代 数 入 門

2019 年度版

中野　伸

（学習院大学・理学部・数学科）

目 次

間違いを見つけたら……，ひそかにそっと連絡して下さい…….

中野　伸　<shin.nakano@gakushuin.ac.jp>

白紙のページ

第1章　はじめに

1.1　不定方程式

中学校で2次方程式の解の公式を学び，整数や有理数でない数，すなわち無理数を導入し，さらに高校では，すべての2次方程式が解をもつように，数の範囲を複素数にまで広げていった． この講義では，素朴な立場に戻り，方程式の解の範囲を整数や有理数に限定して，解の存在やその解き方に着目してみよう．

たとえば，3次方程式

$$x^3 - 3x^2 + 5x - 6 = 0$$

を解くことを考える．高校の【数学II】では，解の候補として，定数項の約数 $\pm 1, \pm 2, \pm 3, \pm 6$ がとれることを学んだ． 実際，この場合 $x = 2$ が解であることが確かめられ，さらに整数解は $x = 2$ だけであることが確認できる． 一般の整数係数 n 次代数方程式

$$c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0 = 0 \qquad (c_k \in \boldsymbol{Z},\ c_n \neq 0)$$

の整数解も，$c_n = 1$ のときには，定数項 c_0 の約数（それは有限個である）をチェックすればすべて得られる． $c_n \neq 1$ の場合も，この方法を少し修正すればすべての整数解を決定できる (考えてみよう)． さらに考察を進めて，すべての有理数解を求める手順を与えることもできるが，ここではあまり深入りしないことにしよう． なお，近似解を求めることも実用的にはきわめて重要ではあるが，この講義では話題にしない．

次に，a, b, c を0でない整数として，2変数の1次方程式

$$ax + by = c$$

を考えよう． 【数学 A】で学んだように，この方程式が整数の組 (x, y) を解としてもつための条件は，c が a, b の最大公約数の倍数となることであった． また，実際に解を求めるには，ユークリッドの互除法が有効であった．

以上のように，ある方程式について，その整数解を問題にしたいとき，その方程式を**不定方程式**または**ディオファントス方程式**と呼ぶ． 解の範囲を狭めて自然数解を問題にしたり、逆に範囲を広げて有理数解に着目することもあり，その場合も不定方程式と呼ばれる．

数学，とくに代数学に属する分野，数論，代数幾何学，表現論などの研究を行うと，問題が不定方程式に帰着することが頻繁にある． それにともない，不定方程式の解法にも様々なアプローチがあるが，初等整数論はそのどれにも共通な基本的な手法になっている。

1.2　ピタゴラス方程式

古典的な不定方程式のひとつの例として**ピタゴラス方程式**を取り上げる．これは，直角 3 角形の 3 辺の関係を表す方程式

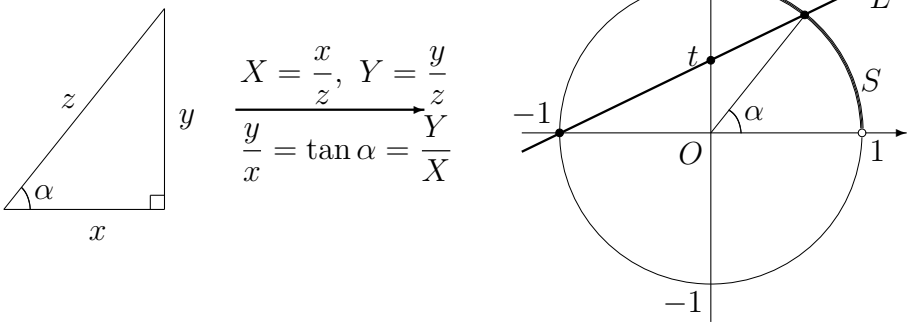
$$x^2 + y^2 = z^2$$

で，とくに辺の長さが自然数であるものに着目したものである．古代から $(x, y, z) = (3, 4, 5), (5, 12, 13)$ などの解が知られており，一般の自然数解の求め方も解明されていたらしい（ネットで調べてみよ）．

ここでは，自然数とは一見関係なさそうな幾何学的な解法を紹介する．ピタゴラス方程式の自然数解を求めることは，

$$X^2 + Y^2 = 1$$

の正の有理数解を求めることと同等であることに注意する．実際，$x^2 + y^2 = z^2$ の自然数解 (x, y, z) から $X = x/z,\ Y = y/z$ とすれば $X^2 + Y^2 = 1$ の正の有理数解が得られ，逆に，$X^2 + Y^2 = 1$ の正の有理数解 (X, Y) を通分して $X = x/z,\ Y = y/z$ と表わせば $x^2 + y^2 = z^2$ の自然数解が得られるからである（くどい？）．このようにして，ピタゴラス方程式の自然数解は，原点を中心とする半径 1 の円周 S の上にある正の有理数を座標にもつ点（つまり第 1 象限にある点）と対応付けられることになる．いま，S 上のそのような点 (X, Y) と点 $(-1, 0)$ を通る直線 L を考えよう．このとき，下図を見れば，(X, Y) は L の Y-切片 t（$0 < t < 1$）と 1 対 1 に対応することがわかる．



直線 L の定義式 $Y = tX + t$ から

$$t = \frac{Y}{X + 1}$$

が得られるが，さらに $S\colon\ X^2 + Y^2 = 1$ と連立させれば，簡単な計算により

$$X = \frac{1 - t^2}{1 + t^2}, \qquad Y = \frac{2t}{1 + t^2}$$

が求まる．これらの式から，X, Y がともに有理数であることと t が有理数であることは同値であることがわかる．そこで，t に 0 と 1 の間の有理数を次々と代入すれば，

$t = \frac{1}{2}, \frac{2}{3}, \frac{1}{4}, \frac{3}{4}, \ldots$ の値から，対応する円周上の点

$$(X, Y) = \left(\frac{3}{5}, \frac{4}{5}\right), \quad \left(\frac{5}{13}, \frac{12}{13}\right), \quad \left(\frac{15}{17}, \frac{8}{17}\right), \quad \left(\frac{7}{25}, \frac{24}{25}\right), \ldots$$

を経由して，ピタゴラス方程式 $x^2 + y^2 = z^2$ の自然数解

$$(x, y, z) = (3, 4, 5), \quad (5, 12, 13), \quad (15, 8, 17), \quad (7, 24, 25), \ldots$$

が得られる． さらに重要なことは，この方法ですべての自然数解が得られることである．

1.3　フェルマーの最終定理

ピタゴラス方程式は 2 次式で表されているが，これを 3 次にするとどうなるか？ フェルマー（17 世紀の人）は，そのような方程式には自然数解がなく，さらに 4 次以上でも同様に自然数解がないと述べている． さらに，ある本の余白に,「その『驚くべき証明』を発見したがそれを記すにはこの余白は狭すぎる」と書き残した． 現在まで彼の証明は見つかっていない．

定理 1.1 (フェルマーの最終定理) 自然数 $n \geq 3$ に対して，方程式

$$x^n + y^n = z^n$$

は自然数解をもたない．

この定理は，長い間証明が知られていなかったので，かつては『フェルマー予想』とも呼ばれ，整数論における難問のひとつであった． フェルマー自身によって $n = 4$ の場合が証明され，$n = 3$ に対してはオイラーが証明を与えている（それぞれ，17, 18 世紀）．その後，ソフィー・ジェルマン，ディリクレ，クンマー等の貢献により，19 世紀中に 100 までのすべての n に対して正しいことが確かめられたが，20 世紀になって整数論や代数幾何学の理論が少しずつ整えられた結果，1994 年ワイルズによって完全な証明が与えられた． その証明は数多くの高度な理論を駆使して構成され，大胆な発想に満ちているが，その概略の一部だけでも紹介するにはこの余白は狭すぎる（なんちゃって）．

1.4　有名な問題

一般に数学の問題は難しい概念を用いて語られ，専門に学んだ人でなければ問題を理解することすら困難であることが多い． しかし，整数論の問題には初等的に表現されるものもあり，それらの多くは中高生でも（小学生でも？）理解できる． ただし，問題が初等的に表わされるからといって，必ずしも初等的に解けるとはいえず，未解決のまま残る

ことも往々にしてある． 前述の『フェルマーの最終定理（フェルマー予想）』も 25 年前まではそんな類の問題であった． 以下，素数に関する有名な予想について述べよう．

● 素数が無限個存在することは古代から知られているが，次の定理は，初項と公比が互いに素な数列上にも素数が無限に現れることを示している．

定理 1.2 (ディリクレ) 互いに素な整数 a, b（ただし $a > 0$）に対して $an+b$ $(n \in \boldsymbol{N})$ の形の素数が無限個存在する．

すなわち，係数が互いに素な 1 次式に自然数を代入していけば，素数が無数に現れる．

それでは，2 次以上の場合はどうか？ 2 次以上の整数係数の多項式（最高次係数は正）$f(x)$ に自然数を順々に代入していくと，$f(1), f(2), f(3), \cdots$ の中に素数が無限に現れるだろうか？ 現在までにそのような多項式 $f(x)$ はひとつも確認されていない（ひとつも！だぜっ）． もっとも簡単なケースとして次の予想がある．

予想 1.3 n^2+1 $(n \in \boldsymbol{N})$ の形の素数が無数に存在するであろう．

● $(3,5), (5,7), (11,13), (17,19)$ のように「差が 2 である素数のペア」も無数にありそうである． このようなペアを**双子素数**という． 計算を続けていくといくらでも大きなペアが見つかる，たとえば $(20200109, 20200111)$ など（Maple を使ってもっと探してみよ）．

予想 1.4 (双子素数予想) 双子素数は無限組存在するであろう．

双子素数は「差が 2 である素数のペア」であるが，2013 年，「差が 7 千万以下である素数のペア」が無数にあることが Y. Zhang によって証明された． “2 と 7 千万” では雲泥の差があるようだが，この証明以前には “2 と無限大” であったのだから，画期的な結果と言って良いであろう． その後すぐに改良が進み，7 千万が 246 に置き換えられることがわかった． いずれ，近いうちに 246 が 2 に改良され「双子素数予想」は解決されるのだろうか，それとも，新たな本質的な困難に突き当たって未解決のままになるのだろうか……．

● その数より小さい約数の和がその数になるとき**完全数**という． たとえば，28 はその約数 $1, 2, 4, 7, 14$ の和と等しいので完全数である． $2^n - 1$ が素数のとき $2^{n-1}(2^n - 1)$ が完全数となることは古代から知られていた． さらにオイラーによって，偶数の完全数は必ずこのように表されることも証明されている (18 世紀)．

予想 1.5 偶数の完全数は無限に存在するであろう．

この予想は，$2^n - 1$ の形の素数が無数にあるだろう ということと同じである． このような素数は**メルセンヌ素数**と呼ばれ，巨大な素数の例として興味深い． 現在 (2019 年 3 月) までに 51 個のメルセンヌ素数が見つかっていて，最大のものは $2^{82589933} - 1$（10 進表記で 24862048 桁）である． これは，明示的に知られている素数全体の中でも最大のものとなっている． なお，奇数の完全数は一つも発見されていない．

予想 1.6 奇数の完全数は存在しないであろう．

第2章　整除関係

2.1　割り算と余り

整数全体の集合 $\boldsymbol{Z}$ では，足し算と掛け算が定義されていて通常の演算規則，すなわち，**結合法則**，**交換法則**，**分配法則**が成り立っている． さらに，$\boldsymbol{Z}$ は 0 と負の数を含むので，引き算もいつでもできる． しかし割り算は必ずしもできない，つまり割り算の値が整数の範囲に納まらないことがある． このような場合でも，小学校で学んだように「余り」付きの割り算はいつでも可能である． すなわち，2 つの整数 a, b に対して，商 q と余り r が定まり，関係式 $a = qb + r$ が成り立つ． この事実を定理として精密に定式化しておこう．

定理 2.1 (割り算の定理) 任意の $a, b \in \boldsymbol{Z}$（ただし $b \neq 0$）に対して，

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

をみたす $q, r \in \boldsymbol{Z}$ が存在し，しかもそれらの組は一意的に定まる．

証明　絶対値の大きい負の整数 x をとれば，$a - x\,|b| \geq 0$ とできるから，集合

$$R = \left\{ a - x\,|b| \;\middle|\; x \in \boldsymbol{Z},\, a - x\,|b| \geq 0 \right\}$$

は空集合ではない． そこで R の最小元 r をとる;　$r = \min R$. この $r \in R$ を実現する $x \in \boldsymbol{Z}$ をあらためて p と書けば，$a = p\,|b| + r$ であるが，ここで，もし $|b| \leq r$ とすると，

$$0 \leq r - |b| = (a - p\,|b|) - |b| = a - (p+1)\,|b| \in R$$

となって，$r = \min R$ に矛盾する． したがって $0 \leq r < |b|$ が成り立つ． さらに，b の正負にしたがって $q = \pm p$ とおけば，$a = qb + r$ が成り立つ．

次に一意性を示すために，整数 q, r, q', r' が

$$a = qb + r = q'b + r', \quad 0 \leq r, r' < |b|$$

をみたすとして，$q = q', r = r'$ を示そう． もし $q \neq q'$ ならば $|q - q'| \geq 1$ であるから，$|r - r'| = |q - q'|\,|b| \geq |b|$ となって $0 \leq r, r' < |b|$ に矛盾する． よって $q = q'$ であり，これから $r = r'$ も得られる． □

2.2　約数・倍数

前節冒頭に述べたように，$\boldsymbol{Z}$ においては加減乗除のうち 3 つの演算，$+, -, \times$ は自由にできて通常の演算規則が成り立つが，除法すなわち割り算 $\div$ は必ずしもできない． そこで,「割り切れる」かどうかが $\boldsymbol{Z}$ における最初の問題として浮上する．

整数 a が整数 b で割り切れるとは，$a = bc$ をみたす整数 c が存在することである． このとき，b は a の**約数**である，または，a は b の**倍数**であるといい，

$$b|a$$

で表す． $b|a$ でないときは $b\nmid a$ と書く． たとえば $2|6,\ 4\nmid 10,\ 17|51$ である． 約数や倍数によって表される整数の関係を**整除関係**という．

1 や -1 はすべての $a \in \boldsymbol{Z}$ の約数であり，0 はすべての $a \in \boldsymbol{Z}$ の倍数である． 一方，1 の約数は 1 または -1 だけであり，0 の倍数は 0 だけである． 記号 $|$ を使って表せば次のようになる;

- すべての $a \in \boldsymbol{Z}$ に対して，$1|a$ かつ $-1|a$ かつ $a|0$.
- $a|1$ ならば $a = \pm 1$.
- $0|a$ ならば $a = 0$.

これらは，1 と 0 にまつわる極端な性質である． とくに 0 との整除関係は小学校では扱わなかったので少し戸惑うこともあるかもしれないけれど，もうこどもじゃないもん，慣れれば難しくないもん． 次の命題もひとりで証明できるもん．

命題 2.2 $a, b, c \in \boldsymbol{Z}$ とする．

(1) $a|b$ かつ $b|a$ ならば，$|a| = |b|$.

(2) $c|a$ かつ $c|b$ ならば，任意の $x, y \in \boldsymbol{Z}$ に対して $c|(ax + by)$.

整数 a, b の**公約数**とは a, b のどちらの約数でもある整数のことであり，**公倍数**とはどちらの倍数でもある整数のことである． さて，次に述べる最大公約数と最小公倍数の定義は，小学校で学んだものとちょっと違っているが，これがおとなの定義である．

定義 2.3 (最大公約数・最小公倍数のホントの定義) a, b を整数とする．

(1) 0 以上の整数 d が a, b の公約数であり，かつ a, b の任意の公約数が d の約数であるとき，d を a, b の**最大公約数**といい $\gcd(a, b)$ で表す．

(2) 0 以上の整数 m が a, b の公倍数であり，かつ a, b の任意の公倍数が m の倍数であるとき，m を a, b の**最小公倍数**といい $\mathrm{lcm}(a, b)$ で表す．

なぜ，このような定義を採用するのか？ 小学校では，正の整数つまり自然数のペアについてだけこれらを定義したのだが，ここでは，負の整数や 0 も含めて例外なしに一般の整数のペアを扱うため，というのが理由のひとつである． $ab \neq 0$ のとき（つまり a も b も 0 でないとき），

$$\gcd(a, b) = \max\left\{ c \in \boldsymbol{N} \,\middle|\, c|a,\ c|b \right\}, \qquad \mathrm{lcm}(a, b) = \min\left\{ c \in \boldsymbol{N} \,\middle|\, a|c,\ b|c \right\},$$

$ab = 0$ のとき（つまり $a = 0$ または $b = 0$ のとき）は，

$$\gcd(a, 0) = |a|, \quad \gcd(0, b) = |b|, \quad \mathrm{lcm}(a, 0) = \mathrm{lcm}(0, b) = 0$$

となっている．

命題 2.4 $a, b \in \boldsymbol{Z}$ とする． 整数を成分とする 2 次正方行列 A に対して，$c, d \in \boldsymbol{Z}$ を

$$A\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} c \\ d \end{pmatrix}$$

によって定めると，次が成り立つ．

(1) $\gcd(a, b) | \gcd(c, d)$.

(2) $\det A = \pm 1$ ならば $\gcd(a, b) = \gcd(c, d)$.

証明 $A = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$ とおくと，$c = ax + by$, $d = az + bw$ である． $g = \gcd(a, b)$ ならば $g|a$, $g|b$ だから，命題 2.2 (2) を使って $g|c$, $g|d$． したがって g は c, d の公約数となるから $g | \gcd(c, d)$ であり (1) が示された． (2) を示すために $\det A = \pm 1$ とすると，A の逆行列 $B = A^{-1}$ も整数を成分とする 2 次正方行列で $B\begin{pmatrix} c \\ d \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix}$ をみたすから，(1) より $\gcd(c, d) | \gcd(a, b)$ であり，これから (2) が成り立つことがわかる． □

2.3 ユークリッドの互除法

割り算の定理の応用として，2 つの整数の最大公約数を効率よく求める方法が，以下に述べる**ユークリッドの互除法**である． 整数 a, b に対して $\gcd(a, b) = \gcd(|a|, |b|)$ かつ $\gcd(a, 0) = |a|$ なので，はじめから $b > 0$ として最大公約数を考えればよい．

定理 2.5 (ユークリッドの互除法) 整数 a, b（ただし $b > 0$）に対して，$a_0 = a$, $a_1 = b$ とおき，数列 $\{a_n\}_{n=0,1,\cdots}$ を，$a_n \neq 0$ である限り

$$a_{n-1} = q_n a_n + a_{n+1}, \quad 0 \leq a_{n+1} < a_n$$

によって定めることができる． さらに，ある $N \geq 1$ に対して $a_{N+1} = 0$ となり，そのとき

$$a_N = \gcd(a, b)$$

が成り立つ．

証明 まず，定理 2.1 を繰り返し適用すれば，数列 $\{a_n\}_{n=0,1,\cdots}$ が定まることはすぐにわかる． また，$0 \leq \cdots < a_2 < a_1 = b$ だから，この操作を（多くとも b 回）繰り返せば

$a_{N+1}=0$ となる $N\geq 1$ が得られることがわかる．一方，

$$\begin{pmatrix} a_{n-1} \\ a_n \end{pmatrix} = \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix}, \qquad \begin{vmatrix} q_n & 1 \\ 1 & 0 \end{vmatrix} = -1$$

なので，命題 2.4 によって $\gcd(a_{n-1},a_n)=\gcd(a_n,a_{n+1})$ であり，これを繰り返せば，

$$\gcd(a,b)=\gcd(a_0,a_1)=\gcd(a_1,a_2)=\cdots=\gcd(a_N,a_{N+1})=\gcd(a_N,0)=a_N$$

となる． □

定理 2.6 $a,b\in \boldsymbol{Z}$ の最大公約数を d とすると，

$$ax+by=d$$

をみたす $x,y\in \boldsymbol{Z}$ が存在する．

証明 $b>0$ のときにのみ確かめれば十分である．このとき，前定理の証明から，2 次正方行列 A で $\begin{pmatrix} a \\ b \end{pmatrix} = A\begin{pmatrix} d \\ 0 \end{pmatrix}$, $\det A=\pm 1$ をみたすものがとれる．そこで，A^{-1} の第 1 行を $(x,\,y)$ とすれば，$x,y\in \boldsymbol{Z}$ であり $ax+by=d$ を得る． □

証明中の A^{-1} は，定理 2.5 の証明に現れる行列 $\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}$ の逆行列 $\begin{pmatrix} 0 & 1 \\ 1 & -q_n \end{pmatrix}$ の積

$$A^{-1}=\begin{pmatrix} 0 & 1 \\ 1 & -q_N \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -q_{N-1} \end{pmatrix}\cdots\begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$$

として計算でき，原理的にはこれから x,y を求めることができる．

例 2.7 ユークリッドの互除法を用いて，190423 と 173419 の最大公約数を求めてみよう．

$$\begin{aligned} 190423 &= 1\cdot 173419+17004, \\ 173419 &= 10\cdot 17004+3379, \\ 17004 &= 5\cdot 3379+109, \\ 3379 &= 31\cdot 109+0 \end{aligned}$$

より $\gcd(190423,173419)=109$ を得る．また，

$$190423x+173419y=109$$

をみたす整数の組 (x,y) を見つけるには，前述のように行列の積を計算すればよいが，ここでは上の計算を逆にたどって求めてみる．

$$\begin{aligned} 109 &= 17004-5\cdot 3379=17004-5\cdot(173419-10\cdot 17004) \\ &= 51\cdot 17004-5\cdot 173419=51\cdot(190423-173419)-5\cdot 173419 \\ &= 51\cdot 190423-56\cdot 173419 \end{aligned}$$

したがって，$(x,y)=(51,-56)$ が得られる．

第3章　最小値原理と数学的帰納法

3.1　最小値原理

自然数は「ものを数えるための言葉」であり，‘個数’を表す一方で‘順序’を表すとも考えられる．‘順序’としての自然数がもつ重要な性質として，次の原理がある．

最小値原理　自然数からなる空でない集合は最小値をもつ．

この原理は【割り算の定理】(定理 2.1) の証明の根拠にもなっている（このことを確かめよ）．

さて，この**最小値原理**は成り立つのが当たり前で，あえて証明する必要はないように見える．しかし，ここでは**数学的帰納法**を用いて厳密な証明を与えてみよう．数学的帰納法とは，自然数 n に関する命題 (性質・条件) $P(n)$ が与えられたとき，

$$\text{すべての } n \text{ に対して } P(n) \text{ が成り立つ}$$

ことを証明するための論法のひとつであり，以下のように定式化される．

数学的帰納法の原理　自然数 n に関する命題 $P(n)$ に対して，次の (1), (2) が成り立つならば，すべての自然数 n について $P(n)$ が成り立つ．
(1)　$P(1)$ が成り立つ．
(2)　任意の n に対して，もし $P(n)$ が成り立つならば $P(n+1)$ が成り立つ．

これを用いて「最小値原理」を証明する．

「【数学的帰納法の原理】⇒【最小値原理】」の証明　S を自然数からなる空でない集合とする．S が最小値をもたないと仮定して矛盾を導く．まず，

$$P(n) : 『\ n \text{ より小さい任意の自然数 } m \text{ について } m \notin S \text{ である}』$$

によって命題 $P(n)$ を定める．
(1)　1 より小さい自然数は存在しないから，明らかに $P(1)$ が成り立つ．
(2)　n を任意にとり，$P(n)$ が成り立つとする．すなわち，$1, 2, \cdots, n-1 \notin S$ である．このとき，もし $n \in S$ ならば，n が S の最小値ということになって，S が最小値をもたないという仮定に反する．したがって $n \notin S$ であり，$P(n+1)$ が成り立つ．
よって，「数学的帰納法の原理」より $P(n)$ がすべての $n \in \boldsymbol{N}$ に対して成り立つ．ところで，$S \neq \phi$ であったから，ある $n_0 \in S$ が存在するが，これは $P(n_0+1)$ が成り立たないことを意味し矛盾である．　□

ええっと，いま,「最小値原理」を「数学的帰納法の原理」から導いたわけであるが，なんとなく違和感を覚えないだろうか？　つまり,「最小値原理」の方が 1 行で書けてカンタンだし，そもそも「数学的帰納法の原理」より当たり前っぽい感じがする (オレだけ？)．

そこで，発想を転換して,「最小値原理」を “基本原理” として捉えることにしよう．この立場をとるならば,「数学的帰納法の原理」を「最小値原理」から導かなくてはならない…が，そんなことできんのかよぉ…と疑心暗鬼のキミに静かに告げたい，……それは可能なのだよ…… と．

「【最小値原理】⇒【数学的帰納法の原理】」の証明　命題 $P(n)$ について，(1), (2) が成り立っているとする．このとき，すべての $n \in \boldsymbol{N}$ について $P(n)$ が成り立つことを示したい．そこで，$P(n)$ が成り立たないような n が存在すると仮定して矛盾を導く．集合 S をそのような自然数 n 全体の集合，すなわち

$$S = \left\{ n \in \boldsymbol{N} \,\middle|\, P(n) \text{ が成り立たない} \right\}$$

とする．仮定より $S \neq \phi$ だから,「最小値原理」より S は最小値 m をもつ．(1) より $1 \notin S$ なので $m > 1$，したがって，ある $l \in \boldsymbol{N}$ によって $m = l + 1$ と表すことができるが，$l < m$ なので m の最小性より $l \notin S$．これは $P(l)$ が成り立つことを意味するので，(2) を用いれば，$P(l+1)$ すなわち $P(m)$ が成り立つことになって $m \in S$ に矛盾する．□

以上の議論により,「最小値原理」は「数学的帰納法の原理」と同等であり，一方がもう一方よりもエライということはない．片方を用いて証明できる命題はもう片方を使っても証明できるはずであり，どっちかじゃないと証明できない命題は（原理的には）ないはずである．たとえば,【割り算の定理】(定理 2.1) は「最小値原理」を使って証明されているが,「数学的帰納法」によっても証明できるはずである．このことを実際に確かめてみよう．

定理 2.1 の別証明　a, b ともに正の場合のみを扱い（他の場合も容易にこの場合に帰着される），q, r の存在を a に関する数学的帰納法によって示そう（一意性については元の証明と同じ）．$a = 1$ のときは，$b = 1$ かそうでないかに応じて $(q, r) = (1, 0), (0, 1)$ とおけばよい．次に，a に対して

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

をみたす整数の組 (q, r) が存在したと仮定する（帰納法の仮定）．このとき，$r + 1 \leq b$ であるが,

$$a + 1 = \begin{cases} qb + (r+1), & (r + 1 < b \text{ のとき}) \\ (q+1)b + 0, & (r + 1 = b \text{ のとき}) \end{cases}$$

を考えれば，$r + 1 < b$ であるか $b = r + 1$ であるかに応じて $(q, r + 1)$ または $(q + 1, 0)$ が $a + 1$ に対応する整数の組としてとれることがわかる．□

3.2 最大公約数再論

前章で最大公約数を定義し，それを計算するためのひとつの方法として，ユークリッドの互除法を提示した． このことは，2 つの整数に対して最大公約数が確かに存在することを示している． この節では，最大公約数への別の方向からのアプローチを試み，さらに，整数係数 1 次方程式の整数解との関連を見る．

整数 a の倍数全体の集合を $a\boldsymbol{Z}$ で表す;

$$a\boldsymbol{Z} = \left\{ ax \,\middle|\, x \in \boldsymbol{Z} \right\}.$$

ここで，$a\boldsymbol{Z} = (-a)\boldsymbol{Z}$ なので，必要ならばいつでも $a \geq 0$ ととり直すことができる．

さて，$\boldsymbol{Z}$ の部分集合に関する次の一般的命題から始める． 最小値原理が証明のキーポイントとなっていることに注意しよう．

命題 3.1 $\boldsymbol{Z}$ の空でない部分集合 I について，次の (i), (ii) は同値である．

(i) $a, b \in I$ ならば $a - b \in I$，すなわち I は差について閉じている．

(ii) $I = m\boldsymbol{Z}$ をみたす $m \in \boldsymbol{Z}$ が存在する．

証明 (i)⇒(ii): $I \neq \phi$ より，少なくともひとつの元 $x \in I$ が存在する． よって，$0 = x - x \in I$ である． $I = \{0\}$ ならば $m = 0$ とおけばよいので，以下，$\{0\} \subsetneq I$ とする． $a \in I$ が負だったら $-a = 0 - a \in I$ を考えることにより，$I \cap \boldsymbol{N} \neq \phi$ がわかる． そこで，最小値原理より $I \cap \boldsymbol{N}$ の最小値 m がとれる． この m について，$m\boldsymbol{Z} \subset I$ および $I \subset m\boldsymbol{Z}$ を順に示す． まず，$-m = 0 - m \in I$ であり，したがって $2m = m - (-m) \in I,\ 3m = 2m - (-m) \in I, \cdots$ のようにして（厳密には数学的帰納法により），任意の $n \in \boldsymbol{N}$ に対して $nm \in I$ が確かめられ，さらに $(-n)m = 0 - nm \in I$ でもあるから，$m\boldsymbol{Z} \subset I$ が示される． 次に，$I \subset m\boldsymbol{Z}$ を示すために，$a \in I$ を任意にとる． 割り算の定理から $a = mq + r$，$0 \leq r < m$ をみたす $q, r \in \boldsymbol{Z}$ がとれるが，$a \in I$ および $mq \in m\boldsymbol{Z} \subset I$ より $r = a - mq \in I$ となるから，もし $r > 0$ ならば m の最小性に矛盾する． よって $r = 0$ すなわち $a = mq \in m\boldsymbol{Z}$ となるから $I \subset m\boldsymbol{Z}$ が得られた．

(ii)⇒(i): $a, b \in I = m\boldsymbol{Z}$ とすると，$a = ma_0,\ b = mb_0$ $(a_0, b_0 \in \boldsymbol{Z})$ と表されるから，$a - b = m(a_0 - b_0) \in m\boldsymbol{Z} = I$ を得る． □

次の補題は，$a\boldsymbol{Z}$ の定義から直ちに確かめられる．

補題 3.2 整数 a, b に対して，

$$a|b, \qquad b \in a\boldsymbol{Z}, \qquad b\boldsymbol{Z} \subset a\boldsymbol{Z}$$

は，どのふたつも互いに同値である．

いま $a, b \in \boldsymbol{Z}$ に対して

$$I = \left\{ ax + by \,\middle|\, x, y \in \boldsymbol{Z} \right\}$$

とおくと，I は差について閉じている，すなわち上の命題 3.1 の (i) が成り立つことが容易にわかる． よって，(ii) も成り立ち，ある $d \in \boldsymbol{Z}$ が存在して $I = d\boldsymbol{Z}$ と表される． こ

こで，$d \geq 0$ であるとしてよい． この d は a, b の最大公約数であることが次のようにして確かめられる（補題 3.2 を何度か援用する）． まず，$a = a \cdot 1 + b \cdot 0 \in I = d\boldsymbol{Z}$ より $d|a$，同様に $d|b$ となるから d は a, b の公約数である． 次に，c を a, b の公約数とする．$d \in I$ と I の定義より，$d = ax + by$ $(x, y \in \boldsymbol{Z})$ と書けていることに注意すれば，命題 2.2 (2) から $c|d$ が導かれる． よって $d = \gcd(a, b)$ が示された．

以上により，与えられた整数 a, b に対して，それらの最大公約数 d の存在が（ユークリッドの互除法によらずに）厳密に証明できた． これを定理としてまとめておく．

定理 3.3 (1) 任意の $a, b \in \boldsymbol{Z}$ に対して

$$\left\{ ax + by \,\middle|\, x, y \in \boldsymbol{Z} \right\} = d\boldsymbol{Z}, \quad d \geq 0$$

をみたす $d \in \boldsymbol{Z}$ が存在し，$d = \gcd(a, b)$ が成り立つ．
(2) 任意の $a_1, \cdots, a_n \in \boldsymbol{Z}$ に対して

$$\left\{ a_1x_1 + \cdots + a_nx_n \,\middle|\, x_1, \cdots, x_n \in \boldsymbol{Z} \right\} = d\boldsymbol{Z}, \quad d \geq 0$$

をみたす $d \in \boldsymbol{Z}$ が存在し，$d = \gcd(a_1, \cdots, a_n)$ が成り立つ．

(1) は上で示したが，(2) も同様に示すことができる． あ，いけね，一般に n が 2 より大きい場合も含めて $a_1, \cdots, a_n \in \boldsymbol{Z}$ の最大公約数 $\gcd(a_1, \cdots, a_n)$ を定義すんの忘れてた． あらためて定義を書いておこうっと（ついでに最小公倍数もね）．

定義 3.4 $a_1, \cdots, a_n \in \boldsymbol{Z}$ とする．
(1) $d|a_i$ $(i = 1, \cdots, n)$, (2) $c|a_i$ $(i = 1, \cdots, n)$ ならば $c|d$
をみたす整数 $d \geq 0$ を $a_1, \cdots, a_n$ の最大公約数といい，$\gcd(a_1, \cdots, a_n)$ で表す． また，
(3) $a_i|m$ $(i = 1, \cdots, n)$, (4) $a_i|l$ $(i = 1, \cdots, n)$ ならば $m|l$
をみたす整数 $m \geq 0$ を $a_1, \cdots, a_n$ の最小公倍数といい，$\mathrm{lcm}(a_1, \cdots, a_n)$ で表す．

最後に，定理 3.3 に関連して，整数係数 1 次方程式の整数解に関する定理を述べる．

定理 3.5 $a_1, \cdots, a_n \in \boldsymbol{Z}$ の最大公約数を d とする． $b \in \boldsymbol{Z}$ に対して，未知数 $x_1, \cdots, x_n$ に関する方程式

$$a_1x_1 + \cdots + a_nx_n = b$$

の整数解が存在するための必要十分条件は，$d|b$ である．

証明 前定理より

$$\left\{ a_1x_1 + \cdots + a_nx_n \,\middle|\, x_1, \cdots, x_n \in \boldsymbol{Z} \right\} = d\boldsymbol{Z}$$

が成り立っている． よって，与えられた方程式が整数解をもつことと，$b \in d\boldsymbol{Z}$ は同値である． 一方，$b \in d\boldsymbol{Z}$ は $d|b$ と同値なので，定理の主張を得る． □

第4章　素数と素因数分解の一意性

4.1　素数の定義

定義 4.1 整数 p が**素数**であるとは，$p>1$ であって，$1<d<p$ をみたす約数 d をもたないものである．

素数でも 1 でも -1 でもない整数を**合成数**という（$1, -1$ は**単数**とよばれるが，いまは忘れちゃってもいい）． 一般に，整数 $n\neq 0$ に対して，$1, -1, n, -n$ を n の**自明な約数**という． したがって，素数とは自明な約数しかもたない 1 より大きい整数のことである． この定義は，“約数” ということばを用いて述べられているが，以下のように “倍数” を用いて素数を特徴づけることもできる．

命題 4.2 整数 p が素数であるためには次が成り立つことが必要十分である； $p>1$ であって，$a, b\in \boldsymbol{Z}$ に対してその積 ab が p の倍数ならば，a または b は p の倍数である．

証明　必要性　p が素数であるとする． いま，$p|ab$ を仮定する． a, p の最大公約数 d は p の正の約数だが，p が素数なので，$d=p$ または $d=1$ となる． $d=p$ のとき，a が p の倍数であることは明らかである． 一方，$d=1$ のときは，定理 2.6（または 3.5）より，$ax+py=1$ $(x, y\in \boldsymbol{Z})$ と表されるから，$b=abx+pby$ は p の倍数となる．
十分性　d を p の約数とすると，$p=cd$ $(c\in \boldsymbol{Z})$ と書ける． もちろん $p|cd$ だから，仮定より $p|c$ または $p|d$ である． $p|c$ ならば $pk=c$ $(k\in \boldsymbol{Z})$ と表されるから，$p=cd=pkd$，よって $kd=1$ より $d=\pm 1$ を得る． $p|d$ のときは，$pl=d$ $(l\in \boldsymbol{Z})$ と書け，$p=cd=cpl$，よって $cl=1$ だから $c=\pm 1$ すなわち $d=\pm p$ となる． 以上より，p は自明な約数しかもたないことが示されたから，p は素数である． □

さて，素数の定義から直接導かれる性質として，任意の自然数 $a>1$ が有限個の素数の積に書けることがあげられる． 実際，素数の積で書けない $a>1$ があったとすると，その様な最小の自然数が存在する（最小値原理）． それをあらためて a とすれば，a はもちろん素数でないから，素数の定義より $a=bc,\ 1<b, c<a$ をみたす $b, c\in \boldsymbol{N}$ がとれるが，a の最小性より b, c は素数の積で書けるので，その積 a も書けることになり矛盾する．

自然数 a を素数の積に表すことを a の**素因数分解**といい，積に現れる素数を a の**素因数**または**素因子**という（$a=1$ のときも 0 個の素因数をもつ分解と考えることにする）．そして，素因数分解の仕方は順序を考えなければ一通りであることもよく知っているはずである． そのこともあわせて，定理としてまとめておく．

定理 4.3 (初等数論の基本定理) 1 より大きい任意の自然数 a は素数 $p_1, \cdots, p_r$ の積

$$a = p_1 \cdots p_r$$

として表すことができ，順序を考えなければその表し方は一意的である． すなわち，二通りの素数の積

$$a = p_1 \cdots p_r = q_1 \cdots q_s$$

に表されたとすると，$r = s$ であって，さらに $q_1, \cdots, q_r$ の番号をうまくとり換えれば $p_1 = q_1, \cdots, p_r = q_r$ とできる． （より正確に書けば，$\{1, 2, \cdots, r\}$ 上の置換 σ で $p_i = q_{\sigma(i)}$ $(i = 1, \cdots, r)$ をみたすものが存在する.）

証明 素因数分解が可能であることはすでに示した． 後半の表し方の一意性を示すために，二通りの素数の積として書ける自然数が存在するとして矛盾を導く． そのような最小の自然数を a とし，$a = p_1 \cdots p_r = q_1 \cdots q_s$ を二通りの素数の積とする． p_1 が素数でかつ $p_1 | q_1 \cdots q_s$ なので，命題 4.2 を（何度か）使えば，$p_1 | q_j$ をみたす j がとれることがわかる． 順序を入れ換えて $j = 1$ すなわち $p_1 | q_1$ であるとしてよい． ここでさらに q_1 が素数であることから $p_1 = q_1$ を得る． したがって，$p_2 \cdots p_r = q_2 \cdots q_s$ であって，仮定より，両辺の積の表し方は（順序を入れかえたとしても）同じにはならない． しかも，この積は a よりも小さいので，a の最小性に矛盾することになる． □

定理 4.3 の後半の主張はとくに**素因数分解の一意性**と呼ばれるが，その証明には，命題 4.2 の形での素数の特徴づけが使われることに注意すべきである． 定理において，p_i のうち同じものをまとめることで，

$$a = p_1^{e_1} \cdots p_r^{e_r} \qquad (p_1, \cdots, p_r \text{ は相異なる素数}，e_i \geq 1)$$

と表すことができる． さらに必要ならば，p_i が素因数でない場合でも $e_i = 0$ として積に含めることができる（このとき $p_i^{e_i} = 1$ に注意）． たとえば，$20 = 2^2 \cdot 5^1 = 2^2 \cdot 3^0 \cdot 5^1$. このような表し方も素因数分解とよぶことにする.

次の定理および系の証明は演習とする.

定理 4.4 自然数 a, b の素因数分解が

$$a = p_1^{e_1} \cdots p_r^{e_r}, \quad b = p_1^{f_1} \cdots p_r^{f_r} \qquad (p_1, \cdots, p_r \text{ は相異なる素数}，e_i, f_i \geq 0)$$

で与えられたとき，次が成り立つ.

(1) $a | b \iff e_i \leq f_i$ $(i = 1, \cdots, r)$.

(2) $d_i = \min(e_i, f_i)$ $(i = 1, \cdots, r)$ とおけば，$\gcd(a, b) = p_1^{d_1} \cdots p_r^{d_r}$.

(3) $m_i = \max(e_i, f_i)$ $(i = 1, \cdots, r)$ とおけば，$\mathrm{lcm}(a, b) = p_1^{m_1} \cdots p_r^{m_r}$.

系 4.5 自然数 a, b に対して $d = \gcd(a, b),\ m = \mathrm{lcm}(a, b)$ とすると，$ab = dm$ が成り立つ．

p を素数とする． 自然数 a に対して，$p^e | a$ であるが $p^{e+1} \nmid a$ であるような整数 $e \geq 0$ がとれる． この e を $v_p(a)$ で表すと，a の素因数分解は

$$a = \prod_{p:\text{素数}} p^{v_p(a)}$$

と表すことができる． $v_p(-a) = v_p(a),\ v_p(0) = \infty$ と定めることで，v_p を $\boldsymbol{Z}$ 上の関数とみなすことができる (ただし，値として ∞ も許す)． この関数 v_p を p **進付値**というが，詳しい性質や使い方については，演習で…．

4.2 素数が無限個あること

次の定理は当たり前のようであるが，定理 4.3 との関連を考えると重要である．

定理 4.6 素数は無数に存在する．

以下において 2 通りの証明を与える（時間が許せば，講義でさらに別の証明も紹介する)． ひとつはユークリッドによる証明であり古代からよく知られていた方法，もうひとつは，オイラーによる示唆に富んだ方法である．

証明 [ユークリッド](古代) 素数が有限個しかないとして矛盾を導く． すべての素数を $p_1, \cdots, p_r$ とし，$M = p_1 \cdots p_r + 1$ とおく． 定理 4.3 より，M はある素数で割り切れるが，素数は $p_1, \cdots, p_r$ のどれかだから，それを p_i とする． このとき，$1 = M - p_1 \cdots p_r$ が素数 p_i の倍数となって矛盾する． □

証明 [オイラー](18 世紀) ここでも，素数は有限個しかなく，それらすべてが $p_1, \cdots, p_r$ であるとして矛盾を導くことにする． いま，等比数列の和の公式より，各素数 $p = p_i$ について

$$\sum_{m=0}^{\infty} \frac{1}{p^m} = \frac{1}{1 - \frac{1}{p}} = \frac{p}{p-1}$$

であり，これらの積をとれば

$$(\spadesuit) \quad \frac{p_1}{p_1 - 1} \cdots \frac{p_r}{p_r - 1} = \left(\sum_{m_1=0}^{\infty} \frac{1}{p_1^{m_1}} \right) \cdots \left(\sum_{m_r=0}^{\infty} \frac{1}{p_r^{m_r}} \right) = \sum_{m_1=0}^{\infty} \cdots \sum_{m_r=0}^{\infty} \frac{1}{p_1^{m_1} \cdots p_r^{m_r}}.$$

最後の等式が正当化される理由は，絶対収束級数においては，和の順序をかってに換えたり，分配法則を自由に使って良いという性質があるからである（「微分積分」で教わったことを思い出そう . . . もし忘れちゃってたら微積の単位没収だぞ！)． ここで，$p_1, \cdots, p_r$ がすべての素数であることから，定理 4.3 より，任意の自然数は

$$p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r} \qquad (m_1, m_2, \cdots, m_r \geq 0)$$

の形に一通りに表されることがいえる． よって，(♠) の最右辺はすべての自然数の逆数和であり

$$\frac{p_1 \cdots p_r}{(p_1-1)\cdots(p_r-1)} = \sum_{n=1}^{\infty} \frac{1}{n}$$

となるが，右辺は収束しない（これも微積でやったはず）から矛盾である． □

4.3 ゼータ関数

オイラーは，自然数 n の代わりにベキ数 n^s の逆数和を考え，無限級数

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

が $s > 1$ のとき収束することに注目し，上の証明の手法を用いて，公式

$$\zeta(s) = \prod_{p} \frac{1}{1-p^{-s}} \qquad (s > 1)$$

を得ている． ここで，右辺は素数全体をわたる積である． さらに，

$$\zeta(2) = \frac{\pi^2}{6}, \qquad \zeta(4) = \frac{\pi^4}{90}, \qquad \zeta(6) = \frac{\pi^6}{945} \quad \text{など} \ldots$$

s が正の偶数のときの $\zeta(s)$ の値を得ている (1730 年代)． ここに円周率 π が現れるのは，なんとも不思議である． その後，リーマンは s の動く範囲を複素数にまで広げ，複素関数としての $\zeta(s)$（これを**ゼータ関数**という）の性質を調べている． その目的はガウスが予想した**素数定理**の証明であったが，研究途上で有名な予想を提唱した (1859 年)．

予想 4.7 (リーマン予想 (Riemann Hypothesis)) $\zeta(s) = 0$ をみたす実部が正の複素数 s はすべて $s = \dfrac{1}{2} + it$ (t は実数) の形をしているであろう．

リーマン予想は 150 年以上経過した現在でも未解決の問題として残っている． なお，素数定理そのものはリーマン予想がなくても証明できることが知られている．

定理 4.8 (素数定理) 正の実数 x に対して，x 以下の素数の個数を $\pi(x)$ とすると，

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x} = 1.$$

すなわち，十分大きな x について $\pi(x)$ は $\dfrac{x}{\log x}$ で近似される． 証明は，アダマールとド・ラ・ヴァレー・プーサンが独立に与えた (1896 年)． その方法は複素関数論（複素数上の微積分学）によるものだが，証明を書き下すだけの余白が，ここにもやっぱ無い．

第5章　整数の合同

5.1　合同式

定義 5.1 $a, b, m \in \boldsymbol{Z}$ に対して，$a - b \in m\boldsymbol{Z}$ （すなわち $m|(a-b)$）であるとき，

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

と書き，a は m **を法として** b **と合同である**という．そうでないときは，$a \not\equiv b \pmod{m}$ と書く．このような式を一般に**合同式**といい，m をその合同式の**法**という．

まず，$m \neq 0$ のとき，整数 a を m で割った余りを r とすると，$a \equiv r \pmod{m}$ が成り立つことに注意しよう．実際，商を q とすれば

$$a = qm + r, \quad 0 \leq r < |m|$$

より $a - r = qm$ は m の倍数である．このことを使えば，$m \neq 0$ のとき

$$a \equiv b \pmod{m} \quad \Longleftrightarrow \quad a, b \text{ それぞれを } m \text{ で割った余りは等しい}$$

と書き換えることができる．とくに，

$$a \equiv 0 \pmod{m} \quad \Longleftrightarrow \quad m|a.$$

次に，“極端” な場合，つまり $m = 0, 1$ のときを考える．

- $m = 1$ のとき，どんな $a, b \in \boldsymbol{Z}$ に対しても $a \equiv b \pmod{1}$ である．
- $m = 0$ のとき，「$a \equiv b \pmod{0} \Leftrightarrow a - b \in 0\boldsymbol{Z} \Leftrightarrow a - b = 0 \Leftrightarrow a = b$」．

これらは例外的に扱われることが多い．また，$-m\boldsymbol{Z} = m\boldsymbol{Z}$ より

- $a \equiv b \pmod{m} \Leftrightarrow a \equiv b \pmod{|m|}$.

したがって，ふつう m としては 2 以上の自然数を想定すればよい．

$m = 2$ ならば，任意の整数 a について，

$$a \equiv 0 \pmod{2}, \qquad a \equiv 1 \pmod{2}$$

のどちらか一方が成り立ち，それぞれ a が偶数，奇数であることを表している．

また，整数 $p > 1$ が素数であることは

$$1 < d < p \text{ である任意の } d \in \boldsymbol{Z} \text{ に対して } p \not\equiv 0 \pmod{d}$$

によって定義され，さらに命題 4.2 は，$p > 1$ が素数であるための必要十分条件が

$$ab \equiv 0 \pmod{p} \text{ ならば，} \quad a \equiv 0 \pmod{p} \text{ または } b \equiv 0 \pmod{p}$$

であることを主張している． このように，前出の定義や定理，証明などを合同式を用いて書き換えることは良い学習になる．

さて，合同式の最も基本的な性質は，

- $a \equiv a \pmod{m}$,
- $a \equiv b \pmod{m} \Longrightarrow b \equiv a \pmod{m}$,
- $a \equiv b,\ b \equiv c \pmod{m} \Longrightarrow a \equiv c \pmod{m}$

であるが，どれも定義から直ちにわかってしまう (はずである (と思う (と信じたい)))．これらは，合同式で表される関係が “同値関係” であることを示している（Wikipedia で調べてみ……）．

次に，和，差，積（足し算，引き算，掛け算）と合同式の関係についての性質をまとめておく（商，つまり割り算については次節で扱う）．

命題 5.2 $a, b, c, d, m \in \boldsymbol{Z}$ が $a \equiv b,\ c \equiv d \pmod{m}$ をみたすならば，

$$a + c \equiv b + d \pmod{m}, \quad a - c \equiv b - d \pmod{m}, \quad ac \equiv bd \pmod{m}$$

がそれぞれ成り立つ．

証明 ええっと，まず仮定から $a = b + mx,\ c = d + my$ $(x, y \in \boldsymbol{Z})$ と書けるから，これらを足したり引いたり掛けたりという方針で…，あとは任せた！ □

次の命題は，どんな場合に法が変化するかを示している． この証明もやってみて．

命題 5.3 $a, b, l, m, n \in \boldsymbol{Z}$ に対して次の (1), (2) が成り立つ．
(1) $m|n$ のとき，$a \equiv b \pmod{n}$ ならば $a \equiv b \pmod{m}$.
(2) $l \neq 0$ のとき，$a \equiv b \pmod{m} \Longleftrightarrow al \equiv bl \pmod{ml}$.

(1) の逆は成り立たないことに注意せよ． たとえば，$3|9$ だけど，$7 \equiv 1 \pmod{3}$ かつ $7 \not\equiv 1 \pmod{9}$ である． また，(2) と

$$\text{(誤)} \qquad l \neq 0 \text{ のとき，} \quad a \equiv b \pmod{m} \Longleftrightarrow al \equiv bl \pmod{m}$$

との違いに注意せよ． 確かに “$\Longrightarrow$” は正しいのだが，逆は一般に正しくない． たとえば，$45 \equiv 15 \pmod{10}$ だが，両辺を 5 で割って $9 \equiv 3 \pmod{10}$ とはできない． 一方，両辺を 3 で割れば，$15 \equiv 5 \pmod{10}$ という正しい合同式を得る． このように，割る数によっては正しい合同式が導かれることもあるが，一般には正しくない． どのような数で割ることができるかは，次節で詳しく述べる．

5.2　法に関する逆元

前節の命題 5.2 で見たように合同式と加減乗算の関係はカンタンであったが，割り算については状況が少し複雑である．

定義 5.4　$a, m \in \boldsymbol{Z}$ に対して，$ax \equiv 1 \pmod{m}$ をみたす $x \in \boldsymbol{Z}$ が存在するとき，a は**法 m に関して可逆**であるといい，x を**法 m に関する a の逆元**という．

逆元はいつも存在するわけではないが，もし存在するならば m を法として一意的に定まる．“m を法として一意的” とは，x と x' がともに a の法 m に関する逆元ならば，$x \equiv x' \pmod{m}$ が成り立つことを意味する．実際，$ax \equiv ax' \equiv 1 \pmod{m}$ から

$$x \equiv x \cdot 1 \equiv x(ax') \equiv (ax)x' \equiv 1 \cdot x' \equiv x' \pmod{m}$$

が得られる．

例 5.5　(1)　$7 \cdot 2 = 14 \equiv 1 \pmod{13}$ より，7 は 13 を法として可逆であり，逆元として 2 がとれる．一方，$7 \cdot 8 = 56 \equiv 1 \pmod{11}$ なので，8 は法 11 に関する 7 の逆元である．
(2)　14 未満のすべての自然数 x に対して，$7x \equiv 0$ または 7 $\pmod{14}$ であることを確かめよ．このことから，7 は法 14 に関して可逆ではないことがわかる．

整数 a, b の最大公約数が 1 のとき，a, b は**互いに素**であるという．次の命題は，法と互いに素な整数による割り算が可能なことを示している．

命題 5.6　互いに素な整数 a, m について次が成り立つ．
(1)　a は法 m に関して可逆である．
(2)　$b, c \in \boldsymbol{Z}$ が $ab \equiv ac \pmod{m}$ をみたすならば，$b \equiv c \pmod{m}$ が成り立つ．

証明　(1)　$\gcd(a, m) = 1$ より $ax + my = 1$ をみたす $x, y \in \boldsymbol{Z}$ がとれるが，これより $ax \equiv 1 \pmod{m}$ であるから a は可逆である．
(2)　$ab \equiv ac \pmod{m}$ の両辺に，a の法 m に関する逆元 x を掛ければよい．　□

さて，a が法 m に関して可逆ならば，逆元 x を用いて $ax = 1 + my$ $(y \in \boldsymbol{Z})$ と書けるが，このことは定理 3.3 より $\gcd(a, m) = 1$ を意味する．上の命題とあわせれば，a が法 m に関して可逆であるためには，a, m が互いに素であることが必要十分であることがわかる．式で書けば，

$$\gcd(a, m) = 1 \quad \Longleftrightarrow \quad ax \equiv 1 \pmod{m} \text{ をみたす } x \in \boldsymbol{Z} \text{ が存在する．}$$

とくに，p が素数のときは，$a \not\equiv 0 \pmod{p}$ である任意の整数 a に対して，法 p に関する逆元が存在する．

一般に，$\gcd(a, m) = 1$ のとき，ax に $x = 1, 2, \cdots$ を順々に代入していって m で割った余りが 1 になるものを探すことで，a の法 m に関する逆元のひとつが求まる．実際に，

計算苦手な私でも $m < 20$ くらいならばこの方法は実用的である（若い皆さんなら計算力もあるから $m < 100$ くらいまで大丈夫？）．しかし，大きな m に対しては効率が悪い．命題 5.6 の証明をみると，$ax + my = 1$ $(x, y \in \boldsymbol{Z})$ のとき，x が a の法 m に関する逆元になっているので，ユークリッドの互除法を用いて x, y を求めれば効率よく計算できる．

例 5.7 (1) 法 2019 に関する 1963 の逆元を求めてみよう．そのために，$1963x$ に $x = 2, 3, \cdots$ を順に代入して 2019 で割り算して余りを求めていくと，いつまで経っても余り 1 が現れない．そこで，$2018, 1963$ に対してユークリッドの互除法を適用すると，

$$2019 = 1 \cdot 1963 + 56, \quad 1963 = 35 \cdot 56 + 3, \quad 56 = 18 \cdot 3 + 2, \quad 3 = 1 \cdot 2 + 1$$

であり，これらから

$$-666 \cdot 2019 + 685 \cdot 1963 = 1$$

と計算され（ホントかな？），法 2019 に関する 1963 の逆元として 685 が求まる．
(2) 一方，法 2015 に関する 1963 の逆元を求めようとして，ユークリッドの互除法を適用すると，最大公約数は 13 となって互いに素ではないから逆元は存在せず，なんだかなあ〜という気分になるので，逆元を求めるときは注意が必要である．

定義 5.8 $a, m \in \boldsymbol{Z}$（ただし $m \geq 2$）とする．$az \equiv 0 \pmod{m}$ かつ $z \not\equiv 0 \pmod{m}$ をみたす $z \in \boldsymbol{Z}$ が存在するとき，a は**法 m に関する零因子**であるという．

たとえば，$4 \cdot 3 \equiv 0 \pmod{6}$，$4 \not\equiv 0 \pmod{6}$，$3 \not\equiv 0 \pmod{6}$ なので，4 と 3 はどちらも法 6 に関する零因子である．なお，どんな法 $m \geq 2$ に対しても，0 は法 m に関する零因子であることに注意せよ（理由を考えてごらん）．

定理 5.9 $a, m \in \boldsymbol{Z}$ $(m \geq 2)$ に対して次は同値である．

(i) a, m は互いに素である．
(ii) a は法 m に関して可逆である．
(iii) a は法 m に関する零因子ではない．

証明 (i) ⇒ (ii): すでに命題 5.6 で示されている．
(ii) ⇒ (iii): 整数 x を法 m に関する a の逆元とする．いま，a が零因子であるとすると，$az \equiv 0,\ z \not\equiv 0 \pmod{m}$ をみたす整数 z がとれるが，

$$z = 1 \cdot z \equiv (ax)z = x(az) \equiv x \cdot 0 = 0 \pmod{m}$$

となって矛盾する．よって a は零因子ではない．
(iii) ⇒ (i): $d = \gcd(a, m)$ とおき，$a = a'd,\ m = m'd$ のように整数 a', m' をとっておく．いま $d > 1$ と仮定すると，$m' \not\equiv 0 \pmod{m}$．一方，

$$am' = (a'd)m' = a'(m'd) = a'm \equiv 0 \pmod{m}$$

だから，a は法 m に関する零因子となって矛盾．したがって $d = 1$． □

第6章　合同式を解く

6.1　1次合同式

整数 a が m を法として可逆であることは，

$$ax \equiv 1 \pmod{m}$$

をみたす整数 x が存在することであった． また，a が零因子であることは，

$$ax \equiv 0, \quad x \not\equiv 0 \pmod{m}$$

をみたす整数 x が存在することであった． これらの性質は，与えられた合同式を未知数 x をもつ方程式のように扱い，その整数解の存在によって特徴づけられていると考えることができる． この章では，方程式としての合同式を扱い，その整数解について述べる．

まず最初に，すでに学んだ1次不定方程式の理論を書き換えることにより，次を得る．

定理 6.1 整数 $a_1, \ldots, a_n, b, m$ に対して合同式

$$a_1x_1 + \cdots + a_nx_n \equiv b \pmod{m}$$

が整数解 $x_1, \ldots, x_n$ をもつための必要十分条件は，b が $\gcd(a_1, \ldots, a_n, m)$ の倍数であることである．

証明　与えられた合同式が整数解 $x_1, \ldots, x_n$ をもつことと，1次不定方程式

$$a_1x_1 + \cdots + a_nx_n + my = b$$

が整数解 $x_1, \ldots, x_n, y$ をもつことは同値，よって，定理 3.5 より定理の主張を得る． □

上記定理を $n = 1, b = 1$ として適用すれば，「合同式 $ax \equiv 1 \pmod{m}$ が整数解もつ」⇔「1 が $\gcd(a, m)$ を約数としてもつ」⇔「$\gcd(a, m) = 1$」，すなわち，定理 5.9 の一部が得られる． さらに，次の系が成り立つこともすぐにわかる．

系 6.2 整数 a, m が互いに素ならば，任意の整数 b に対して，合同式

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

は整数解をもつ． さらに，解は m を法として一意的に定まる． すなわち，$x, x' \in \boldsymbol{Z}$ がともに解ならば $x \equiv x' \pmod{m}$ が成り立つ．

系 6.2 は，以下に述べるように，連立合同式に拡張することができる． いま，整数 a_{ij} および b_i $(i,j=1,\dots,n)$ に対して，$x_1,\dots,x_n$ を未知数とする法 m に関する連立合同式

$$\begin{cases} a_{11}x_1+a_{12}x_2+\cdots+a_{1n}x_n\equiv b_1 \pmod m \\ a_{21}x_1+a_{22}x_2+\cdots+a_{2n}x_n\equiv b_2 \pmod m \\ \quad\vdots \qquad\quad \vdots \quad \ddots \quad \vdots \qquad \vdots \qquad \vdots \\ a_{n1}x_1+a_{n2}x_2+\cdots+a_{nn}x_n\equiv b_n \pmod m \end{cases}$$

を考える． これを，線形代数で学んだときのように，n 次正方行列 $A=(a_{ij})$ と n 次元列ベクトル $\boldsymbol{b}=(b_i)$，および未知数からなる列ベクトル $\boldsymbol{x}=(x_i)$ を用いて

$$A\boldsymbol{x}\equiv\boldsymbol{b} \pmod m$$

と表すと便利である． 次の定理が系 6.2 の一般化になっている．

定理 6.3 A を整数を成分とする n 次正方行列，m を整数とする． $\det A$ と m が互いに素ならば，任意の整数成分 n 次元列ベクトル $\boldsymbol{b}$ に対して，m を法とする連立合同式

$$A\boldsymbol{x}\equiv\boldsymbol{b} \pmod m$$

は整数を成分とするベクトル解をもつ． さらに，解は m を法として一意的に定まる．

証明 A の余因子行列 $\tilde{A}$ は整数を成分とする n 次正方行列であり，

$$\tilde{A}A=A\tilde{A}=(\det A)E$$

が成り立つことに注意する． ここで E は n 次単位行列を表す． 仮定より，$\det A$ の法 m に関する逆元 c がとれて，$c\det A\equiv 1 \pmod m$ をみたすから，

$$A(c\tilde{A}\boldsymbol{b})=c(A\tilde{A})\boldsymbol{b}=(c\det A)\boldsymbol{b}\equiv\boldsymbol{b} \pmod m.$$

よって $\boldsymbol{x}=c\tilde{A}\boldsymbol{b}$ は解である． □

例 6.4 連立合同式 $\begin{cases} 24x-15y\equiv 20 \pmod{16} \\ 11x+71y\equiv 19 \pmod{16} \end{cases}$ を解け．

解 まず，係数行列式は，$\begin{vmatrix} 24 & -15 \\ 11 & 71 \end{vmatrix}\equiv\begin{vmatrix} 8 & 1 \\ -5 & 7 \end{vmatrix}=61\equiv -3 \pmod{16}$ であり，-3 が法 16 と互いに素だから，定理 6.3 より，整数解 x,y をもつことが保証される． 次に，解を求めるために拡大係数行列を “16 を法として” 変形する;

$$\begin{pmatrix} 24 & -15 & 20 \\ 11 & 71 & 13 \end{pmatrix}\equiv\begin{pmatrix} 8 & 1 & 4 \\ -5 & 7 & -3 \end{pmatrix}\xrightarrow[\text{行入替}]{}\begin{pmatrix} -5 & 7 & -3 \\ 8 & 1 & 4 \end{pmatrix}\xrightarrow[1\text{行}\times 3]{}\begin{pmatrix} 1 & 21 & -9 \\ 8 & 1 & 4 \end{pmatrix}\equiv\begin{pmatrix} 1 & 5 & 7 \\ 8 & 1 & 4 \end{pmatrix}$$

$$\xrightarrow[2\text{行}+1\text{行}\times 8]{}\begin{pmatrix} 1 & 5 & 7 \\ 0 & 41 & 60 \end{pmatrix}\equiv\begin{pmatrix} 1 & 5 & 7 \\ 0 & -7 & -4 \end{pmatrix}\xrightarrow[2\text{行}\times(-7)]{}\begin{pmatrix} 1 & 5 & 7 \\ 0 & 1 & 28 \end{pmatrix}\overset{\text{ちょっと略した}}{\xrightarrow[1\text{行}+2\text{行}\times(-5)]{}\equiv}\begin{pmatrix} 1 & 0 & -5 \\ 0 & 1 & -4 \end{pmatrix}$$

この変形から，解 $(x,y)=(-5,-4)$ を得る． $(x,y)=(11,12)$ が解であるとしてもよい．

6.2　中国の剰余定理

前節では，共通の法をもついくつかの合同式からなる連立合同式を扱った． この節では異なる法をもつ連立合同式を考える．

定理 6.5 (中国の剰余定理) $m_1, m_2, \ldots, m_r$ をどの 2 つも互いに素な自然数とすると，任意の整数 $a_1, a_2, \ldots, a_r$ に対して，連立合同式

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \qquad \cdots\cdots \\ x \equiv a_r \pmod{m_r} \end{cases}$$

は整数解 x をもつ． さらに，$M = m_1 \cdots m_r$ とすると，解は M を法として一意的である．

最後の部分，すなわち一意性は次のようにして確かめられる． $x, x' \in \boldsymbol{Z}$ がどちらも上の合同式をみたすならば，$x - x'$ は $m_1, m_2, \ldots, m_r$ すべての倍数である． 一方，仮定より $m_1, m_2, \ldots, m_r$ はどの 2 つも互いに素だから，これらの最小公倍数は $M = m_1 \cdots m_r$ であり，$x - x'$ はその倍数，したがって $x \equiv x' \pmod{M}$ が確かめられた．

以下において，解が存在することの証明を 2 つ与える．

第 1 証明　$r = 1$ のときは明らかなので $r \geq 2$ としよう． まず，第 1 の合同式から解は $a_1 + m_1 y$ の形をしている． これが第 2 の式をみたしているので

$$a_1 + m_1 y \equiv a_2 \pmod{m_2} \quad \text{すなわち} \quad m_1 y \equiv a_2 - a_1 \pmod{m_2}.$$

これを y を未知数とする合同式と考えると，m_1, m_2 が互いに素であることから，系 6.2 より整数解が存在する． そのひとつを k とすれば $y \equiv k \pmod{m_2}$ であり，m_1 を掛けて

$$m_1 y \equiv m_1 k \pmod{m_1 m_2},$$

したがって，第 1，第 2 の合同式はひとつの合同式

$$x \equiv a_1 + m_1 k \pmod{m_1 m_2}$$

に置き換えることができ，$r = 2$ ならば右辺が解を与えることになる． $r \geq 3$ のときも，この操作を繰り返すことで最終的にひとつの合同式に帰着され，それが解を与える（正確には数学的帰納法による）． □

第 2 証明　まず，$n_1, \ldots, n_r \in \boldsymbol{Z}$ を次式で定める;

$$m_i n_i = m_1 \cdots m_r \quad (i = 1, \cdots r).$$

すなわち n_i は $m_1, \ldots, m_r$ から m_i を除いたものの積であり，仮定より m_i, n_i は互いに素である． よって，系 6.2 より，$n_i t_i \equiv a_i \pmod{m_i}$ をみたす整数 t_i がとれる． このとき，n_i の定義から，$1 \leq i, j \leq r$ に対して

$$n_i t_i \equiv \begin{cases} a_i & (i = j) \\ 0 & (i \neq j) \end{cases} \pmod{m_j}$$

であり，したがって $x = n_1 t_1 + \cdots + n_r t_r$ が解を与えることがわかる． □

上記 2 つの証明は，実際に解を求める計算法も与えている． 数学的帰納法による第 1 証明は，合同式を 2 つずつ順々に解いていく方法，第 2 証明はすべての合同式を平等に扱い，解を一気に構成する方法である．

以下ではひとつの例題に対し，第 1 および第 2 証明にそった解法をそれぞれ例示する．

例 6.6 次の連立合同式を解け．

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

解 1 まず第 1 の合同式から，解は $2 + 3k$ の形をしている． これが第 2 の式をみたすから $2 + 3k \equiv 3 \pmod{5}$，これを解いて $k \equiv 2 \pmod{5}$ したがって $3k \equiv 6 \pmod{15}$ となるから，第 1，第 2 の合同式はひとつの合同式 $x = 2 + 3k \equiv 8 \pmod{15}$ に帰着する．続けて，この式から解は $8 + 15l$ の形をしていて，それを第 3 の合同式に当てはめると，l は $8 + 15l \equiv 2 \pmod{7}$ をみたさなければならない． これを解いて $l \equiv 1 \pmod{7}$，したがって $15l \equiv 15 \pmod{105}$． これから，解 $x = 8 + 15l \equiv 23 \pmod{105}$ を得る．

解 2 三つの合同式

$$35t_1 \equiv 2 \pmod{3}, \qquad 21t_2 \equiv 3 \pmod{5}, \qquad 15t_3 \equiv 2 \pmod{7}$$

をそれぞれ解くことで，たとえば $(t_1, t_2, t_3) = (4, 3, 2)$ が求まる． これを用いて，解

$$x = 35 \cdot 4 + 21 \cdot 3 + 15 \cdot 2 = 140 + 63 + 30 = 233$$

を得る． $233 \equiv 23 \pmod{105}$ より，**解 1** と同じ解が得られた（当たり前だ）．

中国の南北朝時代（AD 439–589）に成立したとされる算術書【孫子算経】に，例 6.6 が**解 2** と同じ趣旨の解法とともに書かれており（補遺参照），それが，定理 6.5 が “中国の剰余定理” と呼ばれる理由と言われている． **解 2** は各合同式を同等に扱い（つまり対称性があり）理論的にもシンプルで優れていると思われるが，途中の計算の意味がとらえにくいのが欠点である． また，上の例ではわかりにくいが，法 $m_1, \ldots, m_r$ が大きい場合，**解 1** に比べて**解 2** はかなり大きな整数を扱うことになり計算が大変になる． 私自身は，紙とペンで計算するなら**解 1** を選び、コンピュータ上にプログラミングするなら**解 2** を選びたいが，皆さんならどうする？

第7章　剰余類と剰余環

7.1　剰余類

定義 7.1 整数 m および a に対して，$x \equiv a \pmod{m}$ をみたす整数 x 全体の集合を $a + m\boldsymbol{Z}$ で表し，**法 m に関する（a の属する）剰余類**という;

$$a + m\boldsymbol{Z} = \left\{ x \in \boldsymbol{Z} \,\middle|\, x \equiv a \pmod{m} \right\}.$$

$0 + m\boldsymbol{Z}$ は $m\boldsymbol{Z}$ のことである． 後の説明にもあるように，m が特定されている場合には $\overline{a}$ と略記することがある; $\overline{a} = a + m\boldsymbol{Z}$.

次の命題は剰余類の定義から簡単に示すことができる．

命題 7.2 m および a, b, c を整数とする．

(1) $a + m\boldsymbol{Z} = b + m\boldsymbol{Z}$, $(a + m\boldsymbol{Z}) \cap (b + m\boldsymbol{Z}) = \phi$ のどちらか一方が必ず成り立つ．

(2) $b, c \in a + m\boldsymbol{Z}$ ならば $b \equiv c \pmod{m}$.

(3) 次の 4 つは互いに同値である;

$$a \equiv b \pmod{m}, \quad a \in b + m\boldsymbol{Z}, \quad b \in a + m\boldsymbol{Z}, \quad a + m\boldsymbol{Z} = b + m\boldsymbol{Z}$$

法 m で合同な整数をひとまとめにした $\boldsymbol{Z}$ の部分集合が，m を法とする剰余類である．合同式においては m を法として合同な数を “等しい” とみなして計算する． 言い換えれば，剰余類をあたかも数のように扱うのが合同式の計算であると言える． これについては，次の節で詳しく述べる．

定義 7.3 整数 m に対して，法 m に関するすべての剰余類を元とする集合を，**法 m に関する剰余環**といい，$\boldsymbol{Z}/m\boldsymbol{Z}$ で表す;

$$\boldsymbol{Z}/m\boldsymbol{Z} = \left\{ a + m\boldsymbol{Z} \mid a \in \boldsymbol{Z} \right\}.$$

さて，しばらくの間，自然数 m を固定し，剰余類 $a + m\boldsymbol{Z}$ を $\overline{a}$ と略す． すべての整数は m を法として $0, 1, 2, \cdots, m-1$ のどれかと合同で，これらは互いに合同ではないから

$$\boldsymbol{Z} = \overline{0} \cup \overline{1} \cup \overline{2} \cup \cdots \cup \overline{m-1}, \qquad \overline{a} \cap \overline{b} = \phi \quad (0 \le a < b < m).$$

したがって，剰余類は全部で m 個あり，

$$\boldsymbol{Z}/m\boldsymbol{Z} = \left\{ \overline{0}, \overline{1}, \overline{2}, \cdots, \overline{m-1} \right\}$$

と書くことができる． たとえば，$\boldsymbol{Z}/7\boldsymbol{Z} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$ であるが，これを（いやだけど）

$$\boldsymbol{Z}/7\boldsymbol{Z} = \left\{\overline{49},\ \overline{-13},\ \overline{9^7},\ \overline{5^5},\ \overline{123456},\ \overline{3\cdot 74},\ \overline{66^{33}}\right\}$$

と書いてもかまわない（ホントかな，確かめてね）．

7.2 剰余類の和と積

はじめに，合同式に関して

$$a_1 \equiv a_2,\ b_1 \equiv b_2 \pmod{m} \implies a_1 + b_1 \equiv a_2 + b_2,\ a_1 b_1 \equiv a_2 b_2 \pmod{m}$$

が成り立つことに注意しよう（命題 5.2）． このことは，2 つの剰余類からそれぞれの元を選ぶとき，それらの和や積の属する剰余類が選んだ元によらずに定まることを示している． そこで，剰余環における剰余類の “和” や “積” を以下のように定義できることがわかる．

定義 7.4 剰余類 $a + m\boldsymbol{Z}, b + m\boldsymbol{Z} \in \boldsymbol{Z}/m\boldsymbol{Z}$ に対して，それらの和，積を

$$(a + m\boldsymbol{Z}) + (b + m\boldsymbol{Z}) = (a + b) + m\boldsymbol{Z}, \qquad (a + m\boldsymbol{Z})(b + m\boldsymbol{Z}) = (ab) + m\boldsymbol{Z}$$

によって定める．

この定義による和と積は，略記法で

$$\overline{a} + \overline{b} = \overline{a + b}, \qquad \overline{a}\overline{b} = \overline{ab}$$

と書いても同じである． こう表すとアタリマエのように見えるでしょ？ たとえば，7 を法として $\overline{2} + \overline{3} = \overline{5}$ とか $\overline{2}\cdot\overline{3} = \overline{6}$ など…． 一方，$\overline{3} + \overline{5} = \overline{1}$ や $\overline{4}\cdot\overline{6} = \overline{3}$ となると少しはアタリマエじゃなくなる…． 剰余類の等式

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

における和や積は，合同式

$$a + b \equiv c, \quad ab \equiv d \pmod{m}$$

における整数の和，積を，剰余類の和，積とみなして表したもの，と考えればよい． **「合同式」は「剰余環における等式」**であり，その意味で，剰余類の演算は合同式に現れる演算を，より直感的に表現していると考えられる． たとえば，未知数 x をもつ合同式

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

は，剰余類に関する方程式

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

と同等であり，より簡明になる． ただし，未知数 x として，前者の場合は整数を想定するのに対し，後者は剰余類つまり $\boldsymbol{Z}/m\boldsymbol{Z}$ の元を想定するという違いがある． しかし，慣れてくると，これらをあまり区別せずに議論できるようになる．

なお，“$\equiv \pmod{\ }$” を $\boldsymbol{Z}$ 上の**同値関係**とみなし，それによって $\boldsymbol{Z}$ を**同値類別**して得られる**商集合**として $\boldsymbol{Z}/m\boldsymbol{Z}$ をとらえることもできる． この考え方はめっちゃ一般化され，数学のいろんな分野に現れるけど，詳しくは演習の時間にまかせちゃったりして，ずるい？

7.3 剰余環の分解

自然数 m の倍数 M をとる． いま，整数 a, b が $a \equiv b \pmod{M}$ をみたすならば，$M|(a-b)$ だから $m|(a-b)$，よって $a \equiv b \pmod{m}$ もみたすので，法 M の剰余環 $\boldsymbol{Z}/M\boldsymbol{Z}$ から法 m の剰余環 $\boldsymbol{Z}/m\boldsymbol{Z}$ への写像

$$\boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow \boldsymbol{Z}/m\boldsymbol{Z}, \qquad a + M\boldsymbol{Z} \mapsto a + m\boldsymbol{Z}$$

を定めることができる． さらに，M がふたつの自然数 m, n の公倍数ならば，上と同様にして

$$\boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow \boldsymbol{Z}/n\boldsymbol{Z}, \qquad a + M\boldsymbol{Z} \mapsto a + n\boldsymbol{Z}$$

も定まり，これらをあわせて剰余環の直積への写像

$$F : \boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z}), \qquad a + M\boldsymbol{Z} \mapsto (a + m\boldsymbol{Z}, a + n\boldsymbol{Z})$$

が定義できる． 別の書き方をすれば，$F(\bar{a}) = (\bar{a}, \bar{a})$ となる． ただし，それぞれの $\bar{a}$ は，法 M および法 m，法 n に関する剰余類を考えるわけである． このような写像を**自然な写像**とよぶ．

ここで，とくに M が m, n の最小公倍数のときは，F は単射である． これを確かめるために，$a, b \in \boldsymbol{Z}$ が $F(a + M\boldsymbol{Z}) = F(b + M\boldsymbol{Z})$ をみたすとすると，

$$a + m\boldsymbol{Z} = b + m\boldsymbol{Z} \quad \text{かつ} \quad a + n\boldsymbol{Z} = b + n\boldsymbol{Z},$$

よって $a - b$ は，m の倍数でもあり n の倍数でもあるから，$M = \mathrm{lcm}(m, n)$ の倍数，すなわち $a + M\boldsymbol{Z} = b + M\boldsymbol{Z}$ を得る． これで F が単射であることが確かめられた． 以上は，2 つの自然数 m, n についての話だが，これを次のように一般化するのは難しくない．

命題 7.5 自然数 $m_1, \ldots, m_r$ に対して，M をそれらの公倍数とすると，自然な写像

$$\boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/m_1\boldsymbol{Z}) \times \cdots \times (\boldsymbol{Z}/m_r\boldsymbol{Z})$$

が定義できる． とくに，M が $m_1, \ldots, m_r$ の最小公倍数ならば，この写像は単射である．

次に，自然数 M が 2 つの互いに素な約数の積として表される場合を考えよう． すなわち，$M = mn$ であって，かつ m, n は互いに素とする． このとき，m, n の最小公倍数は M と一致する． したがって，命題 7.5 より，自然な写像

$$F : \boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z})$$

は単射である． さらに今の場合，$\boldsymbol{Z}/M\boldsymbol{Z}$ の元の個数は $M = mn$ で，これは直積集合 $(\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z})$ の元の個数と等しいから，F は全射にもなっている． このことは，元の個数が等しい 2 つの有限集合 A, B に対して，A から B への写像は，単射ならば全射でもある，という事実に着目すれば納得できるはずである． さらに，どの 2 つも互いに素である自然数 $m_1, \ldots, m_r$ の最小公倍数が積 $m_1 \cdots m_r$ と一致することに注意すれば，上と同様にして次が得られる．

定理 7.6 どの 2 つも互いに素な自然数の組 $m_1, \ldots, m_r$ に対して，$M = m_1 \cdots m_r$ とおけば，自然な写像

$$\boldsymbol{Z}/M\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/m_1\boldsymbol{Z}) \times \cdots \times (\boldsymbol{Z}/m_r\boldsymbol{Z})$$

が定義でき，さらにこれは全単射である．

とくに，自然数 n に対して，その素因数分解を

$$n = p_1^{e_1} \cdots p_r^{e_r} \qquad (p_i \text{ は相異なる素数},\ e_i > 0)$$

とすると，自然な写像

$$\boldsymbol{Z}/n\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/p_1^{e_1}\boldsymbol{Z}) \times \cdots \times (\boldsymbol{Z}/p_r^{e_r}\boldsymbol{Z})$$

は全単射であることがわかる． この場合，定理 7.6 は，直積分解を通して，剰余環 $\boldsymbol{Z}/n\boldsymbol{Z}$ の性質が，より単純な剰余環 $\boldsymbol{Z}/p_i^{e_i}\boldsymbol{Z}$ の性質に帰着されることを示唆している．

7.4 中国の剰余定理再論

定理 7.6 を用いて，**中国の剰余定理** (定理 6.5) の別証明を与えることができる．

定理 6.5 の第 3 証明 定理 7.6 の写像を F とする． いま，F が全射であることより，与えられた $a_1, \ldots, a_r \in \boldsymbol{Z}$ に対して $F(x + M\boldsymbol{Z}) = (a_1 + m_1\boldsymbol{Z}, \ldots, a_r + m_r\boldsymbol{Z})$ をみたす $x \in \boldsymbol{Z}$ が存在する． このとき，

$$x + m_1\boldsymbol{Z} = a_1 + m_1\boldsymbol{Z}, \quad \ldots, \quad x + m_r\boldsymbol{Z} = a_r + m_r\boldsymbol{Z}$$

が成り立つが，これらの等式は，x が連立合同式 $x \equiv a_i \pmod{m_i}$ $(i = 1, \ldots, r)$ の解であることを示している． また，x, x' がともに解であるとすると，$F(x + M\boldsymbol{Z}) = F(x' + M\boldsymbol{Z})$ であるが，F が単射であることから，$x + M\boldsymbol{Z} = x' + M\boldsymbol{Z}$，すなわち $x \equiv x' \pmod{M}$ が導かれ，法 M に関する一意性も示されたことになる． □

この証明の逆をたどれば，定理 6.5 から定理 7.6 を導くことが可能である． その意味で，定理 7.6 は**中国の剰余定理**の言い換えとみなすことができる．

第8章　既約剰余類群とオイラー関数

8.1　既約剰余類群

m を 2 以上の整数とし，α を法 m に関する剰余類，すなわち $\alpha \in \boldsymbol{Z}/m\boldsymbol{Z}$ とする． いま，$a \in \alpha$ とすると $\alpha = a + m\boldsymbol{Z}$ である． a が法 m に関して可逆ならば，α に属するすべての整数は法 m に関して可逆となる． さらに，整数 b が m を法とする a の逆元ならば，剰余類 $b + m\boldsymbol{Z}$ に属するすべての整数は法 m に関する a の逆元である． 一方，a が法 m に関する零因子ならば，α に属するすべての整数は法 m に関する零因子である（これらのことを確かめてみよ）． したがって，法 m に関する “可逆”，“逆元”，“零因子” という概念は，どれも法 m に関する剰余類がもっている性質ととらえることができる． 次の定義は，このような考え方によって与えられたものである．

定義 8.1 m を 2 以上の整数とし，$\alpha \in \boldsymbol{Z}/m\boldsymbol{Z}$ を剰余類とする．
(1)　$a \in \alpha$ が法 m に関して可逆であるとき，α は**可逆**であるという．
(2)　整数 b が法 m に関する $a \in \alpha$ の逆元であるとき，b の属する剰余類を α の**逆元**とよぶ．
(3)　$a \in \alpha$ が法 m に関する零因子であるとき，α は**零因子**であるという．

剰余類の逆元は，もし存在するならば一意的である． 実際，β, γ がともに α の逆元であるとすると，$\alpha\beta = \alpha\gamma = \overline{1}$ だから，

$$\gamma = \overline{1}\gamma = (\alpha\beta)\gamma = (\beta\alpha)\gamma = \beta(\alpha\gamma) = \beta\overline{1} = \beta.$$

そこで，剰余類 α の逆元を α^{-1} で表す（場合によっては $1/\alpha$ と書くこともある）． たとえば，$7 \cdot 13 = 91 \equiv 1 \pmod{15}$ なので，$\boldsymbol{Z}/15\boldsymbol{Z}$ において $\overline{7}, \overline{13}$ はともに可逆であり互いに逆元，したがって $\overline{7}^{-1} = \overline{13}$ とか $\overline{13}^{-1} = \overline{7}$ と書くこともできる．

定義 8.2 m を 2 以上の整数とする． $\boldsymbol{Z}/m\boldsymbol{Z}$ に属する可逆な剰余類全体からなる集合を，法 m に関する**既約剰余類群**といい $(\boldsymbol{Z}/m\boldsymbol{Z})^\times$ で表す;

$$(\boldsymbol{Z}/m\boldsymbol{Z})^\times = \{\, \alpha \in \boldsymbol{Z}/m\boldsymbol{Z} \mid \alpha \text{ は可逆} \,\}.$$

この元を，法 m に関する**既約剰余類**ということがある．

定理 5.9 によって，次のように表わすこともできる．

$$\begin{aligned}(\boldsymbol{Z}/m\boldsymbol{Z})^{\times} &= \{\, a+m\boldsymbol{Z} \mid a\in\boldsymbol{Z},\ \gcd(a,m)=1 \,\}\\ &= \{\, a+m\boldsymbol{Z} \mid a\in\boldsymbol{Z},\ a \text{ は } m \text{ を法として可逆} \,\}\\ &= \{\, a+m\boldsymbol{Z} \mid a\in\boldsymbol{Z},\ a \text{ は } m \text{ を法として零因子でない} \,\}.\end{aligned}$$

さらに，それぞれの $a\in\boldsymbol{Z}$ は $1\le a<m$ の範囲に限定してもよい（どうしてかな？）．

例 8.3 $\boldsymbol{Z}/10\boldsymbol{Z}=\{\overline{0},\overline{1},\overline{2},\cdots,\overline{9}\}$ のうち，可逆な剰余類は $\overline{1},\overline{3},\overline{7},\overline{9}$ であり，零因子は $\overline{0},\overline{2},\overline{4},\overline{5},\overline{6},\overline{8}$ である（確かめ～）． とくに，既約剰余類群は $(\boldsymbol{Z}/10\boldsymbol{Z})^{\times}=\{\overline{1},\overline{3},\overline{7},\overline{9}\}$ となる． ここで，$\overline{1},\overline{3},\overline{7},\overline{9}$ のそれぞれの逆元が何かは……，計算してみ．

法 m に関する既約剰余類群 $(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}$ は，『積について閉じていて，各元の逆元がその中でとれる』という性質をもっている． これらの性質は $(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}$ が乗法に関して “群” であることを示しているのだが，詳しくは「代数 I」をお楽しみに．

8.2 オイラー関数

定義 8.4 自然数 m に対して，$0\le a<m$ である整数 a のうち m と互いに素なものの個数を $\varphi(m)$ で表す． また，このようにして定まる自然数上の関数 φ を**オイラー関数**という．

すなわち，

$$\varphi(m)=\left|\{\, a\in\boldsymbol{Z} \mid 0\le a<m,\ \gcd(a,m)=1 \,\}\right|.$$

$m\ge 2$ のときは，法 m に関する既約剰余類の個数が $\varphi(m)$ に他ならない;

$$\varphi(m)=\left|(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}\right|.$$

たとえば，$m=10$ のとき，$(\boldsymbol{Z}/10\boldsymbol{Z})^{\times}=\{\overline{1},\overline{3},\overline{7},\overline{9}\}$ だから $\varphi(10)=4$． 小さい m に対するオイラー関数の値は次の表のようになる (1 個間違いがある，どれでしょう？ もぉ，先生のいじわるぅ)．

m	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
$\varphi(m)$	1	1	2	2	4	2	6	4	6	4	10	4	12	6	8	10	16	6	18

この表からも見えるように，オイラー関数の値は非常に不規則だが，次節で示す定理 8.6 の公式を用いれば，次のような不等式を導くことができる．

命題 8.5 自然数 $m\ge 2$ に対して，$\dfrac{m}{1+\log_2 m}\le\varphi(m)\le m-1.$

この命題から，$\varphi(m)\to\infty$ $(m\to\infty)$ が導かれる． 右側の不等式は φ の定義から明らかだが，左側の証明は少し面倒である（補遺参照）．

8.3　オイラー関数の積公式

次の定理によって，どんなに大きな m についても，その素因数分解さえわかればオイラー関数の値 $\varphi(m)$ を正確に計算できる．

定理 8.6 自然数 m の素因数分解が $m = \prod_{j=1}^{r} p_j^{e_j}$ $(p_j$ は相異る素数で $e_j > 0)$ ならば，

$$\varphi(m) = \prod_{j=1}^{r} \left(p_j^{e_j} - p_j^{e_j - 1} \right) = m \prod_{j=1}^{r} \left(1 - \frac{1}{p_j} \right).$$

たとえば，$20196 = 2^2 \cdot 3^3 \cdot 11 \cdot 17$ だから

$$\varphi(20196) = \varphi(2^2) \cdot \varphi(3^3) \cdot \varphi(11) \cdot \varphi(17) = (4-2)(27-9)(11-1)(17-1) = 5760$$

と計算される． この定理は，以下の 2 つの補題から導くことがキミならできるはずだ．

補題 8.7 素数のべき p^e $(e > 0)$ に対して $\varphi(p^e) = p^e - p^{e-1}$.

証明　φ の定義を見れば，p^e と互いに素なもんの個数を数えればええやん． ある整数が p^e と互いに素っちゅうことは，そいつが p で割り切れないことと同じや． そやから，$\varphi(p^e)$ の値は，$0 \leq a < p^e$ をみたす整数 a 全部の個数 p^e から，p の倍数の個数を引けばええんとちゃう？ ほんでもって，p の倍数は $a = jp,\ 0 \leq j < p^{e-1}$ で表される p^{e-1} 個で全部やから，$\varphi(p^e) = p^e - p^{e-1}$ が答えっちゅうわけや． □

補題 8.8 互いに素な自然数 m, n に対して $\varphi(mn) = \varphi(m)\varphi(n)$.

証明　まず，m, n は互いに素な整数なので，前章，定理 7.6 より，写像

$$F \ : \ \boldsymbol{Z}/mn\boldsymbol{Z} \longrightarrow (\boldsymbol{Z}/m\boldsymbol{Z}) \times (\boldsymbol{Z}/n\boldsymbol{Z}), \qquad a + mn\boldsymbol{Z} \mapsto (a + m\boldsymbol{Z},\, a + n\boldsymbol{Z})$$

は全単射であることに注意しておく． いま，整数 a が mn と互いに素ならば，a は m とも n とも互いに素になることは明らかである． したがって，F を既約剰余類群 $(\boldsymbol{Z}/mn\boldsymbol{Z})^\times$ に制限することにより，写像

$$G \ : \ (\boldsymbol{Z}/mn\boldsymbol{Z})^\times \longrightarrow (\boldsymbol{Z}/m\boldsymbol{Z})^\times \times (\boldsymbol{Z}/n\boldsymbol{Z})^\times$$

が定まる． F が単射なので G も単射であるが，以下において G は全射でもあることを確かめよう． これにより，元の個数を比べて $\varphi(mn) = \varphi(m)\varphi(n)$ となって証明が完了する． そこで，全射性を示すために，$\xi \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times \times (\boldsymbol{Z}/n\boldsymbol{Z})^\times$ を任意にとって，

$$\xi = (a + m\boldsymbol{Z},\, b + n\boldsymbol{Z}), \qquad \gcd(a, m) = \gcd(b, n) = 1$$

のように $a, b \in \boldsymbol{Z}$ で表せば，中国の剰余定理 (定理 6.5) より，

$$x \equiv a \pmod{m}, \qquad x \equiv b \pmod{n}$$

をみたす $x \in \boldsymbol{Z}$ が存在する（ここんとこ，F が全射であることを使ってもよい）． このとき，$\gcd(a, m) = \gcd(b, n) = 1$ から，$\gcd(x, mn) = 1$ が簡単に確かめられる． よって $x + mn\boldsymbol{Z} \in (\boldsymbol{Z}/mn\boldsymbol{Z})^{\times}$ かつ $G(x + mn\boldsymbol{Z}) = \xi$ であり，全射であることが示された． □

上の証明もそのアイデアの出所であった定理 7.6 の証明も，一見，同じことをやっているように見える． しかし，上の証明では，2 つの集合の間に単射があるときに，その写像の全射性から集合の元の個数が等しいことを導いているのに対し，定理 7.6 の証明では，逆に元の個数が等しいことから全射性を導いている． これらに違いに注目して二つの証明のストーリーを味わえるようになれば，キミも立派な数学科学生というわけだにゃん．

8.4 オイラー関数の和公式

自然数 m とその正の約数 d に対して，0 以上 m 未満の整数で，m との最大公約数が d であるもの全体の集合を $A(m, d)$ で表す;

$$A(m, d) = \{\, a \in \boldsymbol{Z} \mid 0 \le a < m,\ \gcd(a, m) = d \,\}.$$

とくに，$|A(m, 1)| = \varphi(m)$，$|A(m, m)| = |\{0\}| = 1$ である． また，0 以上 m 未満の m 個の整数は m との最大公約数によって類別されるから，

$$\bigcup_{d|m} A(m, d) = \{0, 1, 2, \ldots, m-1\}$$

したがって

$$\sum_{d|m} |A(m, d)| = m$$

が成り立っている（m の正の約数 d 全体についての和をとる）．いま，$a \in A(m, d)$ に対して a/d は，集合

$$B = \left\{ b \in \boldsymbol{Z} \,\middle|\, 0 \le b < \frac{m}{d},\ \ \gcd\left(b, \frac{m}{d}\right) = 1 \right\}$$

に属する． すなわち，写像 $A(m, d) \to B,\ a \mapsto a/d$ が定義できるが，この写像が全単射であることを確かめるのは難しくない（実際，$B \to A(m, d),\ b \mapsto bd$ が逆写像となっている）． よって $|A(m, d)| = |B|$． 一方，φ の定義から B の元の個数は $\varphi(m/d)$ だから，$|A(m, d)| = \varphi(m/d)$ が導かれる． さらに，d が m の正の約数全体を動くとき m/d も正の約数全体を動くから，上の総和の式と合わせて次の定理を得る．

定理 8.9 自然数 m に対して，$\displaystyle\sum_{d|m} \varphi(d) = m.$

たとえば，$m = 15$ とすると，$\varphi(1) + \varphi(3) + \varphi(5) + \varphi(15) = 1 + 2 + 4 + 8 = 15$ となる．

第9章　フェルマー，オイラーの定理

9.1　フェルマーの定理

本章の目的は，整数のベキ乗数 a^n の法 m におけるふるまいを考察することである． 素数を法とする場合から始めよう．

定理 9.1 (フェルマーの定理) p を素数とし，a を p と互いに素な整数とすると，

$$a^{p-1} \equiv 1 \pmod{p}$$

が成り立つ．

証明　写像 $f_a : (\boldsymbol{Z}/p\boldsymbol{Z})^\times \to (\boldsymbol{Z}/p\boldsymbol{Z})^\times$ を $f_a(\overline{x}) = \overline{ax}$ によって定義する． a が p を法として可逆であることに注意すれば，f_a が全単射であることが確認できる． したがって，

$$(p-1)! = \prod_{x=1}^{p-1} x \equiv \prod_{x=1}^{p-1} (ax) = a^{p-1} \cdot (p-1)! \pmod{p}.$$

ここで p は素数だから，$(p-1)!$ は p を法として可逆，よって定理の合同式を得る． □

この定理は「フェルマーの小定理」ともよばれる（「フェルマーの最終定理」と区別するため）．

例 9.2 フェルマーの定理を用いると累乗の計算が簡単になることがある． たとえば，5^{6789} は素数 59 を法として以下のように計算できる． フェルマーの定理より $5^{58} \equiv 1 \pmod{59}$ が成り立つことに着目して，6789 の 58 による割り算 $6789 = 117 \cdot 58 + 3$ を用いれば，$5^{6789} = (5^{58})^{117} \cdot 5^3 \equiv 5^3 = 125 \equiv 7 \pmod{59}$ となる．

9.2　フェルマーテスト

フェルマーの定理に現れる合同式は，p が素数であるための必要条件を与えているが，十分条件というわけではない． たとえば，$4^{14} \equiv 1 \pmod{15}$, $19^{48} \equiv 1 \pmod{49}$ であるが，15, 49 のどちらも素数ではない． しかし，多くの a について合同式が成り立てば十分条件にもなり得るかもしれない，と（ダメ元で）考えてみよう．

定義 9.3 n を 2 以上の自然数とする． 整数 a が $a^{n-1} \equiv 1 \pmod{n}$ をみたすとき，n を底 a に関する**確率的素数**という．

フェルマーの定理から，ひとつの底に関して確率的素数になっていなければ合成数である． たとえば，$2^{220} \equiv 16 \neq 1 \pmod{221}$ だから 221 は素数ではない． 一方，十分多くの底に関して確率的素数であるならば，素数である可能性は高いと考えられる． 例として

$$2^{29338} \equiv 3^{29338} \equiv 5^{29338} \equiv 7^{29338} \equiv 11^{29338} \equiv 1 \pmod{29339},$$

（こいつら，どうやって計算すんだよ！ という疑問はごもっとも． 時間があれば講義で説明しましょう.）したがって，29339 は底 $2, 3, 5, 7, 11$ に関する確率的素数であり，実際に素数であることが確かめられる．このような素数判定法（別の言い方をすれば，合成数を排除するための方法）を**フェルマーテスト**という．

フェルマーテストはプログラムも簡単で計算も速く有用であるが，完全な素数判定法ではない． たとえば，$n = 29341$ は，底 $2, 3, 5, 7, 11$ に関する確率的素数であるにもかかわらず，$13|n$ より素数ではないことが確認できる． 2002 年にフェルマーテストを改良した**AKS 素数判定法**が発表され脚光を浴びたが，詳しくは別の機会に…ね．

9.3 オイラーの定理

法 m が素数ではないとき，フェルマーの定理で述べられていることはそのままの形では一般に成り立たないことに注意する． たとえば，$5^{6-1} \equiv 5 \neq 1 \pmod{6}$, $2^{9-1} \equiv 4 \neq 1 \pmod{9}$, etc... フェルマーの定理を，法 m が合成数である場合にも適用できるように一般化するには，$a^N \equiv 1 \pmod{m}$ をみたすベキ指数 N を，m に関連付けて探さなければならない． その際，$a^N = a \cdot a^{N-1} \equiv 1 \pmod{m}$ より，a は m を法として可逆，したがって定理 5.9 から，a, m は互いに素でなければならないことに注意する．

一般の合成数を考える前に，まず m が素数ベキの場合を考えよう．

補題 9.4 p を素数とし，a を p と互いに素な整数とすると，任意の自然数 n に対して

$$a^{(p-1)p^{n-1}} \equiv 1 \pmod{p^n}$$

が成り立つ．

証明 n に関する数学的帰納法を用いる． $n = 1$ のときはフェルマーの定理そのものであり，すでに示されている． n のとき成り立つと仮定すると，$a^{(p-1)p^{n-1}} = 1 + p^n k \quad (k \in \boldsymbol{Z})$ と書ける． これを p 乗すれば，$n + 1 \leq 2n < 3n < \cdots$ に注意して

$$a^{(p-1)p^n} = (1 + p^n k)^p = 1 + p \cdot p^n k + \sum_{j=2}^{p} {}_pC_j p^{jn} k^j \equiv 1 \pmod{p^{n+1}}.$$

これは $n + 1$ のときに成り立つことを示している． □

ここで，定理 8.6（または補題 8.7）によれば，$\varphi(p^n) = (p-1)p^{n-1}$ だから，補題 9.4 の合同式は $a^{\varphi(p^n)} \equiv 1 \pmod{p^n}$ と書き換えることができる． これをふまえて，フェルマーの定理は次の定理に拡張される．

定理 9.5 (オイラーの定理) 自然数 $m > 1$ と互いに素な任意の整数 a に対して

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

が成り立つ．

証明 m を素因数分解して $m = p_1^{n_1} \cdots p_r^{n_r}$ (ただし，p_j たちは相異なる素数で $n_j > 0$) とする． p_j は a を割らないから，補題 9.4 より $a^{\varphi(p_j^{n_j})} \equiv 1 \pmod{p_j^{n_j}}$ を得る． 一方，補題 8.8 より $\varphi(m)$ は $\varphi(p_j^{n_j})$ の倍数だから，$a^{\varphi(m)} \equiv 1 \pmod{p_j^{n_j}}$ が各 j に対して成り立つことになり，これからただちに定理が導かれる． □

この証明において，$\varphi(p_j^{n_j})$ たちの最小公倍数を $\psi(m)$ とすれば，

$$a^{\psi(m)} \equiv 1 \pmod{m}$$

が成り立つこともわかる． 一方，$\varphi(m)$ は $\varphi(p_j^{n_j})$ たちの公倍数なので $\psi(m) | \varphi(m)$，したがって，この合同式はオイラーの定理の精密化を与えていることになる．

9.4 位数

フェルマー，オイラーの定理では，法 m で 1 と合同になるためのベキ指数として $\varphi(m)$ が採用されているが，前節の最後でも見たように $\varphi(m)$ より小さいベキでも 1 と合同になる可能性がある． そのようなベキを特徴付けるために次の定義を導入する．

定義 9.6 m を 2 以上の自然数とする． m と素な整数 a に対して

$$a^k \equiv 1 \pmod{m}$$

をみたす最小の自然数 k を**法 m に関する a の位数**という． また，剰余類 $\alpha \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times$ に対して α に属する元の法 m に関する位数はすべて等しい． それを α の**位数**という．

つまり，整数 a の法 m に関する位数とは

$$\min\left\{ k \in \boldsymbol{N} \,\middle|\, a^k \equiv 1 \pmod{m} \right\} = \min\left\{ k \in \boldsymbol{N} \,\middle|\, \overline{a}^k = \overline{1} \right\}$$

であり，これを簡単に剰余類 $\overline{a}$ の位数というわけである． なお，m と素でない整数 a の位数は定義されないことに注意しよう．

命題 9.7 m を 2 以上の自然数，a を m と互いに素な整数，s を法 m に関する a の位数とする． 自然数 r が

$$a^r \equiv 1 \pmod{m}$$

をみたすならば，位数 s は r の約数である． とくに $s|\varphi(m)$ が成り立つ．

証明 r を s で割り算して，$r = us + v,\ (0 \leq v < s)$ とすると，$1 \equiv a^r = (a^s)^u a^v \equiv a^v \pmod{m}$ だから，もし $v > 0$ とすると位数 s の最小性に矛盾する． よって $v = 0$ であり $r = us$ は s の倍数である． □

例 9.8 $\varphi(100) = 40$ だからオイラーの定理より，$3^{40} \equiv 1 \pmod{100}$． したがって，命題 9.7 によれば，100 を法とする 3 の位数は 40 の約数 $1, 2, 4, 5, 8, 10, 20, 40$ のどれかである． 根気よく（そしてちょっと工夫して）計算すれば，$3^8 \not\equiv 1,\ 3^{10} \not\equiv 1 \pmod{100}$ かつ $3^{20} \equiv 1 \pmod{100}$ が得られ，位数は 20 であることがわかる．

命題 9.9 m を 2 以上の自然数，a を m と互いに素な整数，s を法 m に関する a の位数とする．

(1) $s = uv\ (u, v \in \boldsymbol{N})$ ならば，法 m に関する a^u の位数は v である．
(2) $t \in \boldsymbol{N}$ が s と互いに素ならば，法 m に関する a^t の位数も s である．

証明 簡単のため $\alpha = \overline{a} = a + m\boldsymbol{Z}$ とおき，$\overline{1} = 1 + m\boldsymbol{Z}$ も 1 と略す． したがって，たとえば $\alpha^s = 1$ となる． いま，a, m は互いに素なので α は可逆であり，α^{-1} が定義されることにも注意せよ．
(1) まず $(\alpha^u)^v = \alpha^{uv} = \alpha^s = 1$ が成り立つ． よって，w を α^u の位数とすると，命題 9.7 より $w|v$． 一方，$\alpha^{uw} = 1$ だから，再び命題 9.7 より $s = uv$ は uw の約数であり $v|w$． ゆえに $w = v$．
(2) まず $(\alpha^t)^s = (\alpha^s)^t = 1$ が成り立つ． よって，w を α^t の位数とすると，命題 9.7 より $w|s$． いま，s, t は互いに素だから，$sx + ty = 1\ (x, y \in \boldsymbol{Z})$ と書けて，$\alpha = \alpha^{sx+ty} = (\alpha^s)^x(\alpha^t)^y = (\alpha^t)^y$． 一方，$\alpha^{tw} = 1$ だから $\alpha^w = (\alpha^t)^{yw} = 1$，したがって，再び命題 9.7 より $s|w$ となるから，$w = s$ を得る． □

命題 9.10 m を 2 以上の自然数，a, b をともに m と互いに素な整数とする． 法 m に関する a, b のそれぞれの位数 s, t が互いに素ならば，法 m に関する ab の位数は st である．

証明 前命題の証明と同様に，$\alpha = \overline{a},\ \beta = \overline{b} \in (\boldsymbol{Z}/m\boldsymbol{Z})^\times$ とする． w を $\alpha\beta$ の位数とする． まず，$(\alpha\beta)^{st} = (\alpha^s)^t(\beta^t)^s = 1$ なので，命題 9.7 より $w|st$ が成り立つ． そこで，逆に $st|w$ を確かめればよい． まず，s, t は互いに素なので $sx + ty = 1$ をみたす $x, y \in \boldsymbol{Z}$ がとれる． このとき，$\alpha^s = \beta^t = 1$ に注意すれば，$\alpha = \alpha^{sx+ty} = \alpha^{ty} = (\alpha\beta)^{ty}$． よって，$\alpha^w = (\alpha\beta)^{wty} = 1$ となるから，再び命題 9.7 より $s|w$ である． α, β の役割を入れ換えれば，$t|w$ もわかる． s, t は互いに素なので，結局 w は st の倍数となる． □

第10章　暗号システム

10.1　暗号

本章では，整数論が暗号理論にどのように応用されるか，その概略を解説する．

暗号 (cryptography) あるいは**暗号システム** (cryptosystem) とは，第三者に通信内容を知られないように行う特殊な通信方法で、通信文を見ても特別な知識なしでは読めないように変換する表記法のことである． そのような変換を**暗号化** (encryption) という． 暗号化される前の文を**平文** (plaintext)，暗号化によって第三者に通信内容が知られないようにした文を**暗号文** (ciphertext) という． 平文は暗号化によって暗号文に変換されるが，逆に暗号文をから平文を復活させることを**復号化** (decryption) という． 暗号化，復号化のための手順で用いられるパラメータを**鍵** (key) という． 暗号化は復号化と対をなしていて，単純なシステムでは，暗号化のための手順の逆を行うことで復号化がなされる．

さて，整数論の応用という観点から，平文や暗号文はすべて自然数によって表されているものとする． すなわち，日本語や英語など普通の言語で書かれた文を適切な方法で自然数に変換したものを考える．もともとコンピュータ内部では，文字でも何でもすべてが自然数として表現されていると考えてよい． そこで，鍵も自然数として表し，平文，鍵，暗号文の間に整数論的な操作をほどこすことで暗号システムが構築される．

暗号化の鍵と復号化の鍵が同一である（あるいは片方からもう一方が容易に得られる）暗号を**共通鍵暗号** (common key cryptosystem) という． 古典的な暗号はすべて共通鍵暗号であり，20 世紀後半に**公開鍵暗号** (public key cryptosystem) が現れる以前は「暗号＝共通鍵暗号」であった．

10.2　Diffie-Hellman 鍵共有

一般に共通鍵暗号は，後で解説する公開鍵暗号に比べ単純に設計され，暗号化・復号化も速やかに実行でき大量データの処理が可能である． しかし，通信をしたい両者があらかじめ**鍵を共有**する必要があり，そこで安全性が損なわれる可能性がある． つまり，普通に考えれば，一方が作成した鍵をもう一方に伝えなくてはならず，その際，鍵を盗まれるおそれがある． このような危険を回避するひとつの方法として，1976 年，W. Diffie と M. E. Hellman は，鍵自体を伝えることなしに両者が同一の鍵を共有する方法を提唱した．これを **Diffie-Hellman 鍵共有** (Diffie-Hellman key exchange) という．

一般に，大きな数 b, m を固定し，a, x が関係式 $a \equiv b^x \pmod{m}$ をみたすとする． このとき，x から a は簡単に計算できるが，a から x を求めることは一般には困難である．こ

の困難な問題を**離散対数問題** (discrete logarithm problem) とよぶ．ここでいう離散対数とは，実数における対数の既約剰余類群 $(\boldsymbol{Z}/m\boldsymbol{Z})^{\times}$ における類似である．Diffie-Hellman 鍵共有の安全性は離散対数問題に依拠しており，実際の手順は以下のように説明される．

(1) 太郎と花子が鍵として「大きな数」を共有したいとする．
(2) 太郎と花子は，大きな素数 p と，法 p に関する位数が小さくない自然数 $g < p$ を用意して共有する．p, g は第三者に知られてもかまわない．
(3) 太郎は $p-1$ と互いに素な「大きな数」 x をランダムに選び，g^x を p で割った余り，すなわち

$$i \equiv g^x \pmod{p}, \quad 0 < i < p$$

によって定まる i を花子に伝える．太郎は x を秘密にする．
(4) 花子は $p-1$ と互いに素な「大きな数」 y をランダムに選び，

$$j \equiv g^y \pmod{p}, \quad 0 < j < p$$

によって定まる j を太郎に伝える．花子は y を秘密にする．
(5) 太郎は，花子から届いた j と，秘密の数 x を用いて

$$k_1 \equiv j^x \pmod{p}, \quad 0 < k_1 < p$$

なる k_1 を計算する．
(6) 花子は，太郎から届いた i と，秘密の数 y を用いて

$$k_2 \equiv i^y \pmod{p}, \quad 0 < k_2 < p$$

なる k_2 を計算する．
(7) 以上の方法で得られた k_1 と k_2 は等しいことが，

$$k_1 \equiv j^x \equiv g^{xy} \equiv i^y \equiv k_2 \pmod{p}, \qquad 0 < k_1, k_2 < p$$

よりわかる．これを $k\ (= k_1 = k_2)$ とする．
(8) k が「大きな数」ならば，これを共通の鍵として採用する．もし k が「小さな数」になってしまったら，もう一度はじめからやり直す．

以上の手順において，p, g, i, j は通信路に乗る（太郎と花子の間を行き来する）ので，悪意のある第三者に読み取られる可能性があるが，x, y と鍵 k は通信路に乗らないので読み取られる可能性は小さい．いま，p, g, i, j が第三者に知られているとすると，x, y から鍵 k も簡単に計算できてしまうが，i から x を求めることや，j から y を求めることは離散対数問題であり，非常に困難であると考えられる．すなわち，Diffie-Hellman 鍵共有の安全性は離散対数問題の困難さによるといえる．

10.3 RSA 公開鍵暗号

前節で述べたように，共通鍵暗号は，暗号化の鍵と復号化の鍵が同一，または，一方からもう一方が容易に導出できるものであった． これとは違い，暗号化の鍵がわかっても復号化の鍵を得ることが現実的に困難な場合，暗号化の鍵を公開しても暗号の安全性は保たれると考えられる． たとえば，インターネット上で多くのユーザからの情報（＝平文）を暗号で受け取りたい人Aは，まず，暗号化，復号化の鍵を 1 組だけ生成し，暗号化の鍵のみを公開する． どのユーザもその鍵を使ってそれぞれの平文を暗号化し，暗号文をAに送ることができる． Aは復号化の鍵を用いて，平文，すなわちユーザの情報を得るわけである．

このように，暗号化の鍵を公開しても安全性が保たれるようなシステムを一般に**公開鍵暗号** (public key cryptosystem) という． 暗号化の鍵を**公開鍵** (public key) とよび，復号化の鍵を**秘密鍵** (private key) とよぶ． 公開鍵暗号は，通信相手の各々に対して別々の鍵を用意する必要がなく鍵管理が容易であるなど共通鍵暗号に対する利点が多い反面，“なりすまし” を防ぐ必要や多くの処理時間を要するなどの欠点もある．

以下で解説する **RSA 暗号**は，1978 年に R. L. Rivest，A. Shamir，L. Adleman により開発された代表的な公開鍵暗号であり，現在広く普及している．

花子が太郎からメッセージを受け取りたいとき，RSA 暗号では次のような手順をふむ．

(1) 【準備】 花子は，2 つの異なる大きな素数 p, q を用意し，積 $N = pq$ を計算する． $\varphi(N) = (p-1)(q-1)$ と互いに素な大きな自然数 $d < \varphi(N)$ をランダムに選び，

$$ed \equiv 1 \pmod{\varphi(N)}, \quad 0 < e < \varphi(N)$$

をみたす e を計算する． (e, N) を公開鍵として太郎に知らせ，d を秘密鍵として秘密にする． p, q および $\varphi(N)$ の値も秘密にする．

(2) 【暗号化】 太郎は，メッセージを自然数で表現した平文 T を用意する． 必要ならば修正をほどこして，$T < N$ および $\gcd(T, N) = 1$ が成り立つようにしておく． この T から，公開鍵 (e, N) を用いて

$$C \equiv T^e \pmod{N}, \quad 0 < C < N$$

によって暗号文 C を作成し，花子に送る．

(3) 【復号化】 花子は，届いた暗号文 C から，秘密鍵 d を用いて

$$T' \equiv C^d \pmod{N}, \quad 0 < T' < N$$

を計算する． このとき $T' = T$ となっていて，太郎からのメッセージ T を復元できる． なぜなら，d, e のとり方から $ed = 1 + m\varphi(N)$ と書けるが，オイラーの定理より $T^{\varphi(N)} \equiv 1 \pmod{N}$ だから

$$T' \equiv C^d \equiv T^{ed} = T^{1+m\varphi(N)} = T(T^{\varphi(N)})^m \equiv T \pmod{N},$$

一方 $0 < T, T' < N$ であったから $T' = T$ を得る．

さて，RSA 暗号の安全性は，公開鍵 (e, N) から秘密鍵 d を導出することが困難であることよる． 以下に，暗号の安全性に係わる秘密鍵の管理についてまとめておく．

- 秘密鍵 d は，法 $\varphi(N)$ に関する e の逆元として，ユークリッドの互除法により効率よく計算できてしまうので，受信者にとって $\varphi(N)$ の秘匿は重要である．
- N の素因数 p, q が知られると，$\varphi(N) = (p-1)(q-1)$ と計算され，上述のとおり秘密鍵が知られてしまうので，p, q の秘匿も重要である．
- 逆に $\varphi(N)$ が知られると，

  $$\varphi(N) = (p-1)(q-1) = N - (p+q) + 1$$

  から $p+q$ がわかり，2 次方程式

  $$x^2 - (p+q)x + N = 0$$

  を解くことで p, q が求まってしまう．したがって，N の素因数 p, q が知られることと $\varphi(N)$ が知られることは同等であり，これらの管理は同程度に重要である．

大きな整数の素因数分解は一般には難しく，N だけから p, q を求めることは現実には不可能であると考えられる． すなわち，素因数分解が困難であることが RSA 暗号の安全性の根拠となっているわけである．

10.4 ハイブリッド暗号システム

実際の RSA 暗号では，素数 p, q を選ぶとき，本当に素数であるかどうかの判定をする必要がある． 素因数分解に比べて素数判定は短時間でできること等を考慮して，現状では十進表示で数百桁の素数 p, q を選ぶことになる． したがって N, d, e も数百桁になり，数百桁の数百桁乗の（数百桁の数を法とした）計算を実行することになり，これには相当な時間がかかる． このようなことも含め様々な理由から，一般に公開鍵暗号は大量のデータを即時に暗号化・復号化するのには適さない． そこで，暗号化したい大量のデータは共通鍵暗号によって通信することとし，そこで使う共通鍵のみを公開鍵暗号によって配送する，という方法が考えられる． すなわち，共通鍵暗号のもつ効率性と公開鍵暗号のもつ鍵管理の安全性というそれぞれの特徴を組み合わせるわけである． 組み合せ方も上記のように単純なものから複雑なものまで様々なものが考えられる． このような暗号方式は**ハイブリッド暗号システム**とよばれ，広く実用化されている．

このように，公開鍵暗号のような新しい暗号方式が提唱された後でも，以前に使われていた方式が捨てられるわけではなく，それらを共存させて「効率性と安全性」のバランスをとりながら新たな暗号システムが構築されている． それらの多くが整数論や代数学に依拠している． さらに,「効率性と安全性」の評価にも整数論的な深い考察が必要とされ，暗号理論は整数論の知識なしでは展開できないと言える．

第11章　平方剰余

11.1　平方剰余記号

第 9 章では自然数を法とする整数のベキ乗数のふるまいについて述べ，第 10 章でその暗号への応用を紹介したが，本章ではとくに平方数について考察する．

定義 11.1 p を奇素数（つまり，2 でない素数）とし，a を p で割り切れない整数とする． 合同式

$$x^2 \equiv a \pmod{p}$$

が整数解をもつとき，a は p を法として**平方剰余**であるといい，もたないとき**平方非剰余**であるという． さらに，

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & p\nmid a \text{ かつ } a \text{ が } p \text{ を法として平方剰余のとき,} \\ -1, & p\nmid a \text{ かつ } a \text{ が } p \text{ を法として平方非剰余のとき,} \\ 0, & p \mid a \text{ のとき} \end{cases}$$

と定め，これを p を法とする**平方剰余記号**という．

例 11.2　$1^2 \equiv 1,\ 2^2 \equiv 4,\ 3^2 \equiv 4,\ 4^2 \equiv 1 \pmod 5$ より，5 を法として $1, 4$ は平方剰余であり $2, 3$ は平方非剰余である． また，7 を法とすると，たとえば 2 は平方剰余，5 が平方非剰余であることが確かめられる． さらに，これらは次のように表すことができる;

$$\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1, \quad \left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1, \quad \left(\frac{2}{7}\right) = 1, \quad \left(\frac{5}{7}\right) = -1.$$

さて，奇素数 p と互いに素な整数 a に対して，$(a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) = a^{p-1} - 1 \equiv 0 \pmod p$ がフェルマーの定理からいえる． p は素数なので，$a^{\frac{p-1}{2}} - 1,\ a^{\frac{p-1}{2}} + 1$ のどちらかは p で割り切れ，したがって，$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$ を得る． 次の定理は，この ± 1 が平方剰余記号の値を決めることを示している．

定理 11.3 (オイラーの規準) 奇素数 p と整数 a に対して，

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

が成り立つ．

証明　$p|a$ のときは明らかなので，以下 $p\nmid a$ とする． a が法 p に関して平方剰余ならば，$x^2 \equiv a \pmod{p}$ をみたす整数 x がとれる． このとき，フェルマーの定理より

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 = \left(\frac{a}{p}\right) \pmod{p}.$$

そこで，以下では a は平方非剰余であると仮定する． いま，$A = \{1, 2, \ldots, p-1\}$ として，$r_j, s_j \in A$ $(j = 1, \cdots, (p-1)/2)$ を次の手順で定める． まず，$r_1 \in A$ を任意にとり，$r_1 s_1 \equiv a \pmod{p}$ をみたす $s_1 \in A$ をとる． r_1 は p と互いに素だから，このような s_1 は一意的に存在し，仮定より $r_1 \neq s_1$ である． 次に，$\{r_1, s_1\}$ に属さない $r_2 \in A$ を任意にとって，$r_2 s_2 \equiv a \pmod{p}$ をみたす $s_2 \in A$ をとる． このとき，s_2 は r_1, s_1, r_2 のどれとも異なることが確かめられる． 次に，$\{r_1, s_1, r_2, s_2\}$ に属さない $r_3 \in A$ を任意にとって……，この操作を $A = \{r_1, s_1, \cdots, r_{(p-1)/2}, s_{(p-1)/2}\}$ となるまで繰り返す． そこで，A の元すべての積をとれば，

$$a^{\frac{p-1}{2}} \equiv (r_1 s_1)(r_2 s_2) \cdots (r_{(p-1)/2} s_{(p-1)/2}) = (p-1)! \underset{\Uparrow}{\equiv} -1 = \left(\frac{a}{p}\right) \pmod{p}.$$

ここで，$\Uparrow$ の部分は次の補題による． □

補題 11.4 (ウィルソンの定理) 素数 p に対して $(p-1)! \equiv -1 \pmod{p}$ が成り立つ．

証明　上の証明で，A の代わりに $B = \{2, 3, \cdots, p-2\}$ を用いて，$r_j s_j \equiv 1 \pmod{p}$ をみたす $r_j, s_j \in B$ を順にとることを考えれば，$1 \equiv (r_1 s_1) \cdots (r_{(p-3)/2} s_{(p-3)/2}) = (p-2)! \pmod{p}$ が導かれる． よって，$(p-1)! = (p-1) \cdot (p-2)! \equiv p - 1 \equiv -1 \pmod{p}$． □

定理 11.5 奇素数 p および整数 a, b に対して次が成り立つ．

(1)　$a \equiv b \pmod{p}$ ならば，$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(2)　$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

証明　(1) は平方剰余記号の定義から直ちにわかる． また，定理 11.3 より

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}$$

であるが，平方剰余記号は 0 または ± 1 なので，等式 (2) が確かめられる． □

11.2　平方剰余の相互法則，補充法則

整数 a が奇素数 p を法として平方剰余かどうかは，平方剰余記号をオイラーの規準 (定理 11.3) や定理 11.5 を使って計算すれば，原理的には決定することができる． しかし，一般に p が非常に大きいときは膨大な計算が必要となる．

次の 2 つの定理を用いることで，大きな素数を法とする平方剰余記号の計算が小さな素数を法とする計算に帰着され，簡単になる．

定理 11.6 (平方剰余の相互法則) 相異なる奇素数 p, q に対して，

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

別の書き方をすれば，

$$\left(\frac{q}{p}\right) = \begin{cases} \left(\dfrac{p}{q}\right) & (p \equiv 1 \pmod 4 \text{ または } q \equiv 1 \pmod 4 \text{ のとき}), \\ -\left(\dfrac{p}{q}\right) & (p \equiv q \equiv 3 \pmod 4 \text{ のとき}). \end{cases}$$

定理 11.7 (補充法則) 奇素数 p に対して次が成り立つ．

[**第 1 補充法則**] $\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & (p \equiv 1 \pmod 4 \text{ のとき}), \\ -1 & (p \equiv 3 \pmod 4 \text{ のとき}). \end{cases}$

[**第 2 補充法則**] $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & (p \equiv 1, 7 \pmod 8 \text{ のとき}), \\ -1 & (p \equiv 3, 5 \pmod 8 \text{ のとき}). \end{cases}$

証明は後回しにして，ここでは，これらの定理がどのように使われるかを解説しよう．いま，$1 < a < p$ のとき，その素因数分解を $a = \prod_{j=1}^{r} q_j^{e_j}$ とすれば，定理 11.5 (2) より，

$$\left(\frac{a}{p}\right) = \prod_{j=1}^{r}\left(\frac{q_j}{p}\right)^{e_j} = \prod_{e_j:\text{奇数}}\left(\frac{q_j}{p}\right).$$

ここで，$q_j = 2$ ならば第 2 補充法則が適用でき，$2 < q_j$ ならば相互法則を用いて p より小さな法 q_j の計算に帰着される．

例 11.8　17 を法とする -7 の平方剰余を調べてみる*．

$$\left(\frac{-7}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{5}{17}\right) \underset{\text{S2}}{=} \left(\frac{5}{17}\right) \underset{\text{R}}{=} \left(\frac{17}{5}\right) = \left(\frac{2}{5}\right) \underset{\text{S2}}{=} -1,$$

あるいは，はじめに第 *1* 補充法則を使って

$$\left(\frac{-7}{17}\right) \underset{\text{S1}}{=} \left(\frac{7}{17}\right) \underset{\text{R}}{=} \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) \underset{\text{R}}{=} -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

一方，オイラーの規準を使うとすれば，$(-7)^{\frac{17-1}{2}} = (-7)^8$ を計算すればよいが，$(-7)^2 = 49 \equiv -2 \pmod{17}$ より $(-7)^8 \equiv (-2)^4 = 16 \equiv -1 \pmod{17}$ なので，上と同じ結論を得る（もちろん！）．

*等号の下の R は相互法則を，S1, S2 はそれぞれ第 1，第 2 補充法則を適用したことを示す．

11.3　2次合同式

この節では，奇素数を法とする2次合同式の解が存在するかどうかの判定法について簡単に解説する． 次の定理の証明は，通常の2次方程式と同様，平方完成をすることで得られる（各自，証明してみ）.

定理 11.9　p を奇素数とし，a, b, c を整数，ただし $a \not\equiv 0 \pmod{p}$ とする． 合同式

$$ax^2 + bx + c \equiv 0 \pmod{p},$$

に対して，法 p に関する $b^2 - 4ac$ の平方剰余記号を δ とする; $\delta = \left(\dfrac{b^2 - 4ac}{p}\right)$ （分数じゃないよ，平方剰余記号だよ）． このとき，次が成り立つ.
(1)　$\delta = 0$ ならば，p を法としてただひとつの整数解をもつ.
(2)　$\delta = 1$ ならば，p を法として相異なる2つの整数解をもつ.
(3)　$\delta = -1$ ならば，整数解をもたない.

例 11.10　$2x^2 + 3x + 5 \equiv 0 \pmod{7}$ を解け.

解　判別式は $3^2 - 4 \cdot 2 \cdot 5 \equiv 4 \pmod{7}$ より，7 を法として相異なる2つの解をもつ． 解を求めるには，はじめに2次の係数 2 の逆元 4 をかけることで，

$$x^2 + 12x + 20 \equiv 0 \pmod{7}, \quad \text{簡単化して} \quad x^2 - 2x - 1 \equiv 0 \pmod{7},$$

1次の係数を絶対値の小さな偶数にするところがミソで，1/2 を出さずに平方完成できて

$$(x-1)^2 - 1 - 1 \equiv 0 \pmod{7}, \quad \text{すなわち} \quad (x-1)^2 \equiv 2 \pmod{7}$$

を得る． 最後に $3^2 \equiv 2 \pmod{7}$ より，解 $1 \pm 3 \equiv 4, -2 \equiv 4, 5 \pmod{7}$ が得られる.

例 11.11　$x^2 + x + 7 \equiv 0 \pmod{23}$ を解け.

解　判別式の平方剰余記号を計算すると，

$$\left(\frac{1 - 4 \cdot 7}{23}\right) = \left(\frac{-27}{23}\right) = \left(\frac{-4}{23}\right) = \left(\frac{-1}{23}\right) \underset{\text{S1}}{=} -1$$

なので解をもたない.

例 11.12　$p \equiv 5 \pmod{11}$ をみたす素数 p について，$x^2 + 3x + 5 \equiv 0 \pmod{p}$ が整数解をもつかどうか判定せよ.

解　p を法とする判別式の平方剰余を計算して，

$$\left(\frac{3^2 - 4 \cdot 5}{p}\right) = \left(\frac{-11}{p}\right) \underset{\Uparrow}{=} \left(\frac{p}{11}\right) = \left(\frac{5}{11}\right) \underset{\text{R}}{=} \left(\frac{11}{5}\right) = \left(\frac{1}{5}\right) = 1$$

より整数解をもつ． ここで，等号 $\Uparrow$ は，$p \equiv \pm 1 \pmod{4}$ で場合分けして，相互法則，第1補充法則を援用して確かめられる（ホントかよ！ すぐにはわかんねえよ……，自分の頭で考えなきゃな）.

第12章　補充法則と相互法則の証明

12.1　補充法則の証明

この節では，補充法則 (定理 11.7) を証明する． まず，第 1 補充法則はオイラーの規準から直ちに導かれる． 第 2 補充法則を示すために，恒等式

$$(x^2+1)^p = \sum_{j=0}^{p} {}_pC_j x^{2j} = \sum_{j=0}^{\frac{p-1}{2}} {}_pC_j x^{2j} + \sum_{k=0}^{\frac{p-1}{2}} {}_pC_{p-k} x^{2(p-k)} = \sum_{j=0}^{\frac{p-1}{2}} {}_pC_j (x^{2j} + x^{2p-2j})$$

が成り立つことに注目する（ここで，${}_pC_{p-j} = {}_pC_j$ を用いた）． これを x^p で割れば

$$(\heartsuit) \qquad \left(x + x^{-1}\right)^p = \sum_{j=0}^{\frac{p-1}{2}} {}_pC_j \left(x^{p-2j} + x^{-(p-2j)}\right).$$

一方，1 の 8 乗根 $\eta = e^{\frac{2\pi i}{8}}$ について，$\eta + \eta^{-1} = \sqrt{2},\ \eta^3 + \eta^{-3} = -\sqrt{2}$ を確かめるのは難しくない． さらに，$\eta^8 = 1$ より，

$$\eta^n + \eta^{-n} = \begin{cases} \eta + \eta^{-1} = \sqrt{2} & (n \equiv \pm 1 \pmod 8 \text{ のとき}), \\ \eta^3 + \eta^{-3} = -\sqrt{2} & (n \equiv \pm 3 \pmod 8 \text{ のとき}). \end{cases}$$

すなわち，任意の奇数 n に対して，$\eta^n + \eta^{-n} = (-1)^{\frac{n^2-1}{8}}\sqrt{2}$ が成り立つ． そこで，η を恒等式 $(\heartsuit)$ の x に代入し，両辺を $\sqrt{2}$ で割れば，

$$2^{\frac{p-1}{2}} = \sum_{j=0}^{\frac{p-1}{2}} {}_pC_j (-1)^{\frac{(p-2j)^2-1}{8}} \equiv (-1)^{\frac{p^2-1}{8}} \pmod p.$$

これとオイラーの規準から第 2 補充法則が得られる．

12.2　ガウス和

平方剰余の相互法則 (定理 11.6) には様々なタイプの証明があるが，どれもちょっとずつ難しい． ここではガウス和による証明の概略を述べる． 前節の補充法則の証明では複素数 η (= 1 の 8 乗根) が使われたが，ここでは，奇素数 p に対して，1 の p 乗根

$$\zeta_p = e^{\frac{2\pi i}{p}} = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

を用いる．

定義 12.1 奇素数 p に対して，

$$\tau_p = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^a$$

と定め，これを p に関する**ガウス和**という．

ガウス和 τ_p は，定義だけ見てもどうもよくわからない複素数だが，平方すると簡単な整数になっちゃうというのが次の定理である． これって，ちょっとびっくりだよね．

定理 12.2 p を奇素数とすると，$\tau_p^2 = (-1)^{\frac{p-1}{2}} p$ が成り立つ．

この定理の証明がこの節の目標だが，その前にいくつかの補題を準備する．

補題 12.3 奇素数 p に対して，$\left(\frac{a}{p}\right) = -1$ をみたす整数 a が存在する．

証明 写像 $f : (\boldsymbol{Z}/p\boldsymbol{Z})^\times \to (\boldsymbol{Z}/p\boldsymbol{Z})^\times$ は，$f(\overline{1}) = \overline{1} = f(\overline{-1})$ および $\overline{1} \neq \overline{-1}$ より単射ではないから，全射でもない． これから補題はすぐに導かれる． □

補題 12.4 p を奇素数とすると，$\displaystyle\sum_{t=1}^{p-1} \left(\frac{t}{p}\right) = 0$ が成り立つ．

証明 前補題のような整数 a をとれば，とくに a は p と素だから，$t = 1, 2, \ldots, p-1$ のとき，at の $\boldsymbol{Z}/p\boldsymbol{Z}$ における剰余類は，$\overline{1}, \overline{2}, \ldots, \overline{p-1}$ 全体にわたる． したがって，

$$\sum_{t=1}^{p-1} \left(\frac{t}{p}\right) = \sum_{t=1}^{p-1} \left(\frac{at}{p}\right) = \left(\frac{a}{p}\right) \sum_{t=1}^{p-1} \left(\frac{t}{p}\right) = -\sum_{t=1}^{p-1} \left(\frac{t}{p}\right).$$

よってこの和は 0 であり，示したい等式を得る． □

補題 12.5 奇素数 p と整数 s に対して

$$\sum_{a=0}^{p-1} \zeta_p^{as} = \begin{cases} 0, & p \nmid s \text{ のとき}, \\ p, & p \mid s \text{ のとき} \end{cases}$$

が成り立つ．

証明 $p \mid s$ のときは明らかだから，以下，$p \nmid s$ を仮定して，和が 0 になることを示す． 恒等式 $x^p - 1 = (x-1)(x^{p-1} + \cdots + x^2 + x + 1)$ に $x = \zeta_p^s$ を代入して

$$(\zeta_p^s - 1) \left(\sum_{a=0}^{p-1} \zeta_p^{as} \right) = \zeta_p^{sp} - 1 = 0.$$

s が p の倍数ではないから $\zeta_p^s - 1 \neq 0$ であり，示したい式を得る． □

定理 12.2 の証明　まず，

$$\tau_p^2 = \left(\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\zeta_p^a\right)\left(\sum_{b=1}^{p-1}\left(\frac{b}{p}\right)\zeta_p^b\right) = \sum_{a=1}^{p-1}\left(\sum_{b=1}^{p-1}\left(\frac{ab}{p}\right)\zeta_p^{a+b}\right)$$

の最右辺内側の和について，$b = at$ とおけば，$b = 1, 2, \ldots, p-1$ のとき，t の $\boldsymbol{Z}/p\boldsymbol{Z}$ における剰余類は $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ 全体にわたるから，

$$\tau_p^2 = \sum_{a=1}^{p-1}\sum_{t=1}^{p-1}\left(\frac{a^2t}{p}\right)\zeta_p^{a+at} = \sum_{t=1}^{p-1}\left(\frac{t}{p}\right)\sum_{a=1}^{p-1}\zeta_p^{a(t+1)}.$$

ここで，補題 12.5 から

$$\sum_{a=1}^{p-1}\zeta_p^{a(t+1)} = \begin{cases} p-1, & t = p-1 \text{ のとき}, \\ -1, & 1 \leq t < p-1 \text{ のとき} \end{cases}$$

がわかるから，補題 12.4 より

$$\tau_p^2 = \sum_{t=1}^{p-2}\left(\frac{t}{p}\right)(-1) + \left(\frac{p-1}{p}\right)(p-1) = -\sum_{t=1}^{p-1}\left(\frac{t}{p}\right) + \left(\frac{p-1}{p}\right)p = \left(\frac{-1}{p}\right)p.$$

よって，第 1 補充法則（定理 11.7）より定理を得る． □

12.3　もっとガウス和

前節ではひとつの奇素数 p についてのガウス和 τ_p の性質を見てきたが，この節では別の奇素数 q をとって、τ_p と q がどのように絡むのかを調べる． 実際には，次の定理の証明がこの節での目標である．

定理 12.6 p, q を相異なる奇素数とすると，

$$\tau_p^{q-1} \equiv \left(\frac{q}{p}\right) \pmod{q}$$

が成り立つ．

ここで注意すべきことは，$q-1$ が偶数になるので，定理 12.2 より，$\tau_p^{q-1} \in \boldsymbol{Z}$ となることである (だって，そうじゃないと合同式の意味がわかんなくなっちゃうもん)．

さて，定理 12.6 の証明の前に，集合

$$R = \{\, f(\zeta_p) \mid f(x) \text{ は整数係数の多項式} \,\}$$

を考える． たとえば $\tau_p \in R$ である． R は和，差，積について閉じている． すなわち，R の任意の 2 元 α, β に対して $\alpha+\beta$, $\alpha-\beta$, $\alpha\beta$ は R に属する． また，明らかに $\boldsymbol{Z} \subset R \cap \boldsymbol{Q}$ であるが，次の補題は逆の包含関係が成り立つことを主張している．

補題 12.7　$R \cap \boldsymbol{Q} = \boldsymbol{Z}$.

証明は少しばかり厄介なので（補遺を参照），以下，これを認めて定理 12.6 を証明する．

定理 12.6 の証明　まず，フェルマーの定理と二項定理を繰り返し用いれば，任意の整数係数多項式 $f(x)$ に対して

$$f(x)^q = f(x^q) + qg(x)$$

をみたす整数係数多項式 $g(x)$ がとれることがわかる． よって，ある $\alpha \in R$ があって

$$\tau_p^q = \sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^{aq} + q\alpha$$

と書くことができる． さらに，

$$\sum_{a=1}^{p-1} \left(\frac{a}{p}\right) \zeta_p^{aq} = \sum_{a=1}^{p-1} \left(\frac{aq^2}{p}\right) \zeta_p^{aq} = \left(\frac{q}{p}\right) \sum_{a=1}^{p-1} \left(\frac{aq}{p}\right) \zeta_p^{aq} = \left(\frac{q}{p}\right) \tau_p$$

と変形できるから，

$$\tau_p \left(\tau_p^{q-1} - \left(\frac{q}{p}\right)\right) = q\alpha.$$

両辺に τ_p をかければ，定理 12.2 より

$$\pm p \left(\tau_p^{q-1} - \left(\frac{q}{p}\right)\right) = q\alpha\tau_p$$

を得る． 左辺は整数だから $\alpha\tau_p \in \boldsymbol{Q}$ であるが，一方で $\alpha\tau_p \in R$ だから補題 12.7 より $\alpha\tau_p \in \boldsymbol{Z}$． よって合同式

$$\pm p \left(\tau_p^{q-1} - \left(\frac{q}{p}\right)\right) \equiv 0 \pmod q$$

が成り立つが，p, q が相異なる素数なので示したい合同式が得られる． □

12.4　相互法則の証明

定理 12.6，定理 12.2，およびオイラーの規準を順に用いて

$$\left(\frac{q}{p}\right) \equiv \tau_p^{q-1} = \left(\tau_p^2\right)^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} p^{\frac{q-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right) \pmod q$$

を得るが，両端の辺は ± 1 だから等しくなければならず，相互法則の証明が完了する．

☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆
☆　これで，この講義は終わりです　☆
☆　最後まで付き合ってくれた諸君に感謝の言葉を捧げます　☆
☆ ありがとう，Thank you，Merci，Danke schön，Grazie，Gracias，Obrigado ☆
☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆☆

第13章　補遺

13.1　孫子算経

【孫子算経】は，中国の南北朝時代 (439–589)) の成立と推定される著者不詳の算術書であり，その一題として，第 6 章の例 6.6 と同じ内容が書かれている． これが，定理 6.5 が**中国の剰余定理**と呼ばれる理由である．

該当部分の原文は次の通り（分かりやすいように句読点をほどこしてある）．

> 今有物、不知其数。三・三数之、剰二。五・五数之、剰三。七・七数之、剰二。問物幾何？
> 答曰：二十三。
> 術曰：『三・三数之、剰二』、置一百四十。『五・五数之、剰三』、置六十三。『七・七数之、剰二』、置三十。并之、得二百三十三。以二百一十減之、即得。凡、三・三数之、剰一、則置七十。五・五数之、剰一、則置二十一。七・七数之、剰一、則置十五。一百六以上、以一百五減之、即得。

Wikipedia〈中国の剰余定理〉では，日本語によって次のように解説されている．

> 今物が有るが、その数はわからない。三つずつにして物を数えると、二余る。五で割ると、三余る。七で割ると、二余る。物はいくつあるか？
> 答え：二十三。
> 解法：三で割ると、二余る数として、百四十と置く。五で割ると、三余る数として、六十三と置く。七で割ると、二余る数として、三十と置く。これらを足し合わせて、二百三十三を得る。これから二百十を引いて、答えを得る。一般に、三つずつにして物を数え、一余ると、その度に七十と置く。五で割った余りに二十一をかける。七で割った余りに十五をかける。百六以上ならば、百五を引くことで、答えを得る。

第 6 章の例 6.6 と比べると，**解 2** と同じ趣旨の解答であることがわかる． さらに，最後の「一般に…」以降は，

$$35u_1 \equiv 1 \pmod 3, \qquad 21u_2 \equiv 1 \pmod 5, \qquad 15u_3 \equiv 1 \pmod 7$$

の解 $(u_1, u_2, u_3) = (2, 1, 1)$ から得られる組 $(35u_1, 21u_2, 15u_3) = (70, 21, 15)$ を用いて

$$x \equiv a_1 \pmod 3, \qquad x \equiv a_2 \pmod 5, \qquad x \equiv a_3 \pmod 7$$

の解 $x = 70a_1 + 21a_2 + 15a_3$ が一般的に得られることを説明している．

13.2 命題 8.5 の証明

m を素因数分解して $m = p_1^{e_1} \cdots p_r^{e_r}$ (p_i は相異る素数，$e_i \geq 1$) と表せば，定理 8.6 の公式より

$$\frac{\varphi(m)}{m} = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

ここで $p_1 < p_2 < \cdots < p_r$ であるとしてよいが，このとき（ずいぶん荒っぽい評価だけれども） $2 \leq p_1,\ 3 \leq p_2,\ 4 \leq p_3, \ldots,\ r+1 \leq p_r$ が成り立つ． よって，

$$\begin{aligned}\frac{\varphi(m)}{m} &\geq \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{4}\right)\cdots\left(1 - \frac{1}{r+1}\right) \\ &= \frac{1}{2}\cdot\frac{2}{3}\cdot\frac{3}{4}\cdots\frac{r}{r+1} = \frac{1}{r+1}.\end{aligned}$$

一方，$m = p_1^{e_1} \cdots p_r^{e_r} \geq 2^{e_1+\cdots+e_r} \geq 2^r$（これも荒っぽいよね）より $\log_2 m \geq r$ だから，

$$\frac{\varphi(m)}{m} \geq \frac{1}{\log_2 m + 1}$$

すなわち，左側の不等式が示された． 右側の不等式 $\varphi(m) \leq m - 1$ は φ の定義から明らかである． □

13.3 補題 12.7 の証明

簡単のため，ζ_p を ζ と略記する． 整数係数多項式 $f(x)$ によって $f(\zeta)$ で表される複素数全体の集合が R であった． ところで，$\zeta^p = 1$ なので，$f(x)$ の次数は p 未満であるとしてよい． すなわち，

$$R = \left\{\, a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1} \;\middle|\; a_0, a_1, \ldots, a_{p-1} \in \boldsymbol{Z} \,\right\}.$$

(実は，$p-1$ 次未満にできるが，以下の議論には影響ないのでこのまま証明を続ける．)
さて，$\alpha \in R \cap \boldsymbol{Q}$ を任意にとる． このとき，$\alpha\zeta^i \in R$ だから

$$\alpha\zeta^i = \sum_{j=0}^{p-1} a_{ij}\zeta^j \qquad (i = 0, 1, \ldots, p-1)$$

をみたす $a_{ij} \in \boldsymbol{Z}$ がとれる． p 次正方行列 $A = (a_{ij})$ を考えれば，上式は

$$\alpha \begin{pmatrix} 1 \\ \zeta \\ \zeta^2 \\ \vdots \\ \zeta^{p-1} \end{pmatrix} = A \begin{pmatrix} 1 \\ \zeta \\ \zeta^2 \\ \vdots \\ \zeta^{p-1} \end{pmatrix}$$

と書き換えられ，これは α が A の固有値であることを示している． よって，A の固有多項式を $g(x)$ とすれば $g(\alpha)=0$ である． A の成分はすべて整数であるから，

$$g(x)=x^p+c_{p-1}x^{p-1}+\cdots+c_1x+c_0 \qquad (c_i\in \boldsymbol{Z})$$

の形をしている． いま，$\alpha\in \boldsymbol{Q}$ でもあったから，これを既約分数

$$\alpha=\frac{s}{t} \qquad (s,t\in \boldsymbol{Z}:\text{互いに素，かつ } t\geq 1)$$

で表せば，$g(\alpha)=0$ より

$$\frac{s^p}{t^p}+c_{p-1}\frac{s^{p-1}}{t^{p-1}}+\cdots+c_1\frac{s}{t}+c_0=0,$$

$$\therefore \quad s^p+c_{p-1}s^{p-1}t+\cdots+c_1st^{p-1}+c_0t^p=0.$$

よって，$s^p\equiv 0 \pmod{t}$ となるから，もし $t\neq 1$ ならば，s,t が互いに素であることに反する． したがって $t=1$ であり，$\alpha=s\in \boldsymbol{Z}$． α は $R\cap \boldsymbol{Q}$ から任意にとった元なので，$R\cap \boldsymbol{Q}\subset \boldsymbol{Z}$ が得られたことになる． 逆の包含関係は明らかなので，補題 12.7 が証明された． □

索 引