

第1章 数

はるかな昔，人は2までしかものを数えられない時代もありました．2より多いものは全て“たくさん”といいました．やがて，人は，3まで，5まで，10まで，100まで，1000まで，… と大きな自然数を数えられるようになっていきました．事実，古代ギリシャ最大の学者アルキメデス（Archimedes，前287頃～212）は，小著『砂の計算者』で，もし宇宙を砂の粒で満たしたらその数は 10^{63} （1のあとに0が63個並んだ数）を超えず，それよりいくらかでも大きな数が存在することを示しました．しかしながら，古代のエジプト人やギリシャ人には，まだ，0と負数の考えはありませんでした¹⁾．

0は，何も無いものを在ると見なす認識論的観点というよりは，

1, 2, 3, …, 9, 10, 11, 12, …

などと，0から9までの数字だけを用いて全ての自然数を表すこと，つまり，（10進）「位取り記数法」に決定的でした．これは紀元後6世紀前後になってインドの数学に始まり，それによってどんなに大きな数も簡単に表され，計算も便利になりました．

負の数は小さな数から大きな数を引く必要性があって初めて認められる数です．古代のエジプト・ギリシャ時代には‘小さな数 - 大きな数’は不可能であると思われていました．最近の研究によると，負数の導入とその加法・減法の法則の発見は古代中国でなされたとのことです．現存する中国最古の数学

¹⁾ 歴史的記述に当たっては，労作『グレイゼルの数学史 I-II-III』（保阪秀正・山崎昇 訳，大竹出版）を始め，『数学史』（武隈良一 著，培風館），『現代数学小事典』（寺阪英孝 編，講談社），『数 - 体系と歴史』（足立恒夫 著，朝倉書店），『岩波数学辞典（第3版）』（日本数学会 編，岩波書店），その他，多くのインターネットのウェブサイトを参照しました．

書『九章算術』(紀元前数百年前の著といわれます)では、例えば金額を未知数に選び、負数はその不足を表しました。「負」という漢字はもともと「借り」(負債)を意味するそうです。このような概念がインドに渡り、負数は長い間「借金」とか「不足」といった言葉で表されました。ヨーロッパでは、14世紀以後になって、ようやく一部の学者が負数を借金として解釈しました。しかし、大部分の学者は負数を“うその数”と呼んでいました。‘借金×借金’の解釈、つまり、負数どうしの積の意味付けに当惑と疑いを向けられる有様では、当然といえば当然のことでした。16世紀中頃、ドイツの数学者が負数を‘何も無いものより小さい数’と見なし、理論的基礎付けに前進しましたが、人々は‘何も無いものより小さい量が存在する’という考えに慣れることができませんでした。

しかしながら、17世紀以降、数学・力学・天文学が大きく発展し、負数は正数と同じ計算規則(例えば、 $(-1)+(-2)=(-2)+(-1)$ や $(-3)\times(-4)=(-4)\times(-3)$ などの最も基本的なもの)に従い、それを使うと計算が著しく軽減されるので真に役立つことが認識され、また、矛盾する結果も決して現れないので、しっかりと数学に根付いていきました。そして、19世紀の前半になって、正・負の整数についての厳密な理論が発展して、ついに負数は数として完全に公認されたのでした。それからまだ200年も経っていません。

長さ・面積・体積・重量・時間などの「量」を測定すると、いつも整数で表されるわけではないことから、どうしても分数が必要になります。古代バビロニアでは、紀元前2千年頃には数学が高い水準に達し、60進分数が人々の生活習慣に根付いていました。その数学は、ギリシャ・ヨーロッパの数学に大きな影響を与え、現在でも時間や角度の単位に時・分・秒を用いるのはその名残です。

どりょうこう
度量衡、つまり、長さ・容積・重さなどをより正確に測定する必要が生じると、小数を用いるのは必然になります。15世紀前半、中央アジアのチムール王朝の数学者が、(10進)小数を研究して、整数部分と小数部分を区分する書式を導入しました。17世紀の初めの近代ヨーロッパでは、小数は科学者や技術者に集中的に浸透し始め、小数点(.)などの記号による区分を用いた現在の形になりました。

紀元前6世紀、ピタゴラス(Pythagoras, 前582頃~496頃)に代表される

古代ギリシャでは幾何学が盛んでした。彼の時代に、正方形の対角線と1辺との比(の大きさ)が‘分数で表すことのできない数’ $\sqrt{2}$ になることが示されました。これが最初に発見された無理数でした。当時は自然数や自然数の比(つまり分数)のみを数学の対象としていた時代です。 $\sqrt{2}$ を分数として表すことができないと知ったとき、ピタゴラス派の人々は、無理数を認めると自分たちの数学が否定されると恐れ、数と認めることはおろか無理数の存在そのものをひた隠しにしました。以後、古代ギリシャの学者は、「量」を数ではなく線分として考えるようになりました。

ここで、分数に注意を向けておきましょう。実は分数が数学者に数として認知されるまでには負数と同じくらいの苦難の歴史がありました。ユークリッド(Euclid, 前365頃~275, ギリシャ)は著書『原論』の中で分数にとり組むことを避け、アルキメデスは分数を用いましたがそれを「数」とは認めませんでした。彼らにとって‘数は自然数’を意味していました。分数は数(自然数のこと)の比の $\dot{\text{大}}\dot{\text{き}}\dot{\text{さ}}$ と見なされたのです。大きさは $\dot{\text{量}}$ であって数ではないというのです。同様の理由で小数も数とは認められませんでした。現在から見ると奇異に感じられると思いますが、ピタゴラスは“万物は数である”(世界は数できている)といったくらいです。したがって、昔の数学者の数に対する思い入れはすさまじく、‘自然数のみが万物を創るのにふさわしい完全な存在であり、それ以外は中途半端で不完全極まりないもの’に思えたのでしょう。自然数に対する特別な愛着は17世紀になってもまだ続いていたと思われます²⁾。

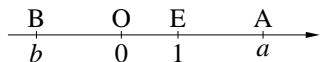
現在、我々は‘数と量は一体のもの’と認識し、量を表すのに数を用い、分数や無理数を自然数と同じ計算方法によって計算し、正しい結果を得ることができます。その考えは、“我思う、ゆえに我あり”の名言で有名なデカルト(René Descartes, 1596~1650, フランス)の著作『幾何学』(1637)に始まり、数と線分の同一視によって数と量の間の溝を埋めることが可能になりました。数と線分の同一視の議論からこの章を始めたほうが数をより深く理解するのに実り多いでしょう。

²⁾ 19世紀になってもまだ自然数信仰は残っていたようです。ドイツの数学者クロネッカー(Leopold Kronecker, 1823~1891)の印象に残る言葉を紹介しましょう：“自然数は神が創りたもうた。その他の数は人の為せる $\dot{\text{業}}$ である”。

§1.1 数直線

分数や無理数が自然数と同等の数であると認められるためには、それらが自然数と同じ基本的な計算の規則に従っていること、および、それらが自然数と平等の立場にあることが一目瞭然であることが必要です。前者のほうは次の § (section) に回して、ここでは‘自然数と平等の立場にある’のほうを議論しましょう。

ユークリッドを引き合いに出すまでもなく、我々が古代から最も信頼してきた数学は幾何学です。定規とコンパスを用いて作図することは中学校で習いましたね。さて、1本の直線を考え、その上の1点 O を片方の端とする線分を考えましょう



(線分は量です)。次に、直線上に O と異なる

1点 E をとり、線分 OE の長さを基準の長さ 1 としましょう。コンパスを用いて OE の整数倍の長さの線分は簡単に求められます。また、定規とコンパスを用いて OE を 2 等分、 3 等分、 \dots 、 n 等分することは、君たちに手ごろなレッスンでしょう。

また、直線上に点 A をとりそれを動かせば、線分 OA は無理数を含むどんな長さにもなります。その意味で線分の長さは‘連続的に存在する量’であると仮定し、その大前提で今後の議論を進めましょう(当たり前のことですね)。

次に線分と正数の対応を考えましょう。デカルトは正数 a を考えるとき長さ a の線分を考えました。数 $a + b$ を考えるときは長さ a と長さ b の線分の和を考えました。積 ab については長さ $a, b, 1$ の線分を考え、比 $1 : a = b : c$ を満たす長さ $c = ab$ の線分を作図することによって、数の積を線分で表しました(作図してみましょう)。よって、この考えに立つと、 a^2 は面積ではなく線分の長さとして解釈されます。同様に、商 $\frac{a}{b}$ を求めることは、比 $a : b = d : 1$ となる長さ d の線分を求めることと同じです。つまり、‘数の演算は、線分の作図に帰着でき、その結果の線分をまた数に対応させることができる’わけです。したがって、数と線分は同一視できることが示されました。

負数を線分に対応させるために、先ほど述べた点 O, E がその上にある直線

を考え、直線上の点に数を対応させましょう。まず、点 O, E に数 $0, 1$ を対応させます。長さ a の線分を OA とするとき、点 A に数 a を対応させましょう。負の数 b を考えるときは、数 b の大きさに等しい長さの線分 OB を考え、点 B を点 O から見て点 E と反対の側にとって、点 B に数 b を対応させます。こうして、直線上の点と正・負の数を対応させることが可能です。

このように点と数を対応させた直線を数直線といい、点 O を原点、点 E を「単位点」といいます。数直線上の点として数を見ると、自然数と分数・無理数・負数はまったく平等の存在であり、自然数が特別ということはありません。こうして、自然数・分数・無理数・負数は平等に数と見なされるようになりました。また、点は連続的に存在するので、それに対応する数も連続量と考えられるようになりました。

ただし、点と数が数直線上で $1:1$ に完全に対応する、つまり数直線上の 1 点にはただ 1 つの数に対応し、逆に 1 つの数にはただ 1 点に対応するかどうかについては疑問の余地が残ります。点のほうは連続量なので完全に揃っていますが、数のほうは慎重に調べる必要があります。有理数までは、分数を用いて具体的に表現できるので、明らかですが、無理数についてはまだ明確ではありません。数直線上に勝手な点をとったとき、その点に対応する数を、例えば、(小数点以下の数が無限に続く) 小数を用いて必ず表現できることを示す必要があります。これは高校生にはハイレベルな問題なので、巧妙な議論を後で紹介するまで先延ばししましょう。ここでは、「数は連続量である」ことが知られているとしておきます。

なお、デカルトは数を表すのに、先ほど見たように、文字 a, b, c などを用い、文字によって数の演算を表現しました。文字を使うと、特定の数でなく、どんな数でも表すことができます。したがって、それらに共通する基本的な計算規則を明らかにし、数の性質や方程式の解法を組織的に研究することが可能になりました³⁾。

これで準備が整いました。いよいよ数の演算の規則に関する議論にとりかかりましょう。まずは自然数・整数・有理数の復習から。

³⁾ 個々の数字の代わりに文字を用いて一般的な数を代表させ、方程式・数の関係・数の性質・数の計算規則などを研究する数学を「代数学」といいます。

§1.2 自然数・整数・有理数

ものの個数や順序を表すのに用いられる数

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

を自然数といいます。自然数の和や積はまた自然数になります。ところが、 $2-3=-1$ のように、差については自然数にならず負数になる場合もあります。負数が使えないとすると、古代人がそうであったように、実に不便ですね。そこで、 0 や $-1, -2, -3, \dots$ などの数をつけ加えて、整数

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

に拡張します。整数の中では加・減・乗の演算が自由にでき、それらの演算結果は、やはり、整数になります。ところが、 $1 \div 2 = 0.5$ のように割り算をすると、整数にならない場合もあります。そこで、分数、つまり‘整数ぶんの整数’の形で表される数

$$\frac{m}{n} \quad (m, n \text{ は整数, ただし } n \neq 0)$$

に数を拡張しましょう。この形の式で表される全ての数を今後は有理数と呼ぶことにしましょう。有理数 $\frac{m}{n}$ は、 $n=1$ のとき $\frac{m}{1}=m$ となり、したがって、有理数は整数を含みます。また、 $n \neq 0$ は 0 で割ることを禁じています(このことについては後ほど議論します)。

実際に、有理数 $\frac{m}{n}$ の m, n にいろいろな整数を代入して、どんな有理数や整数でも表せることを実感するとよいでしょう。数学では、‘文字を用いて表現された式は、その文字に可能な数値を代入して得られる任意の⁴⁾数を表す’と見なされます。有理数の中では、加・減・乗・除が、 0 で割ることを除いて自由にでき、その結果はまた有理数ですね。例えば、

$$\left(\frac{1}{2} - \frac{2}{3}\right) \div \frac{3}{4} = -\frac{2}{9}.$$

⁴⁾ 任意の = 思いのままの ≡ どの … も。用語「任意」は数学では頻繁に用いられます。

§ 1.3 数学の論理

1.3.1 演算の公理

さて、当たり前のように行っている計算ですが、その計算の基本ルールを振り返ってみましょう。計算の基本ルールは、君たちが小・中学校で習った計算の基本公式のうち、さらに基本中の基本となる‘あまりにも当たり前な’数個の公式を選び出したものです。それらをまとめて、このテキストでは、「計算に広い意味で関係する基本的な仮定」という意味で、演算の公理と呼ぶことにしましょう。公理とは、それ以上は(正しいと)証明しなくてよい、基本的な仮定のことです。まずはそれらを復習しましょう。あまりにも当たり前のことから始めますがビックリしないように。このことは、数学の限りなく厳密な論理の展開方法と結びついていることが次第々に理解されるはずですよ。

まずは等号の左辺と右辺を入れ替えることから始めましょう。

$$1 + 2 = 3 \quad \text{ならば} \quad 3 = 1 + 2$$

ですね。左辺の $1 + 2 = 3$ は‘1 に 2 を加えたものは 3 に等しい’ことを表し、右辺の $3 = 1 + 2$ は‘3 は 1 に 2 を加えたものに等しい’ことを表します。両者の意味は本来違うことに気づくと思いますが、 $1 + 2 = 3$ が成り立てば $3 = 1 + 2$ も成り立ちますね。このことを任意の等式に一般化して、「左辺 = 右辺 ならば 右辺 = 左辺」が成り立つと考えるのは極めて自然です。これを、文字を用いて、「 $a = b$ ならば $b = a$ 」と表しましょう。この当たり前の法則の証明はできない相談なので、それは公理と見なされ、いかにも偉そうな名「対称律」がつけられています。「ならば」を表す記号 \Rightarrow を用いて、この基本仮定を数学らしく

$$a = b \Rightarrow b = a \quad (\text{対称律}) \quad (\text{A.1})$$

と表しましょう。記号 \Rightarrow は、一般表現 $p \Rightarrow q$ でいうと、 p から q が必ず導かれることを表します。

次に、「 $1 + 1 = 2$ かつ $2 = 3 - 1$ ならば $1 + 1 = 3 - 1$ 」が成り立つのは当然ですね。これがいわゆる「三段論法」という奴です。このことを一般化して得

られる公理：⁵⁾

$$a = b \text{ かつ } b = c \Rightarrow a = c \quad (\text{推移律}) \quad (\text{A.2})$$

も任意の等式に対して成立すると仮定されます。この公理はやはり偉そうな名「推移律」がつけられ、対称律と並んで数学における最も基本的な仮定とされています。

それから、数の演算に直接関係する法則があります。1 + 2 = 2 + 1 (1 に 2 を加えたものは 2 に 1 を加えたものに等しい) とか、2 × 3 = 3 × 2 (2 に 3 を掛けたものは 3 に 2 を掛けたものに等しい) のように、演算を受けるほうとするほうを入れ替えても結果は同じという交換法則が仮定されます。また、(1 + 2) + 3 = 1 + (2 + 3) や (2 · 3) 4 = 2 (3 · 4) などのように演算を始める順序によらずに結果は等しいという結合法則や、2(3 + 4) = 2 × 3 + 2 × 4 のように、括弧の中から先に計算しても、展開して計算しても同じという分配法則が仮定されます：

$$a + b = b + a, \quad ab = ba, \quad (\text{交換法則}) \quad (\text{A.3})$$

$$(a + b) + c = a + (b + c), \quad (ab)c = a(bc), \quad (\text{結合法則}) \quad (\text{A.4})$$

$$a(b + c) = ab + ac, \quad (a + b)c = ac + bc. \quad (\text{分配法則}) \quad (\text{A.5})$$

これらの基本仮定 (A.3–5) はまとめて計算法則と呼ばれています。計算法則は中学時代から馴染みの公式ですね。

計算法則 (A.3–5) が無理数を含む正の数に対して成立することを納得するには、前の § で議論した数と線分の対応を思い出すとよいでしょう。正の数 a, b については、長さ a, b の線分を考えると、 $a + b = b + a$ が成立することが納得できるでしょう。同様に、 $ab = ba$ については、縦・横が a, b の長方形の面積を考えればよいでしょう。 $(a + b) + c = a + (b + c)$ は、長さ a, b, c の線分の長さの和を測るとき、 $(a + b) + c$ の順でも、 $a + (b + c)$ の順でも全体の長さは変わりませんね。 $(ab)c = a(bc)$ は 3 辺 a, b, c の直方体の体積を測ることを考えればよいでしょう。 $a(b + c) = ab + ac$ については、2 辺が $a, (b + c)$ の長方形の面積を、そのまま $a \times (b + c)$ と測るか、分割して $a \times b + a \times c$ と測る

⁵⁾ 記号 : (コロン) は、説明や引用をする際に、「つまり」の意味でよく用いられます。

かの違いですね．これらの考察から，‘計算法則が無理数を含む正の数に対して成立する’のは間違いありません．

計算法則 (A.3-5) を負の数に拡張して適用する必要性は，方程式を解くための計算から生じました．例えば，方程式 $x + 2 + 2x + 4 = 0$ を解くためには

$$x + 2 + 2x + 4 = x + 2x + 2 + 4 = (1 + 2)x + 6 = 3x + 6 = 0$$

と計算法則を用いて変形し，負の解 $x = -2$ を得ますね．このとき，交換法則 $2 + 2x = 2x + 2$ を用いていますが， $x < 0$ のときこの法則が許されないとして，例えば， $2 + 2x = -2x + 2$ などとするのはどうでしょうか．それはまったく何の根拠もないですね． $x > 0$ のときに仮定された $2 + 2x = 2x + 2$ を， $x < 0$ のときも，受け入れるしかないですね．分配法則 $x + 2x = (1 + 2)x$ についても， $x < 0$ だからといって，これ以外のものを受け入れる根拠はまったくありません．つまり，‘ $x > 0$ のとき成り立つ計算法則 (A.3-5) は， $x < 0$ のときにも，そのまま受け入れる以外に納得できる方法はない’のです．これが意味することは‘負数の性質は正数の性質と同じであると考えるのが自然である’ということです．よって，‘計算法則は，始めから，正数・負数を問わずに成り立つと見なされていた’のです．計算法則をそのまま負数に拡張して適用しても何の矛盾も生じなければ，その一般化を拒絶する理由はまったくなく，むしろそのような仮定は真に自然なものと考えられます．そこで，計算法則は有理数と無理数に対して正・負を問わずに成立すると仮定しましょう．有理数と無理数をあわせて実数 というので，今後は計算法則 (A.3-5) は実数に対して成立するといいいましょう．歴史的なことをいい出さなければ，計算法則を満たすものに実数があり，実数を分類すると正数と負数があるというだけのことです．なお，方程式 $x + 2 + 2x + 4 = 0$ の解が $x = -2$ であることを確かめるのに， $-2 + 2 + 2(-2) + 4 = 0$ と計算しますが，このとき用いられる $2(-2) = -4$ は計算法則を含む演算の公理 (A.1-5) から導かれる定理「正 × 負は負」によって正当化されます．

計算法則 (A.3-5) を眺めてみると，例えば，交換法則 (A.3) $a + b = b + a$ ， $ab = ba$ は‘文字 a にどんな数値を代入しても必ず成立’しますね．そのような等式を文字 a についての恒等式といえます．(A.3) は b についても恒等式になっていますね．結合法則 (A.4)，分配法則 (A.5) でも同様です．そうです，

計算法則はどの文字についても恒等式なのです．よって，我々の行う式変形は，そのほとんどが，恒等式を用いた変形です．‘ある等式が恒等式か方程式かを区別することは決定的に重要’で，そのことは徐々に実感されるでしょう．

なお，計算法則 (A.3-5) では足し算と掛け算のみが現れましたね．しばらくの間，我々はそれらをよく知っているとして話を進めてもよいでしょう．引き算と割り算については，後々のために，ここでそれらを定義⁶⁾しておきましょう．‘引き算 $a - b$ は足し算 $a + (-b)$ によって定義’します．例えば， $1 - 2$ は $1 + (-2)$ のことです．また，‘割り算 $a \div b$ は， $a = bx$ を満たす x を求めることとして，掛け算によって定義’します．引き算や割り算が可能なのは暗黙のうちに仮定されています．君たちがよく知っている割り算の計算法は上の x を具体的に求めるための「アルゴリズム」，つまり‘計算を実行するための手順’です．

不等式については， $a < b$ を「 $a + c = b$ を満たす正数 c が存在する」によって，また $a > b$ を「 $a = b + c$ を満たす正数 c が存在する」によって定義しましょう．すると，演算の公理から以下の基本性質が導かれます：

2 数 a, b について， $a > b$ ， $a = b$ ， $a < b$ のどれか 1 つが成立する．

$$a < b \Rightarrow b > a,$$

$$a < b \text{ かつ } c \leq d \Rightarrow a + c < b + d,$$

$$a < b \text{ かつ } c > 0 \Rightarrow ac < bc,$$

$$a < b \text{ かつ } c < 0 \Rightarrow ac > bc.$$

記号 \leq は $<$ または $=$ のどちらかが成り立つ場合に用います．上の不等式の基本性質はこの § をもう一度読み直すときに確かめればよいでしょう．

1.3.2 演算の公理の意味

さて，演算の公理 (A.1-5) にはどんな意味があるのでしょうか．偉そうな名前がついているのだから，とても重要らしいとは感じるでしょう．そうです，重要な意味があるのです．

⁶⁾ 定義 = 用語についてその意味内容を正確に定めること，または定めた意味．多くの場合，‘定義する’は‘約束する’の意味合いを含んでいます．

数学は「論理」を最も大切に作る学問です。‘その論理は誰に対しても同じ結論に導くもの’でなければなりません。そのためには、まず、用語や記号の意味が明確でなくてはなりません。それ故に数学は定義にうるさいのです。次に、「演繹」、つまり‘論理の展開’が明快に実行できなくてはなりません。そのためには、能力に限りがある人間のために、‘構造が簡単’でなくてはなりません。そこで、‘証明なしに採用される数少ない基本仮定’、つまり公理を出発点におき、それらの公理だけから厳密な演繹によって全ての結果を導き出す構造にしたいわけです。これが現代数学の基本姿勢です。出発点となる公理は、少なすぎると導けることも少ないので使い物にならず、多すぎると無駄が自己矛盾に陥ります。こうして、論理の展開や計算に対して、ちょうどよく選ばれたのが演算の公理 (A.1-5) なのです⁷⁾。

また、日本語や英語のように自然に発生した言語を用いた演繹は曖昧な点があり、厳密な論理を展開したり証明を行うには不向きです。‘ p ならば q が成り立つ’を‘ $p \Rightarrow q$ ’と表しましたが、これは数学的な文章であり、‘論理式’といわれます。数学者は、 $=$ (等しい) や、 \Rightarrow (ならば) の他に、 \wedge (かつ)、 \vee (または)、 \neg (でない)、 \Leftrightarrow (同等である)、 \forall (全ての、任意の)、および \exists (が存在する) などの記号を導入して、‘数学言語’を生み出しました。記号 \forall と \exists はそれぞれ Any (任意の) の A と Exist (存在する) の E をひっ繰り返したものです。

これらの記号を用いると、自然言語の微妙なニュアンスを除いて、文章が表されます。例えば、‘ $x = 1$ または $x = -1$ であることは $x^2 = 1$ と同じことである’は ‘ $x = 1 \vee x = -1 \Leftrightarrow x^2 = 1$ ’ と表され、‘全ての x に対して $x - x = 0$ である’は ‘ $\forall x (x - x = 0)$ ’ です。‘最大の自然数は存在しない(いくらでも大きな自然数が存在する)’は、 x, y を自然数として ‘全ての x に対して、 $x < y$ となる y が存在する’ と意識して、‘ $\forall x (\exists y (x < y))$ ’ と表されます。さらに、‘ x は y が好き’ という文を $L(x, y)$ で表すと、‘全ての人が好かれる人がいる’ などということも ‘ $\exists y (\forall x L(x, y))$ ’ と表されます。このような ‘記号の文章’

⁷⁾ ただし、公理の設定方法はただ1通りではなく、(A.1-5) と同等ですが異なる設定方法もあります。我々の演算の公理 (A.1-5) は最も単純な表現になるものを選んでいますが、後で言及しますが、高校数学では、論理を展開する際に外に2つの公理が必要になります。

を組み立てることによって、数学は完全に厳密な演繹が実行できる構造になっています。したがって、公理から全ての定理が厳密な演繹によって導かれ、それは「証明」という方法で行われます。

1.3.3 命題と証明

公理から定理や公式を導くには「証明」といわれる手続きがなされます。証明はある「主張」に対してそれが正しいかどうかを明らかにすることです。その主張は「正しいかさもなくば正しくないかが判断できる文や式」を指し、それを命題といいます。つまり、ある命題が正しいかどうかを判定することが証明で、正しいと証明された命題が定理です。その意味で公理は証明なしに正しいと見なす特別な命題です。ある命題が正しいとき、その命題は真であるといい、正しくないとき、その命題は偽であるといいます。

命題は、例えば、「 $x = 1 \Rightarrow x^2 = 1$ 」などのように、

$$p \Rightarrow q$$

の形で述べられます。 p をこの命題の仮定、 q を結論といいます。命題が真であることは、仮定 p から結論 q が必ず導かれることと同じです。上の例は真の命題ですね。上の例の仮定と結論を入れ替えた逆と呼ばれる命題「 $x^2 = 1 \Rightarrow x = 1$ 」は、条件 $x^2 = 1$ を満たす一例 $x = -1$ から結論 $x = 1$ を導けないので、偽の命題です。このように命題が偽であることを示すには、それが成立しない例、つまり、反例を挙げれば済みます。今の例でわかるように、元の命題が真であっても、その「逆の命題は必ずしも真とは限りません」。

命題「 $a > b$ ならば $a - b > 0$ 」とその逆「 $a - b > 0$ ならば $a > b$ 」は共に真ですね。ある命題 $p \Rightarrow q$ とその逆 $q \Rightarrow p$ が共に真であることはよくあります。このことは p と q が述べる条件の内容が完全に一致することを意味します。その場合、「 p と q は同値である」といい、記号で「 $p \Rightarrow q$ かつ $q \Rightarrow p$ 」、または、より簡潔に

$$p \Leftrightarrow q$$

と表されます。

「正三角形 \Rightarrow 三角形」の例を持ち出すとわかりやすいと思いますが、命題 $p \Rightarrow q$ が真であるとき、 p は q であるための十分条件 といいます（正三角形ならば‘十分’に三角形である）。このとき、 q は p であるための必要条件 といいます（三角形であることは正三角形であるために‘必要’である）。また、 p と q が同値なとき、つまり、 $p \Leftrightarrow q$ が成り立つときには、 p は q であるための必要十分条件 であるといいます。

等式の命題、例えば、命題「 $(a+b)(a-b) = a^2 - b^2$ 」は、対称律 (A.1) より、命題「 $a^2 - b^2 = (a+b)(a-b)$ 」に等しいので、右辺 $a^2 - b^2$ から左辺 $(a+b)(a-b)$ を導いてもこの命題の正しい証明になります。一般に、数式 A, B が等式 $A = B$ を満たすとき、他の一連の等式 $C = D, E = F, \dots$ を用いて、 $A' = B'$ と変形すると、 $A = B$ と $A' = B'$ は同値であり、 $A' = B'$ から逆に $A = B$ を導くことができます。このことは、必要十分条件を求める問題で、片方の条件のみで済ませられる場合があることを意味します。我々は無意識のうちにそれを行っているようです。

命題「 $x > 3 \Rightarrow x > 2$ 」は、 $x > 3$ となるどの x も $x > 2$ を満たすという意味ですから、真の命題ですね。このとき、命題「 $x > 2$ でない $\Rightarrow x > 3$ でない」、すなわち、「 $x \leq 2 \Rightarrow x \leq 3$ 」も真ですね。また、命題「 $x > 2 \Rightarrow x > 3$ 」は偽ですが、このとき、命題「 $x > 3$ でない $\Rightarrow x > 2$ でない」も偽になります。また、命題「犬 \Rightarrow 動物」は真で、このとき、命題「動物でない \Rightarrow 犬でない」も真ですね。また、考えている対象を動植物とすると、植物は動物でないから命題「犬でない \Rightarrow 動物」は偽で、このとき、「動物でない \Rightarrow 犬」も偽ですね。

一般に、‘ p でない’ことを $\neg p$ または \bar{p} で表し⁸⁾、命題 $p \Rightarrow q$ に対して命題 $\bar{q} \Rightarrow \bar{p}$ をその命題の対偶 といいます。このとき、一般に、‘ある命題の真偽とその対偶の真偽は一致する’ことが証明できます。よって、ある命題の対偶が真であればその命題も真であり、対偶が偽であれば命題も偽です。したがって、この定理は、ある命題を直接に証明するのが難しいときはその対偶を証明すればよいことを意味するので、とても重宝な定理です。この定理の証明には準備が要るので、それは後ほど行いましょう。

⁸⁾ $\neg p$ は not p, \bar{p} は p バーと読みます。

§1.4 基本公式の導出

演算の公理 (A.1-5) のみを用いて、基本公式を実際に導いてみましょう。

1.4.1 移項の公式

演算の公理 (A.1-5) から移項の公式

$$a + b = c \Rightarrow b = c - a, \quad c = a + b \Rightarrow c - a = b$$

を導きましょう。中学校では真っ先に習うこの公式が演算の公理に含まれていなかったのでは？と思った人もいたでしょう。高校では、移項の公式は公理から導かれる定理になります。以下の式変形を (A.1-5) を用いてチェックしてみましょう。

$a + b = c$ が成立する任意の実数 a, b, c を考えて a を移項することを考えます。そのためには、まず、式 $(a + b) - a$ を変形します。引き算の定義と結合法則、交換法則、推移律を用います：

$$(a + b) - a = a + (b - a) = a + (-a + b) = (a - a) + b = 0 + b = b,$$

よって $(a + b) - a = b$.

上式の左辺で $a + b = c$ を用いると

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

よって、 $(a + b) - a = b$ で対称律を適用して、推移律を用いると

$$b = (a + b) - a \text{ かつ } (a + b) - a = c - a \text{ より } b = c - a .$$

よって、 $a + b = c$ から $b = c - a$ が導かれました：

$$a + b = c \Rightarrow b = c - a .$$

これで左辺の a を右辺に移項できました。上式で対称律を用いると

$$c = a + b \Rightarrow c - a = b$$

が得られ、右辺の a を左辺に移項する公式が得られます。

確かに、演算の公理のみから、移項の公式が導かれましたね。これで、今後は、この公式をいつでも使えます。

1.4.2 負数が関係する公式

1.4.2.1 マイナスのマイナスはプラス

負の数を引くときに用いる公式

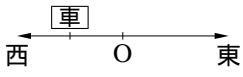
$$-(-a) = +a$$

のことです。中学校では移動の問題として矢印を使った長ったらしい授業があったと思います。中1の教科書を引っ張りだして見てください。ここでは移項の公式を証明したのでそれを用いましょう。 $a = a$ で左辺の a を右辺に移項して $0 = a - a$ 。ここで $-a$ を左辺に移項して、右辺の a を $+a$ と表すと、 $-(-a) = +a$ 。これで証明は終わりです。この等式の導出の正確な意味は、いったん演算の公理を認めてしまうと、 $'-(-a) = +a$ としない限りは矛盾が起こる'、ということです。

あまりにもあっさり導いたので手品のように感じた人もいでしょう。中学校の説明では、抽象的な導出を避けたよりわかりやすいものにしようとして、付加的な説明（つまり余計な仮定）を加えています。高校では、論理的な明快さを重視して、演算の公理から導きます。これは非常に意味があることです。

1.4.2.2 負×負は正

公式 $(-1) \times (-1) = +1$ に対して未だに“^{うな}唸っている”人も多いのではないしょうか。わずか200年前には、世界中の人のほぼ全員が認めなかったことなので、それは無理もないことです。

中1の教科書に以下のような説明がありました：

 （正の時速は東に向っていることを、負の時速は西に向っていることを表すとして）時速 -50 km で走っている自動車は3時間後には $(-50) \times (+3) = -150$ より西へ 150 km の地点にいます。また、3時間前には、東へ 150 km の地点にいますから、 $(-50) \times (-3) = +150$ という計算になるはずというわけです。かなり強引ですね。この例解は、厳密に言えば、少なくともこの例では‘負×負は正’とする必要があるということです。私の経験では、わかったようなわからないような気持ちで、公式「負×負は正」を丸暗記してしまい、その結果未だにモヤモヤしている人が多いようです。

全ての例に当てはまるようにするために，具体例などは一切用いない証明方法が，演算の公理を用いる方法です．その証明方法によるといかなる場合にも‘負×負は正’が導かれます．しかし，そのためには，公理を用いる方法はどうしても‘厳密だが抽象的な導出になる’ことを君たちに受け入れてもらわねばなりません．それが，論理のみを頼りとする数学の宿命であり，「厳密」は具象的実体を捨てる代わりに得られる‘ご褒美’なのです．

その証明は，0の性質⁹⁾をうまく利用することから始まります．以下の式変形において，演算の公理(A.1-5)およびそれから得られた移項の公式のみを用いていることを確認しましょう．

$$0 = (-a) \cdot 0 = (-a)(-b + b) = (-a)(-b) + (-a)b .$$

$$\text{よって } (-a)(-b) + (-a)b = 0 .$$

$$\text{よって } (-a)(-b) = -((-a)b) . \quad \dots\dots\dots \textcircled{1}$$

次に，

$$0 = (-a + a)b = (-a)b + ab ,$$

$$\text{よって } (-a)b = -(ab) (= -ab \text{ と表す}) . \quad \dots\dots\dots \textcircled{2}$$

よって，①と②より

$$(-a)(-b) = -(-ab) . \quad \dots\dots\dots \textcircled{3}$$

また， $ab = a b$ で右辺の ab を先ほどと同様に二度移項して

$$ab = -(-ab) . \quad \dots\dots\dots \textcircled{4}$$

よって，③と④より

$$(-a)(-b) = ab .$$

上式で a, b が正のとき 負×負は正を意味しますね． a, b に何の条件もつけずに導いたので，この等式は全ての実数 a, b について成立します．なお，①において $a < 0, b > 0$ などの場合を考えると，上式は 正×負は負，また負×正は負を示しています．

⁹⁾ 実数の厳密な理論では，0と1に関係する定義が，任意の実数 a に対して

$$a + 0 = a, \quad a + (-a) = 0, \quad a \cdot 1 = a$$

のように表され， $a \cdot 0 = 0 \cdot a = 0$ は証明される定理になります．

以上，計算の基本公式を，演算の公理だけから，いくつか導きました．その他の基本公式を導くことは君たちのレッスンとしましょう．気がついたものがあったらやってみましょう．

§ 1.5 数学の論理構造

数学の論理がどのような仕組みになっているのかも調べてみましょう．

1.5.1 無限大 ∞ は数でない

準備ができましたので，有理数 $\frac{m}{n}$ ($n \neq 0$) における $n \neq 0$ の問題，つまり，‘なぜ 0 で割ることを禁じているのか’ を考えてみましょう．直接 0 で割ることはできないので，0 になっていく正の数で割って調べましょう．まず $n = 0.1$ で割って，次に 0.01 で割って，0.001 で割って，0.0001 で割って，0.00001 で割って，… と繰り返していくと，分子 m を 1 とし， $\frac{m}{n} = \frac{1}{n}$ は

$$10, 100, 1000, 10000, 100000, 1000000, \dots$$

のように，どんどん大きな数になっていくことがわかります．つまり，0 で割ると，‘果てしなく大きな数’ (無限大 ∞ と表しましょう) になってしまい，そんな数が式の中に現れてきます．

無限大 ∞ は果たして‘数’，つまり，演算の公理を満たす実数として認めてよいのでしょうか．数として認めるか認めないかについて判定するのは単なる計算とは違います．判定するための論理が必要です．その論理そのものから議論を始めましょう．

「無限大 ∞ は実数である」という命題，つまり真偽が判断できる文を A としましょう．また， A の否定の命題「無限大 ∞ は実数でない」を \bar{A} (A バーと読みます) としましょう．通常は， A が真なら \bar{A} は偽， A が偽なら \bar{A} は真となり， A と \bar{A} の両方が真または偽になることはありません．よって， A または \bar{A} の片方の真偽を調べるだけで済みます．よくあるのは， A を真とすると矛盾するので A は偽，よって， \bar{A} が真となる場合です．そのような場合は，矛盾を導き出して否定するという証明法，つまり 背理法 が適用できます．

しかしながら、 A と \bar{A} の両方が真または偽になることは決してないのでしょうか。君たちは矛盾にまつわる話を聞いたことがあるでしょう。矛盾の語源である矛と盾の話はよく知っていますね。論理が明確になるように次のように表現しましょう：矛 H は全ての盾を貫き、また盾 T は全ての矛を防ぐという前提で、命題 B 「矛 H は盾 T を貫く」。この問題では、 B が真と仮定すると「盾 T は全ての矛を防ぐ」に反するので B は偽と判断されます。したがって、 B は偽であるかということ、逆に B が偽と仮定すると、「矛 H は全ての盾を貫く」に反するので B は偽でもありません。よって、命題 B は真でも偽でもないことになってしまいます。

この矛盾の話は笑い話で済みました。しかしながら、20 世紀に入って間もなく、数学の世界に激震が走りました。「集合論」という数学の基礎に関わる重要な分野で、真としても偽としても矛盾が起こるパラドックスが見つかったからです。これは、数学が内部矛盾を含む、したがって数学は信用できないという危機でした。

そのパラドックスを直接議論するのはレベルが少々高すぎるので、ここでは「床屋のパラドックス」という例を紹介しましょう：昔々、ある村の男たちは自分でひげを剃るか、その村の床屋（ ）に剃ってもらうかのどちらかでした。そこで問題となった集合論の「集合」というのは物や者全体の集まりのことで、今の場合「村の男たち全員の集まり」を指します。あるとき、床屋が呟きました：“自分で髭を剃らない村の男はわしが剃っている。よって、この村の男たちの集合は「自分で髭を剃る男の集合」と、わしが剃る「自分では剃らない男の集合」に分けられる”。床屋の呟きは正しいでしょうか。すぐ気がつきましたね。床屋自身はいったいどっちの集合に属するのかという問題です。もし、床屋が自分で剃るとすると彼は「自分で髭を剃る男の集合」に属します。すると彼の髭は「わしが剃る」ことになるので、彼は「自分では剃らない男の集合」にも属してしまい、矛盾します。では、彼が「自分では剃らない男の集合」に属するとすると、彼の髭は「わしが剃る」ので、今度は「自分で髭を剃る男の集合」に属してしまい、やはり矛盾が起きます。したがって、床屋の呟きは真としても偽としても矛盾しますね。

この矛盾は「集合」を素朴に「ものの集まり」と定義したことが原因で、集

合に属すか属さないかの吟味ぎんみが不十分なためでした。数学ではこのような曖昧あいまいさは決して許されません。数学の基礎が根底から洗い直され、‘内部矛盾を含まないように数学を再構築する’精力的な試みがなされました。そのために公理と演繹の重要性がますます強調され、公理の立て方はより洗練されていきました。このテキストで公理を強調するのはこの理由によります。現在、当時の集合論は「素朴集合論」と呼ばれ、矛盾を引き起こさない公理によって再構築された集合論は「公理的集合論」といわれます。

以上のような経過を経て、命題の真偽の問題も洗い直されました。そして、

$$\text{排中律: 命題は真または偽のいずれか一方のみが成立する} \quad (\text{A.6})$$

という要請が数学に新たな公理として付加されたのです。排中律が成立するように全体の公理を設定しなさいというわけです。我々が学んでいる実数の理論は、もちろん、その要請を満たすように組み立てられています。よって、命題 A「無限大 ∞ は実数である」が真であると仮定して矛盾を見いだせば、A は偽であることが確定します。

さて、前置きが長くなりましたが、 ∞ が実数であるかどうかを調べましょう。そのためには、演算の公理を用いて判定するわけですから、 ∞ を式に乗せる必要があります。そこで、 ∞ はあまりにも大きすぎて、それに普通の数、例えば 1、を加えても変わらない（区別がつかない）、つまり

$$\infty + 1 = \infty$$

のような性質をもつとしましょう¹⁰⁾。

次に、‘ ∞ を普通の数、つまり実数と仮定’して、演算の公理 (A.1-5) に反しないか検証してみましょう。我々は演算の公理から移項の公式を導いているので、もし ∞ が普通の数ならば、上式 $\infty + 1 = \infty$ より、 ∞ を移項して $1 = \infty - \infty$ 。したがって、直ちに $1 = 0$ を得ます。1 が 0 だなんて、こんな結果は到底認められませんね。つまり、 ∞ を普通の数とすると矛盾が生じるわけです。したがって、排中律により命題「無限大 ∞ は実数である」は偽であることが確定し、無限大 ∞ は実数ではないことが示されました。

¹⁰⁾ 無限大 ∞ は厳密には‘どんな実数よりも大きな数’と定義されます。このとき、 $\infty + 1$ もどんな実数よりも大きくなるので、それも無限大です： $\infty + 1 = \infty$ 。

無限大 ∞ が現れると、公理を満たさない演算が行われて、数学はハチャメチャになります。したがって、‘数学の破壊者 ∞ ’ が現れないようにするために 0 で割ってはいけないというわけです。

1.5.2 $1 + 1 = 2$?

数学の論理構造をもっとよく理解しましょう。そこで、たまに冗談半分で出題される「 $1 + 1 = 2$ か？」という問題を考えてみましょう。これは難問でしょう！ 演算の公理をいくらいじってみても答は出てきません。つまり、この問題は演算の公理とは直接の関係はないのです。この問に答えるには自然数の定義の話から始めないといけません。つまり、‘ 1 とは何か’、‘ 2 とは何か’ から議論を始めよということです。

1 とは 1 個の 1 や 1 番目の 1 などを表す‘自然数の始めの数’のことですね。これが 1 の定義です。では、 2 とは何でしょうか。難しく考えても答は出ないでしょう。単純に、 2 とは $1 + 1$ のことである、つまり、 2 は 1 の次の自然数である、というのが 2 の定義です。いわれてみれば当然ですね。よって、 2 の定義によって、 $2 = 1 + 1$ であるから $1 + 1 = 2$ です。ナンダそういうことか！ ほとんどの人はこの解答で納得できるでしょう。

それでは、 $1 + 1 = 2$ は唯一絶対の解答なのでしょう。以下の議論において数学の理論を 2 つ紹介しますが、そこでは‘等しい’ことを表す記号 $=$ が意味するもの、つまり等号の定義を吟味します。我々は、何を‘等しい’とするかによって、 $1 + 1 = 0$ や $1 + 1 = 1$ のような解答も可能なことを知るでしょう。

ある整数が偶数か奇数かを調べるときには、 2 で割った余りが 0 か 1 かのみに関心があります。そんなときには、計算式に現れる数を 2 で割った余りに置き換えてしまうと素早く求められます。そこで、 2 つの整数 a, b に対して、 a と b をそれぞれ 2 で割ったときそれらの余りが‘等しい’ことを $a = b$ と表しましょう。例えば、 $3 = 1, 5 = 2 \cdot 2 + 1 = 1$ です。すると、 $5 + 3 \cdot 7 = 1 + 1 \cdot 1 = 2 = 0$ のような計算も正当化されます。つまり、この余りの世界では整数は結局のところ 0 か 1 になってしまい、‘ 2 は 0 に等しい’と見なされます。よって、先ほどの $1 + 1 = 2$? の問題では、 $1 + 1 = 0$ も正解になります¹¹⁾。

¹¹⁾ ただし、記号 $=$ の乱用が混乱を引き起さないように、通常は $1 + 1 = 0$ を $1 + 1 \equiv 0 \pmod{2}$ と表し、これを‘合同式’といいます。合同式の詳細については後ほど議論しましょう。

また、コンピュータでは数は電流が流れない OFF の状態に対応する 0 と電流が流れる ON の状態に対応する 1 のみがあり、計算は「2 進法」で行われます。2 進法では $1+1$ は (1 桁上がって) 10 となります。回路を用いた 2 進法の計算は全加算器という演算回路によって行われます。計算を回路で行うのはかなり複雑で、全加算器は種々の基本的な論理回路を組み合わせで作られます。論理回路の 1 つ並列回路は、電池の並列回路と同じように、片方の回路が切れても電流は流れます。

数学者は、以下で解説されるように、並列回路の電流の ON, OFF の状態を等式 $0+0=0$, $1+0=1$, $1+1=1$ などで表すことができることを見いだしました：左辺の 0, 1 は並列回路の各回路のスイッチの OFF, ON を表し、右辺の 0, 1 は並列回路の電流の OFF, ON を表します。「+」は「または」を表す記号として用いられ、並列回路の両方が OFF の状態なら $0+0$ 、片方が ON なら $1+0$ 、両方が ON なら $1+1$ と表されます。よって、 $0+0=0$ は両方のスイッチが OFF なので並列回路に電流は流れないことを表し、 $1+0=1$, $1+1=1$ は片方または両方のスイッチが ON なので電流が流れることを表しますね。これらの等式の「=」は電流の状態が「等しい」ことを表しています。うまいことを考えたものです。このような対応を考えると $1+1=1$ という解も可能ですね。

このように奇妙な数学を用いる回路の理論は、イギリスの数学者ブール (George Boole, 1815~1864) の名を冠する「ブール代数」という数学理論の公理によって、矛盾が起こらないことが保証されています。ブール代数はコンピュータの回路設計に利用され、特にコンピュータの速度を上げるためにはこの数学が不可欠です。また、ブール代数の公理は勝手な発明ではなく、「ある」か「ない」かだけをとり扱うときには、必ずブール代数に従うことが知られています¹²⁾。

¹²⁾ ブール代数の計算規則は

$$\text{並列回路用： } 0+0=0, \quad 0+1=1, \quad 1+0=1, \quad 1+1=1$$

$$\text{直列回路用： } 0 \cdot 0=0, \quad 0 \cdot 1=0, \quad 1 \cdot 0=0, \quad 1 \cdot 1=1$$

です。直列用の積「 \cdot 」は「かつ」と読めばわかるように、両方のスイッチが入っているときだけ電流が流れます。

以上の議論から、「 $=$ 」や「 $+$ 」の意味、さらには0や1の意味をどのように考えるかによって、 $1+1$ は、2にも、0にも、1にもなりました。それらの定義を明確にして初めてその数学が定まるというわけです。逆の言い方をすると、数学は、記号や数の意味を柔軟に解釈すれば、幅広い応用が可能になるということを意味します。そのことは大学の講義で実感するでしょう。

なお、 $a=b$ は a と b が等しいという「関係にある」ことを表しますが、数学は（必ずしも数とは限らない） a と b が何らかの関係にあることに着目して理論を展開することもできます。 a と b の何らかの関係を一般に $a\sim b$ と表しましょう。等式 $a=b$ や、合同式 $a\equiv b\pmod{2}$ などは $a\sim b$ の例です。関係「 \sim 」に対して、「 $a\sim b\Rightarrow b\sim a$ 」(対称律)、および「 $a\sim b$ かつ $b\sim c\Rightarrow a\sim c$ 」(推移律)に加えて、あまりにも当たり前の関係

$$\text{任意の } a \text{ に対して } a\sim a \quad (\text{反射律}) \quad (\text{A.0})$$

が成り立つとき、これらの関係「 \sim 」は「同値関係」であるといい、その関係にある対象物を類別に分けることができます。例えば、整数を偶数と奇数に分けるようなことですが、その他に高校数学では「ベクトル」と呼ばれる量がその類別に関係しています。ベクトルの章でそのことにちょっと触れましょう。

1.5.3 現代数学の公理

この§§では公理や定義に関する現代数学の姿勢について議論します。かなりレベルが高い内容なので、「お話」と考えて「フーン、そういうことか」程度の理解で十分でしょう。難しいのは数式ではなく、今まで当たり前の常識だと思っていたことを根本から考え直すことの難しさです（筆者自身も含めて）。古代ギリシャの哲学者ソクラテス（Socrates, 前470~399）は“知らないことは知らないと自覚しなさい”と強調したそうですが、この種の議論ではよく知っていると思いついでいる「常識」が論理の展開を邪魔します。本当は知らないから、どこが確かでどこが疑わしいかの区別が付きにくいのです。

この他に、1方向にだけ電流を流すために、否定（または反対）を表す記号'があり、 $1'=0$ 、 $0'=1$ と定義されます。対称律・推移律・交換法則・結合法則・分配法則も成り立ちます。

1.5.3.1 ペアノの公理系

前の §§ の議論から、定義、つまり用語や記号の意味を明確に定めることの重要性も認識されたと思います。現代数学ではそのとり扱う対象を‘ほとんど呆れるほど’^{あき}厳密に定義して理論を展開します。参考のために、自然数さえも定義する「ペアノ¹³⁾の公理系¹⁴⁾」と呼ばれる一連の公理群を紹介しましょう。この公理系は自然数を系列 $1, 2, 3, 4, \dots$ として捉えようとする理論で、自然数は個々の自然数の「集まり」と見なされます。一般に、ものの集まりを集合といい、それに入っている「もの」を要素といいます。ペアノの公理系は自然数全体を1つの集合として定義しようというわけです。

では、ペアノの公理系(1-5)を見てみましょう。理解の助けに、^{にわとり}鶏のたとえ話をつけ加えておきましょう。鶏にはその先祖の鶏がいたとします。

- (1) 1 は自然数 N の要素である。(先祖鶏は鶏である)
- (2) n が N の要素なら、 n の次の者 n' も N の要素である。
(鶏の子は鶏である)
- (3) (1), (2) の過程によって得られるものだけが N の要素である。
(先祖鶏と子孫鶏を結ぶ家系の線は1本だけ)
- (4) N の任意の要素 n に対して $n' \neq 1$ 。(子孫鶏は先祖鶏でない)
- (5) N の2つの要素 n と m について、 $n = m$ のときに限り $n' = m'$ 。
(親鶏が違えば子鶏は違う)

ここで、用語‘自然数 N ’は正しくは‘仮に自然数 N と名づけられた未知の集まり’のことであり、それは公理(1-5)によって‘未知の集まり’ N から真の自然数(の集合)に絞り込まれます。また、‘次の者’も正確には定義されていない用語で、その意味は公理が明らかにします。

まず、公理(1)で自然数 N を生み出すための「元素」とでもいうべき1を用意します。この世の全ての物質は元素から作られ、もし元素がなかったらこの世はありませんね。自然数も完全な無からは創ることはできないわけです。

¹³⁾ ペアノ (Giuseppe Peano, 1858 ~ 1932, イタリア)。

¹⁴⁾ 系 = 一定の相互連関をもつものの集合体。または、1つの定理からすぐに導かれる利用価値の高い定理。

公理系 = 数学の理論体系を構成するに当たって、その理論の基礎となる公理の全体。

公理 (2) は N の要素であるための条件を述べています . n が N のある要素のとき , n から n の次の者といわれる 1 つの数 n' が作られ , n' は N の要素です . よって , n' の次の者 $(n)'$ も N の要素です . この手順を続けていくと , N の要素の系列

$$n, n', (n)', ((n))', \dots$$

が得られます . 「 \dots 」はこの系列が果てしなく続くことを表し , N の要素が無数にあることを意味します . ここで , 公理 (1) , (4) を付加して上の系列を絞り込みましょう . (1) は上の系列のどれかが 1 であることを要請し , (4) は系列の先頭以外のものは 1 でないことを要求します . よって , N の系列は先頭が 1 の

$$1, 1', (1)', ((1))', \dots$$

に絞られます . ただし , N が複数の独立な系列からなる可能性も否定できないので , N が系列

$$\begin{aligned} &1, 1', (1)', ((1))', \dots \\ &1, 1', (1)', ((1))', \dots \end{aligned}$$

であるような可能性は残っています .

公理 (3) は N の系列をさらに絞り込みます . (1) , (2) の過程によって得られるのは単純な系列で , 先に述べた複数の系列は除かれます . よって , N の系列は単純な系列 $1, 1', (1)', ((1))', \dots$ となります .

公理 (5) を付加すると N の要素は互いに異なることがわかります . (5) の n と m は $n \neq m$ のとき $n' \neq m'$ ですね . よって , 任意の $n \neq 1$ について $n' \neq 1'$ であり , (4) より $1' \neq 1$ ですから , N の系列の 2 番目の要素 $1'$ は他の全ての要素と異なります . また , $n \neq 1'$ のとき $n' \neq (1)'$ で $(1)' \neq 1'$ ですから , $(1)'$ も他の全ての要素と異なります . 以下 , m を順次 $(1)'$, $((1))'$, \dots としていくと , 同様にして , ' N の全ての要素は互いに異なる' ことがわかります (各自確かめましょう) .

以上の議論から N の系列 $1, 1', (1)', ((1))', \dots$ は自然数の系列と同じものになります . それを明示するために , N の任意の要素 n とその ' 次の者 ' n' の関係を定めましょう . 我々が知っている数は (1) より 1 のみであるという前

提に立っているのです，その関係は 1 のみを巻き込むものです．そこで，その関係を

$$n' = n + 1$$

と書いて，和 $n + 1$ を定めましょう．これが 1 を加える加法 '+1' の定義です．

いよいよ最後の仕上げです． $n' = n + 1$ の n に $1, 1', (1)', ((1)'), \dots$ を代入していくと

$$1' = 1 + 1, (1)' = 1' + 1 = (1 + 1) + 1, ((1)')' = (1')' + 1 = ((1 + 1) + 1) + 1, \dots$$

が得られます．ここで，

$$1' = 2, (1)' = 3, ((1)')' = 4, \dots$$

と書いて，自然数を表す文字 $2, 3, 4, \dots$ を導入する（定義する）と

$$2 = 1 + 1, 3 = 2 + 1 = (1 + 1) + 1, 4 = 3 + 1 = ((1 + 1) + 1) + 1, \dots$$

と，全ての自然数が 1 とその和の形で定義されていることがわかりますね．

この後，公理や定義をつけ加えながら，‘まだるっこいほどに’一歩々々，しかし着実に理論を展開し，自然数の四則や整数・有理数およびその四則を定める方向に進んでいきます．例えば，加法に関する 0 の定義「全ての自然数 n に対して $n + 0 = n$ 」と公理「2 つの自然数 m, n に対して $m + n' = (m + n)'$ 」をつけ加えると自然数の和が定義できます．また，乗法に関する 1 の定義「全ての自然数 n に対して $n \times 1 = n$ 」と公理「2 つの自然数 m, n に対して $m \times n' = m \times n + m$ 」をつけ加えると自然数の積が定義できます．また，自然数 n に対して $n + x = 0$ を満たす x を負の整数 $-n$ と定め，これから 2 つの自然数 m, n に対して引き算 $m - n$ が $m + (-n)$ として定義されます．

ペアノの公理系の議論で注意すべきことは，自然数を言葉を用いて定義したのではなく，自然数が満たすべき一連の数学的条件を公理としておくことによって定義したことです．それによって自然数は論理という土俵の上に乗りました．その結果，自然数の演算は明確に定義され，そして基本的な定理が証明されました．ペアノの公理系の下では，交換法則・結合法則・分配法則の計算法則はもはや基本的な仮定ではなく証明された定理になります．現在，これらの 3 法則は実数の演算に関する定理となっています．

1.5.3.2 公理主義

定義や公理を強調する話をしてきました。それらは論理の基本だからです。数学は、絶対に間違った結果を導いてはいけないという宿命があります。そのために、他の分野と比べて、桁外れに厳しい論理が要求されます。その厳しさに応えるために、必然的に、単純な論理構造が要求されました。その単純な構造が公理という形で現れたのでした。

公理は、高校数学においては演算の公理のことであり、それは正しく「公^{まさ}（万人）に通用する^{ことわり}理（真理）です。公理から、演繹的に、内部矛盾のない全ての結果が導かれれば、その方法は完全です。我々はそれが可能であろうことをある程度納得しました。また、我々の公理体系では、認められないものについて、否定的な証明もできます。それによって、例えば、無限大が普通の数（実数）ではないことが示されました。

また、定義の明確さは論理においては決定的です。我々は、 $1 + 1 = 2$? の例で、そのことを痛感しました。数学では、このようなことがないように、定義は慎重に行います。古代ギリシャ時代、ユークリッドは不朽の名著『原論』をあらわし、その中で公理から厳密な論理によって幾何学を構成しました。彼は「点とは部分をもたないものである」等と定義したのです。彼の厳密な定義は、その幾何学の公理系と共に、2000年もの間、数学の見本とされてきました¹⁵⁾。

数学に現れる用語の意味をより明確に定義する試みもなされました。例えば、ほとんど自明とも思われた自然数の定義です。そこでは、自然数を、説明の語句によって直接定義するのではなく、公理系の中で一連の条件を課して、それらを満たすものとして定義しました。自然数は公理系の中で定義され、定義と公理は渾然一体となりました。

自然数の定義は、数学に現れる概念^{がいねん}¹⁶⁾をより基本的な概念によって定義しようという試みの現れです。このことを究極まで追及していくとどうなるので

¹⁵⁾ ユークリッドのに述べられた定義をいくつか列記します。(1) 点とは部分をもたないものである。(2) 線とは幅のない長さである。(3) 線の端は点である。(4) 直線とは、その上にある全ての点について一様に横たわる線である。(5) 面とは長さのみをもつものである。(6) 面の端は線である。(7) 平面とは、その上にある全ての直線について一様に横たわる面である。等等。

¹⁶⁾ 概念 = 個々の事物から共通な性質をとり出して抽象化し、それによって把握される一般的性質。

しょうか．例えば，点の定義で，‘点とは部分をもたないものである’の‘部分’も，基本的とはいいいくいと定義してみましょう．‘部分’を辞書で調べると，‘全体をいくつかに分けたものの1つ’となっています．さらに，‘全体’とはと追求すると，‘全ての部分’と，また‘部分’が出てきます．これでは堂々巡りで行き詰ってしまいます．つまり，このような方法では点は定義できないわけです．

19世紀末期，ドイツの数学者ヒルベルト（David Hilbert, 1862～1943）は，著書『幾何学基礎論』において，点・直線・平面が関係するある公理系を提唱しました¹⁷⁾．彼は，点・直線・平面といった基本的対象，および，‘存在する’，‘の間に’，‘と合同’といった基本的関係を「基本概念」と考えて，それらに直接的な定義を与えず，基本概念は，その公理系の中で，それらが満たすべき条件によって間接的に定義されていると見なしました．つまり，点・直線・平面は，公理系に述べられている，それらの間の相互関係によって定義され，また‘存在する’，‘の間に’，‘と合同’などの基本的関係も定義されるというわけです．このようなことはペアノの公理系が自然数を定義するだけでなく，未定義な‘次の者’ n から‘1を加える’演算が自然に定義されたことに対比できるところでしょう．

彼が友人の数学者と酒場でビールを飲みながら，“点・直線・平面という代わりに，テーブル・椅子・ビールジョッキと言うことができる”といったことは有名です：公理系の中で，点・直線・平面の用語を，例えば， $T \cdot C \cdot H$ と置き換えたとしましょう．まず， $T \cdot C \cdot H$ は公理系の中で，それぞれ，点・直線・平面が満たすべき基本的性質を当然ながら満たします．次に， $T \cdot C \cdot H$ に

¹⁷⁾ 一部の公理群のみ挙げておきます．(1) 任意の2点に対して，それらを通る直線が存在する．(2) 異なる2点に対して，それらを通る直線は1本より多くは存在しない．(3) 直線上には少なくとも2点が存在する．同一直線上にない少なくとも3点が存在する．(4) 同一直線上にない3点に対して，それらを含む平面が存在する．(5) 上述の3点を含む平面は1つより多くは存在しない．(6) 直線上の2点がある平面上にあるならば，この直線上の全ての点はその平面上にある．(7) 2平面が共有点をもつならば，それらは少なくとももう1つの共有点をもつ．(8) 1つの平面上にない少なくとも4点が存在する．(9) 点Bが点AとCの間にあるならば，A, B, Cは1直線上の異なる点であって，BはCとAの間にある．(10) 1直線上の任意の2点AとCに対して，少なくとも1点Bが存在して，BはCとAの間にある．(11) 1直線上にある任意の3点のうちで，他の2点の間にあるものは，1点より多くはない．等等．

課せられた公理系の条件によって、理論は公理系のみから完全に演繹的に展開され、 $T \cdot C \cdot H$ に課せられた一連の定理が得られます。それらの定理は点・直線・平面が満たすべき定理に一致します。したがって、 $T \cdot C \cdot H$ は、それぞれ、点・直線・平面と同一視せざるを得ないこととなります。このことを指して、点・直線・平面は間接的に定義されているというわけです。このような定義の方法はまさに究極の定義といえるでしょう。点・直線・平面などの基本概念は、直接的定義を必要としない「無定義用語」になりました。

ヒルベルトの公理系は人々の公理に対する考え方も変えました。公理は、‘証明を要しない明白な真実’である必要はなく、理論を厳密に構成する目的のために証明なしに採用される、基本仮定としての命題であると見なされるようになりました。このような考え方は「公理主義」と呼ばれています。

ヒルベルトによって完全に仕上げられた公理的方法は、20世紀に他の数学分野の隅々にまで浸透していきました。無定義の基本概念と、間接的にそれらを定義している一連の公理群によって、各数学理論を厳密に公理的に構成するようになっていったのでした。

§1.6 集合

1.6.1 集合

前の§で自然数の集合が出てきたので、集合の意味を明確にしましょう。

簡単にいえばものの集まりを集合といいます。数学では集合の定義を曖昧にしておくことができないため、‘それに属するか属さないかの区別が明確なもの’だけを集合といい、集合に属する個々のものを要素といいます。例えば、自然数の集まりはそれに属するのが数 $1, 2, 3, \dots$ であることが明確なので集合です。君のクラスの生徒の集まりも、(国籍の有無によって判別される)日本人も集合ですね。ただし、大きい数の集まりとか美人の集まりとかは、それに属する基準が明確でないため、集合ではありません。数直線上の区間、例えば閉区間 $[0, 1]$ ($0 \leq x \leq 1$ である任意の実数 x の集まり)は重要な集合です。要素が有限個である集合を有限集合、有限でない集合を無限集合といいます。自然数の集合や区間は無限集合ですね。

集合を表すには記号を用いるのが便利です．例えば，自然数（の集合） N は

$$N = \{1, 2, 3, \dots\}$$

と中括弧 $\{ \}$ の中にその要素を書き並べて表したり，または

$$N = \{n \mid n \text{ は自然数}\}$$

のように，要素を n などの記号で代表させ， n が集合に属する条件を縦棒 $|$ の後に示す方法もあります．後者のほうが便利なが多く，例えば区間 $[0, 1]$ は

$$[0, 1] = \{x \mid 0 \leq x \leq 1\}$$

と表されます．なお，ただ1つの要素を含んでも集合です．例えば， $\{x \mid x = 0\}$ ．

集合の要素を表すにも便利な記号があります．例えば，1 が自然数 N の要素であることは

$$1 \in N \quad \text{または} \quad N \ni 1$$

と表されます．記号 \in は element（要素）の頭文字 e のギリシャ文字 ϵ （イブシロンと読みます）が変化したという説が有力です．また， $\frac{1}{2}$ が自然数でないことは

$$\frac{1}{2} \notin N \quad \text{または} \quad N \not\ni \frac{1}{2}$$

と表されます．

なお，§§1.5.1 で出てきた「集合論」というのは無限集合を扱う理論であり，特に「公理的集合論」は無限集合と数学言語である論理式を用いて理論を完全に展開する数学の基礎理論です．

1.6.2 真理集合と対偶

§§1.3.3 で ‘ある命題とその対偶の真偽は一致する’らしいことを議論しましたね．集合を用いるとそれをきちんと示すことができます．後で対偶を用いた証明を行うので，ここでやっておきましょう．

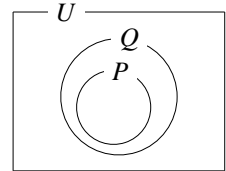
命題「 $x > 3 \Rightarrow x > 2$ 」は真ですが，その意味は集合を用いて表すことができます． $x > 3$ を満たす実数 x の集合は区間 $(3, \infty) = \{x \mid 3 < x < \infty\}$ で，同様に

$x > 2$ の集合は开区間 $(2, \infty) = \{x \mid 2 < x < \infty\}$ です．このとき，区間 $(3, \infty)$ は区間 $(2, \infty)$ にすっぽり ‘含まれ’ ますね¹⁸⁾．同様に，「犬 \Rightarrow 動物」も真の命題なので，犬の集合 [犬] と動物の集合 [動物] を考えると，[犬] は [動物] に含まれますね．一方，偽の命題「 $x > 2 \Rightarrow x > 3$ 」においては区間 $(2, \infty)$ は区間 $(3, \infty)$ に含まれません．また，命題「犬でない \Rightarrow 動物」については，考えている全対象が動植物のとき，集合 [犬でない] は集合 [動物] に含まれないので (犬でないもの，例えば，そこの赤いバラ \notin [動物])，その命題は偽となります．

上の議論はそのまま一般化できます．一般の命題「 $p \Rightarrow q$ 」においてもその命題で対象とする集合 U があり， p と q は U の要素 x についての条件を与えていると考えられます．その条件を表すために p, q を $p(x), q(x)$ と書き，命題を $p(x) \Rightarrow q(x)$ と考えましょう．すると，条件を成り立たせる集合 $P = \{x \mid p(x)\}$ と $Q = \{x \mid q(x)\}$ を考えたとき，

命題 $p \Rightarrow q$ が真であることは $P \subseteq Q$ が成り立つことであると定める，

つまり， P が Q に含まれることをもって命題 $p \Rightarrow q$ を真と定めることができます． p や q の条件が成り立つような要素 x の集合 P, Q を $p(x), q(x)$ の 真理集合 (条件が真となる集合の意味) といいます．真理集合の



相互関係は右のベン図によって表すのが便利で，集合

P の要素は P を表す円の内部に， Q の要素は Q を表す円の内部にあります．すると， $P \subseteq Q$ であるとき， P を表す円は Q を表す円の内部にありますね．

ここで練習問題．命題「 $a < x < b \Rightarrow c < x < d$ 」(ただし， $a < b$) が真であるための条件を述べよ．ヒントは不要でしょう．答は，条件 $a < x < b, c < x < d$ の真理集合 $P = \{x \mid a < x < b\}$ ， $Q = \{x \mid c < x < d\}$ に対して $P \subseteq Q$ が成り立つことですから， $c \leq a < b \leq d$ ですね．等号の有無に注意しましょう．

¹⁸⁾ 集合 A の任意の要素 x が集合 B の要素になっているとき，‘ A は B の部分集合である’，または ‘ A は B に含まれる’ といい，それを記号

$$A \subseteq B \quad \text{または} \quad B \supseteq A$$

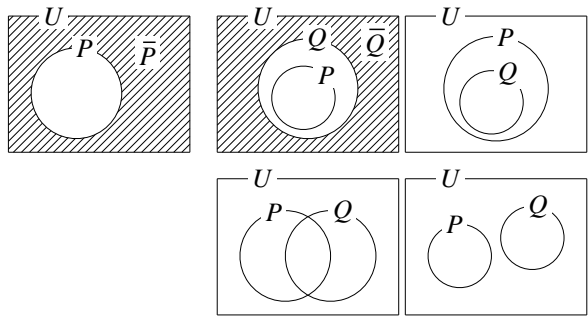
で表します．

次に、命題 $p \Rightarrow q$ の対偶 $\bar{q} \Rightarrow \bar{p}$ を考えましょう (\bar{p} は ' p でない ' の記号). p が $x > 3$ のとき、 \bar{p} は $\overline{x > 3}$ で、考えている対象は実数ですから U は実数の集合であり、よって $\overline{x > 3}$ は $x \leq 3$ です. したがって、 p の真理集合が $P = \{x | x > 3\}$ のとき、 \bar{p} の真理集合を \bar{P} と書くと、 $\bar{P} = \{x | x \leq 3\}$ となります. 同様に、 q が $x > 2$ のとき、 \bar{q} の真理集合は $\bar{Q} = \{x | x \leq 2\}$ となりますね. 以上のことから、真の命題「 $x > 3 \Rightarrow x > 2$ 」の対偶「 $\overline{x > 2} \Rightarrow \overline{x > 3}$ 」については、 $\overline{x > 2}$ の真理集合が $\bar{Q} = \{x | x \leq 2\}$ 、 $\overline{x > 3}$ の真理集合が $\bar{P} = \{x | x \leq 3\}$ です. よって、 $\bar{Q} \subseteq \bar{P}$ が成り立ち、対偶も真となります.

考えている対象が動植物のとき、偽の命題「犬 \Rightarrow 動物」については犬の真理集合が $P = \{x | x \text{ は犬}\}$ 、動物の真理集合が $Q = \{x | x \text{ は動物}\}$ です. その対偶「動物 \Rightarrow 犬」の動物の真理集合は $\bar{Q} = \{x | x \text{ は植物}\}$ 、犬の真理集合は $\bar{P} = \{x | x \text{ は犬}\}$ ですから、 $\bar{Q} \subseteq \bar{P}$ が成り立たず、対偶も偽になりますね.

一般の場合はベン図を用いて議論されます. \bar{p} の真理集合 \bar{P} は、下のベン図にあるように、 P の外、つまり対象とする全体集合 U から p の真理集合 P をとり去った部分です. \bar{q} の真理集合 \bar{Q} についても同様です.

真理集合 P と Q の相互関係は、 $P \subseteq Q$ つまり P が Q にすっぽり入る場合のほか、右図で表されるように、 $Q \subseteq P$ の場合、 P と Q が一部の要素を共有する場合、共通する要素がまっ



たくない場合の4通りが考えられます. 命題 $p \Rightarrow q$ が真の $P \subseteq Q$ の場合は、図から明らかなように、 $\bar{Q} \subseteq \bar{P}$ が成り立つので対偶も真です. それ以外の3つの場合は、どれも $P \subseteq Q$ が成り立たないので $p \Rightarrow q$ は偽で、そのとき $\bar{Q} \subseteq \bar{P}$ も成り立たないので対偶も偽となります. そのことを各自で確かめましょう.

以上の議論から、

命題とその対偶の真偽は一致する

ことが示されました.

§1.7 2 進法

「 $1 + 1 = 2?$ 」のところで出てきた 2 進法に慣れていない人のためにこの § を用意しました。

10 進法の 23.75 を $(23.75)_{10}$ と表すことにしましょう。23.75 は簡略表現であり、その正確な表現は

$$(23.75)_{10} = 2 \cdot 10 + 3 + \frac{7}{10} + \frac{5}{10^2}$$

となります。2 進法の $101.1 = (101.1)_2$ は同様に

$$(101.1)_2 = 1 \cdot 2^2 + 0 \cdot 2 + 1 + \frac{1}{2}$$

です。2 進数では位の数 n が 2 以上だと桁が上がるので、位 n の数は 0 か 1 のみです。

$(23.75)_{10}$ を 2 進法で表してみましよう。10 進法の整数部分は 2 進法でも整数部分、10 進法の小数部分は 2 進法でも小数部分となることに注意して、まず整数部分を分離して調べましよう。2 進法表現の不明な部分は未知数を導入すると（以下、10 進数 $(23)_{10}$ などは 23 と表して）

$$23 = a2^n + b2^{n-1} + \cdots + c2 + d$$

のように表されます。ただし、係数 a, b, \dots, c, d は 0 または 1 の未知数、 2^n (2 の n 乗と読みます) は 2 を n 回掛けたもの、その n を 指数 といい、今の場合 n は未知の自然数です¹⁹⁾。さて、どうやって a, b, \dots, c, d を決めるかとい

¹⁹⁾ 複雑な式が出てきて、わからなくなったという人もいかもしれませんが、しかし、心配することはありません。2 進法の表現からどんな形になるかはわかっていますね。わからないのは 2 の何乗から始まるかということですね。こんなときは、方程式のときに未知数 x を導入したときと同じように、“わかった振りをして”，未知のべき数 2^n を導入すればよいのです。その係数も 0 か 1 がわからないので a とでもしておきます。次の項は 1 次下がるので $+b2^{n-1}$ という具合ですね。以下、項がたくさん現れるので ‘ \cdots ’ 等とごまかしの表現法を使い、最後の 2 項 $+c2 + d$ で締めくくります。このようにして、多くの未知数を含む方程式を得たわけです。あとはこの方程式を解くだけです。未知数が多くても心配は要りません。1 個ずつ順に求まれば、未知数が 1 個の方程式と大差ありません。

参考： n については $2^5 = 32 > 23 > 16 = 2^4$ なので、 n は 4 以下だとわかります。よって、 $n = 4$ として上式を書き下しても構いません。

うと、両辺を2で割って、10進法の小数部分は2進法でも小数部分となることを利用します：

$$\frac{23}{2} = 11 + \frac{1}{2} = a2^{n-1} + b2^{n-2} + \cdots + c + \frac{d}{2}$$

2	23	
2	11	…1 = d
2	5	…1 = c
2	2	…1
2	1	…0 = b
0		…1 = a

これから $d = 1$ を得ます。つまり d は 23 を 2 で割った余りですね。残った整数部分は

$$11 = a2^{n-1} + b2^{n-2} + \cdots + c$$

となり、この両辺をさらに2で割ると c が1と求まります。このとき、左辺の11が23を2で割ったときの商であることに注意しましょう。つまり、 $c = 1$ は23を2で割ったときの商をさらに2で割ったときの余りです。これで求め方のコツがつかめてきたと思います。23を2で割って、商11余り1 = d 。商11をさらに2で割って、その商5余り1 = c 。また商5を2で割って、その商2余り1 = ‘…項’の係数。以下同様にして、最終結果

$$(23)_{10} = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1 = (10111)_2$$

を得ます。

次に、23.75の小数部分0.75を2進法で表してみましよう。整数部分のときの議論と同様に、未知数を導入して

$$0.75 = \frac{a}{2} + \frac{b}{2^2} + \cdots$$

を得ます。ここで、 a, b は0または1の未知数です（もちろん、整数部分のときの a, b とは無関係）。さて、どうやって a, b, \dots を求めたらよいでしょうか。整数部分のときの解法を思い出せば、すぐわかるはずですよ。そうです、両辺に2を掛けて、今度は整数部分を比較すればよいのですね：

$$1.5 = a + \frac{b}{2} + \cdots$$

これから、1.5の整数部分 $1 = a$ ということですね。 b についても同様ですね。1.5の小数部分0.5を2倍して1.0、その整数部分 $1 = b$ 。1.0の小数

部分は 0 なのでこれで終り．よって， $(0.75)_{10} = (0.11)_2$ ．以上のことから， $(23.75)_{10} = (10111.11)_2$ が得られます．

10 進数を 2 進数に直すとき，2 で割ったり 2 を掛けたりしました．10 進数を任意の p 進数にするときは，今度は， p で割ったり p を掛けたりすればよいですね．

最後に，練習問題をやっておきましょう． $(23.23)_5$ を 10 進法で表せ．ヒント：10 で割ったり掛けたりするまでもありません．答は $(23.23)_5 = (13.52)_{10}$ ですね．もう 1 題． $(0.1)_3$ を 10 進法で表せ．ヒント： $(0.1)_3 = \frac{1}{3}$ ですね．定義にしたがって

$$\frac{1}{3} = \frac{a}{10} + \frac{b}{10^2} + \frac{c}{10^3} + \cdots \quad (a, b, c, \cdots = 0, 1, 2, \cdots, 9)$$

とすると，かえって面倒になるかな．答は $(0.1)_3 = (0.333\cdots)_{10}$ だね．

§1.8 実数の小数表示

有理数は分数によって表されました．では， $\sqrt{2}$ を代表とする無理数はどう表されるのでしょうか．無理数は，この章の始めに述べたように，分数で表すことができない数のことです（後でそのことを $\sqrt{2}$ について証明しましょう）． $\sqrt{(\cdot)}$ は 2 乗すると (\cdot) になる正の数という意味で使われた単なる記号です．そこで，有理数や無理数を小数を用いて表現してみましよう．すると両者の違いが浮かび上がってきます．

1.8.1 有理数の性質

有理数を小数で表してその性質を調べてみましょう．例えば，

$$\frac{3}{2} = 1.5, \quad \frac{1}{5} = 0.2, \quad \frac{2}{16} = \frac{125}{1000} = 0.125$$

などのように，分子・分母を整数倍したとき分母が $10 \cdots 0$ の形に書けるものは有限小数，つまり小数点以下のある位で終わる小数になります．整数は特別な有限小数と見なしましょう．

そうでない有理数，例えば，

$$\frac{4}{3} = 1.3333\cdots (= 1.\dot{3} \text{と表しましょう}),$$

$$\frac{3}{7} = 0.42857142857142\cdots (= 0.4\dot{2}857\dot{1})$$

などは循環小数，つまり，小数点以下のある位から，ある数字の列が繰り返し限りなく続く小数になります．このように有理数は有限小数または循環小数で表されます．

循環小数になるメカニズムを $\frac{3}{7}$ で調べてみましょう．まず， $3 < 7$ より整数部分は 0 です．3 を 10 倍して 7 で割ると，商 4 (小数第 1 位の数)，そのときの余り 2．以下同様に続けていって，それらを書き下していくと，余りが 0 となることはなく，

$$\begin{array}{l} \text{商} \quad 4, 2, 8, 5, 7, 1, 4, 2, 8, 5, 7, 1, 4, 2, 8, 5, 7, \cdots \\ \text{余り} \quad \underline{2}, 6, 4, 5, 1, 3, \underline{2}, 6, 4, 5, 1, 3, \underline{2}, 6, 4, 5, 1, \cdots \end{array}$$

と続きます．余り < 7 より，少なくとも 7 回に 1 回は同じ余り，例えば 2 が現れますね (上の表の余りが 2 のところを参照)．余りが同じ 2 とすると，10 倍して 7 で割った商 2 (次の小数位の数) も余り 6 も同じになります．よって，次の次の小数位の数 8 も余り 4 も同じです．そして，次の次の次の小数位も同じ， \cdots ．これらのことから，小数第 2 位の 2 と小数第 8 位の 2 のように，7 位の差以内に同じ数が現れ，いったん同じ数になると，それらに続く数も同じになります．こうして循環小数になるのですね．

以上の議論から，任意の有理数は有限小数または循環小数で表されることがわかるでしょう．任意の有限小数・循環小数は，また逆に，有理数の形に表すことができます．例えば， $N = 0.\dot{1}2 = 0.12121212\cdots$ なら，100 倍すると $100N = 12.12121212\cdots$ だから， $(100 - 1)N = 12$ ．よって， $N = \frac{4}{33}$ ．

最後に，注意すればすぐに気がつくことですが，有理数 $\frac{m}{n}$ が循環小数になるか有限小数になるかは，何進法で考えているかによります．例えば， $\frac{3}{7} = 0 + \frac{3}{7} = (0.3)_7$ ですね．つまり，有理数 $\frac{m}{n}$ は n 進法では有限小数になります．このことは，有限小数と循環小数の間に本質的な差はないことを意味します．

1.8.2 循環小数でない無限小数

任意の有理数 $\frac{m}{n}$ は、必ず有限小数か循環小数で表されることがわかりました。では、数にはその2種類しかないのかと考えてみましょう。循環小数は、小数点以下の数字がある周期で無限に循環する無限小数ですね。ということは、「循環しないで無限に続く無限小数」があっても不思議はありませんね。有理数の加減乗除の計算をすると結果は有理数ですから、加減乗除によってはそんな数は決して現れません。

しかしながら、図形を扱う幾何の計算では、直角三角形の斜辺の長さ等を扱います。このとき、三平方の定理を用いるので、根号計算を行います。そして、 $\sqrt{2}$ などの無理数が現れます。根号 $\sqrt{\quad}$ の定義に従って計算して、小数で表していくと

$$\sqrt{2} = 1.4142135623730950488016887242097 \dots$$

となります²⁰⁾。 $\sqrt{2}$ はいくら桁を増やして精確に計算しても有限小数にも循環小数にもなりません。つまり、 $\sqrt{2}$ は循環しない無限小数なのです。よって、 $\sqrt{2}$ は有理数ではないはずで、分数で表すことはできませんね。

そのことを、 $\sqrt{2}$ が有理数であると仮定して否定する証明、つまり背理法を用いて確かめてみましょう。 $\sqrt{2}$ が

$$\sqrt{2} = \frac{p}{q}$$

と分数で表せたとしましょう。ただし、 $\frac{p}{q}$ が既約分数になるように、 p, q は(1以外の)公約数のない自然数とします。ここがミソです。両辺を2乗して、分母を払うと

$$2q^2 = p^2.$$

²⁰⁾ $\sqrt{2}$ の求め方の一例を示します。 $\sqrt{2}$ は2乗して2になる正の数というのがその定義です。そこで、小数第1位の1.4まではわかっていたとすると、小数第2位の数を a ($a = 0, 1, 2, \dots, 9$) として、 $(1.4a)^2 < 2$ を満たす最大の a を $0, 1, 2, \dots, 9$ の中から探します。電卓でやるとたいして手間はかかりません。こうして、 $(1.41)^2 < 2$ 、 $(1.42)^2 > 2$ なので $a = 1$ 、よって1.41まで決まります。下位の数字も同様です。試しにやってみることをお勧めします。 $\sqrt{2}$ の感触がつかめます。

左辺は偶数だから，右辺 p^2 も偶数．そのためには p が偶数．よって， $p = 2p'$ (p' は自然数) とおけば

$$2q^2 = 4p'^2, \quad \text{よって} \quad q^2 = 2p'^2.$$

$2p'^2$ は偶数だから q^2 は偶数，よって， q は偶数です．すると p も q も偶数になるので， p, q は公約数 2 をもつことになり， p, q は公約数のない自然数としたことに反しますね．この矛盾は $\sqrt{2}$ が有理数であると仮定したために生じました．したがって， $\sqrt{2}$ は有理数ではない実数，つまり無理数であることが証明されました．

同様にして， $\sqrt{3}, \sqrt{5}, \sqrt{6}, \dots$ も， $1 + \sqrt{2}, 1 + \sqrt{3}, 1 + \sqrt{5}, \dots$ も， $\sqrt[3]{2}, \sqrt[3]{3}, \sqrt[3]{4}, \dots$ も無理数であることがわかります²¹⁾．これらの例から，無数に多くの無理数が存在し，無理数のほうが有理数よりはるかに多そうです．

さらに，円周率 π ：

$$\pi = 3.1415926535897932384626433832795 \dots$$

も無理数であることが示されました²²⁾．

§1.9 実数の連続性

我々は §1.1 で直線上の点と実数の対応を考えました．点は連続的に動かすことができるので「連続量」ですが，点と 1:1 に対応して実数が存在して，実数も連続量になるかどうかはまだ定かではありません．実数を有限小数や無限小数で表したとして，それらの全体，つまり実数の集合を想像すると，いかにも連続的に存在すると思われるほどの多さです．また，任意の無限小数を考えると，その数と小数 ∞ 位で異なる小数を想像することはできます．しかしながら，きちんとした証明となると，想像を絶するほど難しそうです．

²¹⁾ $\sqrt[n]{\cdot}$ は n 乗して (\cdot) になる実数です．

²²⁾ 2002 年 12 月，日本の数学者とコンピュータ会社の技術者チームが π を 1 兆 2411 億桁まで計算し，自ら樹立していた世界記録 2061 億桁をさらに更新しました．関心のある人はホームページ <http://pi2.cc.u-tokyo.ac.jp/index-j.html> をご覧ください．

実数が連続量であること、つまり、実数が連続的に存在することは真に重要なことです。例えば、連続的に流れている時間は実数で表現されますが、実数がどこかで不連続ならば、そこで時間が存在しないのと同じくらいに由々しいことです。また、数学の根幹に関わる「関数の連続性」に関する定理は実数の連続性から導かれます。それほど重要なことなのですが、高校数学はそれを暗黙の了解事項にしています。以下の議論で、実数の連続性を保障するデデキンント (Julius Wilhelm Richard Dedekind, 1831 ~ 1916, ドイツ) の理論にある程度踏み入ってみましょう。その議論をするときは、我々は有理数についてはよく知っている、つまり有理数の厳密な理論があるとして話を進めましょう。

1.9.1 有理数と無理数の特徴

有理数と無理数の特徴を今までとは違う角度から調べてみましょう。両者を小数表示して近似を考えると違いが見えてきます。

k を任意の整数, n を (大きくできる) 自然数として、有理数

$$a = k + \frac{m}{n} \quad (m = 0, 1, \dots, n-1)$$

を考えてみましょう。 a が表すことができる有理数は

$$k, \quad k + \frac{1}{n}, \quad k + \frac{2}{n}, \quad \dots, \quad k + \frac{n-1}{n} \quad (k \text{ は任意の整数})$$

なので、これらの有理数の集合は、隣の有理数との差が $\frac{1}{n}$ の、0 を含む、全ての有理数を表します。分母 n を大きくすれば、隣との差 $\frac{1}{n}$ はいくらでも小さくできるので、有理数は、 $-\infty$ から $+\infty$ まで、限りなく小さな間隔でびっしり並んでいることがわかります。つまり、' 任意の実数に対して、その数にいくらでも近い有理数が存在する ' ことになります。

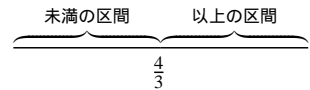
数直線上の 1 点から左右の有理数を眺めてみましょう。左右の有理数は、遠くから近くまで、そして ' すぐ隣 ' までぎっしりとあります。しかし、無限に拡大してよく見るとスカスカで、その間には無理数? が連なっているようです。

次に、有理数の近似を考え、近似を上げていったときに、その有理数のごく近くでどのような状況になっているかを見てみましょう。例えば、 $\frac{4}{3} = 1.333\dots$

の第 n 位近似 (小数点以下第 $n+1$ 位以下切り捨て) を考えます. 第 3 位近似は 1.333 ですが, $1.333 < \frac{4}{3}$ です. 第 4 位近似でも, $1.3333 < \frac{4}{3}$. 第 5 位近似でも, $1.33333 < \frac{4}{3}$, \dots となって, 切り捨て近似は近似を上げていくと $\frac{4}{3}$ に近づいていきますが, どの近似も $\frac{4}{3}$ より小さい値になりますね.

さて, 全ての有理数の集合を有理数 $\frac{4}{3}$ によって 2 つの集合に分けましょう. それらは, 数直線を $\frac{4}{3}$ で切断したとき, $\frac{4}{3}$ ‘未満の区間’ に含まれる有理数の集合と $\frac{4}{3}$ ‘以上の区間’ に含まれる有理数の集合です. このように分けると, 近似 1.333, 1.3333, 1.33333, \dots は全て未満の区間における近似ですね. また, これらは全て有理数であり, それらは近似を上げるにつれて増加し, $\frac{4}{3}$ に下のほうから限りなく近づいていきます.

よって, 未満の区間では, 増加する無数の有理数が存在することになります. しかしながら, そのうちのどれが最大のものかは特定でき



ません. このようなとき, 最大のものとは存在しないということにします. よって, 有理数 $\frac{4}{3}$ 未満の区間では最大の有理数は存在しません. 一方, $\frac{4}{3}$ 以上の区間では, 最小の有理数は特定できます. $\frac{4}{3}$ それ自身が最小になりますね.

負数 $-1 = -1.000\dots$ についても同様です. -1 未満の区間での近似 -1.1 , -1.01 , -1.001 , \dots (< -1) も全て有理数ですが, 最大のものはありません. -1 以上の区間では -1 が最小の有理数です. 他の有理数についても同様で, 有理数については, その未満の区間では最大の有理数がなく, その以上の区間ではその有理数それ自身が最小の有理数です.

無理数ではどうでしょうか. $\sqrt{2} = 1.41421356\dots$ でも同様に近似してみましょう. 未満の区間での近似は 1.4, 1.41, 1.414, 1.4142, \dots ($< \sqrt{2}$) となり最大の有理数はありません. 以上の区間での近似は, $\sqrt{2}$ 以上になるように第 n 位近似では小数第 $n+1$ 位を切り上げます. それは未満の区間での近似に, それぞれ, 0.1, 0.01, 0.001, 0.0001, \dots をつけ加えて得られます: 1.5, 1.42, 1.415, 1.4143, \dots ($> \sqrt{2}$). こちらのほうは小さくなっていく有理数ですが, 最小と特定できるものがないので, 無理数 $\sqrt{2}$ は以上の区間においても最小の有理数は存在しません. 他の無理数についても同様ですね.

1.9.2 実数の新たな定義

前の §§ の議論をまとめましょう：有理数は未満の区間で最大の有理数がなく、以上の区間で最小の有理数（その有理数自身）がある．無理数は未満の区間で最大の有理数がなく、以上の区間でも最小の有理数がない．

次に、上のまとめの文の主部と述部を入れ替えて、元の主語に‘その境目の’をつけてみましょう：未満の区間で最大の有理数がなく、以上の区間で最小の有理数があるのは‘その境目の’有理数である．未満の区間で最大の有理数がなく、以上の区間で最小の有理数がないのは‘その境目の’無理数である．

新たな主部を見ると‘有理数’だけが現れ‘無理数’は消えています．そこで、述部の‘その境目’を決める条件が有理数だけを用いて以下のように表現できます．

全区間に存在する全ての有理数を考えます．そして、全ての有理数を、以下の条件で、未満の区間のものと以上の区間のものにふるい分けします：未満の区間のどの有理数も以上の区間の全ての有理数より小さい．また、未満の区間に最大の有理数は存在しないという条件をつけ加えます．

このとき、以上の区間に対して、2通りの場合があります：

- (A) 最小の有理数がある． (B) 最小の有理数はない．

デデキントは著作『連続性と無理数』(1872)の中で次のように述べました：(A)の場合には未満の区間と以上の区間の「境目」は有理数を表すと定義し、(B)の場合にはその境目は無理数を表すと定義する．無理数を定義するとは無理数の存在を定義するということです．これは凄いことをいっています．つまり、彼は無理数を定義によって‘創造し’、それが理論の出発点の公理であると宣言しているのです．こういわれたらその定義を受け入れるか受け入れないかの二者択一です．そして、全ての数学者がこの定義を受け容れたのです．

次のようにいうとわかりやすいでしょうか．数直線上で、未満の区間と以上の区間を設定すると、全ての有理数は両区間のどちらかにふるい分けられて、その境目の点に対応する数が有理数か無理数かに定義されます．そこで、両区間の設定を連続的に変化させると、つまり境目を連続的に移動させると、有理数のふるい分けも連続的に変化し、境目の点の実数も連続的に有理数か無理数

に定義されていきます。つまり、連続的に全てのふるい分けを実行すると、有理数と有理数の間に潜んでいた無理数が境目として全て^{あぶ}炙り出されるというわけです。

こうして、 $-\infty$ から $+\infty$ まで実数が連続的に存在することになり、‘実数の連続性が保障された’こととなります。我々は、以後、この新しい定義による実数を実数としましょう。

なお、この実数についての理論では加減乗除もきちっと定義して、‘実数は計算法則を満たす’ことを証明しています。また新しい定義による無理数は循環しない無限小数に一致することが示されました²³⁾。

これでひとまず実数の基礎についての議論を終えましょう。

§1.10 整数の性質

整数の性質についての基本的な議論を行いましょう。その中には §§1.5.2 の「 $1 + 1 = 2?$ 」で出てきた合同式もあります。今までに公理 (A.1-6) を議論しましたが、高校数学で必要なもう 1 つの公理も簡単に議論しておきます。

1.10.1 自然数の因数分解

以下、この §§ で表れる数は、簡単のために、全て自然数としましょう。

1.10.1.1 約数・倍数・素数

自然数 a が自然数 b で割り切れるとき、 b は a の約数 (divisor) といい (しばしば、 b は a の因数ともいいます)、 a は b の倍数 (multiple) といいましたね。‘ a が b で割り切れる’ことを正確に表すと

$$a = bk \text{ を満たす自然数 } k \text{ が存在する}$$

となります。自然数のうち、1 と自分自身以外に約数をもたない 2 以上の自然数を素数といい、残りの 1 以外の自然数を合成数といいます。1 は素数でも合成数でもありません。

²³⁾ ここに紹介したのは「デデキントの切断」という有名な理論です。興味のある人は、集合と数列の極限を学んだ後、挑戦されるとよいでしょう。

素数を小さい順に並べると、2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, … となり、大きくなるにつれてだんだん^{まば}疎らになっていきますが、いくらでも大きなものがありそうですね。実際、2000年以上前にユークリッドはいくらでも大きな素数が存在することを証明しています：素数が有限個であると仮定して、それらを $p_1, p_2, p_3, \dots, p_n$ としましょう。そこで、自然数

$$N = (p_1 \cdot p_2 \cdot p_3 \cdots p_n) + 1$$

を考えましょう。このとき、もし N が合成数だとすると、 N は素数 $p_1, p_2, p_3, \dots, p_n$ のどれかで必ず割り切れるはずですが、実際には、 N はどの p_k ($k = 1, 2, \dots, n$) で割っても1余るので、 N は素数でなければなりません。しからば、 N は p_k のどれかに一致するかというと、どの p_k についても $p_k < N$ は明らかで、 N はどの p_k にも一致しない素数ということになります。よって、素数は $p_1, p_2, p_3, \dots, p_n$ の有限個しかないと仮定すると矛盾するので、命題「素数は有限個しかない」は否定され、したがって、排中律の公理（つまり背理法）により命題「素数は無限にある」が成立します。

2004年8月現在、知られている最大の素数は $2^{24036583} - 1$ のようです²⁴⁾。これは「メルセンヌ素数」といわれるタイプです。素数探しはコンピュータの性能試験にも役立っています。

1.10.1.2 素因数分解の一意性

素因数分解の例 $420 = 2^2 \cdot 3 \cdot 5 \cdot 7$ からわかるように、「自然数は素数の積に一意に²⁵⁾因数分解される」ことは経験的によく知られていますね。これは完全に一般的な事実で、素因数分解の一意性定理と呼ばれ、整数論の基本定理になっています。素因数分解の一意性は、数学的に重要なことはもちろんのこと、現在では、インターネット通信の秘密保持のための「暗号鍵」の原理として役立っています。

素因数分解の一意性定理の厳密な証明には「数列」の知識が必要になりますが、君たちはその証明を授業で教わることはまずないので、ここでは証明に近い形で解説しましょう。

²⁴⁾ 素数に関心のある人はウェブサイト <http://www.utm.edu/research/primes/largest.html> で調べられます。

²⁵⁾ 一意に = ただ1通りに。

まずは、2以上の自然数が必ず素因数分解されることから、例えば、10以下の自然数は全て素因数分解ができるので、‘ある自然数 N までは素因数に分解できることがわかっている’ としましょう。証明の核心は、自然数 N が素因数分解できれば $N+1$ も素因数分解できることが示され、その結果を用いて、まったく同様に $N+2$ についても示され、 $N+3$ でも同様、 \dots と、芋づる式に、または将棋倒しのように、いくらでも大きな自然数についても示すことができることです。

ある自然数 N までは素因数に分解できることが示されていると仮定します。次に、自然数 $N+1$ が素数ならば既に素因数分解されています。もし $N+1$ が合成数ならば、その定義によって、 $N+1 = ab$ と2以上の自然数 a, b の積に因数分解できます。このとき、 a, b は明らかに N 以下の自然数になるので、仮定「 N までは素因数分解できる」によって、自然数 a, b は共に素因数分解でき、よって、 $N+1$ が素因数分解できます。したがって、 $N+1$ まで素因数分解できます。そこで今度は‘ $N+1$ まで素因数分解できる’ことを利用すると、同様にして、 $N+2$ まで素因数分解できることが示されます（ $N+2$ が合成数のとき $N+2 = a'b'$ とでもして確かめましょう）。以下、このことを繰り返していくと、原理的には、‘いかに大きな自然数についても’素因数分解できることがわかりますね。このような証明法は 数学的帰納法 と呼ばれ、§§1.3.1 の演算の公理 (A.1–5) を排中律の公理 (A.6) と共に補う、現代数学の基本公理として仮定されています²⁶⁾。数学的帰納法の原理を公理 (A.7) としましょう。以上のことから、全ての自然数は素因数に分解できることが示されました。

次は、素因数分解の一意性のほうです。まず、 p を素数として、 $pa = bc$ が成立するならば、 p は b または c の約数になることを示しましょう： $pa = bc$ の両辺を p で割ると

$$a = \frac{bc}{p} .$$

左辺 a は自然数ですから、右辺も自然数でなければならず、 (bc) は p の倍数です。このとき、 $b, c, (bc)$ は素因数分解できることが既に示されていることに注意しましょう。 p は素数、 b, c は自然数ですから、 b と c の両方が p の倍数

²⁶⁾ 同様の論法はペアノの公理系のところでも現れ、そこでは当然のこととして黙って用いられました。数学的帰納法の詳細は「数列」の章で扱います。

でないとする (bc) は、 p を因数として含まなくなるので、 p で割り切れなくなり、右辺は自然数になりません。よって、 b または c の少なくとも一方は p の倍数です。 $pa = bcd$ が成立する場合も、 b, c, d のどれも p の倍数でないとする \Rightarrow 矛盾します。まったく同様に、補助定理

$$pa = b_1 b_2 \cdots b_n \Rightarrow b_1, b_2, \dots, b_n \text{ のどれかは } p \text{ の倍数}$$

が任意の自然数 n に対して得られます。

これで準備が整いました。2 以上の任意の自然数 N が、素数の 2 つの組 p_1, p_2, \dots, p_m と q_1, q_2, \dots, q_n を用いて

$$N = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$$

と 2 通りに表されたとしましょう。補助定理より、素数 p_1 は q_1, q_2, \dots, q_n のどれかの約数です。 p_1 が q_k の約数だとすると、 q_k も素数なので、両者は一致する、つまり、 $p_1 = q_k$ が成り立ちます。そこで、上式の両辺を p_1 で割って、素数 p_2 について同じ議論をします。 p_3, \dots, p_m についても同じことを繰り返して、それらで割っていくと左辺は 1 になります。このとき、右辺が 1 でないと矛盾するので、 $p_1 p_2 \cdots p_m$ と $q_1 q_2 \cdots q_n$ は完全に同じ素数の積の形をしていなければなりません。つまり、両者とも素数を小さい順に並べてあれば、

$$p_1 = q_1, \quad p_2 = q_2, \quad \dots, \quad p_m = q_n \quad (m = n)$$

が成立します。少々長くなりましたが、これで素因数分解の一意性定理が示されました。

1.10.1.3 公約数・公倍数

3 つの自然数 a, b, c について、 c が a の約数でもあり、かつ b の約数でもあるとき、つまり

$$a = ck, \quad b = ck' \quad \text{を同時に満たす自然数 } k, k' \text{ が存在する}$$

とき、 c を a, b の公約数 (common divisor) といいます。公約数のうち最大のもを最大公約数 (greatest common divisor, 略して、GCD) といいます。 a, b の最大公約数を表すときに、記号 $\text{GCD}(a, b)$ はよく用いられます。例え

ば, 10 と 20 の公約数は, 1, 2, 5, 10 の 4 個あり, 最大公約数 $\text{GCD}(10, 20)$ は 10 です. 1 は任意の自然数の約数であることに注意しましょう. 自然数 a, b が 1 以外に公約数をもたないことを, “ a, b は互いに素” であるといい, しばしば, $\text{GCD}(a, b) = 1$ と表されます. 2 つの異なる素数 p, q は, もちろん, 互いに素なので $\text{GCD}(p, q) = 1$ です.

3 つの自然数 a, b, c について, c が a の倍数でもあり, かつ b の倍数でもあるとき, つまり

$$c = ak, \quad c = bk' \quad \text{を同時に満たす自然数 } k, k' \text{ が存在する}$$

とき, c を a, b の公倍数 (common multiple) といいます. 公倍数のうち最小のものを最小公倍数 (least common multiple, 略して, LCM) といいます. a, b の最小公倍数を表すときに, 記号 $\text{LCM}(a, b)$ はよく用いられます. 例えば, 10 と 15 の公倍数は 30, 60, 90, ... と無数にあり, 最小公倍数 30 は $\text{LCM}(10, 15) = 30$ と表します.

2 つの自然数 a, b とそれらの最大公約数 $\text{GCD}(a, b) = G$ を用いて a, b の最小公倍数 $\text{LCM}(a, b)$ を表すことができます: $a = Ga', b = Gb'$ とおくと, a' と b' は互いに素だから

$$\text{LCM}(a, b) = Ga'b'$$

となりますね. したがって,

$$\text{LCM}(a, b) = \frac{ab}{\text{GCD}(a, b)} \Leftrightarrow \text{GCD}(a, b)\text{LCM}(a, b) = ab$$

が成り立ちます. これは最大公約数と最小公倍数の基本的な関係です.

1.10.2 整数の割り算

約数や倍数は, 問題にしている数が整数の場合には, 一般に整数の範囲で考えます. ただし, 最大公約数は正の公約数のうちで最大のもの, 最小公倍数は正の公倍数のうちで最小のものとしします. なお, 0 については, 任意の整数 k に対して $0 = k \times 0$ (0 を k で割ると割り切れる) が成り立つので, ‘0 は任意の整数の倍数’ です.

1.10.2.1 ユークリッドの互除法

自然数 a, b の最大公約数 GCD を求める素朴な方法は a, b を素因数分解することですが、数が大きくなるにつれて耐えがたい負担になります。例えば、13256 と 123 の GCD が 1、つまりそれらが互いに素であることを示すのに君は何分かかるでしょうか？ 割り算を何度か繰り返して最大公約数を求めるユークリッドの互除法 というのがあります。その方法は理論的考察をする際にも重要です。

自然数 a, b ($a > b$) に対して、 a を b で割った商を q 、余りを r とすると

$$a = bq + r, \quad 0 \leq r < b$$

を満たす自然数 q, r がただ 1 通りに定まります。この式は、 $a = bq + r$ を $a - b \times q = r$ と変形すればわかるように、 a から b を繰り返して引き、その残り r が $0 \leq r < b$ となるまで続けたとすると、引いた回数が q であることを意味しています。この見方をすると、商 q 、余り r がただ 1 通りに定まること、および、割り算は引き算の繰り返しであることが納得できるでしょう。

ユークリッドの互除法の原理は a, b の最大公約数を G 、また b, r の最大公約数を G' とすると、 $G = G'$ となることです：まず、 $a = Ga', b = Gb'$ とおくと a', b' は自然数で、このとき $a = bq + r$ より $r = Ga' - Gb'q = G(a' - b'q)$ となって G は r の約数です。よって、 $b = Gb'$ も成り立つから、 G は b, r の公約数です： G は G' の約数。次に、 $b = G'b'', r = G'r''$ とおくと b'', r'' は自然数で、 $a = bq + r = G'(b''q + r'')$ だから、 G' は a, b の公約数です： G' は G の約数。したがって、 G は G' の約数かつ G' は G の約数となるので、 $G = G'$ が成り立ちます：

$$a = bq + r \text{ のとき } \quad \text{GCD}(a, b) = \text{GCD}(b, r).$$

そこで、今度は b を r で割ると、同様にして

$$b = rq_1 + r_1 \text{ のとき } \quad \text{GCD}(b, r) = \text{GCD}(r, r_1)$$

が得られます。これで見えてきたと思います。この割り算の手続きを繰り返すと、最後には必ず割り切れて（何故でしょう）、 $r_{n-1} = r_n q_{n+1} + 0$ のような形になり

$$\text{GCD}(a, b) = \text{GCD}(r_n, 0)$$

が得られます。 $0 = r_n \times 0$ ですから， $\text{GCD}(a, b) = r_n$ と最大公約数が求まります。

ユークリッドの互除法を用いて 13256 と 123 の最大公約数を求めてみましょう。まず，13256 を 123 で割ると， $13256 = 123 \times 107 + 95$ 。次に，123 を 95 で割ると， $123 = 95 \times 1 + 28$ 。以下同様にして， $95 = 28 \times 3 + 11$ 。 $28 = 11 \times 2 + 6$ 。 $11 = 6 \times 1 + 5$ 。 $6 = 5 \times 1 + 1$ 。 $5 = 1 \times 5 + 0$ 。したがって， $\text{GCD}(13256, 123) = \text{GCD}(1, 0) = 1$ が得られますね。これらの計算は右の表のように行うのがよいでしょう。

107	13256	123	1
	13161	95	
3	95	28	2
	84	22	
1	11	6	1
	6	5	
5	5	1	
	5		
	0		

では，ここで練習です。 $\text{GCD}(13256, 1234)$ を求めよ。右表のように計算しましょう。答は 2 です。

1.10.2.2 合同式

日常生活では，時刻をいう場合に午前・午後を省略して，“8時”などと言っただけで意味が通じる場合がほとんどですね。午後 8 時の場合は 20 時から 12 時を引いた 8 時，もしくは，20 時を 12 で割った余り 8 時のことを指していますね。時計の針は何年も回り続けるので，‘12 で割った余り’のほうが一般的な議論に適しています。授業で，1234567 を 3 で割った余りを求めなさい等という問題が出たこともあったでしょう。実際に 1234567 を 3 で割らずとも， $1+2+3+4+5+6+7 = 28$ を 3 で割ったときの余り 1 が答であることを習ったと思います。割り算で余りにだけ関心がある場合は結構多いようです。

19 世紀の超偉大なドイツの数学者ガウス (Karl Friedrich Gauss, 1777 ~ 1855) は，ある自然数が素数かどうかを研究する際に，‘等しい’に似た合同という考えを導入しました。例えば， $20 \equiv 8 \pmod{12}$ と書いて²⁷⁾，“20 と 8 は 12 を法として合同”とか“20 と 8 は mod 12 で合同”などと読み，この式を合同式といいます。20 を 12 で割った余りと 8 を 12 で割った余りが‘等しい’という意味です。一般には， x, y を整数， m を自然数としたとき，合同式

²⁷⁾ $\text{mod} = \text{modulo} = \overset{\text{モジュロ}}{\sim}$ を法として．「法」は‘測定のもととなるもの’の意味で用いられています。

$x \equiv y \pmod{m}$ は「 x は y に m の倍数を加えたもの」として定義されます：

$$x \equiv y \pmod{m} \Leftrightarrow x = y + km \text{ となる整数 } k \text{ がある.}$$

感覚的には $m \equiv 0$, つまり ‘ m は 0 と同じと見なす’ のが $\text{mod } m$ の合同式と思ってよいでしょう。

合同式の定義より, 整数 x, y, z に対して任意の $\text{mod } m$ で, $x \equiv x$ (反射律), $x \equiv y \Rightarrow y \equiv x$ (対称律), および $x \equiv y$ かつ $y \equiv z \Rightarrow x \equiv z$ (推移律) が成り立ちます. これらは, 合同式についてはもちろん, §§1.5.2 で紹介した同値関係 \sim を厳密に扱うときには重要です. 交換・結合・分配の計算法則は等号 = の段階で成り立つので, $x = y \Rightarrow x \equiv y$ より, もちろん成り立ちます. その他に, 我々が必要な基本定理は合同式の加・減・乗に関するものです: x, y, z, w を整数として, 任意の自然数 m に対して

$$x \equiv y \text{ かつ } z \equiv w \pmod{m} \Rightarrow x + z \equiv y + w \pmod{m},$$

$$x \equiv y \text{ かつ } z \equiv w \pmod{m} \Rightarrow x - z \equiv y - w \pmod{m},$$

$$x \equiv y \text{ かつ } z \equiv w \pmod{m} \Rightarrow x \cdot z \equiv y \cdot w \pmod{m}$$

が成り立ちます. これらの定理は, 合同式の定義と x, y, z, w を m で割った余りを考え, $x = mk + x'$ ($0 \leq x' < m$) などと表して両辺を比較すると容易に示されます. それは練習問題にしましょう. ヒント: y を m で割った余りを y' とすると, $xy \equiv x'y' \pmod{m}$ などが成り立ちます.

積の定理から, x の n 乗に関する重要な定理

$$x^n \equiv x'^n \pmod{m} \quad (x = mk + x')$$

が得られます. これも練習問題にしましょう. ヒント: $x \equiv x'$ を用いて, $x^2 = x \cdot x, x^3, x^4, \dots$ を計算しましょう.

これで準備ができました. 1234567 を 3 で割った余りはその数の各位の数の和を 3 で割った余りであることを示しましょう. 1234567 は 10 進数ですから

$$1234567 = 7 + 6 \cdot 10 + 5 \cdot 10^2 + \dots + 1 \cdot 10^6$$

と表されますね. ここで, $10 \equiv 1 \pmod{3}$ ですから, $10^n \equiv 1 \pmod{3}$ が成り立ち, よって, 合同式の定理より, 簡単に

$$1234567 \equiv 7 + 6 + 5 + 4 + 3 + 2 + 1 (= 28 \equiv 1) \pmod{3}$$

であることが示されます．3 で割った余りを考えるときは 10 を 1 と見なして計算してよいということですね．同様のことは 9 で割るときにも起こります．1234567 を 9 で割ると余りは \square ですね．

では，ここで問題をやってみましょう．連立方程式

$$\begin{cases} N \equiv 1 \pmod{2} & \dots\dots\dots ① \\ N \equiv 2 \pmod{3} & \dots\dots\dots ② \end{cases}$$

を満たす整数 N を求めよ．

① は N が奇数，② は N が 3 で割ると余りが 2 であることを表し，そのような N は無数にあります．合同式の定義より ①，② の書き方は 1 通りでなく，① の右辺の 1 は任意の奇数で置き換えてもよく，② の右辺は 3 で割ると 2 余る任意の整数で構いません．そこで，上の連立方程式の右辺を，奇数かつ 3 で割ると 2 余る整数，例えば 5 で置き換えて

$$\begin{cases} N \equiv 5 \pmod{2} \\ N \equiv 5 \pmod{3} \end{cases}$$

と右辺の数が一致するようにすると解法が見えてきます．つまり，

$$\begin{cases} N - 5 \equiv 0 \pmod{2} \\ N - 5 \equiv 0 \pmod{3} \end{cases}$$

ですから， $N - 5$ は 2 でも 3 でも割り切れる数，つまり 2 の倍数かつ 3 の倍数ですね．よって， $N - 5$ は 2 と 3 の最小公倍数 6 の倍数：

$$N - 5 \equiv 0 \pmod{6} \Leftrightarrow N = 5 + 6k \quad (k \text{ は任意の整数})$$

となります．

練習問題を 1 題．7 で割ったら 1 余り，11 で割ったら 4 余る整数 N を求めよ．ヒントは不要でしょう．答は $N \equiv 15 \pmod{77}$ です．

合同式の加減乗の定理では mod が変わりませんが，合同式の商の定理では注意が必要です： x, y を整数， m, a を自然数とするとき，定理

$$ax \equiv ay \pmod{m} \Rightarrow x \equiv y \pmod{\frac{m}{\text{GCD}(m, a)}}$$

が成り立ちます． $\text{GCD}(m, a) > 1$ のときは mod が変わります．

この定理を証明するには $ax \equiv ay \pmod{m}$ を

$$ax = ay + mk \quad (k \text{ は整数})$$

と書いて、両辺を a で割ります： $\text{GCD}(m, a) = G$, $m = Gm'$, $a = Ga'$ とすると

$$x = y + \frac{mk}{a} = y + \frac{m'k}{a'}$$

ここで、 x, y は整数だから $\frac{m'k}{a'}$ も整数であり、 m' と a' は互いに素なので k が a' の倍数になります。よって、 $k = a'k'$ (k' は整数) と書くと、上式は

$$x = y + m'k' = y + \frac{m}{G}k', \text{ よって } x \equiv y \pmod{\frac{m}{\text{GCD}(m, a)}}$$

となり、証明されました。

1.10.3 整数論の基本定理

前の §§ の合同式の連立方程式 $N \equiv 1 \pmod{2}$ かつ $N \equiv 2 \pmod{3}$ は $N = 2x + 1 = 3y + 2$ となる整数 x, y を求めることと同じなので、その問題は整数係数の1次方程式

$$2x + 1 = 3y + 2 \Leftrightarrow 2x - 3y = 1 \quad (x, y \text{ は整数})$$

を解くことと同じになります。一般に、整数解に限定した整数係数の1次方程式

$$ax + by = c \quad (a, b, c; x, y \text{ は整数}) \quad (\text{不定方程式})$$

を1次の「不定方程式」といい古代ギリシャ時代から研究されてきました。この方程式は無数の整数解をもつか、 $2x + 4y = 3$ の例からわかるように(左辺は偶数)、1つも整数解がないかのどちらかです。1次不定方程式が解をもつ条件を求めることは重要で、それは以下に述べられる 整数論の基本定理：

整数 a, b が互いに素のとき $ax + by = 1$ は整数解をもつ

から得られます。この定理を証明し、不定方程式が解をもつ条件を調べましょう。

整数論の基本定理の証明には種々の方法がありますが、最も簡明と思われる方法で行いましょう。GCD(a, b) = 1 として、整数 x, y の式

$$N = ax + by$$

を考えます。 x, y がいろいろな整数値をとると、それに対応して N はいろいろな整数値になります。例えば、 $x = ka, y = kb$ (k は整数) としてみると明らかかなように、 N は正にも負にも、また 0 にもなります。この証明法は、全ての整数 x, y を考えて、 $N = ax + by$ がとり得る値のうちで正で最小のものを仮に $N = c_0$ としたとき、 $c_0 = 1$ を示そうという方法です。 N の正の最小値を c_0 とすると、可能な N の値は $N \geq c_0$ または $N \leq 0$ であることに注意しましょう。

$N = c_0$ のとき、仮定により方程式

$$ax + by = c_0$$

は整数解をもちます。その解の 1 組を $(x, y) = (x_0, y_0)$ としましょう：

$$ax_0 + by_0 = c_0.$$

さて、係数 a, b を c_0 で割って、余りをそれぞれ r_1, r_2 とします：

$$a = c_0q_1 + r_1 \quad (0 \leq r_1 < c_0),$$

$$b = c_0q_2 + r_2 \quad (0 \leq r_2 < c_0).$$

このとき、上式と等式 $ax_0 + by_0 = c_0$ から

$$\begin{aligned} r_1 &= a - c_0q_1 = a - (ax_0 + by_0)q_1 \\ &= a(1 - q_1x_0) + b(-q_1y_0) \end{aligned}$$

と表され、 $1 - q_1x_0$ および $-q_1y_0$ は整数なので、 r_1 は N の可能な値の範囲 ($N \geq c_0$ または $N \leq 0$) にあります： $r_1 \geq c_0$ または $r_1 \leq 0$ 。一方、 r_1 は c_0 で割った余りなので、その範囲は $0 \leq r_1 < c_0$ です。よって、両方の条件を満たすためには

$$r_1 = 0$$

でなければなりません。同様に、 $r_2 = 0$ も成立します (確かめましょう)。

$r_1 = r_2 = 0$ より $a = c_0q_1$, $b = c_0q_2$ となるので, c_0 は a と b の公約数です. ところが仮定によって $\text{GCD}(a, b) = 1$ でしたから, それを満たすためには $c_0 = 1$ が必要です. 以上の議論から $ax_0 + by_0 = 1$ となり, 互いに素な整数係数の 1 次不定方程式 $ax + by = 1$ は整数解をもつことが示されました.

次に, 整数論の基本定理を用いて一般の 1 次不定方程式が解をもつ条件を調べましょう. 上の議論から $ax_0 + by_0 = 1$ が成り立ちました. この両辺に整数 c を掛けると

$$a(cx_0) + b(cy_0) = c$$

ですが, これは, a, b が互いに素のとき, 1 次不定方程式 $ax + by = c$ は任意の整数 c に対して解をもつことを意味しますね.

今度は, 一般の整数係数不定方程式 $a'x + b'y = c'$ を考えましょう. このとき, $\text{GCD}(a', b') = G$, $a' = Ga$, $b' = Gb$ とします. 両辺を G で割ると,

$$ax + by = \frac{c'}{G}$$

となりますが, 左辺は整数なので右辺も整数です. 右辺を c と書くと, c が整数のときは互いに素な整数係数の不定方程式 $ax + by = c$ となって解をもち, そうでないときは解がありません. したがって, 定理

一般の整数係数 1 次不定方程式 $a'x + b'y = c'$ が整数解をもつための必要十分条件は c' が $\text{GCD}(a', b')$ で割り切れることである

が示されました.

不定方程式の例としてとり上げた

$$(N =) 2x + 1 = 3y + 2$$

を合同式を用いずに解いてみましょう. 2 と 3 は互いに素だから整数解があることは保証されています. 解の 1 組は $x = 2$, $y = 1$ よって $N = 5$ のときで, それを $(5 =) 2 \cdot 2 + 1 = 3 \cdot 1 + 2$ と表して方程式から辺々引くと, 方程式

$$(N - 5 =) 2(x - 2) = 3(y - 1)$$

が得られます. 2 と 3 は互いに素より, k を任意の整数として, 解 $x - 2 = 3k$,

よって

$$y - 1 = 2k, \quad N - 5 = 6k$$

が得られます。

練習問題は前の §§ で練習問題にした $(N =) 7x + 1 = 11y + 4$ です。合同式を用いずに解きなさい。ヒント：方程式を満たす整数解の 1 組を探しましょう。答は、解の 1 組を $x = 2, y = 1$ とすると、 k を任意の整数として、 $x - 2 = 11k$ 、よって $y - 1 = 7k, N - 15 = 77k$ です。ただし、解の表し方は解の 1 組の選び方によって見かけ上変わるので、 k に全ての整数を代入して得られる解の集合が一致すれば正しい解です。例えば、 $x = 2 + 11(k - 1) = -9 + 11k$ などと表すこともできます。

§1.11 素数を利用した暗号

整数の基本的性質を学んできましたが、それが何の役に立つの？と思う人も多いでしょう。整数、それも最も実用にならないと考えられていた素数が、コンピュータ社会においては、なくてはならない存在になったのです。

3713 を素因数分解してみましょう。小さな素数 2, 3, 5, … の順で割っていくと、47 で割り切れるので、 $3713 = 47 \times 79$ と 2 つの素数の積で表されますね。4 桁の自然数の素因数分解はたいしたことはありません。アメリカの科学雑誌が、1977 年の 8 月号で、ある暗号技術の紹介と共に、百ドルの懸賞金付きで、129 桁の自然数の素因数分解の問題を載せました。600 人の若者がこれに応じ、各自の分担を決めて、コンピュータを駆使して答を探しました。その数が 64 桁の素数と 65 桁の素数の積であることを彼らが報告したのは 1994 年の 4 月といえますから、なんと 17 年後のことでした。もし 1 桁大きい 130 桁の自然数の問題だったらその 10 倍ぐらいの計算が必要なので、解くのに 100 年以上はかかるでしょう。非常に大きな自然数の素因数分解は短日では不可能ですね。以下、そのことを利用した暗号の原理を議論しましょう。

1.11.1 フェルマーの小定理

まずは必要な数学の準備です。実数 a を n 個掛けた数を a^n と表しましたね。 $a^m \times a^n$ は、 a を m 個掛けてさらに n 個掛けたもの、つまり a を $m + n$ 個掛け

たものなので

$$a^m \times a^n = a^{m+n}$$

ですね．次に， $(a^m)^n$ は a^m を n 個掛けたもの，つまり a を $m \times n$ 個掛けたものです：

$$(a^m)^n = a^{mn} .$$

コンピュータでは文字は全て 2 進数の自然数に置き換えられるので文字と自然数は同じであり，ディスプレイ画面に表示するときだけ異なります．そこで，ある自然数 a はある文字を表すとして，自然数 a を ‘文字’ a と呼びましょう．そこで，§§1.10.2.2 で学んだ合同式を利用します． a を m 乗して適当な $\text{mod } s$ をとると， a は異なる ‘文字’ $a' \equiv a^m \pmod{s}$ に変換されます．これが暗号文字 a' です．ところが， $a' \equiv a^m$ を n 乗したとき，もし $(a^m)^n \equiv a \pmod{s}$ が成り立つならば，暗号は元の文字 a に戻るので解読できます．そんなことが可能なことを以下に示しましょう．

まず，「フェルマー²⁸⁾の小定理」と呼ばれる整数論の重要な定理を導きます． $\text{mod } 5$ で 2 の 2 乗，3 乗，4 乗，5 乗を計算してみてください． $2^4 = 16 \equiv 1 \pmod{5}$ ，よって， $2^5 \equiv 2 \pmod{5}$ ですね． $\text{mod } 5$ で 2 を 5 乗すると 2 に戻りましたね．これは単なる偶然ではありません．3 についても， $3^4 = 81 \equiv 1 \pmod{5}$ ，よって， $3^5 \equiv 3 \pmod{5}$ です．このようなことが一般に成り立つことを示したのがフェルマーの小定理です：

p を任意の素数とする．このとき，任意の整数 a に対して

$$a^p \equiv a \pmod{p} \quad (a \text{ は任意の整数})$$

が成り立つ．特に， a が p で割り切れないとき

$$a^{p-1} \equiv 1 \pmod{p} \quad (a \not\equiv 0 \pmod{p})$$

が成り立つ．

‘小’定理といわれる理由は，君たちも知っている「フェルマーの大定理」：

2 より大きい自然数 n に対して

$$\text{不定方程式 } x^n + y^n = z^n \text{ は自然数解をもたない}$$

²⁸⁾ フェルマー (Pierre de Fermat, 1601 ~ 1655, フランス) .

があるからです．大定理は，多くの努力にもかかわらず，300年以上にわたって証明されずにいましたが，ついに1995年，イギリスの数学者ワイルズ(Andrew John Wiles, 1953 ~) がそれをなし遂げました．

フェルマーの小定理の証明には興味ある補助定理を使います． $\text{mod } 5$ で $0, 1, 2, 3, 4$, のそれぞれに 2 を掛けてみてください．それぞれ $0, 2, 4, 1, 3$ と互いに異なる数になりましたね．このことは一般に成り立ちます：

$$p \text{ を素数, } a \text{ を } p \text{ で割り切れない整数, } k \text{ と } l \text{ を任意の整数とするとき}$$

$$k \not\equiv l \pmod{p} \Rightarrow ka \not\equiv la \pmod{p} \quad (a \not\equiv 0 \pmod{p})$$

が成り立つ．

§§1.6.2 で命題とその対偶の真偽は一致することを議論しましたね．上の命題の対偶は

$$ka \equiv la \pmod{p} \Rightarrow k \equiv l \pmod{p}$$

なので，対偶のほうを調べましょう． $ka \equiv la \pmod{p}$ より $(k-l)a \equiv 0 \pmod{p}$ ですが， $a \not\equiv 0 \pmod{p}$ としているので， $k-l \equiv 0 \pmod{p}$ よって $k \equiv l \pmod{p}$ が得られます．したがって，対偶が真となるので命題も真です．なお，背理法を用いても証明できますが，それは練習問題としましょう．ヒント：「 $k \not\equiv l \pmod{p} \Rightarrow ka \equiv la \pmod{p}$ 」が偽であることを示します．

上の補助定理より， a が p で割り切れないとき， $1a, 2a, 3a, \dots, (p-1)a$ は $\text{mod } p$ で互いに全て異なり，よって

$$1a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$$

が成り立ちます．そこで，商の定理

$$ax \equiv ay \pmod{m} \Rightarrow x \equiv y \pmod{\frac{m}{\text{GCD}(m, a)}}$$

を利用して，両辺を $1 \cdot 2 \cdot 3 \cdots (p-1)$ で割ると $a^{p-1} \equiv 1 \pmod{p}$ が得られます．この式の両辺に a を掛けて， $a^p \equiv a \pmod{p}$ が得られます．この等式は， $a \equiv 0 \pmod{p}$ のとき $a^p \equiv 0 \equiv a \pmod{p}$ だから，任意の整数 a に対して成り立ちますね．

1.11.2 RSA 公開鍵暗号

素因数分解が難しい素数の積を作り，暗号を解読するための仕掛けをするために，フェルマーの式を細工しましょう． p, q を異なる素数， a を p でも q でも割り切れない整数とすると，フェルマーの小定理より

$$a^{p-1} \equiv 1 \pmod{p}, \quad a^{q-1} \equiv 1 \pmod{q}$$

が成り立ちます． $a^{p-1} \equiv 1$ を $q-1$ 乗， $a^{q-1} \equiv 1$ を $p-1$ 乗すると， $(a^m)^n = a^{mn}$ より

$$a^{(p-1)(q-1)} \equiv 1 \pmod{p}, \quad a^{(q-1)(p-1)} \equiv 1 \pmod{q}$$

となります．暗号を解く鍵づくりに，さらに n 乗しておきましょう：

$$a^{n(p-1)(q-1)} \equiv 1 \pmod{p}, \quad a^{n(q-1)(p-1)} \equiv 1 \pmod{q}.$$

暗号を元に戻すために，さらに a を掛けます： $(a^m a^n = a^{m+n}$ に注意して)

$$a^{n(p-1)(q-1)+1} \equiv a \pmod{p}, \quad a^{n(q-1)(p-1)+1} \equiv a \pmod{q}.$$

フェルマーの小定理のところで注意したように，この2式は任意の整数 a に対して成立しますね．

以上で素数の積を作る準備が整いました．上の2式は mod だけが異なるので，mod を使わずに等式で表すと

$$a^{n(p-1)(q-1)+1} = pk + a = ql + a \quad (k, l \text{ は整数})$$

です．よって， $pk = ql$ ですが， p と q は異なる素数なので， $k = qk'$ (k' は整数) が成り立ちます．よって， $pk + a = pqk' + a \equiv a \pmod{pq}$ と表すと， p, q を異なる素数として

$$a^{n(p-1)(q-1)+1} \equiv a \pmod{pq} \quad (a \text{ は任意の整数})$$

が成り立ちます．

整数 a を文字 a と呼ぶと，文字 a を暗号文字 a' に変換し，元の a に戻すには， E, D をある自然数として，上式が

$$a^{n(p-1)(q-1)+1} = a^{ED} = (a^E)^D \equiv a \pmod{pq}$$

のように表され、

$$a' \equiv a^E \pmod{pq}, \quad a'^D \equiv a \pmod{pq}$$

となっていればよいですね。その条件は

$$n(p-1)(q-1)+1 = ED$$

です。それは素数 p, q を定めたとき、自然数 n をうまく選んでやると、左辺が自然数の積の形にできるので可能です。自然数 E は「公開鍵」と呼ばれ、 D は「秘密鍵」と呼ばれています。

この暗号の仕組みを整理してみましょう。まず 100 桁以上の 2 つの素数 p, q を用意します。それらの積 $N = pq$ は公開しても、素因数分解の難しさのために p と q が知られることはありません。公開鍵 E も公開しますが秘密鍵 D がばれる心配はありません。公開された N と E を用いて暗号文を書きます。例えば、元の文が「これは解けない暗号」(各文字は自然数に直されているとします)とすると、 $\text{mod } N$ で各文字(またはいくつかまとめたもの)を E 乗して暗号文にします。例えば、 $c' \equiv c^E \pmod{N}$ 、 $\text{解}' \equiv \text{解}^E \pmod{N}$ などとすると、暗号文は「こ'れ'は'解'け'ない'暗'号'」と意味不明な文になります。この文を秘密鍵 D を知っている人に送ると、各文字を D 乗して、 $c'^D \equiv c \pmod{N}$ などと元の文字に直せるので、元の文「これは解けない暗号」に解読できるというわけです。

なお、秘密鍵 D を知っている者どうしであれば、署名の際に名を D 乗して暗号にしておけば、受け取ったほうはそれを E 乗して本人と確認できます。

このような暗号は「RSA 公開鍵暗号」といわれ、R, S, A はこの暗号を考案した 3 人の数学者 (R.L.Ribest, A.Shamir, L.M.Adleman) の頭文字です。公開鍵と秘密鍵という 2 つの鍵を用いる暗号方式は暗号理論に飛躍的發展をもたらしました。今のところ RSA 暗号が破られる心配はありません²⁹⁾。

²⁹⁾ 最近、「量子コンピュータ」という原子の世界の現象を利用する革命的コンピュータが注目されています。原子の世界ではコンピュータのメモリーが 0 の状態と 1 の状態が重ね合わされた状態が作れます。そのことを利用すると、 $N = pq$ の素因数 p, q の「全ての候補」を同時に用意でき、 N を「全ての候補」で「同時に割る」ような計算が可能になります。現在のところは 15 の素因数 3 と 5 を確認した程度ですが、あと数十年もすると実用化できるといわれています。