了します。

図 4: 可能な最大の正方形で順に敷き詰める

最後の 1 辺の長さ 2 は、各段階の正方形の 1 辺の長さの公約数になっているので、各段階の正方形を 1 辺 2 の正方形に分割することができ、すると、もとの長方形が 1 辺 2 の正方形で敷き詰められたことになります。

図 5: 敷き詰めの完成



これが敷き詰め可能な最大のタイルであることは、次のようにしてわかります。敷き詰めが可能な最大の正方形の 1 辺の長さを a とします。1 辺 a の正方形で敷き詰めたときにできる格子を、1 辺 a の格子と呼ぶことにします。

上の手順の 1 辺 26 の正方形は、縦の長さが a の倍数になるので、どの辺も 1 辺 a の格子の上にあります。次の 1 辺 8 の正方形も同様にどの辺も 1 辺 a の格子の上にあります。こうして、最後の 1 辺 2 の正方形も 1 辺 a の格子の上にるので、a の最大性から $a = 2$ となります。

上では具体例で説明しましたが、どんなサイズの長方形でも、この方法によって可能な最大の正方形で敷き詰めることができます。つまり、最大公約数を求めることができます。

4.2 ユークリッドの互除法

ユークリッドの互除法の原理は、上の長方形の敷き詰めと同じです。長方形の敷き詰めでは、同じサイズの正方形を何個か敷き詰めますが、その個数は割り算で求めればよことから、下のように表せます。

定理 21 (ユークリッドの互除法)**.** 正整数 a, b があるとき、以下の手順を実行すると、a と b の最大公約数が求まる。

1. a を b で割り商を p、余りを r とする。
2. $r = 0$ ならば、b が最大公約数である。
3. $r \neq 0$ ならば、a の代わりに b、b の代わりに r に置き換えて、1. に戻る。

例 22. 前節の例と同じ数値で、ユークリッドの互除法を実行してみます。

$$\begin{aligned} 60 \div 26 &= 2 \text{ あまり } 8 \\ 26 \div 8 &= 3 \text{ あまり } 2 \\ 8 \div 2 &= 4 \text{ あまり } 0 \end{aligned}$$

最後の割る数 (あるいは、最後から 2 番目の余り) である 2 が最大公約数です。

定理 21 は前節でも本質的には証明されていますが、もう少し数学的に扱いやすい (書くのが楽な) 証明を下に記します。まず、補題を示します。

補題 23. 正整数 a と b の最大公約数を (a, b) という記号で表す。a を b で割った余りを r とすると、

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

が成り立つ。ただし、正整数 a に対して $(a, 0) = a$ である。

(証明) a を b で割り、商が p、余りが r とすると、$a = bp + r$ と書けます。b も r も (b, r) の倍数だから、a もそうです。よって、(b, r) は a と b の公約数となるから、(a, b) の約数です。

他方、$r = a - bp$ であり、a も b も (a, b) の倍数だから、r もそうです。よって、(a, b) は b と r の公約数となるから (b, r) の約数です。

以上より、(a, b) と (b, r) は互いに他の約数となったので等しいとわかります。□

この補題の意味するところは、上の例の各段階の割り算、$60 \div 26$、$26 \div 8$、$8 \div 2$ に現れる割られる数と割る数の最大公約数は等しいということです。このことを念頭に置けば、定理 21 が証明できます。

(定理 21 の証明) 上の補題より、互除法の手順 1. における割り算 $a \div b$ は、手順を重ねて数値が変化しても、a と b の最大公約数は変化しないことがわかります。数値は次第に小さくなるので、いずれ $r = 0$ となり手順は止まり、そのときの $(b, 0) = b$ は、元々の求めたかった最大公約数に等しいです。 □

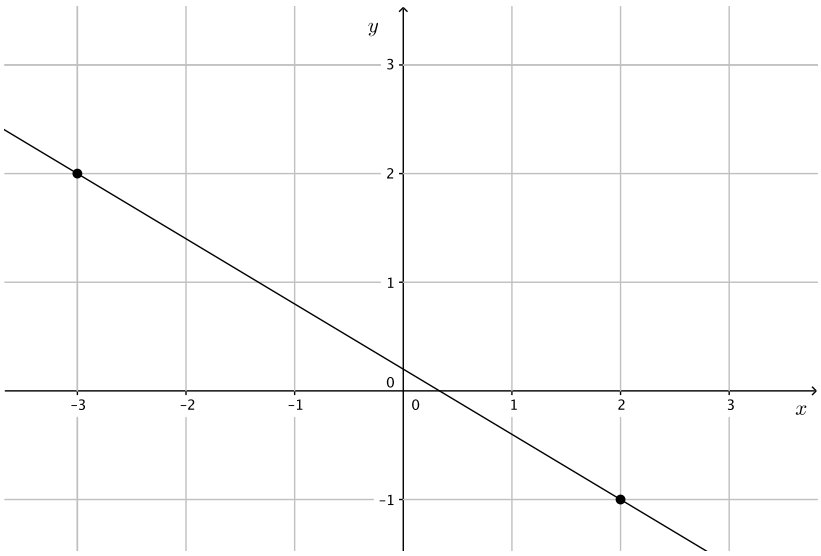
4.3　2 元 1 次不定方程式

整数 a と b に対して、方程式

$$ax + by = 1 \quad (x \text{ と } y \text{ は整数})$$

を考えます。これは、平面において直線 $ax + by = 1$ の上にある x 座標も y 座標も整数である点を求めることに相当します。

図 6: 2 元 1 次不定方程式



整数 a と b が互いに素ならば、この方程式が整数解を持つことが以下にようにユークリッドの互除法を用いて証明できます。

a を b で割り、商が p で余りが r とすると、

$$a = bp + r$$

です。ここで、1 が b の倍数と r の倍数の和、つまり、$bm + rn = 1$ (m、n は整数) と書けているとします。すると、$r = a - bp$ ですから、$bm + (a - bp)n = 1$、従って、$b(m - pn) + an = 1$ となり、1 は a の倍数と b の倍数の和で表せます。

a と b が互いに素であれば、最後は $(b', r') = 1$ に到達しているはずなので (b' と r' は最後の割り算の割る数と余り)、1 は b' の倍数と r' の倍数の和で表せます。そして、互除法の手順を遡れば、前段落のことから、1 は a の倍数と b の倍数の和で表せることがわかります。

例 24. 方程式

$$31x + 11y = 1$$

の整数解を求めてみます。最初に 1 つの解を求めた後に、すべての整数解を求めます。

(解)

$$31 \div 11 = 2 \text{ あまり } 9 \qquad \text{より } 9 = 31 - 11 \cdot 2, \tag{a}$$
$$11 \div 9 = 1 \text{ あまり } 2 \qquad \text{より } 2 = 11 - 9, \tag{b}$$
$$9 \div 2 = 4 \text{ あまり } 1 \qquad \text{より } 1 = 9 - 2 \cdot 4, \tag{c}$$

したがって、

$$\begin{aligned} 1 &\overset{\text{c}}{=} 9 - 2 \cdot 4 \\ &\overset{\text{b}}{=} 9 - (11 - 9) \cdot 4 = 9 \cdot 5 - 11 \cdot 4 \\ &\overset{\text{a}}{=} (31 - 11 \cdot 2) \cdot 5 - 11 \cdot 4 = 31 \cdot 5 - 11 \cdot 14. \end{aligned}$$

よって、$(x, y) = (5, -14)$ がひとつの解である。

$31x + 11y = 1$ と $31 \cdot 5 + 11 \cdot (-14) = 1$ の辺々を引くと、$31(x-5) + 11(y+14) = 0$ となるが、31 と 11 は互いに素だから、$x - 5$ は 11 の倍数である。$x - 5 = 11k$ (k は整数) と置くと、

$$\begin{aligned} 31 \cdot 11k + 11(y + 14) &= 0, \\ 31k + (y + 14) &= 0, \\ y &= -14 - 31k. \end{aligned}$$

まとめると、$(x, y) = (5 + 11k, -14 - 31k)$ (k は整数)。

4.4 2 元 1 次連立方程式の解の存在

整数 a と b に対して、前節の方程式

$$ax + by = 1 \quad (x \text{ と } y \text{ は整数})$$

が整数解を持つことは、別の方法でも証明できます。こちらの証明も参考になる点が多いので紹介します。まず補題を証明します。

補題 25. a と b を互いに素な整数とする。x が 0 から $b - 1$ までの整数を動き、y が 0 から $a - 1$ までの整数を動く、ab 通りの場合に対して、$ax + by$ を ab で割った余りはすべて異なる。

(証明) 整数 x, y $(0 \leqq x, x' < b, 0 \leqq y, y' < a)$ に対して、$ax + by$ を ab で割った余りと、$ax' + by'$ を ab で割った余りが等しいとします。すると、$(ax + by) - (ax' + by')$ は、

ab の倍数になります。特に、これが a の倍数であることから、$by - by' = b(y - y')$ が a の倍数であることになり、a と b が互いに素だから $y - y'$ が a の倍数になります。y も y' も 0 以上 a 未満なので、$-a < y - y' < a$ ですから、$y - y' = 0$ となります。同様にして、$x - x' = 0$ もわかります。

つまり、余りが一致するときは、x と x'、y と y' も一致するので、余りに重複がないことがわかります。 □

整数 x, y $(0 \leqq x < b, 0 \leqq y < a)$ に対して、$ax + by$ を ab で割った余りに重複がないということは、x と y が動く ab 通りの場合に、ab で割ったときの可能な余り 0 から $ab - 1$ までの ab 通りがすべて出現することになります。従って特に、余り 1 の場合がありますので、$ax + by$ が ab の倍数に 1 を加えた値になる場合があります。その解を x_0, y_0 とすると、

$$ax_0 + by_0 = abk + 1 \quad (k \text{ は整数})$$

と書けます。これを変形して、$a(x_0 - bk) + by_0 = 1$ とできますから、問題の方程式には、$x = x_0 - bk$, $y = y_0$ という解があることがわかります。

4.5 合同式

0 ではない整数 m と、整数 a, b があるとき、$a - b$ が m の倍数であることを

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

と表します。これを**合同式**と呼び、m を法として a と b は合同であると言います。

合同式も、通常の等式のような規則を満たします。

(1) $a \equiv a \pmod{m}$
(2) $a \equiv b \pmod{m}$ ならば $b \equiv a \pmod{m}$
(3) $a \equiv b \pmod{m}$ かつ $b \equiv c \pmod{m}$ ならば $a \equiv c \pmod{m}$

また、$a \equiv b \pmod{m}$ かつ $c \equiv d \pmod{m}$ の時、次が成り立ちます。

(4) $a \pm c \equiv b \pm d \pmod{m}$ (複号同順)
(5) $ac \equiv bd \pmod{m}$

(1) から (3) までの証明は省略します。

(4) については、$a-b$ も $c-d$ も m の倍数ならば、$(a \pm c) - (b \pm d) = (a-b) \pm (c-d)$ も m の倍数になることからわかります。

(5) は、$a - b$ も $c - d$ も m の倍数ならば、$ac - bd = (a - b)c + b(c - d)$ と変形できることから、これが m の倍数になることがわかります。

例 26. 89^{2017} を 17 で割った余りを求めてみます。

(解) 17 を法とする合同式を計算します。まず、$89 \equiv 4 \pmod{17}$ なので、

$$89^{2017} \equiv 4^{2017} \pmod{17}$$

です。次に、$4^4 \equiv 1 \pmod{17}$ が計算できるので、

$$4^{2017} \equiv 4^{4\cdot 504+1} \equiv (4^4)^{504} \cdot 4 \equiv 4 \pmod{17}$$

となり、従って、求める余りは 4 です。

4.6 2 元 1 次連立合同方程式

ここでは、ユークリッドの互除法や合同式の応用として、互いに素な整数 a, b に対して、合同式の連立方程式

$$\begin{cases} x \equiv s \pmod{a} \\ x \equiv t \pmod{b} \end{cases}$$

を考えてみます。

a と b が互いに素なので、$au + bv = 1$ を満たす整数 u, v があります。ここで、$x = tau + sbv$ と置くと[5]、

$$x \equiv tau + sbv \equiv tau + s(1 - au) \equiv s + a(tu - su) \equiv s \pmod{a}$$
$$x \equiv tau + sbv \equiv t(1 - bv) + sbv \equiv t + b(-tv + sv) \equiv t \pmod{b}$$

となるので、問題の方程式の解を与えることがわかります。また、x に ab の倍数を加えても解であることがわかります。

例 27. 31 で割ると 9 余り、11 で割ると 8 余る最小の正整数を求めてみます。

(解) $31u + 11v = 1$ の整数解の 1 つとして、$u = 5$, $v = -14$ があります。そこで、$x = 8 \cdot 31 \cdot 5 + 9 \cdot 11 \cdot (-14)$ と置きます。すると、$x \equiv 8 \pmod{31}$, $x \equiv 9 \pmod{11}$ となりますから、31 で割った余りが 8、11 で割った余りが 9 です。

$x = -146$ ですが、$31 \cdot 11$ の倍数を加えても、解であることに変わりがないので、$-146 + 31 \cdot 11 = 195$ も解であり、これが、求める最小の正整数です。

5 濃度

ここでは、「無限」の大きさを測るともいえる濃度を紹介します。要素が増えても濃度が変わらないなど、有限集合では起こり得ない例を見たり、数の集合の濃度を考えます。

[5] この置き方は「発見的」ではありませんが、こう置くとうまくいくので、とりあえず受け入れて先に進むことにします。

5.1 無限集合の濃度

定義 28. (有限とは限らない) 集合 A と B の間に 1 対 1 対応があるとき、A と B の**濃度**は等しいと定め、$|A| = |B|$ と書く。有限集合の濃度は、その集合の要素の個数のことである。

集合 A と B の間に 1 対 1 対応があるということは、全単射 $f : A \to B$ が存在するといっても同じです。

自然数全体の集合 $\mathbb{N}$ の濃度を、**可算濃度**、実数全体の集合 $\mathbb{R}$ の濃度を、**連続体濃度** と呼びます。

例 29. 次が証明できます。
(1) 整数全体の集合 $\mathbb{Z}$ は可算濃度を持つ。
(2) 偶数全体の集合は可算濃度を持つ。
(3) 正の実数全体の集合 $\mathbb{R}_+$ は連続体濃度を持つ。
(4) $0 < x < 1$ を満たす実数全体の集合は連続体濃度を持つ。

(解) (1) ある集合が可算濃度を持つことを言うには、その集合の要素に自然数で番号付けできればよい。整数を、

$$0, 1, -1, 2, -2, 3, -3, \ldots$$

と並べて先頭から自然数で番号付ければ、$\mathbb{Z}$ が可算濃度を持つことがわかる。

(2) 今度は、具体的な対応を式で作ってみる。偶数全体の集合を A と表すと、$\mathbb{Z}$ から A への写像 $f : \mathbb{Z} \to A$ を

$$f : \mathbb{Z} \to A \qquad (f(x) = 2x)$$

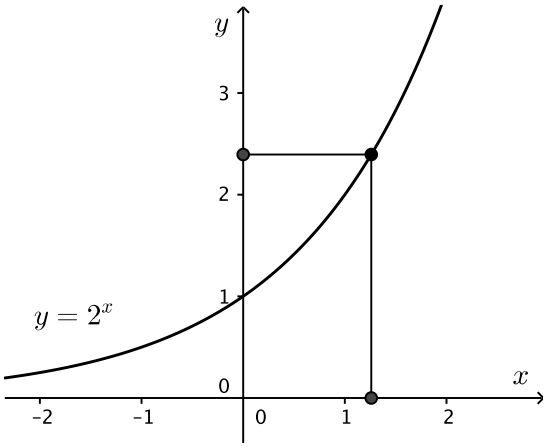
で定めると 1 対 1 対応であるから、A は $\mathbb{Z}$ と同じ濃度を持つので、可算濃度を持つことがわかる。

(3) $\mathbb{R}$ から $\mathbb{R}_+$ への写像 $f : \mathbb{R} \to \mathbb{R}_+$ を、

$$f : \mathbb{R} \to \mathbb{R}_+ \qquad (f(x) = 2^x)$$

と定めると、1 対 1 対応を与えるので、$\mathbb{R}_+$ は $\mathbb{R}$ と同じ濃度、つまり、連続体濃度を持つ。

図 7: $\mathbb{R}$ と $\mathbb{R}_+$ の 1 対 1 対応

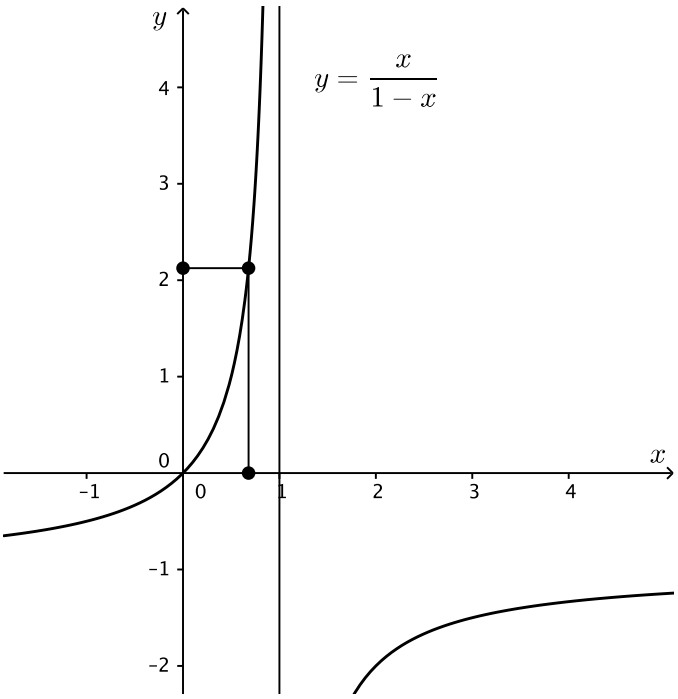


(4) $B = \{x \mid 0 < x < 1\}$ と置き、B から $\mathbb{R}_+$ への写像 $g : B \to \mathbb{R}_+$ を

$$g : B \to \mathbb{R} \qquad \left(g(x) = \frac{x}{1-x} \right)$$

と定めると、下図からわかるように、1 対 1 対応を与えるので、B は $\mathbb{R}_+$ と同じ濃度、つまり、連続体濃度を持つ。

図 8: $\mathbb{R}_+$ と $\{x \mid 0 < x < 1\}$ の 1 対 1 対応



□

例えば、整数全体の集合 $\mathbb{Z}$ と、その真部分集合である自然数全体の集合 $\mathbb{N}$ は、同じ可算濃度を持つことがわかりましたが、これは無限集合特有の現象で、有限集合では起こりません。

問題 30. 奇数全体の集合が可算濃度を持つことを、自然数全体の集合との 1 対 1 対応を具体的に構成して証明せよ。

5.2 有理数全体の集合の濃度

自然数と有理数では、その「個数」は有理数の方がはるかに多く思えますが、実は次の定理が成り立ちます。

定理 31. 有理数全体の集合 $\mathbb{Q}$ は可算濃度を持つ。

(証明) まず、正の有理数全体の集合 $\mathbb{Q}_+$ が可算濃度を持つことを示します。正の有理数は a/b (a と b は自然数) と表せますから、下の図のように、表に表せます。

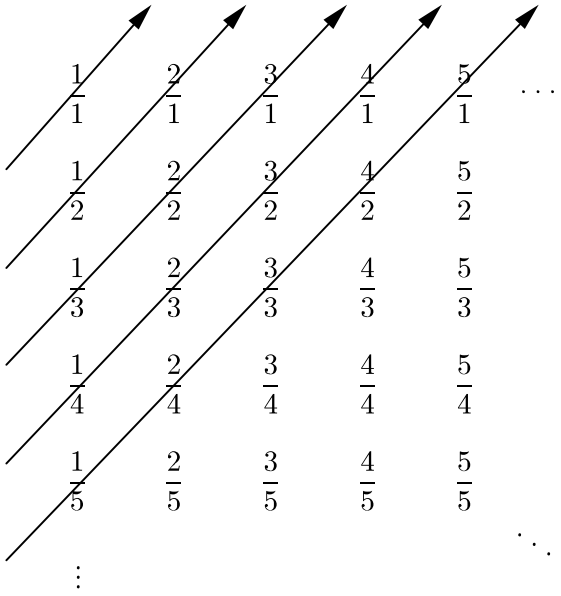
図 9: 正の有理数

$$\begin{array}{ccccccc}
\frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \frac{4}{1} & \frac{5}{1} & \cdots \\
\frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \frac{4}{2} & \frac{5}{2} & \\
\frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \frac{4}{3} & \frac{5}{3} & \\
\frac{1}{4} & \frac{2}{4} & \frac{3}{4} & \frac{4}{4} & \frac{5}{4} & \\
\frac{1}{5} & \frac{2}{5} & \frac{3}{5} & \frac{4}{5} & \frac{5}{5} & \\
\vdots & & & & & \ddots
\end{array}$$

これを下図の矢印のように斜めに辿ると、正の有理数に自然数で番号付けできます[6]。ただし、既約分数だけを辿ることにして、同じ数を 1 度だけ番号付けるようにします。以上で、$\mathbb{Q}_+$ が可算濃度を持つことが言えました。

図 10: 正の有理数の番号付け

[6]同じようでも、上の行から順に左から右へ辿るのではうまくいきません。1 行目の番号付けが有限のうちには終わらず、2 行目の先頭には、有限の番号が付かないからです。



次に、有理数全体の集合 $\mathbb{Q}$ が可算濃度を持つことを示します。まず、正の有理数は自然数で番号付けできるので、それを $a_1, a_2, \ldots$ と書きます。具体的には、

$$
\begin{aligned}
&a_1 = \frac{1}{1},\\
&a_2 = \frac{1}{2}, \quad a_3 = \frac{2}{1},\\
&a_4 = \frac{1}{3}, \quad a_5 = \frac{3}{1},\\
&a_6 = \frac{1}{4}, \quad a_7 = \frac{2}{3}, \quad a_8 = \frac{3}{2}, \quad a_9 = \frac{4}{1},\\
&a_{10} = \frac{1}{5}, \ldots
\end{aligned}
$$

です。すると、有理数全体は、

$$0, a_1, -a_1, a_2, -a_2, a_3, -a_3, \ldots$$

と並べることができるので、$\mathbb{Q}$ が可算濃度を持つことがわかります。 □

また、正の有理数全体 $\mathbb{Q}_+$ が可算濃度を持つことを、素因数分解を利用して証明できるので、これも紹介します。

(定理 31 の証明) 正の有理数全体 $\mathbb{Q}_+$ が可算濃度を持つことの別証明をします。

正の有理数を a/b (a と b は自然数) と表し、a と b の素因数分解を、

$$
\begin{aligned}
a &= 2^{s_2}3^{s_3}5^{s_5}\cdots,\\
b &= 2^{t_2}3^{t_3}5^{t_5}\cdots
\end{aligned}
$$

と表します。ただし、s_i と t_i は 0 以上の整数であり、s_i も t_i も有限個以外はすべて 0 です。すると、

$$\frac{a}{b} = \frac{2^{s_2}3^{s_3}5^{s_5}\cdots}{2^{t_2}3^{t_3}5^{t_5}\cdots} = 2^{s_2-t_2}3^{s_3-t_3}5^{s_5-t_5}\cdots$$

となるので、すべての正の有理数は、

$$2^{u_2}3^{u_3}5^{u_5}7^{u_7}\cdots \qquad (u_i \text{ は整数で有限個以外はすべて } 0) \qquad (*)$$

と一意に表せます。

整数 u と、0 以上の整数 v との 1 対 1 対応を、

$u \in \mathbb{Z}$	0	1	−1	2	−2	3	−3	⋯
$v \in \mathbb{Z}_+$	0	1	2	3	4	5	6	⋯

で定めることができるので、式 (*) において、この対応で u_i を v_i に写すことで、

$$2^{v_2}3^{v_3}5^{v_5}7^{v_7}\cdots \qquad (v_i \text{ は } 0 \text{ 以上の整数で有限個以外はすべて } 0) \qquad (**)$$

となります。これは、ちょうど、自然数の素因数分解になっています。

以上より、正の有理数 a/b を (*) を経由して (**) に対応させることで、自然数との 1 対 1 対応が作れます。つまり、$\mathbb{Q}_+$ は可算濃度を持ちます。 □

5.3 実数全体の集合の濃度

前節では、自然数全体の集合 $\mathbb{N}$ と有理数全体の集合 $\mathbb{Q}$ がともに可算濃度を持つという、直観に反する事実が証明されました。

既に、実数全体の集合 $\mathbb{R}$ の濃度を連続体濃度と定義していますので、暗黙のうちに、$\mathbb{R}$ の濃度は可算濃度ではない (言い換えると可算濃度と連続体濃度は異なる) ことを認めていましたが、ここではこれを証明します。この証明の手法は**対角線論法**と呼ばれています。

定理 32. $\mathbb{R}$ の濃度は可算濃度ではない。

(証明) $\mathbb{R}$ と $B = \{x \mid 0 < x < 1\}$ は同じ濃度を持つことが、例 29 (4) で示されていますから、B の濃度が可算濃度ではないことを示せばよいです。そこで、B の濃度が可算濃度ではないことを背理法で証明します。

B の濃度が可算濃度であると仮定します。すると、B の元は自然数で番号付けできますので、$B = \{x_1, x_2, \ldots\}$ とします。各 x_i は $0 < x_i < 1$ なので、10 進小数

表示[7] をすると、整数部分が 0 である小数になります。$x_1, x_2, \ldots$ を 10 進小数表示したものを並べると、下にようになります。

$$
\begin{aligned}
x_1 &= 0.a_1\, a_2\, a_3\, a_4\, a_5\, a_6 \cdots \\
x_2 &= 0.b_1\, b_2\, b_3\, b_4\, b_5\, b_6 \cdots \\
x_3 &= 0.c_1\, c_2\, c_3\, c_4\, c_5\, c_6 \cdots \\
x_4 &= 0.d_1\, d_2\, d_3\, d_4\, d_5\, d_6 \cdots \\
x_5 &= 0.e_1\, e_2\, e_3\, e_4\, e_5\, e_6 \cdots \\
&\vdots
\end{aligned}
$$

ここで、$a_i, b_i, c_i, \ldots$ はすべて、0 から 9 までの数字で、小数表示の各桁を表しています。

さて、実数 y を次のように作ります。

(1) 小数表示すると、整数部分は 0。
(2) 小数第 1 位は、a_1 と異なる数字にする。
(3) 小数第 2 位は、b_2 と異なる数字にする。
(4) 小数第 3 位は、c_3 と異なる数字にする。
⋮

ただし、末尾に 9 が続かないようにします。例えば、各位を選ぶときに、9 を許さないようにすることで、そうできます。

こうしてできた実数 y は $0 < y < 1$ を満たしますから、$y \in B$ であるはずです。しかし、y は B のどの元とも、小数表示のどこか 1 桁が異なります。例えば、x_1 とは小数第 1 位が異なり、x_2 とは小数第 2 位が異なるなどとなっています。従って、$y \notin B$ であり、矛盾が生じます。よって、背理法の仮定が誤りで、B の濃度は可算濃度ではないことが証明できました。 □

5.4 連続体仮説

可算濃度と連続体濃度は異なることが前節で示されましたが、この「間」に別の濃度がないという予想が**連続体仮説**です。以前は「予想」でしたが、現在では、次のように結論が出ています。

[7] 有限小数は末尾に 0 が無限に続いていると考え、小数表示と言えば無限小数を指すことにします。また、末尾に 9 が続く無限小数表示は許さないことにします。つまり、例えば、$0.23999\cdots$ とは表示せず、$0.24000\cdots$ という表示のみ考えることにします。

定理 33. 現在の標準的な数学の枠組みでは、連続体仮説は証明も反証もできない。

現在の標準的な数学の枠組みとは、正確には、ツェルメロ・フレンケルの公理系に「選択公理」と呼ばれる公理を追加した体系ですが、詳細は触れません。

つまり、可算濃度と連続体濃度の「間」に別の濃度があることもないことも証明できないということになります。連続体仮説が真でも偽でも数学の体系の無矛盾性ほどの大きな影響はないため、真の立場をとる数学者も偽の立場をとる数学者もいると思われます (一番多いのはあまり気にしていない立場かも知れません)。

6 おわりに

自然数や整数は非常に身近な数学の対象ですから、面と向かって厳密に取り扱うことはあまりないかも知れません。今回の講習を通して、「はじめに自然数ありき」ではなく、厳密に取り扱うことができることを再認識していただければさいわいです。また、素因数分解の一意性のような、重要だけれども普段顧みる機会の少なかったものの重要性を認識していただければと思います。

ユークリッドの互除法は非常に広い応用を持ち、この講習ではその非常に少ない例しか紹介できていませんが、少しでもその背景を知っていただけたのではないかと思います。

このような整数に関する問題は、少ない予備知識で取り組めることが多いですが、解決の糸口が見付けづらいなど案外難しいことがあり、公式に基いた計算で済む微分・積分の問題の方がかえって簡単だったりします。つまり、計算力だけではない数学的な思考力を培うには整数問題は良い題材であると思います。ちなみに、他の分野では、場合の数や確率の問題にも、計算力よりも思考力を必要とするものが多いと思います。

最後になりますが、本講習を選択していただきありがとうございます。この資料の内容には、時間の都合で講習では省略した部分もありますので、興味のある方は是非いろいろ調べていただけたらと思います。すべての人に 100%満足していただける内容を準備できたとはとても言えませんが、講習の 6 時間で、興味の持てる新しい話題に触れられて、少しでも、今後の教育活動の役に立つと感じていただけたならばさいわいです。

参考文献

ここでは、この資料を作成するにあたり参考にした文献や、資料や講習では触れられなかった関連する文献を紹介します。

まず、次の文献は、自然数から実数や複素数に至るまで、様々な話題が盛り込まれた本です。ペアノの公理や、負の数どうしの積が正であることも含め、様々な話題が書かれており、本資料の作成で参考にしました。特に、本資料の、有理数が可算濃度を持つことの 2 つ目の証明は、この本にあるものです。また、講習では触れることができませんでしたが、一般向けの数学書として、実数の連続性について正確な記述がされている貴重な本です[8]。

[一松] 一松信. 数の世界 丸善出版, 東京, 2015

次の本では、資料で少しだけ触れたゲーデルの不完全性定理はもちろんのこと、ペアノの公理や、対角線論法についても触れられています。ガチガチの数学書ではなく、ライトな読み物のシリーズなので、一般の方にも読み易いはずです。このシリーズの本は他にも多くでていて、どれもお薦めです。しかし、この本の不完全性定理の部分はシリーズ中随一の難解さです。

[結城] 結城浩. 数学ガール / ゲーデルの不完全性定理 ソフトバンククリエイティブ, 東京, 2009

次の本は古い本ですが、無限集合の濃度や、1 対 1 対応を理解するには良い本です。有理数が可算濃度を持つことなどにも触れていますし、遠山氏らしく、りんごとみかんの集合に 1 対 1 対応を作るという段階から始めるなど、丁寧な記述がなされています。

[遠山] 遠山啓. 無限と連続 岩波新書, 東京, 1952

[8]実数の連続性は、$0.999\cdots = 1$ を説明するためだとか、「アキレスと亀」として知られるパラドックスで、アキレスが亀に追いつけることのために必要だと記述する文献をたまに見かけますが、多くの場合は自然数のアルキメデス性だけが必要な例にしかなっていません。