初等整数論

青空学園数学科

2008 年 11 月 19 日

はじめに

整数は人間にとって大変身近なものであり，整数の性質を調べる整数論は高校数学のなかでも大切な分野です．しかし，現在の高校の教科書ではまったく軽視されています．高校生向けの参考書にいちおうは載っているのですが，どうしても入試問題に引きずられて記述されるため，行きあたりばったりで体系的でない切れ切れの知識が積みあげられて，かえってわかりにくくなっているのが現状です．

これはたいへん残念なことです．整数論は数学のおもしろさ，美しさが実感できるうえに，体系立てて学ぶことができ，そうすれば「少ない原理・自由な応用」という数学の大切な精神を身につけることができます．さらにその結果，入試問題も見通しよく解くことができます．

青空学園の『初等整数論』は，高校生から大学初年級の諸君が体系的に初等整数論の基本を学ぶ教科書です．おおよそ『初等整数論講義』(高木貞治, 共立出版) の第 1 章，第 2 章に対応しています．現代的な抽象代数学を用いない有理整数の古典理論を集大成するものです．

演習問題もできるだけ入試問題からとって，再構成しています．大学入試問題のなかで整数を取りあげいてる意味のある問題を紹介し，関連して学べるようにします．

「定理」一般的な結果で,「演習問題」は入試問題やその他一般性のある重要な問題です．これらは通し番号になっています．演習問題の解答は巻末にまとめました．

「練習問題」はその内容を理解するのに適した問題です．これは節毎に【節番号-番号】の形で番号をつけています．

■ は証明など論述文の終わりを意味しています．

高校生の皆さんがとおして勉強するのは大変です．次のようにするとよいでしょう．●のところを勉強してください．次にできれば○を，前半だけでも読む．そして各節末の「演習問題」に取り組む．これはほぼすべてが最近の入試問題です．●や○以外のところの演習問題もやってみてください．残ったところは大学生になってからぜひ読んでほしいです．

1. 整数の除法● 2. 最大公約数と最小公倍数● 3. 一次不定方程式● 4. 素数● 5. 合同式○ 6. オイラーの関数 ○ 7. 1 の n 乗根○ 8. フェルマの小定理○ 9. 原始根と指数 10. 平方剰余の相互法則 11. ガウス整数 12. ペル方程式の解の構造● 13. 実数の近似○ 14. 二次行列と実数の連分数展開 15. 数の幾何○ 16. 二次無理数の連分数展開 17. ペル方程式の解の構成

目 次

1　整数の除法

1.1　整数の除法

整数の系統だった勉強をはじめよう．第 1 節は除法，つまり割り算だ．割り算などと簡単に考えてはならない．割り算がただ一通りにでできる，このことが整数の論証の土台になっている．つまり，割り算の可能性と一意性，これが「除法の原理」であるが，整数の多くの事実が成り立つ根拠はここにある．

この節では自然数の性質に基礎づけて,「除法の原理」を証明しよう．そのために，証明の根拠となる自然数の性質についてまとめておく．整数の性質は土台としての自然数の性質から証明される．

自然数とは何か．人間がはじめて身につける数が自然数である．子供ははじめ，三つのリンゴと，3 枚の皿，の「3」が同じことであることを知らない．あくまで「三つのリンゴ」と「3 枚の皿」だ．それが同じ「3」であることを知ることができるのは，2〜3 歳のころではないかと思う．これが自然数の始まりだ．

が，あらためて自然数とは何か，それはどんなものか．われわれは自然数とは【1 からはじめて,「1 たす」という操作で作られる数の集合】と定義しよう．この集合を N と記す．すると自然数は次のような性質をもつ．

(1) 自然数の部分集合には最小の要素が存在する．

(2) 自然数の部分集合 A で「 $1 \in A$ かつ $x \in A$ なら $x+1 \in A$ 」が成り立つなら， A は N 自身である (数学的帰納法の原理).

(3) $a < b$ である任意の自然数に対し， $b < na$ となる自然数 n が存在する．

この自然数の集合は，演算として加法が定義され，さらに積が定義される．ところが，任意の N の要素 x に対して $x+e=x$ となる e は N にはない．さらに x に対して $x+y=e$ となる y もまた N には存在しない．これらの要素を含むように拡大されたものが整数である．このとき e を 0 と，また $x+y=0$ となる y を $-x$ と記す.「整数」とは自然数にこれらを付け加えた次の集合 Z のことをいう．

$$Z = \{\cdots,\ -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ \cdots\}$$

整数の和・差・積は再び Z に属する，つまり整数である．これを「整数の集合は加法・減法・乗法の演算で閉じている」という．

整数の集合でもう一つの演算「除法」の定義は次の定義による．

定理 1 (除法の原理)

a を任意の整数, b は $b > 0$ の整数とする．このとき，

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

となる整数 $q,\ r$ がただ 1 組，存在する．

証明　整数 a に対して

$$qb \leqq a < (q+1)b$$

となる整数 q が存在する．それを示すために十分小さい整数 i で $bi < a$ となるものを一つとる．自然数の構成から $|a| < bi$ となる自然数 i が存在する．このとき $b(-i) < a < bi$ なので． a の正

負にかかわらずこのような i は存在する．i が負のときは自然数の集合 N と集合 $\{i,\ i+1,\ \cdots,\ 0\}$ の和集合を M ．i が正なら N 自身を M とする．

M の部分集合

$$\{\ t \mid a < (t+1)b, t \in M\ \}$$

を考える．この集合は自然数と有限個の集合の和集合 M の部分集合であるから，この集合の中に最小のものがある．それを q とする． $q-1$ はもはやこの集合に属さない．すなわち $a < (q-1+1)b$ を満たさない．つまり， $qb \leqq a$ が成立する．そこで $r = a - qb$ とおく． $qb \leqq a < (q+1)b$ より $0 \leqq r < b$ で

$$a = qb + r$$

である．つぎに，もしこのような q, r が二通りあったとし，それを q_1, r_1 と q_2, r_2 とする．$q_1 = q_2$ なら $r_1 = r_2$ である．$q_1 > q_2$ とする．つまり, $q_1 \geqq q_2 + 1$ とする．このとき，

$$a \geqq q_1 b \geqq (q_2+1)b = q_2 b + b > q_2 b + r = a$$

となり，矛盾である． $q_1 < q_2$ のときも同様．よって $q_1 = q_2$ であり，その結果 $r_1 = r_2$ である．
■

$r = 0$ であるときが a が b で割り切れる場合である．$[x]$ で x を超えない最大の整数を表すと，$q = \left[\dfrac{a}{b}\right]$ である．

除法の原理が成り立つことが，様々の整数問題の証明の根幹になる．整数 $a,\ b$ に対し， $bx = a$ となる x ，つまり商 $\dfrac{a}{b}$ は一般に Z の要素ではない．商 $\dfrac{a}{b}$ が Z に属するとき， a は b で割り切れるという．このことを $b|a$ と書く．

この商を整数 q とすると，

$$a = bq \quad (b \neq 0)$$

となるので，a は b の倍数, b は a の約数である，という．

初等整数論の世界，つまり集合 Z の世界では除法の原理が土台になる．代数的整数といわれる世界では，この除法の原理は成り立たない．そこでは新たな考え方が必要になる．われわれの整数を有理整数という．有理整数でない整数は後に「ガウス整数」で端緒を紹介するが『整数論入門』は基本的に有理整数の世界の探求である．

この後，記号 $N,\ Z,\ Q,\ R,\ C$ は特に断らなければそれぞれ，自然数，整数，有理数，実数，複素数の集合を表す．

例 1.1　$b = 12$ とする．

- $a = 50 \div 50 = 4 \cdot 12 + 2$ ． $q = 4 = \left[\dfrac{50}{12}\right]$ ． $r = 2$
- $a = -50 \div -50 = (-5) \cdot 12 + 10$ ． $q = -5 = \left[\dfrac{-50}{12}\right]$ ． $r = 10$
- $a = -5 \div -5 = (-1) \cdot 12 + 7$ ． $q = -1 = \left[\dfrac{-5}{12}\right]$ ． $r = 7$

1.2 整式の除法

ところでこの定理をよくみると，同様なことが整式でも成り立つことに気づく．

整式は，それを x の整式とみなしたとき，つぎの基本性質をもつ．ここで $\deg f(x)$ は整式 $f(x)$ の次数を表す．

定理 2 (整式の除法の原理)

整式 $f(x),\ g(x)(\deg g(x) \geqq 1)$ とする．このとき，

$$f(x) \ = \ g(x) \cdot q(x) \ + \ r(x),\ \deg r(x) < \deg g(x)$$

となる整式 $q(x),\ r(x)$ がただ 1 組，存在する．

証明 $\deg f(x) < \deg g(x)$ ならば $q(x) = 0,\ r(x) = f(x)$ でよい．

$\deg f(x) \geqq \deg g(x)$ のとき, $\deg f(x) = n,\ \deg g(x) = m$ とする． $f(x)$ と $g(x)$ の n, m 次の項をそれぞれ $a_0x^n,\ bx^m$ とする．

$$f_1(x) = f(x) - \frac{a_0}{b}x^{n-m}g(x)$$

と定めれば, $\deg f_1(x) < \deg f(x)$ である．$f_1(x)$ と $g(x)$ について同様の操作を繰り返す． $f_k(x)$ の次数が n_k で最高次数の係数が a_k とすれば

$$f_{k+1}(x) = f_k(x) - \frac{a_k}{b}x^{n_k-m}g(x)$$

l 回の操作の後, $\deg f_l(x) < \deg g(x)$ となったとき，

$$f_l(x) = r(x),\ q(x) = \sum_{k=0}^{l-1}\frac{a_k}{b}x^{n_k-m}$$

とする．この $f_1(x)$ に対し

$$\begin{aligned} f(x) &= g(x)\frac{a_0}{b}x^{n-m} + f_1(x) \\ &= g(x)\frac{a_0}{b}x^{n-m} + g(x)\frac{a_1}{b}x^{n_1-m} + f_2(x) \\ &\cdots \\ &= g(x)q(x) + f_l(x) \end{aligned}$$

となるので，定理の等式を満たす．

これが 1 組しかないことを示す．2 組あったとする．

$$\begin{aligned} f(x) &= g(x)\cdot q_1(x) \ + \ r_1(x) \\ &= g(x)\cdot q_2(x) \ + \ r_2(x) \end{aligned}$$

すると，

$$g(x)\cdot\{q_1(x) - q_2(x)\} \ = \ r_2(x) - r_1(x) \tag{1}$$

となる．ここでもし $q_1(x) - q_2(x) \neq 0$ なら $\deg(r_2(x) - r_1(x)) \geqq \deg g(x)$ である．

ところが一方，$\deg r_1(x) \ < \ \deg g(x),\ \deg r_2(x) \ < \ \deg g(x)$ だから，$\deg(r_2(x) - r_1(x)) < \deg g(x)$．これは矛盾．

ゆえに等式 (1) が成立するのは，$q_1(x) \ = \ q_2(x)$ のときのみである．このとき, $r_1(x) \ = \ r_2(x)$ となる． ■

1.3 演習問題

演習問題 1 (解答 1) ［96 大教大］

(1) $F(x) = 2x^3 + 5x^2 - 3x + 7$, $G(x) = x - 3$ とする．このとき，$F(x) = G(x)Q(x) + r$ を満たす x の整式 $Q(x)$ と実数 r を求めよ．

(2) $F(x)$ を x の 1 次以上の整式， $G(x) = x - a$ ，ただし a は実数とする．このとき，

(i) $F(x) = G(x)Q_1(x) + F_1(x)$ を満たす x の整式 $Q_1(x)$, $F_1(x)$, ただし $F_1(x)$ の次数は $F(x)$ の次数より小さい，が存在することを示せ．

(ii) $F(x) = G(x)Q(x) + r$ を満たす x の整式 $Q(x)$ と実数 r が存在することを $F(x)$ の次数に関する数学的帰納法を使って証明せよ．

(3) $F(x)$ を x の整式とする．実数 a に対して， $F(a) = 0$ となるなら $F(x) = (x - a)Q(x)$ を満たす x の整式 $Q(x)$ が存在することを示せ．

(4) $F(x)$ を x の n 次式とする．このとき，方程式 $F(x) = 0$ の相異なる実数解は n 個以下であることを示せ．

2　最大公約数と最小公倍数

2.1　最大公約数と最小公倍数

最大公約数と最小公倍数，小学校や中学校で習ったままである．そのときにはしっかりとした証明もなかった．24，180，42　の最大公約数を求めるのに

$$\begin{array}{r|lll} 2 & 24 & 180 & 42 \\ \hline 3 & 12 & 90 & 21 \\ \hline & 4 & 30 & 7 \end{array}$$

$$\therefore \quad 24,\ 180,\ 42 \text{ の最大公約数は } 2 \times 3 = 6$$

と習っただろう．しかしこのときに，もし素因数が 37 等ととか大きかったら簡単には見つけられない，と思った人はいないだろうか．いつでも最大公約数を見つけることはできるのだろうか．

実は常に最大公約数を求める方法がある．それを学ぶことがこの節の内容である．

二つ以上の整数 $a,\ b,\ c,\ \cdots$ に共通な倍数をそれらの整数の公倍数という．0 は常に公倍数である．それを除けば公倍数の中に正で最小のものがある．それを最小公倍数 (least common multiple 略して L.C.M.) という．二つ以上の整数 $a,\ b,\ c,\ \cdots$ に共通な約数をそれらの整数の公約数という．1 は常に公約数である．公約数の中に最大のものがある．それを最大公約数 (greatest common measure 略して G.C.M.) という．

定理 3

(1) 二つ以上の整数の公倍数は，最小公倍数の倍数である．

(2) 二つ以上の整数の公約数は，最大公約数の約数である．

(3) $a,\ b$ の最小公倍数を l ，最大公約数を d とすれば $ab = dl$.

(4) $a,\ b$ が互いに素で，他の整数 c と b との積 bc が a で割りきれるなら，実は c が a で割りきれる．

証明

(1) $a,\ b,\ c,\ \cdots$ の最小公倍数を l とし, m を任意の公倍数とする．m を l で割った商を q ，余りを r とすると

$$m = ql + r, \quad 0 \leqq r < l$$

となる．l も m も a の倍数であるから $l = al',\ m = am'$ とおくと

$$r = m - ql = a(m' - ql')$$

より, r は a の倍数である．同様に $b,\ c,\ \cdots$ の倍数でもあり，r は $a,\ b,\ c,\ \cdots$ の公倍数となる．ところが l は正で最小の公倍数であったから，もし r が 0 でないとすると, l より小さい正の公倍数があることになり, l の最小性に反する．

$$\therefore \quad r = 0$$

つまり m は l の倍数である．

(2) $a,\ b,\ c,\ \cdots$ の最大公約数を d とし, m を任意の公約数とする．l を d と m の最小公倍数とする． a は m の倍数であり，d の倍数である．つまり m と d の公倍数であるから (1) より a は l の倍数である．同様に $b,\ c,\ \cdots$ も l の倍数である．つまり l は $a,\ b,\ c,\ \cdots$ の公約数である． d が最大の公約数なので，

$$l \leqq d$$

一方, l は d と m の最小公倍数なので $d \leqq l$

$$\therefore \quad l = d$$

d と m の最小公倍数 l が d に一致したので d は m の倍数，つまり任意の公約数 m は最大公約数 d の約数である．

(3) l は $a,\ b$ の最小公倍数であるから

$$l = ab' = ba'$$

とおける．ab は $a,\ b$ の公倍数だから (1) から ab は l の倍数である．

$$ab = ml$$

とする．よって

$$ab = ml = ma'b, \qquad ab = ml = mab'$$

$$\therefore \quad a = ma',\ b = mb'$$

つまり m は $a,\ b$ の公約数であり (2) より $d = me$ とおける．

一方 d は $a,\ b$ の最大公約数なので $a = da'',\ b = db''$ とおける．よって

$$a = da'' = mea'' = ma',\ b = db'' = meb'' = mb'$$

$$\therefore \quad a' = ea'',\ b' = eb''$$

よって

$$l = ab' = aeb'',\ l = a'b = ea''b$$

$$\therefore \quad \frac{l}{e} = ab'' = a''b$$

ところがこれは $\dfrac{l}{e}$ が $a,\ b$ の最小公倍数であることを示している．l が最小公倍数なのでその最小性により $e = 1$ ．

$$\therefore \quad m = d \quad \text{つまり} \quad ab = dl$$

(4) $a,\ b$ の最大公約数が 1 なので $a,\ b$ の最小公倍数は ab である．仮定から bc は a の倍数であり，したがって a と b の公倍数である．よって bc は ab の倍数であり，

$$\frac{bc}{ab} = \frac{c}{a} \quad \text{が整数}$$

つまり c は a の倍数である． ■

この定理の証明において，前節の「除法の原理」が基本定理として用いられてることがわかる．日頃当然のように論証で使っていることが,「除法の原理」を基礎に厳密に示される．

整数 $a,\ b,\ c,\ \cdots$ の最大公約数を，座標と混同する恐れのないときは $(a,\ b,\ c,\ \cdots)$ と書く．

整数 $a,\ b,\ c,\ \cdots$ が ± 1 以外に公約数をもたないことを簡単に「公約数をもたない」という．この場合，$(a,\ b,\ c,\ \cdots) = 1$ ．特に二つの整数 $a,\ b$ が公約数をもたないとき，つまり $(a,\ b) = 1$ のとき，$a,\ b$ は**互いに素**であるという．

2.2 ユークリッドの互除法

ここで，はじめに述べた最大公約数を求める一般的な方法をまとめよう．

定理 4 (ユークリッドの互除法)

(1) $a > b > 0$ を整数とし, a を b で割った余りを r とする．このとき

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

が成り立つ．

(2) 数列 $\{r_n\}$ を次のように定める．

$$\begin{cases} r_1 = a,\ r_2 = b \\ n \geqq 2 \text{ のとき} \\ \quad r_n > 0 \text{ なら}, r_{n+1} = r_{n-1} \text{を} r_n \text{で割った余り} \\ \quad r_n = 0 \text{ なら}, r_{n+1} = 0 \end{cases}$$

このときある番号 N で $r_N \neq 0$ で $r_{N+1} = 0$ となるものがあり，このとき

$$r_N = (a,\ b)$$

が成り立つ．

証明

(1) $(a,\ b) = d_1$ とすると $a = a'd_1,\ b = b'd_1$ とおける．

$$r = a'd_1 - b'd_1 q = d_1(a' - b'q)$$

これより r も d_1 で割れる．よって,d_1 は b と r の公約数なので, $d_1 \leqq (b,\ r) = d_2$．次に $(b,\ r) = d_2$ とすると, $b = b'd_2,\ r = r'd_2$ とおける．

$$a = b'd_2 q + r'd_2 = d_2(b'q + r')$$

より同様に $d_2 \leqq (a,\ b) = d_1$．よって $d_1 = d_2$ ，つまり

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

(2) 除法の原理から $r_k > 0$ なら

$$r_1 = a > r_2 = b > r_3 > \cdots > r_k > r_{k+1} \geqq r_{k+2} \geqq \cdots \geqq 0$$

自然数の単調減少列なのである番号 N で

$$r_N > 0 \text{ かつ } r_{N+1} = 0$$

となる．このとき r_{N-1} は r_N の倍数になる．よって (1) より

$$(a,\, b) = (b,\, r_3) = \cdots = (r_{N-1},\, r_N) = r_N$$

■

これが最大公約数を求める一般的な方法で，**「ユークリッドの互除法」** といわれる．このように「必ずできる一般的方法」をアルゴリズムという．ユークリッドの互除法はアルゴリズムの基本例である．

三つ以上の整数 $a,\, b,\, c,\, \cdots$ の最大公約数もこれを応用して求めることができる．a が $a,\, b,\, c,\, \cdots$ のなかの最小の数とする． a で他の数を割った余りを $b',\, c',\, \cdots$ とする．すると上の定理と同様に

$$(a,\, b,\, c,\, \cdots) = (a,\, b',\, c',\, \cdots)$$

この操作を繰り返すと余りのなかに 0 が現れる．それを取り除いてさらに同様の操作を繰り返す．ついにはただひとつの数が残る．それが $a,\, b,\, c,\, \cdots$ の最大公約数である．

例 2.1　$(6188, 4709)$ を求めよう．

順次割り算を行うことにより次の系列を得る．

$$\begin{aligned}(6188,\, 4709) &= (4709,\, 1479)\\ &= (1479,\, 272)\\ &= (272,\, 119)\\ &= (119,\, 34)\\ &= (34,\, 17) = 17\end{aligned}$$

例 2.2

$$(629, 391, 255) = (119, 136, 255) = (119, 17, 17) = 17$$

練習問題 2.1（解答 1）　n を整数とするとき，次のことを示せ．

(1) $n(n+1)(n+2)(n+3)$ は 24 の倍数である．

(2) n が奇数ならば，$n^3 - n$ は 24 の倍数である．

(3) n が 2 でも 3 でも割り切れないならば，$n^2 - 1$ は 24 の倍数である．

(4) $n(n+1)(2n+1)$ は 6 の倍数である．

(5) $n^3 - 3n^2 + 8n$ は 6 の倍数である．

練習問題 2.2（解答 2）　a, b は互いに素な正の整数とするとき，次の問に答えよ．

(1) 分数 $\dfrac{7a+2b}{3a+b}$ は既約分数である．

(2) $ps-qr=1$ なる正の整数 p,q,r,s に対して，分数 $\dfrac{pa+qb}{ra+sb}$ は既約分数である．

(3) $\dfrac{11n-42}{3n-13}$ が既約分数にならないような自然数 n を，小さい方から順に三つ求めよ．

2.3 演習問題

演習問題 2 (解答 2) ［98 お茶の水］

正の数 $k,\ l$ $(k \geqq l)$ に対して 数列 $\{a_n\},\ \{b_n\}$ を次のように定義する．

$a_1=k,\ b_1=l$

$n \geqq 1$ について

$$a_{n+1}=\begin{cases} b_n & (b_n \neq 0 \text{ のとき}) \\ a_n & (b_n=0 \text{ のとき}) \end{cases},\ b_{n+1}=\begin{cases} a_n \text{を } b_n \text{で割った余り} & (b_n \neq 0 \text{ のとき}) \\ b_n & (b_n=0 \text{ のとき}) \end{cases}$$

(1) $k=1998,\ l=185$ について，$\{a_n\},\ \{b_n\}$ をそれぞれ第 5 項まで計算せよ．

(2) 任意の $k,\ l,\ n$ について $b_n \geqq b_{n+1}$ (等号は $b_n=0$ のときに限る) を示せ．

(3) 任意の $k,\ l$ について $b_n=0$ となる n が存在することを示せ．

(4) $b_n=0$ となる n について a_n が k と l の最大公約数になっていることを示せ．

演習問題 3 (解答 3) ［阪大 91 年理後期］

条件 $a \geqq b$ を満たす正の整数 $a,\ b$ から数列 $\{r_n\}$ を $r_1=a,\ r_2=b,$

$$n \geqq 3 \text{ に対して, } r_n=\begin{cases} r_{n-2} \text{を } r_{n-1} \text{で割った余り} & (\ r_{n-1}>0 \text{ のとき}) \\ 0 & (\ r_{n-1}=0 \text{ のとき}) \end{cases}$$

によって定める．

また，数列 $\{f_n\}$ を $f_1=0,\ f_2=1,\ f_n=f_{n-1}+f_{n-2}(n \geqq 3 \text{ のとき})$ によって定める．このとき，以下のことがらを示せ．

(1) $r_N>0,\ r_{N+1}=0$ となる整数 N が存在する．以下，N はこの整数を表す．

(2) $r_{N+2-k} \geqq f_k\ (k=1,2,\cdots,N+1)$

(3) $f_{n+1} \geqq \left(\dfrac{3}{2}\right)^{n-2}\quad (n=1,2,\cdots)$

(4) $N \leqq 2+\log_{\frac{3}{2}} a$

3　一次不定方程式

3.1　一次不定方程式の解の存在

今回は一次不定方程式の整数解を問題にする．一次不定方程式の整数解とは何か．整数 $a,\ b,\ c,\ k$ を係数とする方程式

$$ax + by + cz = k$$

を考える．未知数が 2 個以上あるので不定方程式と言われる．この一次不定方程式を満たす整数の組 $(x_0,\ y_0,\ z_0)$ を一次不定方程式の整数解という．

このような方程式を「ディオファントスの方程式」ともいう．ディオファントス (Diophantos 前 3 世紀ごろ) はアレキサンドリアにいたとされるギリシア時代の数学者．幾何学的であったそれまでの数学に代数学を導入, 著書のなかで二次方程式や不定方程式を解いた．大学入試で頻出なのは

$$2x + 13y = 1$$

のような 2 変数の場合である．

まず 2 変数の場合に調べ，それを一般化するという方向で考えよう．2 変数の不定方程式では次のことが入試問題としてよく出題される．

(1) $ax + by = 1$ は a と b が互いに素なら整数解をもつ．

(2) 解の一般形がかける．

(3) つねに解を実際に構成することができる．

これが大切な基本事項である．

本節ではこれをふり返り，さらに一般的に整数係数の一次不定方程式

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = k$$

を考える．

まず解が存在するための必要十分条件を確定しよう．

2 変数の場合，一次不定方程式 $ax + by = 1$ は a と b が互いに素なら整数解をもつが，この事実はどのように示されるのか．$a > b \geqq 0$ として良い．このとき 3 通りの証明法があった．

- **b についての数学的帰納法**

  $b = 0$ のとき, $(a,\ b) = 1$ より $a = 1$．ゆえに $1 \cdot x + 0 \cdot y = 1$ であるから，解 $(1,\ 0)$ をもつ．

  $0 \leqq k < b$ の k と $a > k$ で k と互いに素な a に対して $ax + ky = 1$ が解をもつとする．このとき $ax + by = 1$ $(a > b \geqq 0)$ が解をもつことを示す．

  $$a = bq + r \quad (0 \leqq r < b)$$

  とする．このとき,

  $$ax + by = (bq + r)x + by = b(qx + y) + rx$$

  a と b が互いに素なので b と r も互いに素である．ゆえに，仮定より $bX + rY = 1$ は解 $(X_0,\ Y_0)$ をもつ．この解に対して $\begin{cases} qx_0 + y_0 = X_0 \\ x_0 = Y_0 \end{cases}$ を解く．$\begin{cases} x_0 = Y_0 \\ y_0 = X_0 - qY_0 \end{cases}$ となる．

この $x_0,\ y_0$ は $ax+by=1\ (a>b\geqq 0)$ の解となっている．実際

$$\begin{aligned} ax_0+by_0 &= aY_0+bX_0-bqY_0 \\ &= bX_0+rY_0=1 \end{aligned}$$

つまり，b のときも成立する．

よって, 数学的帰納法により, すべての $b\ (b\geqq 0)$ と, $a>b$ なる a に対し $ax+by=1$ は解をもつ. ■

- **受験数学で良く用いられる方法**

$i=0,\cdots,b-1$ に対して ai を b で割った余りを r_i とする．

$$A=\{r_0,\cdots,r_{b-1}\},\quad B=\{0,\cdots,b-1\}$$

とおく. 各 r_i は 0 から $b-1$ のどれかであるから, $A\subset B$.

次に $B\subset A$ を示す. A の要素 r_i と r_j が $r_i=r_j$ とする. つまり

$$\begin{aligned} ai &= bq_i+r_i \\ aj &= bq_j+r_j \end{aligned}$$

より

$$a(i-j)=b(q_i-q_j)$$

よって a と b が互いに素なので $i-j$ が b の倍数である.

$$0-(b-1)\leqq i-j\leqq b-1-0$$

より，$i-j=0$ 以外にない.

対偶をとると,

$$i\neq j \quad\Longrightarrow\quad r_i\neq r_j$$

したがって, A の要素はすべて異なる.

よって $n(A)=n(B)$ かつ $A\subset B$ より,

$$A=B$$

よって特に $1\in A$ である. つまり $ai=bq_i+1$ となる i がある. このとき $ai-bq_i=1$ なので, $(x,\,y)=(i,\,-q_i)$ が $ax+by=1$ の解である. ■

注意 3.1　これは解の作り方も教えている．例えば $37x+13y=1$ の一組の解を見つけるためには次のようにすればよい.

$u=1,\ 2,\ \ldots,\ 12$ に対して $37u$ を 13 で割った余りを書いていく.

$$11,\ 9,\ 7,\ \cdots$$

かならず 1 が出てくる．実際

$$37\times 6=13\times 17+1 \quad\Rightarrow\quad 37(6)+13(-17)=1$$

ゆえに $(x,\ y)=(6,\ -17)$ が解である.

- **自然数の基本性質を用いる証明**

  $A = \{\, ax + by \mid x,\, y : \text{整数} \,\}$ とする．A の要素で正の最小のものを d とする．

$$d = ax_0 + by_0$$

  $a,\ b$ をそれぞれ $d\ (>0)$ で割る．

$$\begin{aligned} a &= dq_1 + r_1 \quad 0 \leqq r_1 < d \\ b &= dq_2 + r_2 \quad 0 \leqq r_2 < d \end{aligned}$$

  ここで

$$\begin{aligned} r_1 &= a - dq_1 = a - (x_0 + by_0)q_1 \\ &= a(1 - q_1x_0) + b(-q_1y_0) \end{aligned}$$

  よって r_1 も A の要素となる．d が A の要素のなかで正で最小のものなので $r_1 = 0$ でなければならない．同じく $r_2 = 0$ でも成立する．

  つまり d は a と b の公約数である．ところが $(a,\, b) = 1$ より $d = 1$ である．つまり $1 = ax_0 + by_0$ となり $ax + by = 1$ には解 $(x_0,\ y_0)$ が存在した． ■

この三つの証明のなかで，未知数が 3 個以上ある場合に拡張しうるのはどれか．

数学的帰納法は $b = 0$ のときが未知数がひとつ減るだけでしかない．したがって未知数に関する帰納法と b に関する帰納法を組み合わせなければならない．第二の証明はそのままでは未知数が増えたら使えない．第三の証明はどうだろうか．次のようにそのまま拡張される．

定理 5 (一次不定方程式の解の存在定理)

整数 $a_1, a_2,\ \cdots,\ a_n,\ k$ を係数とする一次不定方程式

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = k \tag{2}$$

が解をもつための必要十分条件は，整数 k が整数 $a_1,\, a_2,\, \cdots,\, a_n$ の最大公約数 $d = (a_1,\, a_2,\, \cdots,\, a_n)$ で割り切れることである．

証明　必要条件であることは明らかである．つまり (2) を満たす整数解があればその解を代入したとき (2) の左辺は各 a_i が d の倍数なので d の倍数である．つまり k は d の倍数である．

十分条件であることを示す．そのために集合

$$J = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n \,|\, x_1,\ x_2, \cdots,\ x_n\text{は整数}\}$$

を考える．

J に含まれる正で最小の整数を e とする．

$$e = \sum_{k=1}^{n} a_k l_k$$

となる $l_k\ (k = 1,\ 2,\ 3,\ \cdots,\ n)$ がある．

$a_1,\ a_2,\ \cdots a_n$ をそれぞれ $e>0$ で割る．

$$\begin{aligned} a_1 &= eq_1 + r_1 \quad 0 \leqq r_1 < e \\ a_2 &= eq_2 + r_2 \quad 0 \leqq r_2 < e \\ &\cdots \\ a_n &= eq_n + r_n \quad 0 \leqq r_n < e \end{aligned}$$

ここで各 j $(j=1,\ 2,\ 3,\ \cdots,\ n)$ に対して

$$\begin{aligned} r_j &= a_j - eq_j = a_j - \left(\sum_{k=1}^{n} a_k l_k\right) q_j \\ &= a_1(-l_1)q_j + a_2(-l_2)q_j + \cdots a_j(1-l_j)q_j + \cdots a_n(-l_n)q_j \in J \end{aligned}$$

e が正で最小のものなので $r_j = 0$ $(j=1,\ 2,\ 3,\ \cdots,\ n)$．つまり e は $a_1,\ a_2,\ \cdots,\ a_n$ の公約数でありしたがって $e \leqq d$ である．

一方必要性の証明で示したように J の要素はすべて d の倍数であるから e も d の倍数であり，$d \leqq e$ である．

$$\therefore \quad e = d$$

k が d の倍数で $k = dn$ とする．

$$d = \sum_{k=1}^{n} a_k l_k$$

と表されるとき任意の d の倍数 dn は

$$dn = \sum_{k=1}^{n} a_k (l_k n)$$

と表される．ゆえに $l_k n = \alpha_k$ とおけば

$$k = \sum_{k=1}^{n} a_k \alpha_k$$

となる．つまり不定方程式 (2) に解 $(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)$ が存在することが示せた． ■

集合の言葉でいえば必要条件は

$$J \subset \{dn \mid n \text{ は整数}\}$$

である．十分条件は

$$\{dn \mid n \text{ は整数}\} \subset J$$

である．

$$\therefore \quad J = \{dn \mid n \text{ は整数}\}$$

これが本定理を集合の言葉で表したものである．

この一次不定方程式の解の存在は，一節での注意から整式の場合にも成立する．それを互いに素な二つの整式の場合に証明する．

定理 6

$f(x), g(x)$ をたがいに素な整式とする．すると，二つの整式, $k(x),\ h(x)$ で

$$f(x)h(x) + g(x)k(x) = 1$$

となるものが，存在する．

証明　$f(x)h(x) + g(x)k(x)$ の形の整式の集合を考える．すなわち，

$$\{f(x)h(x) + g(x)k(x) | h(x),\ k(x) \text{ は整式 }\}$$

とする．この集合に含まれる整式のなかで，0 でなくかつ次数（0 でもよい）がいちばん低い整式の一つを $t(x)$ とする．

さて, $f(x) = f(x)\cdot 1 + g(x)\cdot 0$ なので $f(x)$ 自身もこの集合の要素である．$f(x)$ を $t(x)$ で割る．その余りを $r(x)$ とすれば,

$$r(x) = f(x) - t(x)Q(x)$$

である．ゆえに $r(x)$ もこの集合に含まれる．かつその次数は $t(x)$ より低い．ところが $t(x)$ の次数が 0 でないもののなかで最低のものであるから, $r(x) = 0$ ，つまり, $t(x)$ は $f(x)$ を割り切る．

同様に, $g(x)$ も $t(x)$ で割り切れるので, $t(x)$ は $f(x)$, $g(x)$ の公約数である．ところが，これらは互いに素であるから，結局 $t(x)$ は定数でなければならない．よって $f(x)h(x) + g(x)k(x)$ の形の整式の集合には, 0 でない定数のものがあることがわかった．

$$f(x)h(x) + g(x)k(x) = c$$

のとき, $h(x)/c$, $k(x)/c$ を改めて $h(x)$, $k(x)$ にとることにより,

$$f(x)h(x) + g(x)k(x) = 1$$

となるものの存在が証明された．　■

このように整式でも本質的に同様である．整数や整式のように割り算ができ，さらに余りを何らかの自然数で表される大きさで制限することで，割り算の一意性が成り立つ「環」を「ユークリッド環」と呼ぶ．後に『ガウス整数』でまた別の「ユークリッド環」に出会うだろう.「ユークリッド環」の意味も含めてその節を参考にしてほしい．

練習問題 3.1 (解答 3)　整数からなる集合 A は次の性質を持つ．

$$A \text{ の任意の要素 } a,\ b \text{ に対して常に, } a + b \in A,\ a - b \in A$$

このとき A の要素はすべてある定まった数の倍数であることを示せ．

3.2　一次不定方程式の解の構成と一般解

ここではより一般的に一次不定方程式

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = k$$

の解の構成と一般解について考える．

まず「一般解」を正確に定義しておこう．2 変数の場合についてのべる．

x と y との不定方程式 $f(x,y)=0$ がある．t を整数値をとる媒介変数として，その関数 $p(t)$, $q(t)$ で t が整数値を動くとき, $x=p(t)$, $y=q(t)$ が不定方程式 $f(x,y)=0$ のすべての解をつくすとき, $x=p(t)$, $y=q(t)$ を不定方程式 $f(x,y)=0$ の**一般解** という．

変数が多い場合も同様に定義される．例として

$$32x+57y+68z=1$$

を考えよう．(32, 57, 68) の最大公約数を求めるとき（2 節「最大公約数と最小公倍数」参照）と同様に，いちばん小さい 32 で他の 2 数を割る．

$$\begin{aligned} 57 &= 32\times 1+25 \\ 68 &= 32\times 2+4 \end{aligned}$$

これを係数に代入し同様の操作を繰り返す.

$$\begin{aligned} 32x+57y+68z &= 32x+(32\times 1+25)y+(32\times 2+4)z \\ &= 32(x+y+2z)+25y+4z \\ &= (4\times 8)(x+y+2z)+(4\times 6+1)y+4z \\ &= 4\{8(x+y+2z)+6y+z\}+y+0(x+y+2z) \end{aligned}$$

ここで

$$l=8(x+y+2z)+6y+z=8x+14y+17z,\ m=y,\ n=x+y+2z \tag{3}$$

とおく.

$$4l+m+0n=1$$

の一般解を求める．これは例えば.

$$l=t,\ m=1-4t,\ n=s\quad t,\ s\ \in Z$$

がとれる．これより (3) は

$$\begin{aligned} 8x+14y+17z &= t \\ y &= 1-4t \\ x+y+2z &= s \end{aligned}$$

となる．これから一般解は

$$x=11-46t+17s,\ y=1-4t,\ -6+25t-8s\quad t,\ s\ \text{は任意整数}$$

となる．今は，適宜（てきぎ）式を整理したのでわかりにくいが，この方法をまねて一般解を構成するアルゴリズムを定式化することができる．

上の例からわかることは，除法をおこなうことで少ない変数の場合に帰着させ，2 変数の一般解を用いて一般解を構成できるのではないか，ということである．そのためにまず 2 変数の場合について，確認しなければならない.

2 変数の場合の一般解を構成するアルゴリズム

まず一組の解を見いださなければならない．$3x+2y=1$ なら暗算でできる．しかし $127x+52y=1$ となると，一組見つけるのも暗算というわけにはいかない．ところが，ユークリッドの互除法を用いた一組の解を構成する一般的方法ながある．

互除法を用いて不定方程式 $ax+by=k$ の一つの解を構成する一般的方法を考えよう．a と b の最大公約数が 1 より大きいとき，k が，a と b の最大公約数の倍数でなければ，解はない． k が最大公約数の倍数なら全体をその最大公約数で割って，初めから a と b の最大公約数は 1，つまり a と b は互いに素であるとしてよい．

このとき $ax+by=1$ に解が見つかれば x と y の各々に k を乗じることにより，$ax+by=k$ の解ができる．結局 a と b が互いに素なときに $ax+by=1$ の解が構成できればよいことがわかる．

$a>b$ とし，$a=bq+r, (0 \leqq r<b)$ とする．$ax+by=(bq+r)x+by=rx+b(qx+y)$ であるから，ここで $y'=qx+y$ とおくと $ax+by=1$ は $rx+by'=1$ となる． $rx+by'=1$ の解 (x_0, y_0') が構成できれば, $y_0=y_0'-qx_0$ によって定めた (x_0, y_0) が $ax+by=1$ の解となる．

これは解の存在証明の第二の方法と同じ内容であることに注意しよう．

a と b が互いに素なら b と r も互いに素であるから，こうして係数のより小さい方程式が得られ，しかもその解からもとの方程式の解が構成できる．この過程を繰り返すと，最後は係数の一方は 1 となる．

$sx+y=1$ または $x+ty=1$ の解として $(0,1)$ か $(1,0)$ をとれる．ここから逆に戻っていけば $ax+by=1$ の解が得られる．

この方法で $127x+52y=1$ の解を構成しよう．まず互除法で方程式を変換する．

(1) $127x+52y=1$

(2) $127=52\cdot 2+23$, $y'=2x+y$, $23x+52y'=1$

(3) $52=23\cdot 2+6$, $x'=x+2y'$, $23x'+6y'=1$

(4) $23=6\cdot 3+5$, $y''=3x'+y'$, $5x'+6y''=1$

(5) $6=5\cdot 1+1$, $x''=x'+y''$, $5x''+y''=1$

ここから逆に解を構成していく．

(1) $(x'', y'')=(0,1)$

(2) $x''=x'+y''$ より $(x', y'')=(-1,1)$

(3) $y''=3x'+y'$ より $(x', y')=(-1,4)$

(4) $x'=x+2y'$ より $(x, y')=(-9,4)$

(5) $y'=2x+y$ より $(x, y)=(-9,22)$

確かに, $127\cdot(-9)+52\cdot 22=-1143+1144=1$ である．これは 2 変数の不定方程式の解を構成する一般的な方法である．

この過程を具体的に記述するのは二次行列を使うのが適切である．二次行列の演算と行列式についてまとめておこう．

行列 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ とベクトル $\begin{pmatrix} x \\ y \end{pmatrix}$ に対し，$\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$ と定める．

A, B を二つの行列とし，$\overrightarrow{X} = \begin{pmatrix} x \\ y \end{pmatrix}$ とする．このとき計算によって確認できるように，

$$A(B\overrightarrow{X}) = (AB)\overrightarrow{X}$$

が成り立つ．また，行列 $\begin{pmatrix} s & t \\ u & v \end{pmatrix}$ に対して, $\Delta(A) = sv - tu$ とおくと，

$$\begin{aligned} \Delta\left(\begin{pmatrix} s & t \\ u & v \end{pmatrix}\begin{pmatrix} x & y \\ z & w \end{pmatrix}\right) &= \Delta\begin{pmatrix} sx+tz & sy+tw \\ ux+vz & uy+vw \end{pmatrix} \\ &= (sx+tz)(uy+vw) - (sy+tw)(ux+vz) \\ &= tzuy + sxvw - twux - syvz \\ &= (sv-tu)(xw-yz) \\ &= \Delta\begin{pmatrix} s & t \\ u & v \end{pmatrix}\Delta\begin{pmatrix} x & y \\ z & w \end{pmatrix} \end{aligned}$$

が成り立つ．$\Delta(A)$ のことを行列 A の「行列式」という．

以上を前提に，2 変数一次不定方程式の一般解の構成を含めて定理にまとめる．

定理 7

(1) $a, b \in Z,\ a > b > 0$ とする．a を b で割った商を q_0 ，余りを r_1 とするとき，次式が成り立つ．

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} b \\ r_1 \end{pmatrix}$$

(2) 同様の操作を繰り返すことにより，除法の列

$$a = q_0 b + r_1,\ b = q_1 r_1 + r_2,\ \cdots, r_{k-1} = r_k q_k + r_{k+1}$$

に対して，

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix}$$

が得られる．ここで

$$\begin{pmatrix} P_k & X_k \\ Q_k & Y_k \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$$

と置く．このとき次式が成り立つ．

$$X_k = P_{k-1},\ Y_k = Q_{k-1},\ P_k Q_{k-1} - P_{k-1} Q_k = (-1)^{k+1}$$

(3) a と b の最大公約数を d とするとき，

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix}\begin{pmatrix} d \\ 0 \end{pmatrix}$$

となる番号 n が存在する．

(4) このとき， $x = (-1)^{n-1}Q_{n-1},\ y = (-1)^n P_{n-1}$ が不定方程式 $ax + by = d$ の一組の解となる．

(5) $ax + by = 1$ の 1 組の解があるとし，それを $x_0\,, y_0$ とする．このとき $ax + by = 1$ の一般解は，

$$x = x_0 - bt\ \ ,\ \ y = y_0 + at$$

である．ただし， t は任意の整数である．

証明

(1) $a = bq_0 + r_1$ である．よって，

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} bq_0 + r_1 \\ b \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} b \\ r_1 \end{pmatrix}$$

(2)

$$\begin{aligned} \begin{pmatrix} P_k & X_k \\ Q_k & Y_k \end{pmatrix} &= \begin{pmatrix} P_{k-1} & X_{k-1} \\ Q_{k-1} & Y_{k-1} \end{pmatrix}\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \\ &= \begin{pmatrix} P_{k-1}q_k + X_{k-1} & P_{k-1} \\ Q_{k-1}q_k + Y_{k-1} & Q_{k-1} \end{pmatrix} \end{aligned}$$

よって，

$$X_k = P_{k-1}, \quad Y_k = Q_{k-1}$$

である．

$$\begin{aligned} P_kQ_{k-1} - P_{k-1}Q_k &= \Delta\begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} \\ &= \Delta\left(\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}\right) \\ &= (-1)^{k+1} \end{aligned}$$

(3) a を b で割った除法の式を

$$a = bq_0 + r_1$$

とする．この式の形より，a と b の公約数は r_1 を割り，b と r_1 の公約数は a を割るので，a と b の最大公約数と b と r_1 の最大公約数は等しい (ユークリッドの互除法の原理)．

次に，除法の原理より，

$$b > r_1 \geqq 0$$

である．同様に

$$\begin{pmatrix} a \\ b \end{pmatrix}, \begin{pmatrix} b \\ r_1 \end{pmatrix}, \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}, \cdots$$

はそれぞれの組の最大公約数がつねに等しく，かつ

$$b > r_1 > r_2 \cdots$$

と減少してゆく列である．ゆえに，ある番号 n が存在して，

$$r_n \neq 0, \quad r_{n+1} = 0$$

となる．このとき，a と b の最大公約数が r_n と 0 の最大公約数 (0 は 0 でない任意の整数を約数にもつものとする) となるので，r_n そのものが a と b の最大公約数 d である．つまり，この n に対して，

$$\begin{aligned}\begin{pmatrix} a \\ b \end{pmatrix} &= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} d \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix}\begin{pmatrix} d \\ 0 \end{pmatrix}\end{aligned}$$

となる．

(4)

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

の両辺に $\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix}$ の逆行列を左からかけると，

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix}^{-1} = (-1)^{n+1}\begin{pmatrix} Q_{n-1} & -P_{n-1} \\ -Q_n & P_n \end{pmatrix}$$

であるから，

$$(-1)^{n+1}\begin{pmatrix} Q_{n-1} & -P_{n-1} \\ -Q_n & P_n \end{pmatrix}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

つまり，

$$a\{(-1)^{n+1}Q_{n-1}\} + b\{(-1)^n P_{n-1}\} = 1$$

よって，$x = (-1)^{n-1}Q_{n-1},\ y = (-1)^n P_{n-1}$ は $ax + by = 1$ の解である．

(5) $(x,\ y)$ を $ax + by = 1$ の任意の解の組とすると，

$$\begin{cases} ax + by &= 1 \\ ax_0 + by_0 &= 1 \end{cases}$$

これより，

$$a(x - x_0) + b(y - y_0) = 0$$

となり，a と b は互いに素であるから，$x - x_0$ は b の倍数である．よって，$x - x_0 = -bt$ (t は整数) とおくと，$y - y_0 = +at$ となる．つまり，このときある t に対し，

$$x = x_0 - bt, \quad y = y_0 + at$$

となる．逆に，任意の整数 t に対し，$x = x_0 - bt,\ y = y_0 + at$ とおくと，

$$ax + by = a(x_0 - bt) + b(y_0 + at) = ax_0 + by_0 = 1$$

となるので，$(x,\ y)$ は $ax + by = 1$ の解である． ■

例 3.1　$127x + 52y = 1$ の一般解を以上の方法で求めよう.

$$\begin{aligned}
\begin{pmatrix} 127 \\ 52 \end{pmatrix} &= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 52 \\ 23 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 23 \\ 6 \end{pmatrix} \\
&= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 6 \\ 5 \end{pmatrix} \\
&= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 \\ 1 \end{pmatrix} \\
&= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}
\end{aligned}$$

そして,

$$\begin{aligned}
&\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix} \\
= &\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 5 & 1 \\ 1 & 0 \end{pmatrix} \\
= &\begin{pmatrix} 5 & 2 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 23 & 4 \\ 6 & 1 \end{pmatrix} = \begin{pmatrix} 127 & 22 \\ 52 & 9 \end{pmatrix}
\end{aligned}$$

なので,

$$x = -9,\ y = 22$$

が 1 組の解である. 実際,

$$127 \cdot (-9) + 52 \cdot 22 = -1143 + 1144 = 1$$

よって, 一般解は任意の整数 t に対し, 次式で与えられる.

$$\begin{cases} x &= -9 - 52t \\ y &= 22 + 127t \end{cases}$$

n 変数の場合に一般解を構成するアルゴリズム

このように 2 変数の場合について構成法が確立した. これをもとに一般の n 変数の場合に, 帰納的に解を構成していくことができる.

(1) 2 変数の場合, ユークリッドの互除法によって個別解が求まり, それを用いて一般解を作ることができる.

(2) $n-1$ 変数のとき一般解を構成することができるとする.

(3) $a_1,\ a_2,\ \cdots,\ a_n$ で a_1 が絶対値最小とする.

$$a_k = q_k a_1 + r_k,\ (k = 2,\ 3,\ \cdots,\ n)$$

とする．はじめの方程式は

$$\begin{aligned} a_1x_1+a_2x_2+\cdots+a_nx_n &= a_1x_1+(q_2a_1+r_2)x_2+\cdots+(q_na_1+r_n)x_n \\ &= a_1(x_1+q_2x_2+\cdots+q_nx_n)+r_2x_2+\cdots+r_nx_n=k \end{aligned}$$

となる．ここで $X_1=x_1+q_2x_2+\cdots+q_nx_n,\ X_k=x_k\ (k=2,\ \cdots,\ n)$ とおく．

$$a_1X_1+r_2X_2+\cdots+r_nX_n=k \tag{4}$$

ここで (4) の解 $X_1=\alpha_1,\ X_2=\alpha_2,\ \cdots,\ X_n=\alpha_n$ が構成できたとする．このとき

$$\begin{aligned} k &= a_1\alpha_1+r_2\alpha_2+\cdots+r_n\alpha_n \\ &= a_1\alpha_1+(a_2-a_1q_2)\alpha_2+\cdots+(a_n-a_1q_n)\alpha_n \\ &= a_1(\alpha_1-q_2\alpha_2-\cdots-q_n\alpha_n)+a_2\alpha_2+\cdots+a_n\alpha_n \end{aligned}$$

であるから

$$x_1=\alpha_1-q_2\alpha_2-\cdots-q_n\alpha_n,\ x_k=\alpha_k\ (k=2,\ \cdots,\ n)$$

は

$$a_1x_1+a_2x_2+\cdots+a_nx_n=k$$

の解である．

よって (4) の解が構成できればよい．ところが，方程式 (4) を作った操作を繰り返すと，ついにはいずれかの係数が 0 になる．その 0 のものを除いた $n-1$ 変数の不定方程式は一般解が構成できる．係数 0 の未知数を新たな任意整数におく．こうして得られた一般解から上の手順でもとの方程式の解を構成していけば，必ずもとの不定方程式の解が構成される．■

一般的な構成アルゴリズムの存在は，解の存在証明の別解になっていることに注意しよう．

練習問題 3.2 (解答 4)　次の不定方程式の一般解を求めよ．

(1) $25x+13y+15z=1$

(2) $2x+6y+5z+7w=1$

3.3　演習問題

演習問題 4 (解答 4) ［89 京大］

座標平面において，x 座標，y 座標がともに整数である点を格子点と呼ぶ．

四つの格子点 $\mathrm{O}(0,\ 0),\ \mathrm{A}(a,\ b),\ \mathrm{B}(a,\ b+1),\ \mathrm{C}(0,\ 1)$ を考える．ただし，$a,\ b$ は正の整数で，その最大公約数は 1 である．

(1) 平行四辺形 OABC の内部 (辺，頂点は含めない) に格子点はいくつあるか．

(2) (1) の格子点の全体を $\mathrm{P}_1,\ \mathrm{P}_2,\ \cdots,\ \mathrm{P}_t$ とするとき，$\triangle\mathrm{OP}_i\mathrm{A}\ \ (i=1,\ 2,\ \cdots,\ t)$ の面積のうちの最小値を求めよ．ただし $a>1$ とする．

演習問題 5 (解答 5) ［91 東大］

xy 平面上，x 座標，y 座標がともに整数であるような点 (m, n) を格子点と呼ぶ．

各格子点を中心として半径 r の円がえがかれており，傾き $\dfrac{2}{5}$ の任意の直線はこれらの円のどれかと共有点をもつという．このような性質をもつ実数 r の最小値を求めよ．

演習問題 6 (解答 6) ［93 早稲田］

(1) α, β を互いに素な正の整数とする．

(i) $\alpha x - \beta y = 0$ の整数解をすべて求めよ．

(ii)

$$\frac{\alpha}{\beta} = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4}}} (a_1, a_2, a_3, a_4 \text{は正の整数})$$

と書けるとする．

$$a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3}}$$

を通分して得られる分子 $a_1a_2a_3 + a_1 + a_3$ を p，分母 $a_2a_3 + 1$ を q とするとき，

$$\alpha q - \beta p$$

の値を求めよ．

(2) $157x - 68y = 3$ の整数解をすべて求めよ．

演習問題 7 (解答 7) ［立命改題］

$a,\ b,\ c$ は正の整数とし $a,\ b$ は互いに素であるとする． $x_0,\ y_0$ は整数で， $ax_0 + by_0 = c$ を満たすものとする．このとき次のことを証明せよ．

(1) 整数 l ， m が $al + bm = c$ を満たすとき

$$l = x_0 + bu,\ m = y_0 - au$$

を満たす整数 u が存在する．

(2) $c = ab$ のとき $ax + by = c$ を満たす正の整数の組 $(x,\ y)$ は存在しない．

(3) $c > ab$ のとき $ax + by = c$ を満たす正の整数の組 $(x,\ y)$ が存在する．

(4) $ax + by = k,\ 0 < k \leqq ab$ を満たす正の整数の組 $(x,\ y)$ が存在しない k はいくつあるか．

演習問題 8 (解答 8) ［00 京大理系後期］

xy 平面上の点で x 座標，y 座標がともに整数である点を格子点という．

$a,\ k$ は整数で $a \geqq 2$ とし，直線

$$L\ :\ ax + (a^2 + 1)y = k$$

を考える．

(1) 直線 L 上の格子点を一つ求めよ.

(2) $k = a(a^2+1)$ のとき， $x > 0,\ y > 0$ の領域に直線 L 上の格子点は存在しないことを示せ.

(3) $k > a(a^2+1)$ ならば， $x > 0,\ y > 0$ の領域に直線 L 上の格子点が存在することを示せ.

演習問題 9 (解答 9) ［00 阪大］

どのような負でない二つの整数 m と n をもちいても

$$x = 3m + 5n$$

とは表すことができない正の整数 x をすべて求めよ.

演習問題 10 (解答 10) ［00 大阪女子大］

$a,\ b$ は互いに素な正の整数とする.

(1) $4m + 6n = 7$ を満たす整数 $m,\ n$ は存在しないことを示せ.

(2) $3m + 5n = 2$ を満たすすべての整数の組 $(m,\ n)$ を求めよ.

(3) k を整数とするとき， ak を b で割った余りを $r(k)$ で表す. $k,\ l$ を $b-1$ 以下の正の整数とするとき， $k \neq l$ ならば $r(k) \neq r(l)$ であることを示せ.

(4) $am + bn = 1$ を満たす整数 $m,\ n$ が存在することを示せ.

演習問題 11 (解答 11) ［90 京大後期］

n を奇数とし， $f(x) = \left|\sin\dfrac{2\pi x}{n}\right|$ とする.

(1) 集合 $\{f(k) | k$ は整数 $\}$ は何個の要素をもつか.

(2) m を n と素な整数とする.

集合

$$\left\{ f(mk) \middle| k \text{ は } 0 \leqq k \leqq \frac{n-1}{2} \text{なる整数} \right\}$$

は m によらず一定であることを示せ.

演習問題 12 (解答 12) ［02 金沢後期理系］

$p,\ q$ は互いに素な整数とし， $1 < p < q$ とする. 座標平面内の集合 L を

$$L = \{\ (m,\ n)\ |\ m,\ n \text{ は整数で } 0 \leqq m < q-1,\ 0 \leqq n < p-1\ \}$$

とし，L の各元 $\mathrm{A}(m,\ n)$ に対し $N(\mathrm{A}) = mp + nq$ とおく.

(1) L の各元 A, B について，$N(\mathrm{A}) = N(\mathrm{B})$ ならば $\mathrm{A} = \mathrm{B}$ であることを示せ.

(2) L の各元 $\mathrm{A}(m,\ n)$ に対し，L の元 $\mathrm{A}^{\#}(q-2-m,\ p-2-n)$ を対応させる. $\mathrm{A}^{\#} \neq \mathrm{A}$ を示せ.

(3) $N(\mathrm{A}) \leqq pq - (p+q)$ となるためには，$N(\mathrm{A}^{\#}) \geqq pq - (p+q)$ であることが必要十分条件であることを示せ.

(4) $N(\mathrm{A}) \leqq pq - (p+q)$ を満たす L の元 A の個数を求めよ.

4 素数

4.1 素数

本節では素数に関する基礎を学ぶ．入試問題では整数の論証で素数のいろんな性質を根拠まで考えることなく比較的直感的に使っていることが多い．ここでは素数の基礎を学ぶが，実は素数はいまもって人間にとって未知の世界で，次のような問題が未解決である．

(1) ［ゴールドバッハの問題］任意の自然数 ($n \geqq 6$) は，$6 = 2+2+2$，$7 = 2+2+3$，$\cdots$，$20 = 2+5+13$ のように常に三つの素数の和に表せるか．

(2) 任意の偶数は，$100 = 103-3$，$102 = 119-17$ のように常に二つの素数の差で表せるか．

(3) ［双子素数の問題］(11 と 13)，(17 と 19)，(29 と 31) のように p と $p+2$ がどちらも素数となるような組は無限にあるか．

(4) ［メルセンヌ数］ 2^e-1 (e 素数) の形をした素数は無数にあるか．
$e=3$ なら $2^3-1=7$，$e=5$ なら 31 ところが $2^{11}-1=2047=23\cdot 89$
$e=2,\ 3,\ 5,\ 7,\ 13$ などは素数であるが $e=23,\ 29$ などは素数にならず，e が大きくなるとめったに素数は出てこない．

(5) ［フェルマ数］ $2^{2^n}+1$ (n 自然数) の形をした素数は無数にあるか．
$n=1,\ 2,\ 3,\ 4$ なら $5,\ 17,\ 257,\ 65537$ は素数，$n=5$ のとき $2^{2^5}+1$ は 641 で割れる

(6) n^2+1 の形をした素数は無数にあるか．また与えられた自然数 k に対して n^2+k の形をした素数は無数にあるか．
$2^2+1=5,\ 4^2+1=17,\ 6^2+1=37,\ 10^2+1=101$ などいくらでもできそうだが，無限にあるかどうかはわからない．

このほかに「リーマン予想」と呼ばれる決定的な問題が未解決である．これらはいずれも当面解けるめどはまったくない．入試の整数問題というのは，こういう整数の世界の大海のほんの一滴で，簡単に解けるものだけが出されている．基本事項を練習問題として多数掲載した．入試という点からいえば，第 1 節からここまででほぼ整数問題の 7 割方を含んでいる．

この節では，整数の約数．倍数を考えるので，正の数について考えればよい．以下特に断ることなく文字で整数を表すときは，正の整数，つまり自然数であるとする．$a>1$ の整数 a は少なくとも 1 と a 自身の二つの約数を持つ．1 および a 以外の約数を「真の約数」ともいう．$a>1$ の整数 a が真の約数を持たないとき a を **素数** という．逆に真の約数を持つ整数を **合成数** という．合成数は素数の積として表すことができる (定理 8 参照)．

整数を，どのような約数を持つかという観点から分類すると，四種類に分かれる．

0	: 無数の約数をもつ
1	: ただ一つの約数 1 をもつ
素数	: 真の約数を持たない
合成数	: 真の約数を持つ

整数全体のなかで 1 と -1 は「逆数もまた整数である」という性質を持つ．この二つが整数のなかの「単数」と呼ばれる数である．

定理 8
合成数を素数の積に分解することができる．かつ，その分解の結果は（因数の順序をのぞけば）一意である．

証明　数学的帰納法で示す.
最小の合成数は 4 で $4 = 2 \times 2$ でありこれ以外にないから，成立.
a よりも小さい (正の) 整数で成立しているとする.
分解の可能性.　a は合成数であるから

$$a = b \times c \quad (1 < b < a,\ 1 < c < a)$$

と分解される．帰納法の仮定により b も c も素数の積に分解されるので，a も素数の積に分解される.
分解の一意性.　a を素因数に分解して二つの分解

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

を得たとする．定理 3 の (4) より，二つの整数の積が素数 p で割り切れるなら，因数のなかの少なくとも一つがその素数で割り切れる.. 三つ以上の数以上の積の場合も $abc = (ab)c$ のように括弧でくくり順次考えればいずれかが p の倍数になる．したがって，$p_1,\ p_2,\ \cdots,\ p_m$ のいずれかは q_1 で割り切れる．いま p_1 が q_1 で割りきれるとすれば, p_1 は素数なので, $p_1 = q_1$ である.

$$\therefore \quad p_2 \cdots p_m = q_2 \cdots q_n$$

この両辺の数を b とすれば $b < a$ なので帰納法の仮定からこの分解は一意である.
したがって帰納法により分解は順序を除いて一意であることが示された.　■

次の証明は古来背理法の典型として有名なものである.

定理 9
素数の数は無限である.

証明　背理法で示す．素数の個数が有限であると仮定する．その個数を n 個とし，$p_1,\ p_2,\ \cdots,\ p_n$ をすべての素数とする．このとき

$$a = p_1 p_2 \cdots p_n + 1$$

は，$p_1,\ p_2,\ \cdots,\ p_n$ のいずれで割っても 1 余るので, $p_1,\ p_2,\ \cdots,\ p_n$ を因数に持たない．したがって, a の素因数分解に現れる素数は $p_1,\ p_2,\ \cdots,\ p_n$ 以外である．つまり $p_1,\ p_2,\ \cdots,\ p_n$ がすべての素数ということと矛盾した.
ゆえに素数の数は無限である.　■

練習問題 4.1 (解答 5)　$a = p^\alpha q^\beta r^\gamma \cdots$ を a の素因数べきへの分解とする．以下の命題を示せ.

(1) a のすべての約数は

$$p^x q^y r^z \cdots$$

において $0 \leqq x \leqq \alpha$, $0 \leqq y \leqq \beta$, $0 \leqq z \leqq \gamma$, $\cdots$ を動くことで漏れなくまた重複なく得られる.

(2) a の約数の個数 $T(a)$ は

$$T(a) = (1+\alpha)(1+\beta)(1+\gamma)\cdots$$

で与えられる.

(3) a のすべての約数の和 $S(a)$ は

$$S(a) = \frac{p^{\alpha+1}-1}{p-1} \cdot \frac{q^{\beta+1}-1}{q-1} \cdot \frac{r^{\gamma+1}-1}{r-1} \cdot \cdots$$

で与えられる.

(4) $a,\ b, c$, が互いに素なとき,

$$T(abc) = T(a)T(b)T(c)$$

また

$$S(abc) = S(a)S(b)S(c)$$

(5) a のすべての約数の積は

$$a^{\frac{T(a)}{2}}$$

に等しい.

練習問題 4.2 (解答 6)　古代ギリシアの数学では整数 a の約数 (1 を入れて a 自身を入れない) の和が a に等しいとき a を **完全数** と称していた. すなわち練習問題 4.1 の記号では

$$S(a) = 2a$$

のとき a を完全数という.

(1) $n > 1$ に対して $a = 2^{n-1}(2^n - 1)$ とおく. $2^n - 1$ が素数になるとき, a は完全数であることを示せ.

(2) 逆に偶数の完全数はこのような形の数しかないことを示せ.

練習問題 4.3 (解答 7)　次のことを示せ.

(1) $a,\ a',\ a'',\ \cdots$ がおのおの $b,\ b',\ b'',\ \cdots$ と互いに素なら $aa'a''\cdots$ と $bb'b''\cdots$ も互いに素である. とくに $(a,\ b) = 1$ なら $(a^n,\ b^n) = 1$

(2)

$$(a_1,\ a_2,\ \cdots,\ a_m)(b_1,\ b_2,\ \cdots,\ b_n) = (a_1b_1,\ a_1b_2,\ \cdots,\ a_2b_1,\ \cdots,\ a_mb_n\ )$$

(3) $a_1,\ a_2,\ \cdots,\ a_n$ のなかの少なくとも一つの素因数分解に現れる素数を $p,\ q,\ \cdots$ とし, 現れたすべての素数に関する積を

$$a_k = \prod^{p} p^{\alpha_k}\ (\alpha_k \geqq 0)$$

とおく. $a_1,\ a_2,\ \cdots,\ a_n$ の最大公約数を m , 最小公倍数を l とするとき,

$$m = \prod^{p} p^{\mathrm{Min}(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)}$$
$$l = \prod^{p} p^{\mathrm{Max}(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)}$$

ただし Min はいずれより大きくない数, Max はいずれより小さくない数, を表す.

(4) $a_1,\ a_2,\ \cdots,\ a_n$ の最大公約数を d_1 , $a_1a_2,\ a_1a_3,\ \cdots,\ a_{n-1}a_n$ の最大公約数を d_2 , 一般に $a_1,\ a_2,\ \cdots,\ a_n$ のなかの k 個づつの積の最大公約数を d_k とし，特に $a_1a_2\cdots a_n = d_n$ とする．

(i) $k = 2,\ \cdots n$ に対して d_k は d_{k-1} で割りきれる．

(ii) $\dfrac{d_k}{d_{k-1}} = e_k$ (ただし $e_1 = d_1$) とおくと e_k は e_{k-1} で割りきれる．

(iii) また

$$e_1e_2\cdots e_n = a_1a_2\cdots a_n$$

(iv) e_n は $a_1,\ a_2,\ \cdots,\ a_n$ の最小公倍数に等しい．

(5) 仮に $a,\ b,\ c,\ \cdots$ の最小公倍数を $\{a,\ b,\ c,\ \cdots\}$ で表すことにする．

$$\{(a_1,\ m),\ (a_2,\ m),\ \cdots,\ (a_n,\ m)\} = (\{a_1,\ a_2,\ \cdots,\ a_n\},\ m)$$

(6) l を $a,\ b,\ c,\ \cdots$ の最小公倍数とする．$a_0,\ b_0,\ c_0,\ \cdots$ をそれぞれ $a,\ b,\ c,\ \cdots$ の約数で二つずつ互いに素であるとする．このとき

$$l = a_0b_0c_0\cdots$$

練習問題 4.4 (解答 8)

(1) p が素数ならば二項係数 ${}_p\mathrm{C}_k$ $(p > k > 0)$ は p で割り切れることを示せ．

(2) k がちょうど p の l 乗で割りきれるならば, ${}_{p^n}\mathrm{C}_k$ $(p^n > k > 0)$ は p^{n-l} で割り切れることを示せ．

練習問題 4.5　解答 9　$n!$ の因数分解に含まれる素因数 p の最高べきの指数は,

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]$$

であることを示せ．ただし $[x]$ は実数 x を超えない最大の整数を表す．

練習問題 4.6 (解答 10)　$\dfrac{m}{n}$ $(m > 0,\ n > 1)$ を既約分数とする．分母 n の素因数分解を $n = p^\alpha q^\beta\cdots$ とすれば，分数 $\dfrac{m}{n}$ は，$0 < x < p^\alpha,\ 0 < y < q^\beta,\ \cdots,\ s \geqq 0$ である整数 $x,\ y,\ \cdots,\ s$ を用いて

$$\frac{m}{n} = \frac{x}{p^\alpha} + \frac{y}{q^\beta} + \cdots \pm s$$

と一通りに部分分数に分解されることを示せ．

4.2　演習問題

演習問題 13 (解答 13) ［88 群馬］

自然数 k を 2 の累乗と奇数の積として $k = 2^a m$ (a は 2 の累乗の指数, m は奇数) と表すとき, $f(k) = a$ と定める．

$$S_n = \sum_{k=1}^{n} f(k)$$

とするとき,

(1) S_{50} を求めよ.

(2) n が 2 の累乗のとき S_n を n の式で表せ.

(3) $\dfrac{n-1}{2} \leqq S_n < n$ であることを示せ.

演習問題 14 (解答 14) ［97 京大文］

自然数 n の約数の個数を d とする． n の約数をすべて並べて得られる 数列を a_k $(1 \leqq k \leqq d)$ とする．したがって，$a_1 = 1$ ， $a_d = n$ ， $a_k < a_{k+1}$ $(1 \leqq k < d)$ である．このとき，n に対する次の二つの条件 (イ)，(ロ) は互いに同値 ((イ) $\Longleftrightarrow$ (ロ)) であることを示せ.

(イ) n は 60 の倍数である.

(ロ) n は 6 個以上の約数を持ち，$\dfrac{1}{a_3} + \dfrac{1}{a_6} = \dfrac{1}{a_2}$ となる.

演習問題 15 (解答 15) ［98 上智］

(1) 81 のすべての正の約数 1,⋯,81 の和を求めよ.

(2) 378 の正の約数の個数と，それらの和を求めよ.

(3) 自然数 N のすべての正の約数の和は 60 であるという．このような N はいくつあるか．そのうち 2 と 3 のみの積で表せるものは何か.

演習問題 16 (解答 16) ［98 京大文］

a, b, p, q はすべて自然数で,

$$\frac{p^2+q^2}{a} = \frac{pq}{b}$$

を満たしている． a と b の最大公約数が 1 のとき以下の問いに答えよ.

(1) pq は b で割り切れることを示せ.

(2) $\sqrt{a+2b}$ は自然数であることを示せ.

演習問題 17 (解答 17) ［99 京大文］

自然数 a , b , c について，等式 $a^2+b^2=c^2$ が成り立ち，かつ a , b は互いに素とする．このとき，次のことを証明せよ.

(1) a が奇数ならば， b は偶数であり，したがって c は奇数である.

(2) a が奇数のとき,

$$a+c = 2d^2$$

となる自然数 d が存在する.

演習問題 18 (解答 18) ［02 九大前期理系］

正の整数 a に対し, a の正の約数全体の和を $f(a)$ で表す．ただし，1 および a 自身も約数とする．たとえば $f(1)=1$ であり，$a=15$ ならば 15 の正の約数は 1,3,5,15 なので $f(15)=24$ となる．次の問いに答えよ.

(1) a が正の奇数 b と正の整数 m を用いて $a = 2^m b$ と表されるとする．このとき

$$f(a) = (2^{m+l} - 1) f(b)$$

が成り立つことを示せ．

(2) a が 2 以上の整数 p と正の整数 q を用いて $a = pq$ と表されるとする．このとき

$$f(a) \geqq (p+1)q$$

が成りたつことを示せ．また，等号が成り立つのは，$q = 1$ かつ p が素数であるときに限ることを示せ．

(3) 正の偶数 $a,\ b$ は，ある整数 $m,\ n$ とある奇数 $r,\ s$ を用いて $a = 2^m r,\ b = 2^n s$ のように表すことができる．このとき $a,\ b$ が

$$\begin{cases} f(a) = 2b \\ f(b) = 2a \end{cases}$$

をみたせば，$r,\ s$ は素数であり，かつ $r = 2^{n+1} - 1,\ s = 2^{m+1} - 1$ となることを示せ．

5　合同式

5.1　合同式

合同式は，高校の教科書には載っていない．しかし学校では習ったり自分で学習した人もいるだろう．やる以上は正しく自分のものにしてほしい．

整数 a と b の差が m の倍数であるとき, a と b は m を法として互いに**合同** であるいい，次のように記す.

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

$a - b = mq$ とおく．ここで a と b を m で割った商と余りをそれぞれ q_1, q_2 , r_1, r_2 とする．

$$\begin{aligned} a &= mq_1 + r_1 \\ b &= mq_2 + r_2 \end{aligned}$$

辺々引いて $a - b = mq$ を用いると

$$mq = (q_1 - q_2)m + r_1 - r_2$$

つまり

$$|m||q - q_1 + q_2| = |r_1 - r_2|$$

もし $q - q_1 + q_2 \neq 0$ なら，$|m||q - q_1 + q_2| \geqq |m|$ であるが，右辺は m で割った余りの差なので $|r_1 - r_2| < m$ となり矛盾する．

$$\therefore \quad q - q_1 + q_2 = 0, \quad r_1 - r_2 = 0$$

つまり，m を法として合同な二数は， m で割った二つの数の余りが等しい．逆も明か.

二数が合同，という関係は，余りが等しいという関係，なので，合同の関係は，等号や図形の相似，合同などと同じく，次の三つの規律に従う.

反射律　$a \equiv a \pmod{m}$
対称律　$a \equiv b \pmod{m}$ ならば $b \equiv a \pmod{m}$
推移律　$a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$ ならば $a \equiv c \pmod{m}$

これが成り立つ関係を**同値関係**という.「二つの命題が同値である」の「同値」と混同しないようにしよう.

ある集合 A の要素の間に，同値関係の規律が成り立つ関係が定義されているとする．すると集合 A を互いに同値な要素からなる部分集合に分けることができる．合同の関係も同値関係の規律が成立しているから，整数を互いに合同なものを同じ類に，合同でないものを異なる類に，確定的に分類することが出来る.「3 で割ると 2 余る数」という表現が意味を持つのは，この原則が成立しているからである．m を法とする整数の一つの類とは, m を法として互いに合同なすべての数の集合である．例えば 3 を法とする 1 の類とは,「3 で割ると 1 余る整数全体の集合」である．また，2 を法とすればすべての整数は偶数と奇数の二つの集合に分かれる.

任意の整数 n を整数 m で割り，余り r を $0 \leqq r \leqq m - 1$ にとる.

$$n = mq + r, \ r = 0, \ 1, \ \cdots, \ m - 1$$

となる．ゆえに任意の n は m を法として $0,\ 1,\ \cdots,\ m-1$ のただ一つと合同である．つまり，整数を, m を法として互いに合同な整数よりなる集合に分けると, m 個の集合に分かれる．

各集合について，その集合に属する一つの要素 a をとれば，同じ集合に属するすべての要素は

$$mk+a,\ k:\ \text{整数の全体}$$

となる．

m を法として m 個に分けられた各集合から一つずつ代表を取り出したとき，それを**完全な代表の一組**(または**剰余系**) という．例えば

$$\{0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6\}$$
$$\{0,\ 1,\ 2,\ 3,\ -3,\ -2,\ -1\}$$
$$\{7,\ -6,\ 9,\ -4,\ -10,\ -9,\ 13\}$$

はいずれも 7 を法とする完全な代表の一組になっている．

定理 10

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

ならば

$$\begin{aligned} a\pm b &\equiv a'\pm b' \pmod{m} \\ ab &\equiv a'b' \pmod{m} \end{aligned} \tag{5}$$

一般に

$$a\equiv a'\ (\mathrm{mod.}\ m),\ \ b\equiv b'\ (\mathrm{mod.}\ m),\ \ c\equiv c'\ (\mathrm{mod.}\ m),\ \cdots$$

で $f(x,\ y,\ z,\ \cdots)$ が $x,\ y,\ z,\ \cdots$ に関する整数係数の整式ならば

$$f(a,\ b,\ c,\ \cdots)\equiv f(a',\ b',\ c',\ \cdots)\pmod{m} \tag{6}$$

証明　仮定によって

$$\begin{aligned} &a\equiv a'\pmod{m} \quad \text{したがって } a-a' \text{ は } m \text{ の倍数} \\ &b\equiv b'\pmod{m} \quad \text{したがって } b-b' \text{ は } m \text{ の倍数} \end{aligned}$$

ゆえに $(a+b)-(a'+b')=(a-a')+(b-b')$ は m の倍数である．また, $ab-a'b'=(a-a')b+a'(b-b')$ も m の倍数である．すなわち (5) が示された．

(5) から $a\equiv a'\pmod{m}$ なら任意の整数 N に対して

$$Na\equiv Na'\pmod{m}$$

および

$$Na^{\alpha}b^{\beta}c^{\gamma}\cdots\equiv Na'^{\alpha}b'^{\beta}c'^{\gamma}\cdots\pmod{m}$$

ふたたび (5) から

$$\sum Na^{\alpha}b^{\beta}c^{\gamma}\cdots\equiv\sum Na'^{\alpha}b'^{\beta}c'^{\gamma}\cdots\pmod{m}$$

すなわち (6) が示された．■

等式での

$$ab=ac,\ a\neq 0\Rightarrow b=c$$

に対応する合同式の定理は次のものである．

定理 11

$$ac \equiv bc \pmod{m} \text{ かつ } (c,\ m) = 1 \ \Rightarrow a \equiv b \pmod{m}$$

一般に $(c,\ m) = d$ のとき, $m = dm'$ とおけば,

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

が成り立つ.

証明　前半は $d = 1$ の場合だから後半を示せばよい.
$m = dm',\ c = dc'$ とおく. このとき m' と c' は互いに素である.
仮定から $ac - bc$ は m の倍数つまり整数 N で

$$ac - bc = mN$$

となるものがある. ゆえに

$$(a - b)c' = m'N$$

m' と c' は互いに素なのでこれから $a - b$ が m' の倍数であることがわかる. つまり

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

が示された. ■

練習問題 5.1 (解答 11)　a を十進法で表して

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_1 10 + a_0$$

となるとする. このとき,

$$a \equiv a_0 + a_1 + \cdots + a_n \pmod{9}$$
$$a \equiv a_0 - a_1 + \cdots + (-1)^n a_n \pmod{11}$$

練習問題 5.2 (解答 12)　今日が金曜日であるとする.　10^6 , 10^{100} , 3^{100} 日後はそれぞれ何曜日か. ■

練習問題 5.3 (解答 13)

(1) $2^{65} + 1$ は 11 で割り切れることを示せ.

(2) n が正の整数のとき, $13^{2n} + 6$ は 7 で割り切れることを示せ.

(3) 3^{15} および $(3^{15})^{15}$ の 1 の位の数を求めよ.

(4) $(2^{100} - 1)^{99}$ を 100 で割ったときの余りを求めよ.

練習問題 5.4 (解答 14)　n を整数とする.

(1) n^2 を 7 で割るとあまりは 0, 1, 2, 4 のいずれかである.

(2) $n^5 - n$ は 10 の倍数である.

(3) n が奇数なら $n^2 - 1$ は 8 で割り切れる.

(4) $n^4 + 2n^3 + 11n^2 + 10n$ は、24 の倍数である.

練習問題 5.5 (解答 15)

(1) 整数 $a,\ b$ に対して，$a^2 + b^2 = c^2$ となる整数 c が存在するとき，a, b の少なくとも一方は 3 の倍数であるとを示せ.

(2) 整数 $a,\ b,\ c$ が $a^2 + b^2 = c^2$ を満たすとき，$a,\ b,\ c$ のうち少なくとも 1 つは 5 の倍数であることを示せ.

練習問題 5.6 (解答 16)　$a,\ b$ は正の整数で，a を 11 で割ると余りが 3，$a^3 + b$ を 11 で割ると余りが 4 であるという．このとき b を 11 で割ると，余りはいくらか.

5.2　一次合同方程式

$f(x)$ が整数係数の整式であるとき,

$$f(x) \equiv 0 \pmod{m}$$

を**合同方程式**と呼び，この合同式を満たす未知の整数 x を求めることを「合同方程式を解く」という．簡単に「合同式を解く」ともいう.

x_0 をこの合同式の一つの解とし, $x_1 \equiv x_0$ とすれば，定理 10 より

$$f(x_1) \equiv f(x_0) \pmod{m}$$

すなわち m を法として x_0 と合同な数はすべてこの合同方程式の解である．ゆえに合同式を解くことは，それを満たす整数の類を求めることである．以下，合同方程式の解といえば，解の類の意味とする．よって合同方程式のすべての解を求めようとすれば, $x = 0,\ 1,\ \cdots,\ m-1$ の m 個の値をあてはめてみればよい．つまりどんな合同方程式も，有限回の計算で求めることが出来る.

定理 12

一次合同方程式

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

は $(a,\ m) = 1$ のときただ一つの解がある.

$(a,\ m) = d > 1$ のときは，b が d で割り切れるときにかぎって解がある．その解の個数は d である．解の個数とは, m を法としての類に関していう.

証明

(i) $(a,\ m) = 1$ のとき.

$$\{x_1,\ x_2,\ \cdots,\ x_m\}$$

を m を法とする剰余系とする．このとき

$$\{ax_1,\ ax_2,\ \cdots,\ ax_m\}$$

もまた m を法とする剰余系である．なぜならもし

$$ax_i \equiv ax_j \pmod{m}$$

なら, a が m と互いに素であることから

$$x_i \equiv x_j \pmod{m}$$

となる．それは $i = j$ のときにかぎるからである．

ゆえに任意の b に対して $\{x_1,\ x_2,\ \cdots,\ x_m\}$ のなかのただ一つ

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

となる x_i が存在する．

(ii) $(a,\ m) = d > 1$ のとき．

$$ax \equiv b \pmod{m} \tag{7}$$

に解があるとすると, $ax - b = mN$ (N は整数) と表される．ゆえに $b = ax - mN$ は $d = (a,\ m)$ で割りきれる．そこで

$$a = da',\ m = dm',\ b = db'$$

とおく．(7) は定理 11 より

$$a'x \equiv b' \pmod{m'} \tag{8}$$

と同値である．ここで a' と m' は互いに素であるから (8) を満たす x は m' を法とする一つの類である．それを $x \equiv x_0 \pmod{m}$ とする．(8) の解は

$$x = x_0 + m't \quad t \text{ は任意の整数} \tag{9}$$

によって与えられる． t_1 と t_2 に対する x が m を法として合同になるのは

$$m'(t_1 - t_2) \equiv 0 \pmod{m}$$

つまり

$$t_1 - t_2 \equiv 0 \pmod{d}$$

となるときにかぎる．したがって，(9) で t を d を法とする剰余系 $\{0,\ 1,\ \cdots,\ d-1\}$ の値を与えるとき, m を法とする (7) のすべての解が得られる．すなわちその解の個数は d である． ■

このように合同方程式 (7) を解くことは，一次不定方程式

$$ax + my = b$$

の整数解を求めることと同じである．

定理 13

$m_1,\ m_2,\ \cdots,\ m_k$ が二つずつ互いに素で, $a_1,\ a_2,\ \cdots,\ a_k$ は任意の整数であるとする.

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\cdots \\ x &\equiv a_k \pmod{m_k} \end{aligned} \tag{10}$$

を満たす x は $M = m_1 m_2 \cdots m_k$ を法としてただ一つ存在する.

証明　第一の合同式を満たす x は

$$x = a_1 + m_1 t \tag{11}$$

と書ける. これが第二の合同式も満たすのは

$$a_1 + m_1 t \equiv a_2 \pmod{m_2}$$

すなわち

$$m_1 t \equiv a_2 - a_1 \pmod{m_2}$$

のときである. ところが, m_1 と m_2 は互いに素なのでこれには

$$t = t_0 + m_2 s$$

のように m_2 を法とするただ一つの類が解として存在する. これを (11) に代入して

$$x = a_1 + m_1 t_0 + m_1 m_2 s$$

つまり

$$x \equiv a_1 + m_1 t_0 \pmod{m_1 m_2}$$

この一つの合同式を (10) の最初の二つの合同式に置き換えてよい. 同様の操作を繰りかえすことができる. ついには

$$x \equiv x_0 \pmod{M}$$

を得る. ■

この定理は **中国の剰余定理 (Chinese Remainder Teorem)** と呼ばれる. 中国古代 (一世紀頃) の書『孫子算経』の中に,「3 で割れば 2 余り, 5 で割れば 3 余り, 7 で割れば 2 余るような数は何か」という問いと解の求め方が述べられている. この種の問題が孫子以降の中国の算術の書に見られる. 下って 16 世紀の終わり頃の『算法統宗』(程大位) にはこの孫子の問いに対する解の求め方が歌で述べられている. このような歴史があるのでこの定理が上のように呼ばれるのである.

ここでガウス (Gauss) による対称性を用いたより美しい別証を紹介する.

ガウスの別証明

$M = m_1 m_2 \cdots m_k$ に対し

$$M = m_1 M_1 = m_2 M_2 = \cdots = m_k M_k \tag{12}$$

とおく．そして

$$M_n t_n \equiv 1 \pmod{m_k} \quad (n = 1,\ 2,\ \cdots,\ k)$$

となる t_n $(n = 1,\ 2,\ \cdots,\ k)$ を求める．このとき (10) の解は

$$x \equiv a_1 M_1 t_1 + a_2 M_2 t_2 + \cdots + a_k M_k t_k \pmod{M}$$

である．実際，(12) から

$$a_n M_n t_n \equiv a_n \pmod{m_n}$$

で, $M_1,\ \cdots,\ M_k$ のうち M_n 以外はすべて m_n で割りきれるので,

$$x \equiv a_n \pmod{m_n} (n = 1,\ 2,\ \cdots,\ k)$$

である．

唯一の解であることは, x_1 と x_2 がともに (10) を満たせば

$$x_1 \equiv x_2 \pmod{m_n} (n = 1,\ 2,\ \cdots,\ k)$$

なので, $m_1,\ m_2,\ \cdots,\ m_k$ の最小公倍数 M に関して

$$x_1 \equiv x_2 \pmod{M}$$

となるからである． ■

練習問題 5.7 (解答 17)

$$26x \equiv 1 \pmod{57}$$

を解け.

練習問題 5.8 (解答 18)　3 で割れば 1 余り，5 で割れば 2 余り，7 で割れば 3 余る正で最小の整数を求めよ.

練習問題 5.9 (解答 19)　法 $m,\ n$ の最大公約数を d ，最小公倍数を l とする.

$$\begin{cases} x \equiv a \pmod{m}, \\ x \equiv b \pmod{n}. \end{cases}$$

が解を持つ必要十分条件は

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

であることを示せ．またこのとき，解は l を法としてただ一つであることを示せ.

練習問題 5.10（解答 20）　n 個の合同方程式

$$x \equiv a_i \pmod{m_i},\ i = 1,\ 2,\ \cdots,\ n$$

が解を持つための必要十分条件は

$$a_i \equiv a_j \pmod{(m_i,\ m_j)},\ i,\ j = 1,\ 2,\ \cdots,\ n$$

であることを示せ．このとき解は $m_1,\ m_2,\ \cdots,\ m_n$ の最小公倍数を法としてただ一つであることを示せ．

5.3　合同方程式の解法

$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$ が整数係数の多項式であるとき，合同方程式

$$f(x) \equiv 0 \pmod{m}$$

を満たす x(の類) を求めることを考える．このときは，各係数 a_i をそれと合同な数で置き換えてもかまわない．特に m で割りきれる係数は消し去ってかまわない．このような消去をおこなった後に $a_0 \not\equiv 0 \pmod{m}$ なら，この合同方程式を n 次という．合同方程式の解法に関する三つの基本定理を証明しよう．

定理 14

法 p が素数であるとき, n 次の合同方程式

$$f(x) \equiv 0 \pmod{p} \tag{13}$$

は n 個より多くの解を有することはない．解の数とはもちろん p を法として互いに合同でないものの個数，つまり異なる類の個数のことである．

証明　次数 n に関する数学的帰納法で示す.

$n = 1$ のとき．一次の合同方程式

$$a_0x + a_1 \equiv 0 \pmod{p},\ (a_0,\ p) = 1$$

は定理 5 によって, p を法としてただ一つの解を有する.

$n - 1$ 次のとき解が $n - 1$ 個以下であることが示されたとする.

(13) が解を有するときその一つを $x \equiv a \pmod{p}$ とする．すなわち $f(a) \equiv 0 \pmod{p}$. このとき多項式の除法の原理 (定理 2) によって

$$f(x) = (x - a)f_1(x) + f(a)$$

となる $n - 1$ 次の多項式 $f_1(x)$ がある．$f(x) = \sum_{k=0}^{n} a_kx^{n-k}$ とおくと

$$f(x) - f(a) = \sum_{k=0}^{n-1} a_k(x^{n-k} - a^{n-k})$$

なので, $f_1(x)$ は整数が係数の多項式である．このとき合同方程式 (13) は

$$(x - a)f_1(x) \equiv 0 \pmod{p}$$

と同一の解を有する． p が素数であるからこの合同式は $(x-a)$ または $f_1(x)$ が p で割り切れるときにかぎって成り立つ．ゆえに $x \equiv a \pmod{p}$ 以外の解は $n-1$ 次の合同方程式

$$f_1(x) \equiv 0 \pmod{p}$$

の解でなければならない．帰納法の仮定によりこの解は $n-1$ 個以下である．

よって (13) の解は n 個以下である． ■

さて一般の合同方程式

$$f(x) \equiv 0 \pmod{m}$$

は， m が素数の場合に解ければ解くことが出来る．それを次に二段階に分けて示そう．

まず， m が素数 p のべきつまり $m = p^e$ のときの解は, $m = p$ のときの解から構成することが出来ることを示す (定理 15).

次に， m が $m = p^e q^f \cdots$ と因数分解されるときの解は, $m = p^e,\ m = q^f,\ \cdots$ のときの解から構成することが出来ることを示す (定理 16).

定理 15

合同方程式

$$f(x) \equiv 0 \pmod{p^e} \tag{14}$$

の解は

$$f(x) \equiv 0 \pmod{p} \tag{15}$$

の解から構成することが出来る．実際 x_0 を (15) の一つの解とするとき

(1)

$$f'(x_0) \not\equiv 0 \pmod{p}$$

ならば

$$f(x) \equiv 0 \pmod{p^e}$$

の解のなかに $x \equiv x_0 \pmod{p}$ であるものが mod. p^e に関してただ一つある．

(2)

$$f'(x_0) \equiv 0 \pmod{p}$$

ならば

$$f(x) \equiv 0 \pmod{p^e}$$

が $x \equiv x_0 \pmod{p}$ の解をもつときに，その解から

$$f(x) \equiv 0 \pmod{p^{e+1}}$$

の p 個の解が構成されることもあり，あるいは

$$f(x) \equiv 0 \pmod{p^{e+1}}$$

は $x \equiv x_0 \pmod{p^e}$ なる解をもたないこともある．

証明　e に関する帰納法で示す.

1.　$e=2$ のときに示す.

$$f(x)\equiv 0 \pmod{p^2} \tag{16}$$

(16) の解はもとより (15) を満たす．したがって (16) の解 x は p を法として (15) の何らかの解 x_0 と一致しなければならない．つまり (16) の解 x は

$$x = x_0 + py \tag{17}$$

という形をしたもののなかから求められる．ここで整数係数の整式 $f(x)$ に対して

$$f(x+y) = f(x) + yf'(x) + \cdots + y^k \frac{f^{(k)}(x)}{k!} + \cdots + y^n \frac{f^{(n)}(x)}{n!}$$

と展開され，さらに各 $\dfrac{f^{(k)}(x)}{k!}$ は x の $n-k$ 次の整数係数の整式であることに注意する．そこで (17) を (16) に代入する.

$$\begin{aligned} f(x) &= f(x_0+py) \\ &= f(x_0) + pyf'(x_0) + p^2y^2\frac{f''(x_0)}{2!} + \cdots \equiv 0 \pmod{p^2} \end{aligned}$$

上の注意から各 $f'(x_0)$, $\dfrac{f''(x_0)}{2!}$ $\cdots$ は整数である．ゆえにこの展開式の第 3 項以下は p^2 で割りきれる．よって (17) の数で (16) を満たすものを求めることは,

$$f(x_0) + pyf'(x_0) \equiv 0 \pmod{p^2}$$

を満たす y を求めることに帰着する．同じことであるが $f(x_0)$ は p で割り切れるので

$$\frac{f(x_0)}{p} + yf'(x_0) \equiv 0 \pmod{p} \tag{18}$$

ここで二つの場合を区別する.

(1) $f'(x_0)\not\equiv 0 \pmod{p}$ のとき．このときは (18) はただ一つの解をもつ．それを

$$y \equiv y_0 \pmod{p}$$

とする．このとき $py \equiv py_0 \pmod{p^2}$ だから (17) より

$$x \equiv x_0 + py_0 \pmod{p^2}$$

を得る．つまり (16) の解が得られた.

(2)$f'(x_0)\equiv 0 \pmod{p}$ のとき．このときは (18) は $\dfrac{f(x_0)}{p}$ がさらに p で割り切れなければ解がない．$\dfrac{f(x_0)}{p}$ が p で割り切れるなら任意の y が解になる．つまり

$$x_0,\ x_0+p,\ x_0+2p,\ \cdots,\ x_0+(p-1)p \qquad \pmod{p}$$

が (16) を満たす．すなわち (17) の形の数 x は一つも (16) の解を与えないか，あるいは p^2 を法として p 個の解を与える.

2.　e のとき，つまり (14) の解 x_0 が得られたとして，$e+1$ のときの解の構成法を示す.

このときも $(\mathrm{mod.}\ p)$ の解から $(\mathrm{mod.}\ p^2)$ の解を構成したのと同様に出来る．すなわち

$$x = x_0 + p^e y$$

の形の数で

$$f(x) \equiv 0 \pmod{p^{e+1}}$$

を満たすものは次のように構成される．

(A) $f'(x_0) \not\equiv 0 \pmod{p}$ なら p^{e+1} を法としてただ一つ定まる．

(B) $f'(x_0) \equiv 0 \pmod{p}$ なら p^{e+1} を法として一つもないか，または p 個ある． p 個あるのは $f(x_0) \equiv 0 \pmod{p^{e+1}}$ のときである． ■

例 5.1 $p \neq 2$ が素数で, a は p で割り切れないとする．そのとき

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

に解があるときは，その解は二つある．それを $\pm x_0$ とする．

$$x_0 \not\equiv 0 \pmod{p},\ x_0 \not\equiv -x_0 \pmod{p}$$

この場合には, $f(x) = x^2 - a,\ f'(x) = 2x$ である．ゆえに

$$f'(\pm x_0) = \pm 2x_0 \not\equiv 0 \pmod{p}$$

これは上定理の (1) の場合である．ゆえに

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

には二つの解がある．

例えば,

$$x^2 \equiv 2 \pmod{7}$$

の解は $x_0 \equiv \pm 3$ である．これから

$$x^2 \equiv 2 \pmod{49}$$

の解を求めてみよう．そのために $x = 3 + 7y$ とおく．

$$\begin{aligned}
& (3+7y)^2 \equiv 2 \pmod{49} \\
\text{から} \quad & 9 + 42y \equiv 2 \pmod{49} \\
\text{つまり} \quad & 6y \equiv -1 \pmod{7} \\
\therefore \quad & y \equiv 1 \pmod{7} \\
\text{したがって} \quad & x \equiv 10 \pmod{49} \\
\text{他の解は} \quad & x \equiv -10 \equiv 39 \pmod{49}
\end{aligned}$$

定理 16

法 m を素数べきに因数分解して

$$m = p^e q^f \cdots$$

とするとき,

$$\begin{aligned} f(x) &\equiv \quad (\text{mod. } p^e) \qquad (19)\\ f(x) &\equiv \quad (\text{mod. } q^f) \qquad (20)\\ &\cdots \end{aligned}$$

がそれぞれ $l,\ l',\ \cdots$ 個の解をもつとすれば,

$$f(x) \equiv 0 \pmod{m} \qquad (21)$$

は $ll'\cdots$ 個の解をもつ．それれは

$$\begin{aligned} x &\equiv \alpha \pmod{p^e}\\ x &\equiv \beta \pmod{q^f} \qquad (22)\\ \cdots &\qquad \cdots \end{aligned}$$

から求められる．ここで $\alpha,\ \beta,\ \cdots$ はそれぞれ $p^e,\ q^f,\ \cdots$ を法としての $f(x) \equiv 0$ の任意の解の一組である．

証明　x が (21) の解ならば (19)，(20) の解である．したがって (22) を満たす．
逆に (21) を満たす x は，(19)，(20) を満たすから，(21) を満たす．　■

例 5.2

$$\begin{aligned} x^2 &\equiv 1 \pmod{3}\\ x^2 &\equiv 1 \pmod{4} \end{aligned}$$

の解はそれぞれ二つある．それらを $\alpha \equiv \pm 1 \pmod{3}$ と $\beta \equiv \pm 1 \pmod{4}$ とする．

$$x^2 \equiv 1 \pmod{12}$$

は四つの解をもつ．それらは,

$$\left.\begin{matrix} x \equiv 1\\ x \equiv 1 \end{matrix}\right\} \quad \left.\begin{matrix} x \equiv 1\\ x \equiv -1 \end{matrix}\right\} \quad \left.\begin{matrix} x \equiv -1\\ x \equiv 1 \end{matrix}\right\} \quad \left.\begin{matrix} x \equiv -1\\ x \equiv -1 \end{matrix}\right\} \begin{matrix}(\text{mod. } 3)\\ (\text{mod. } 4)\end{matrix}$$

から求められる．

$$\therefore \quad x \equiv 1,\ x \equiv 7,\ x \equiv 5,\ x \equiv 11 \pmod{12}$$

練習問題 5.11 (解答 21)　次の合同方程式を解け.

(1) $x^2 + x + 1 \equiv 3 \pmod{25}$

(2) $x^2 \equiv 1 \pmod{39}$

5.4 演習問題

演習問題 19 (解答 19) ［82 名古屋市大］
n を自然数とするとき， $3^{n+1}+4^{2n-1}$ は 13 で割りきれることを証明せよ.

演習問題 20 (解答 20) ［東工大］
n を正の整数とするとき、$19^n+(-1)^{n-1}2^{4n-3}$ は、 7 の倍数であることを示せ.

演習問題 21 (解答 21) ［82 九大］
整数を係数とする n 次の多項式

$$f(x)=x^n+a_1x^{n-1}+\cdots a_{n-1}x+a_n\ (n>1)$$

について次のことを証明せよ.

(1) 有理数 α が方程式 $f(x)=0$ の 1 つの解ならば，α は整数である.

(2) ある自然数 $k(>1)$ に対して， k 個の整数 $f(1),\ f(2),\ \cdots,\ f(k)$ のどれもが k で割り切れなければ方程式 $f(x)=0$ は有理数の解をもたない.

演習問題 22 (解答 22) ［01 京大文系］任意の整数 n に対し， n^9-n^3 は 9 で割り切れることを示せ.

演習問題 23 (解答 23) $\alpha\equiv 1\,(\mathrm{mod.}\ 8)$ であるとする．このとき $e\geqq 3$ に対して

$$x^2\equiv\alpha\,(\mathrm{mod.}\ 2^e)$$

の解は四つあり，その一つを x_0 とすれば解は

$$\pm x_0,\ \pm x_0+2^{e-1}$$

であることを示せ.

6　オイラーの関数 $\varphi(n)$

6.1　オイラーの関数 $\varphi(n)$

自然数 $1,\ 2,\ \cdots,\ n$ のなかに n と互いに素な数 x がいくつあるか．その数を $\varphi(n)$ で表す．
例えば，

$$\begin{aligned}
&\varphi(1) = 1, \qquad (x = 1)\\
&\varphi(2) = 1, \qquad (x = 1)\\
&\varphi(3) = 2, \qquad (x = 1,\ 2)\\
&\varphi(4) = 2, \qquad (x = 1,\ 3)\\
&\varphi(5) = 4, \qquad (x = 1,\ 2,\ 3,\ 4)\\
&\varphi(6) = 2, \qquad (x = 1,\ 5)
\end{aligned}$$

この $\varphi(n)$ を**オイラーの関数**という．これは整数を定義域とする関数である．
p が素数ならば，明らかに

$$\varphi(p) = p - 1$$

である．また同じく p が素数ならば

$$\varphi(p^e) = p^e - p^{e-1} = p^e\left(1 - \frac{1}{p}\right)$$

である．なぜなら 1 から p^e までの数のなかで p^e と互いに素ではないものは p で割り切れるものに他ならず，それは

$$1 \cdot p,\ 2 \cdot p,\ \cdots,\ p^{e-1} \cdot p$$

の p^{e-1} 個だけあるからである．

ここで $\varphi(n)$ の意味を次のように集合論的に考えよう．整数の集合 Z を n を法として互いに合同な整数の集合に分ける．

$$Z_n(k) = \{x \,|\, x \equiv k \pmod{n}\}$$

を k と合同な整数の集合とする．もちろん $k \equiv k' \pmod{n}$ なら

$$Z_n(k) = Z_n(k')$$

である．集合 $Z_n(k)$ を n **を法とする剰余類**という．この分類よって Z が重なりなく抜けなく n 個の部分集合

$$Z_n(1),\ Z_n(2),\ \cdots,\ Z_n(n)$$

に分けられる．
例えば $n = 2$ とすれば，

$$\begin{aligned}
Z_2(1) &= \{\cdots -3,\ -1,\ 1,\ 3,\ \cdots\}\\
Z_2(2) &= \{\cdots -4,\ -2,\ 0,\ 2,\ 4,\ \cdots\}
\end{aligned}$$

と整数を奇数，偶数の集合に分けることに他ならない．各剰余類から代表を一つずつ選んだものが「剰余系」である (5 節「合同式」の冒頭参照)．上の n 個は剰余系として $1,\ 2,\ \cdots,\ n$ を用いた表現である．

さて，一つの $Z_n(k)$ 内の要素はすべて n と互いに素であるか，すべて n と互いに素でないか，のいずれかであって，一部のみが互いに素ということはない．なぜなら $Z_n(k)$ の要素 x はすべて $x = k + nt$ (t 整数) と書け，

$$(k + nt,\ n) = (k,\ n)$$

となるからである (この等号の証明はユークリッドの互除法の原理の証明と同じ)．

したがって「剰余類 $Z_n(k)$ が n と互いに素である」と言うことが意味を持つ．n と互いに素な剰余類 $Z_n(k)$ を**既約類**という．またすべての既約類の代表の一組を**既約剰余系**という．

以上の準備の上で $\varphi(n)$ の意味を考えれば，$\varphi(n)$ は n を法とする既約類の個数である．

整数で定義された関数 $F(x)$ が互いに素な二つの整数 a と b に対してつねに

$$F(ab) = F(a)F(b)$$

が成り立つとき，**乗法的関数**という．

定理 17

$\varphi(ab)$ は乗法的関数である．すなわち a と b が互いに素ならば，

$$\varphi(ab) = \varphi(a)\varphi(b) \tag{23}$$

証明　a を法とする既約類 $Z_a(k)$ ，b を法とする既約類 $Z_b(l)$ をとる．

集合

$$A = \{bx + ay \,|\, x \in Z_a(k),\ y \in z_b(l)\}$$

を考える．これは ab を法とする既約類になっている．なぜなら，整数 s, t を用いて $x = k+as$, $y = l + bt$ と表すと

$$bx + ay = bk + al + ab(s + t)$$

となり，整数 s, t の取り方を変えても ab を法として合同だから剰余類 $A = Z_{ab}(bk + al)$ となる．

さらにこれは既約類である．なぜならもし $bx + ay$ が ab と互いに素でないとする． a と b が互いに素なので a または b と互いに素でない． a と互いに素でないとする．

$$(bx + ay,\ a) \neq 1 \iff (bx,\ a) \neq 1 \iff (x,\ a) \neq 1 \iff (k,\ a) \neq 1$$

となり $Z_a(k)$ が a を法とする既約類であることに反するからである．

ここで $k' \not\equiv k \pmod{a}$ なる k' をとると

$$bk' + al \not\equiv bk + al \pmod{ab}$$

である．なぜならもし $bk' + al \equiv bk + al \pmod{ab}$ なら $bk' \equiv bk \pmod{ab}$ であるが a と b が互いに素なので $k' \equiv k \pmod{a}$ とならねばならないからである．

つぎに ab を法とする任意の剰余類 $Z_{ab}(m)$ をとる．a と b が互いに素なので $bk + al = m$ となる k, l が存在する．ゆえに既約類 $Z_{ab}(m)$ は既約類 $Z_a(k)$ と既約類 $Z_b(l)$ から上の方法で作られる．したがって a を法とする既約類 $Z_a(k)$ と b を法とする既約類 $Z_b(l)$ の一組と ab を法とする既約類 $Z_{ab}(m)$ は一対一に対応する．この組は $\varphi(a)\varphi(b)$ 個あるので (23) が示された　■

これが基本的な事実である．この証明は剰余類の定義にたちかえって行った．もし 5 節定理 13 を用いれば簡明である．すなわち次のようになる．

いま $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_m\ ,\ m=\varphi(a)$ および $\beta_1,\ \beta_2,\ \cdots,\ \beta_n\ ,\ n=\varphi(b)$ をそれぞれ a と b を法とする既約な代表の一組とする．$mn=\varphi(a)\varphi(b)$ 個の組合せの一つ $\alpha_i,\ \beta_j$ に対して

$$\gamma\equiv\alpha_i\ (\mathrm{mod.}\ a)\ ,\quad \gamma\equiv\beta_j\ (\mathrm{mod.}\ b) \tag{24}$$

となる γ が ab を法として一つずつある． γ は ab と互いに素である．

逆に $(\gamma,\ ab)=1$ とすると，(24) となる $\alpha_i,\ \beta_j$ が一意に決まる．ゆえに ab を法とする既約代表の一組の各数 γ と $\alpha_i,\ \beta_j$ の組の間に一対一の対応が成り立つ．したがって (23) が示された．

$\varphi(n)$ は次の定理によって計算される．

定理 18

a と b が互いに素ならば,

n を素数べきに分解して

$$n=p^{\alpha}q^{\beta}r^{\gamma}\cdots$$

とすると

$$\varphi(n)=n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots \tag{25}$$

証明　定理 17 から

$$\begin{aligned}
\varphi(n) &= \varphi(p^{\alpha}q^{\beta}r^{\gamma}\cdots)\\
&= \varphi(p^{\alpha})\varphi(q^{\beta})\varphi(r^{\gamma})\cdots\\
&= (p^{\alpha}-p^{\alpha-1})(q^{\beta}-q^{\beta-1})(r^{\gamma}-r^{\gamma-1})\cdots\\
&= p^{\alpha}\left(1-\frac{1}{p}\right)q^{\beta}\left(1-\frac{1}{q}\right)r^{\gamma}\left(1-\frac{1}{r}\right)\cdots\\
&= n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots
\end{aligned}$$

■

例 6.1　$a=3,\ b=5,\ ab=15$ とする．

$$\alpha=1,\ 2,\ \beta=1,\ 2,\ 3,\ 4 \qquad \varphi(3)=2,\ \varphi(5)=4$$
$$\gamma=1,\ 2,\ 4,\ 7,\ 8,\ 11,\ 13,\ 14 \qquad \varphi(15)=8$$

であるが, γ を $5\alpha+3\beta$ で計算すると

α	1	1	1	1	2	2	2	2
β	1	2	3	4	1	2	3	4
γ	1	7	13	4	11	2	8	14

$d|n$ は d が n を割り切ることを意味する (1 節)．　$d=1,\ n$ のときも $d|n$ である．

定理 19

$$\sum_{d|n}\varphi(d)=n \tag{26}$$

和は n のすべての約数 (1 も n も含む) にわたる．

証明　d を n の約数として，1 から n までの数 x で，$(x,\ n) = d$ となるものはいくつあるか．

$$(x,\ n) = d \quad \Longleftrightarrow \quad \left(\frac{x}{d},\ \frac{n}{d}\right) = 1$$

であるから，その個数は 1 から $\dfrac{n}{d}$ までの中にある $\dfrac{n}{d}$ と互いに素な数の個数，つまり $\varphi\left(\dfrac{n}{d}\right)$ である．

1 から n までの数 x は $(x,\ n)$ の値が等しいものに分類できる．つまり

$$\{\ 1,\ 2,\ \cdots,\ n\ \} = \cup_{d\ |\ n}\{\ x \mid (x,\ n) = d,\ 1 \leqq x \leqq n\ \}$$

である．したがって，d が n の約数全体を動くとき (1 と n を含む)．この方法で 1 から n までの数はちょうど一度づつ数えられる．

$$\therefore \quad \sum_{d|n} \varphi\left(\frac{n}{d}\right) = n$$

d が n の約数全体を動くとき $\dfrac{n}{d}$ も n の約数全体を動くので，(26) が示された．　■

例 6.2　$n = 15$ とする．

d	x	$\varphi\left(\dfrac{n}{d}\right)$
1	1, 2, 4, 7, 8, 11, 13, 14	$8 = \varphi(15)$
3	3, 6, 9, 12	$4 = \varphi(5)$
5	5, 10	$2 = \varphi(3)$
15	15	$1 = \varphi(1)$
		計 15

練習問題 6.1 (解答 22)

(1) 1 から 1512 までの自然数で 1512 と互いに素なものはいくつあるか．

(2) それらの和はいくらか．

練習問題 6.2 (解答 23)　xy 平面で $0 \leqq x \leqq 12,\ 0 \leqq y \leqq 12$ で囲まれた正方形の周と内部にある格子点を考える．

原点とこれらの格子点を結ぶ線分をで，両端以外に格子点が乗っていないものは何本あるか．

練習問題 6.3 (解答 24)　$a,\ b,\ c,\ \cdots$ は二つずつ互いに素であるとし，$\Phi(x)$ は実数 x を越えない自然数のなかで a でも，b でも，c でも，$\cdots$ 割り切れないものの個数を表すとする．

$$\begin{aligned}\Phi(x) \quad = \quad & [x] - \left[\frac{x}{a}\right] - \left[\frac{x}{b}\right] - \left[\frac{x}{c}\right] - \cdots \\ & + \left[\frac{x}{ab}\right] + \left[\frac{x}{ac}\right] + \left[\frac{x}{bc}\right] - \cdots \\ & - \left[\frac{x}{abc}\right] - \cdots\end{aligned}$$

を示せ．ただし $[x]$ は x を超えない最大の整数を表す．

6.2 メービスの反転公式

一般に整数で定義されたふたつの関数 $F(x),\ G(x)$ に対して

$$\sum_{d|n} F(d) = G(n) \tag{27}$$

が成り立つとき，これを逆に解いて $F(x)$ を $G(x)$ で表すことができる．

そのために**メービス (Möbius) の関数** $\mu(n)$ を次のように定義する．

$$\mu(n) = \begin{cases} 1 & (n = 1 \text{ のとき}) \\ (-1)^k & (n \text{ が } k \text{ 個の相異なる素数の積のとき}) \\ 0 & (n \text{ がある素数の平方で割り切れるとき}) \end{cases}$$

例 6.3

$$\mu(1) = 1,\ \mu(2) = -1,\ \mu(3) = -1,\ \mu(4) = 0,\ \mu(5) = -1,\ \mu(6) = 2,\ \cdots$$

補題 1　$n > 1$ なら

$$\sum_{d|n} \mu(d) = 0$$

証明　$n > 1$ であるから n を素数のべきに因数分解して

$$n = {p_1}^{e_1} {p_2}^{e_2} \cdots {p_k}^{e_k}$$

とする．よって

$$\sum_{d|n} \mu(d) = \sum^{x} \mu({p_1}^{x_1} {p_2}^{x_2} \cdots {p_k}^{x_k})$$

ここで和は $0 \leqq x_1 \leqq e_1,\ 0 \leqq x_2 \leqq e_2,\ \cdots,\ 0 \leqq x_k \leqq e_k$ の範囲内のすべての $x_1,\ x_2,\ \cdots,\ x_k$ を動く．この和の中で 0 になるもの，つまり素数べき指数が 2 以上のものを除くと，

$$\begin{aligned} \sum_{d|n} \mu(d) &= \mu(1) + \{\mu(p_1) + \mu(p_2) + \cdots + \mu(k)\} \\ &\quad + \{\mu(p_1 p_2) + \mu(p_1 p_3) + \cdots + \mu(p_{k-1} p_k)\} \\ &\quad + \cdots \\ &\quad + \mu(p_1 p_2 \cdots p_k) \\ &= 1 - k + {}_k\mathrm{C}_2 - {}_k\mathrm{C}_3 + \cdots + (-1)^k \\ &= (1-1)^k = 0 \end{aligned}$$

■

この $\mu(n)$ を用いると $F(n),\ G(n)$ に関する問題を解くことができる．

定理 20 (メービスの反転公式)

整数で定義された二つの関数 $F(x),\ G(x)$ について次の二つの命題は同値である．

$$\sum_{d|n} F(d) = G(n)$$

$$F(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) G(d)$$

証明　すべての n に対して第一式が成り立てば，それを第二式の右辺に代入して

$$\sum_{d|n}\sum_{\delta|d}\mu\left(\frac{n}{d}\right)F(\delta)$$

δ は d の約数なので, $\dfrac{n}{d}$ は $\dfrac{n}{\delta}$ の約数になる．したがって和の順序を逆にすると

$$=\sum_{\delta|d}\left[F(\delta)\sum_{\delta'|\frac{n}{\delta}}\mu(\delta')\right]$$

補題 1 によってかっこ内の和で $\dfrac{n}{\delta}>1$ のものは 0 になり，$F(n)\mu(1)$ のみが残る．

$$\therefore\quad\sum_{d|n}\mu\left(\frac{n}{d}\right)G(d)=F(n)$$

つぎにすべての n に対して第二式が成り立てば，同様に

$$\begin{aligned}\sum_{d|n}F(d) &= \sum_{d|n}\sum_{\delta|d}\mu\left(\frac{d}{\delta}\right)G(\delta)\\ &= \sum_{\delta|n}\left[\sum_{\delta'|\frac{n}{\delta}}\mu(\delta')\right]G(\delta)=G(n)\end{aligned}$$

■

特に $F(n)=\varphi(n)$ のときは $G(n)=n$ である．整数で定義された関数で定理 19 の等式 (26) がすべての n について成り立つものはオイラーの関数 $\varphi(n)$ のみである．そして

$$\varphi(n)=\sum_{d|n}\mu\left(\frac{n}{d}\right)d$$

となる．実際 $n=p^\alpha q^\beta r^\gamma\cdots$ とすると

$$\begin{aligned}\varphi(n) &= \sum_{d|n}\mu\left(\frac{n}{d}\right)d=\sum_{d|n}\mu(d)\frac{n}{d}\\ &= \mu(1)n+\mu(p)\frac{n}{p}+\mu(q)\frac{n}{q}+\mu(r)\frac{n}{r}+\cdots\\ &\quad +\mu(pq)\frac{n}{pq}+\mu(pr)\frac{n}{pr}+\cdots\\ &\quad +\cdots+\mu(pqr\cdots)\frac{n}{pqr\cdots}\\ &= n-\frac{n}{p}-\frac{n}{q}-\frac{n}{r}+\cdots+\frac{n}{pq}+\frac{n}{pq}\\ &\quad +\cdots-\frac{n}{pqr}-\cdots\\ &= n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\cdots\end{aligned}$$

練習問題 6.4　解答 25　整数で定義された関数 $F(n)$ が乗法的関数のとき $G(n) = \sum_{d|n} F(d)$ で定義された関数 $G(n)$ も乗法的関数であることを示せ．また，この事実を用いて補題 1 の別証を考えよ．

練習問題 6.5　解答 26　正の実数 x を超えない自然数のうちで n と互いに素であるものの個数を $\varphi(n,\ x)$ とおく．$\varphi(n,\ n) = \varphi(n)$ である．$[x]$ で x を超えない整数を表すと定理 19，定理 20 の一般化として

$$\begin{aligned} \sum_{d|n} \varphi(d,\ dx) &= [nx] \\ \varphi(n,\ x) &= \sum_{d|n} \mu(d) \left[\frac{x}{d}\right] \end{aligned}$$

が成り立つことを示せ．

7　1の n 乗根

7.1　1の n 乗根

1 の n 乗根，すなわち方程式

$$x^n - 1 = 0 \tag{28}$$

の根は n 個ある．それらは

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ (k = 0,\ 1,\ \cdots,\ n-1) \tag{29}$$

である．実際これらはすべて偏角の異なる複素数なので異なる．しかも n 乗すると 1 になるので，方程式 (28) の解である．簡単のために

$$\alpha = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},\ (k = 0,\ 1,\ \cdots,\ n-1)$$

とおくと，(29) はド・モアブルの定理より，

$$\alpha^k \quad (k = 0,\ 1,\ \cdots,\ n-1)$$

と表される．このとき因数定理から $x^n - 1$ は $x - \alpha^k$ を因数にもつ．したがって $x^n - 1$ は

$$x^n - 1 = Q(x)(x-1)(x-\alpha)\cdots(x-\alpha^{n-1})$$

の因数分解をもつ．次数と最高次数の係数を考えると $Q(x) = 1$ がわかり，この n 個がちょうど方程式 (28) の解であることがわかる．

ここで $\alpha^n = 1$ なので，(29) において k に与えるべき値は n を法としての一つの剰余系である．さらに $(k,\ n) = 1$ のとき (29) において $\dfrac{2k\pi}{n}$ は n 倍してはじめて 2π になるので，α^k は n 乗してはじめて 1 に等しくなる．1 の n 乗根のうち n 乗してはじめて 1 のなるものを**1の原始 n 乗根**という．

定理 21

1 の原始 n 乗根は $\varphi(n)$ 個ある．それらは

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

において, k に n を法としての既約剰余系の値を与えて得られるものである．

証明　すでに述べたように $(k,\ n) = 1$ のとき (21) において $\dfrac{2k\pi}{n}$ は n 倍してはじめて 2π になるので，α^k は n 乗してはじめて 1 に等しくなる．つまり α^k は原始 n 乗根である．

逆に β が原始 n 乗根であるとする．　β は $x^n - 1 = 0$ の根であるから $\beta = \alpha^l$ と表される．

もし $(l,\ n) = d > 1$ なら $n = dn',\ l = dl'$ とおくとき

$$\cos\frac{2l\pi}{n} + i\sin\frac{2l\pi}{n} = \cos\frac{2l'\pi}{n'} + i\sin\frac{2l'\pi}{n'}$$

なので, $(\alpha^l)^{n'} = 1$ となり, n 乗してはじめて 1 となる，という仮定に反する．ゆえに $(l,\ n) = 1$ となる．

ゆえに α^k が原始 n 乗根となるのは，n と互いに素な k を用いて α^k と表されるときにかぎるので，その個数は $\varphi(n)$ 個である．ちなみに α^l は原始 n' 乗根である．　■

例 7.1　1 の 6 乗根は

$$1,\ -1,\ \frac{-1\pm\sqrt{3}i}{2},\ \frac{1\pm\sqrt{3}i}{2}$$

そのうち原始 6 乗根は最後の二つだけである．$\frac{-1\pm\sqrt{3}i}{2}$ は原始 3 乗根，-1 は原始 2 乗根，1 は 1 乗根である．

定理 22

n の素因数分解を $n=p^\alpha q^\beta r^\gamma\cdots$ とし，

$$\begin{aligned} F_n(x) &= \frac{(x^n-1)(x^{\frac{n}{pq}}-1)(x^{\frac{n}{qr}}-1)\cdots\cdots}{(x^{\frac{n}{p}}-1)(x^{\frac{n}{q}}-1)\cdots(x^{\frac{n}{pqr}}-1)\cdots} &(30)\\ &= \prod_{d|n}(x^{\frac{n}{d}}-1)^{\mu(d)} &(31)\end{aligned}$$

とすれば, $F_n(x)$ は 1 の原始 n 乗根のみを根とする多項式である．$F_n(x)$ は $\varphi(n)$ 次で，その最高次数の係数は 1，その他の係数もすべて整数である．ここに $\mu(n)$ はメービスの関数である．

証明　1 の原始 n 乗根のみを単根とする方程式で最高次数の係数が 1 であるものを $F_n(x)=0$ とする．定理 21 の証明より，その他の n 乗根は n の約数 d に対し、原始 $\frac{n}{d}$ 乗根になるが，d が 1 以外の約数を動けば $\frac{n}{d}$ は n 以外の約数を動くので，原始 n 乗根以外の n 乗根は n の真の約数 d を次数とする原始 d 乗根になる．原始 n 乗根と合わせた全体がちょうど 1 の n 乗根の全体である．つまり $\prod_{d|n}F_d(x)=x^n-1$ となる．x を十分大きく各 $F_d(x)$ が正の値をとるように固定する．それぞれの最高次数の係数が正なのでそれは可能である．その上で両辺の対数をとる．

$$\sum_{d|n}\log F_d(x)=\log(x^n-1)$$

整数 n と d に関する等式と見ればメービスの反転公式 (6 節定理 20) が使え

$$\log F_n(x)=\sum_{d|n}\mu(d)\log(x^{\frac{n}{d}}-1)$$

つまり

$$F_n(x)=\prod_{d|n}(x^{\frac{n}{d}}-1)^{\mu(d)}$$

両辺 x の多項式で，十分大きい x でつねに成立するので x に関して恒等的に成立する．したがって (31) が示された．

$F_n(x)$ の次数は定理 21 より $\varphi(n)$ でその係数は (31) より明らかに整数である．式 (30) の分子分母の最高次数の係数はともに 1 なので分母を払って係数比較すれば $F_n(x)$ の最高次数の係数が 1 であることがわかる．■

例 7.2

$$F_6(x) = \frac{(x^6-1)(x-1)}{(x^2-1)(x^3-1)}=x^2-x+1$$

$$F_{12}(x) = \frac{(x^{12}-1)(x^2-1)}{(x^6-1)(x^4-1)} = x^4 - x^2 + 1$$

p が素数なら

$$F_p(x) = \frac{x^p-1}{x-1} = x^{p-1} + x^{p-2} + \cdots + 1$$

$$F_{p^e}(x) = \frac{x^{p^e}-1}{x^{p^{e-1}}-1} = x^{p^{e-1}(p-1)} + x^{p^{e-1}(p-2)} + \cdots + 1$$

練習問題 7.1 (解答 27)　$F_n(x)$ の定数項は $n=1$ の場合以外 $+1$ であることを示せ.

練習問題 7.2 (解答 28)　$F_n(x)$ の第二項 ($\varphi(n)-1$ 次の項) の係数は $-\mu(n)$ に等しいことを示せ. つまり 1 の原始 n 乗根の和は $\mu(n)$ である.

練習問題 7.3 (解答 29)　α を 1 の原始 n 乗根とすれば

$$\alpha^k \ (k = 0,\ 1,\ \cdots,\ n-1)$$

がすべての n 乗根で, そのうち $(k,\ n) = 1$ なる k に対するものがちょうど原始 n 乗根になることを示せ.

練習問題 7.4 (解答 30)　次のことを示せ.

(1) 互いに素な二つの整数 $a,\ b$ に対し, 1 の a 乗根と b 乗根をすべての組合せについて掛けて得られる ab 個の積が 1 の ab 乗根の全部になる.

(2) 1 の 原始 a 乗根と 原始 b 乗根をすべての組合せについて掛けるなら 1 の 原始 ab 乗根の全部が得られる.

7.2　演習問題

演習問題 24 (解答 24)　［70 東大］i を虚数単位とし $\alpha = \cos\dfrac{\pi}{3} + i\sin\dfrac{\pi}{3}$ とおく. また n はすべての自然数にわたって動くとする. このとき

(1) α^n は何個の異なる値をとりうるか.

(2)

$$\frac{(1-\alpha^n)(1-\alpha^{2n})(1-\alpha^{3n})(1-\alpha^{4n})(1-\alpha^{5n})}{(1-\alpha)(1-\alpha^2)(1-\alpha^3)(1-\alpha^4)(1-\alpha^5)}$$

の値を求めよ.

演習問題 25 (解答 25) α を絶対値が 1 で偏角が $\dfrac{2\pi}{n}$ の複素数とする（ n は正の整数）.

次の問に答えよ.

(1) 方程式 $x^n - 1 = 0$ の相異なる解は $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ であることを示せ.

(2) $x^n - 1 = 0$ を因数分解せよ.

(3) $(1+\alpha)(1+\alpha^2)\cdots(1+\alpha^{n-1})$ の値を求めよ.

(4) m を n と互いに素な正の整数とする．このとき，$(1+\alpha^m)(1+\alpha^{2m})\cdots(1+\alpha^{(n-1)m})$ の値を求めよ．

演習問題 26 (解答 26) ［01 京大理系］

p を 2 以上の整数とする．2 以上の整数 n に対し，次の条件 (イ)，(ロ) をみたす複素数の組 $(z_1,\ z_2,\ \cdots,\ z_n)$ の個数を a_n とする．

(イ)　$k=1,\ 2,\ \cdots,\ n$ に対し，${z_k}^p=1$ かつ，$z_k\neq 1$

(ロ)　$z_1z_2\cdots z_n=1$

このとき次の問いに答えよ．

(1) a_3 を求めよ．

(2) a_{n+2} を a_n ，　a_{n+1} の一方または両方を用いて表せ．

(3) a_n を求めよ．

演習問題 27 (解答 27) ［01 京都府立医大］

0 でない複素数からなる集合 G は次を満たしているとする．

G の任意の要素 $z,\ w$ の積 zw は再び G の要素である．

(1) ちょうど n 個の複素数からなる G の例をあげよ．

(2) ちょうど n 個の複素数からなる G は (1) の例以外にないことを示せ．

8　フェルマの小定理

8.1　フェルマの小定理

ここではいわゆる「フェルマの小定理」呼ばれる定理の証明とその応用を学ぶ.「フェルマの小定理」は高校数学の範囲で十分証明できる．それを練習問題にしておいた．その解答は合同式の記号も使わないでしておいた.「フェルマの小定理」の意味はさらに次節で学ぶ．まず「フェルマの小定理」とそれを一般的にした「オイラーの定理」を証明しよう．その応用として,「4n+1 型の素数が無限に存在すること」，および循環小数への応用を学ぼう.

定理 23 (オイラーの定理)
m を正整数とし a を m と互いに素な整数とする．このとき

$$a^{\varphi(m)} \equiv 1 \pmod{m} \tag{32}$$

が成り立つ．とくに $m = p$ (素数) に対しては, $(a,\ p) = 1$ のとき

$$a^{p-1} \equiv 1 \pmod{p} \tag{33}$$

が成り立つ．これを**フェルマの定理**という.

証明　m を法とする既約類の個数は $\varphi(m)$ 個ある．その一組を

$$x_1,\ x_2,\ \cdots,\ x_{\varphi(m)}$$

とする．このとき

$$ax_1,\ ax_2,\ \cdots,\ ax_{\varphi(m)}$$

もまた一組の既約剰余系である．なぜなら $(a,\ m) = 1$ より

$$x \equiv y \pmod{m} \quad \Longleftrightarrow \quad ax \equiv ay \pmod{m}$$

であるから x が剰余系なら ax も剰余系である．つまり x と m を法として合同な整数の集合とすれば，その集合の要素にすべて a を乗じた整数の集合は確かに ax と合同な整数の全体なっており, ax も剰余系である．さらに x が m と互いに素なら ax も m と互いに素なので，既約剰余系からは既約剰余系が得られることもわかる.

したがって二つの数の集合

$$\{x_1,\ x_2,\ \cdots,\ x_{\varphi(m)}\} \quad と \quad \{ax_1,\ ax_2,\ \cdots,\ ax_{\varphi(m)}\}$$

の各要素は m を法として互いに合同なものが一対一に対応している.

その積は m を法として互いに合同である．つまり

$$\begin{aligned} x_1x_2\cdots x_{\varphi(m)} &\equiv ax_1ax_2\cdots ax_{\varphi(m)} \pmod{m} \\ &\equiv a^{\varphi(m)}x_1x_2\cdots x_{\varphi(m)} \pmod{m} \end{aligned}$$

$(x_1x_2\cdots x_{\varphi(m)},\ m) = 1$ であるから

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

である．オイラーの定理 (32) が示された.

$m = p$ なら $\varphi(p) = p - 1$ であるから，オイラーの定理の特別な場合としてフェルマの定理 (33) が成り立つ. ■

例 8.1

$$\begin{array}{lll}
\varphi(5)=4 & 13^4\equiv 1 \pmod 5 & 13^4-1=5\times 5712 \\
\varphi(5)=4 & 11^4\equiv 1 \pmod 5 & 11^4-1=5\times 2928 \\
\varphi(11)=10 & 2^{10}\equiv 1 \pmod{11} & 2^{10}-1=11\times 93 \\
\varphi(12)=5 & 5^5\equiv 1 \pmod{12} & 5^5-1=12\times 52 \\
\varphi(60)=60\left(1-\dfrac{1}{2}\right) & & \\
\times\left(1-\dfrac{1}{3}\right)\left(1-\dfrac{1}{5}\right)=16 & 7^{16}\equiv 1 \pmod{60} & 7^{16}-1=(7-1)(7+1) \\
 & & \times(7^2+1)(7^4+1)(7^8+1)
\end{array}$$

上の例で 13 の場合は 4 乗して初めて $1 \pmod 5$ となるが，11 の場合は 2 乗した段階ですでに $1 \pmod 5$ である．

a のべきの中で $a^e \equiv 1 \pmod m$ となる最小の e を a **の法** m **に関する指数**という．

定理 24

a の法 m に関する指数を e とする．このとき $a^k \equiv 1 \pmod m$ となったとすれば k は e の倍数である．特に $\varphi(m)$ は e の倍数である．逆にいうと法 m に関する指数となりうるのは $\varphi(m)$ の約数にかぎる．

証明 k を e で割った商を q，余りを r とする．

$$1 \equiv a^k = a^{eq+r} \equiv a^r \pmod m$$

ここで $0 \leqq r < 1$ であるが，もし $r \neq 0$ なら $a^r \equiv 1 \pmod m$ となる正の整数 r があることになり e の最小性に反する．ゆえに $r = 0$．つまり k は e の倍数である． ■

練習問題 8.1 (解答 31) ［奈良女子大改題］

(1) 素数 p と $1 \leqq r \leqq p-1$ なる整数 r に対して, 二項係数のについての等式 $r\,{}_p\mathrm{C}_r = p\,{}_{p-1}\mathrm{C}_{r-1}$ を証明し, ${}_p\mathrm{C}_r$ は p の倍数であることを示せ.

(2) 素数 p に対して 2^p を p で割った余りを求めよ.

(3) 自然数 n に対して n^p を p で割った余りを推測し, 数学的帰納法で証明せよ.

練習問題 8.2 解答 32) a の法 m に関する指数を e とする．整数 a^k の指数は $\dfrac{e}{(k,\ e)}$ である．

8.2 素数分布論への応用

自然数を大きさの順に 1, 2, 3, $\cdots$ と並べたなかに素数がどのような法則にしたがって分布しているのか? これは極めて難しい問題である．4 節『素数』の冒頭にも述べたように多くの問題が未解決である．そのなかで素数の分布に関する著しい大定理を紹介し，フェルマの小定理の応用として，特別な場合を証明しよう．

算術級数の定理 (ディリクレの定理)

初項 $a(>0)$ と公差 $d(>0)$ がともに自然数でかつ互いに素であるような算術級数 (無限等差数列) の項の中には素数が無数に存在する.

算術級数の定理を完全に証明したのはディリクレ (Dirichlet) である (1837). この定理の証明は難しい. 級数の理論を整数問題に応用する『解析的整数論』の発端となった. ここで $a=1$ の場合について証明をしよう.

定理 25
m を任意の自然数とする. $mt+1$ 型の素数が無限に存在する.

証明
【1】 $4n-1$ **型の素数が無数にある**ことを示す.
$4n-1$ 型の素数が有限個しかないとし, その最大のものを p とする. $4n-1$ 型の素数すべての積に 4 をかけ 1 を減じた数を a とする. つまり

$$a = 4(3\cdot 7\cdot 11\cdot\cdots\cdot p) - 1$$

a が素数なら, これが p より大きい $4n-1$ 型の素数である.
a は合成数とする. a は 4 で割ると -1 余るので奇数である. したがってその約数はすべて奇数であるから, 4 で割って 1 または -1 余る. $4k+1$ 型の数をいくらかけても $4k+1$ 型の数になるので, $4n-1$ 型の数の約数の中には必ず $4n-1$ 型の数がある. したがって a が合成数ならその素因数の中に $4n-1$ 型のものがある.
ところがこれは 3 から p の $4n-1$ 型の素数のいずれとも互いに素であるから, それより大きい. したがって p が $4n-1$ 型の素数の最大のものであることと矛盾した. つまり $4n-1$ 型の素数が無数にあることが示された.

【2】 $4n+1$ **型の素数が無数にある**ことを示す.
$4n+1$ 型の素数が無数にあることは簡単ではない. その証明にはフェルマの小定理が必要である. フェルマの小定理を応用して $4n+1$ 型の素数が無数にあることを証明しよう.
その基本となる事実は, x^2+1 の形をした数の素因数は 2 かまたは $4n+1$ 型の素数にかぎる, ということである. いくつか調べてみると

$$1^2+1=2,\ 2^2+1=5,\ 3^2+1=2\cdot 5,\ 4^2+1=17,\ 5^2+1=2\cdot 13,\ 6^2+1=37,\ \cdots$$

で確かにそうなっている.
つねに成立することは, 次のように示される.
x^2+1 が 2 以外の素数 p で割り切れるとする.

$$x^2+1 \equiv 0 \pmod{p}$$

つまり

$$x^2 \equiv -1 \pmod{p}$$

ゆえに

$$x^4 \equiv 1 \pmod{p}$$

ところが x の指数は 4 である．そうでなければ 4 の約数の 1 か 2 の指数で

$$x \equiv 1 \pmod{p} \quad , \text{または} \quad x^2 \equiv 1 \pmod{p}$$

いずれからも $x^2 + 1 \equiv 0 \pmod{p}$ とあわせて

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

となる． $p \neq 2$ なのでこれはあり得ない．したがって定理 24 により， $p - 1$ は 4 の倍数である．これを $p - 1 = 4n$ とすれば

$$p = 4n + 1$$

この事実の応用として $4n + 1$ 型の素数が無数にあることが示される．

$4n + 1$ 型の素数が有限個しかないとする．その最大のものを p とし，2 とそれら $4n + 1$ 型の素数すべての積の平方に 1 を加えた数を a とする．つまり

$$a = (2 \cdot 5 \cdot 13 \cdot \cdots \cdot p)^2 + 1$$

このとき，もし a が素数なら $a = 4(5 \cdot 13 \cdot \cdots \cdot p)^2 + 1$ より $4n + 1$ 型の素数である．

もし合成数ならその素因数 q は奇数であるから 2 ではなく $4n + 1$ 型の素数である．しかし a は p までの $4n + 1$ 型の素数では割り切れないから，q は p より大きい $4n + 1$ 型の素数である．

つまり p が $4n + 1$ 型の素数で最大のものであることに反した．ゆえに $4n + 1$ 型の素数が無数にあることが示された．

【3】　$mt + 1$ 型の素数は無数に存在することを示す．

m を 2 以上の任意の整数とする．初項が 1 で公差が m の等差数列の中に無数の素数が存在している．

この証明は， $m = 4$ の場合つまり $4n + 1$ 型の素数が無数に存在することの証明を一般化することで得られる．$4n + 1$ 型の素数が無数に存在することの証明に現れた $x^2 + 1$ は何か．それは定理 19 の $F_4(x)$ に他ならない．1 の原始 4 乗根 $\pm i$ のみを根とする多項式である．

そこで与えられた m に対して $F_m(x)$ を考えよう．まず a を任意の整数として $F_m(a) \neq \pm 1$ のとき $F_m(a)$ の素因数は m の約数，または $mt + 1$ の型のものにかぎられことを示さなければならない．定理 22 によって次の等式が成り立つ．

$$x^m - 1 = F_m(x)G(x)$$

ここで $G(x)$ は x の整数係数の整式である．ゆえに

$$a^m - 1 = F_m(a)G(a)$$

において， $F_m(a)$, $G(a)$ は整数であるから，いま素数 p を $F_m(a)$ の素因数とすれば， $a^m - 1$ も p の倍数である．つまり

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

a の指数を e とする．定理 21 から e は m の約数で

$$m = ef$$

とおける．ここで $m > e$ とすれば $x^m - 1$ は $x^e - 1$ を因数にもつが，一方 $x^e - 1$ と $F_m(x)$ は共通因数をもたないので ($F_m(x)$ の根は m 乗してはじめて 1 となるものであるから)

$$x^m - 1 = (x^e - 1)F_m(x)H(x)$$

ここで $G(x) = (x^e - 1)H(x)$ が整数係数なので $H(x)$ も整数係数の整式である．両辺を $x^e - 1$ で割る．

$$x^{e(f-1)} + x^{e(f-2)} + \cdots + x^e + 1 = F_m(x)H(x)$$

$x = a$ を代入して $a^e \equiv 1 \pmod{p}$ を用いれば

$$f \equiv F_m(a)H(a) \equiv 0 \pmod{p}$$

ゆえに p は f の約数，したがって $m = ef$ の約数である．

次に $m = e$ なら m が a の指数であるから m は $p-1$ の約数である．つまり $p = mt+1$ と書ける．ゆえに，$F_m(a) \neq \pm 1$ のとき $F_m(a)$ の素因数は m の約数，または $mt + 1$ の型のものであることが示せた．特に a を m に含まれるすべての素因数の積の倍数とすれば， $a^m \equiv 1 \pmod{p}$ より $(a,\ p) = 1$ なので p は m の約数ではあり得ない．したがってこのような a をとるなら p は必ず $mt + 1$ の型の素数である．

例えば $m = 12$ とする．

$$x^{12} - 1 = (x^6 - 1)(x^6 + 1) = (x^6 - 1)(x^2 - 1)(x^4 + x^2 + 1)$$

で $F_{12}(x) = x^4 + x^2 + 1$ ． $a = 6$ とすると

$$F_{12}(6) = 6^4 - 6^2 + 1 = 1261 = 13 \times 97$$

で

$$13 \equiv 1,\ 97 \equiv 1 \pmod{12}$$

$F_m(a) \neq \pm 1$ を仮定しているが，$F_m(a) = \pm 1$ となる a はもちろん有限個なのでそれ以外の a はをとればよい．ゆえに任意の整数 m に対して $mt + 1$ 型の素数が存在することが示された．

もし $mt + 1$ 型の素数が有限個しかなければ，最大のものを $p = mt + 1$ とする．

m は任意なので m の代わりに mp をとると $p' = mpt + 1$ 型の素数もまた存在する．ところが p' は $mt + 1$ 型の素数でもありしかも p より大きい．したがって p の最大性と矛盾するので，$mt + 1$ 型の素数は無数に存在する． ■

次の練習問題と演習問題は,『めざせ，数学オリンピック』(J. コフマン，現代数学社) に教えられた．

練習問題 8.3 (解答 33)　因数分解

$$x^{2k+1} + 1 = (x + 1)(x^{2k} - x^{2k-1} + x^{2k-2} - \cdots - a + 1)$$

を活用して，任意の自然数 n に対して $(n!)^2 + 1$ の素因数はすべて $4n + 1$ 型の素数であることを示せ．これから $4n + 1$ 型の素数が無数にあることを示せ．

8.3 循環小数

既約分数を小数表示すると，有限小数かまたは循環小数になる．循環節の長さはフェルマの小定理によって決定される．

定理 26
$\frac{m}{n}$ は既約真分数で分母 n は $(10,\ n)=1$ とする．このとき $\frac{m}{n}$ は循環小数に展開され，循環節の桁数を e とすれば, e は

$$10^e \equiv 1 \pmod{n}$$

となる最小の正整数である． e は $\varphi(n)$ の約数で, n のみによって定まる．

証明 今

$$10^e - 1 = n \cdot a$$

とおく．このとき

$$\begin{aligned} \frac{m}{n} &= \frac{ma}{na} = \frac{ma}{10^e - 1} \\ &= \frac{ma}{10^e} + \frac{ma}{10^{2e}} + \frac{ma}{10^{3e}} + \cdots \end{aligned}$$

仮定から $m < n$ なので $ma < na < 10^e$ ．ゆえに確かに $\frac{m}{n}$ は循環節の桁数 e の循環小数に展開されている．

逆に $\frac{m}{n}$ が e 桁の循環節 c をもつ循環小数なら

$$\frac{m}{n} = \frac{c}{10^e} + \frac{c}{10^{2e}} + \frac{c}{10^{3e}} + \cdots = \frac{c}{10^e - 1}$$

m と n は互いに素なので $10^e - 1 = na,\ c = ma$ となり

$$10^e \equiv 1 \pmod{n}$$

最小性は循環節の桁数の定義，つまりくりかえす最短の桁数，より明か． ■

$(10,\ n) = 1$ でないときはどうなるか．このとき $n = 2^u 5^v n'$ とおく．u と v の小さくない方を k とする． $k = max(u,\ v)$ ．そして $\frac{10^k m}{n}$ を約分して既約分数 $\frac{m'}{n'}$ を得るとする．すると $(10,\ n') = 1$ である． 10 の n' を法とする指数を e とすれば， $\frac{m'}{n'}$ は e 方の循環節をもつ循環小数になる．なお $n' = 1$ になればこれは有限小数である．

この定理は実例によって納得するのがよい．

例 8.2 $n = 7$ とする．

$$\begin{aligned} &10^1 \equiv 3 \pmod{7},\ 10^2 \equiv 2 \pmod{7},\ 10^3 \equiv 6 \pmod{7}, \\ &10^4 \equiv 4 \pmod{7},\ 10^5 \equiv 5 \pmod{7},\ 10^6 \equiv 1 \pmod{7} \end{aligned}$$

10 の法 7 に対する指数 e は 6 である．つまり 10 は素数 7 の原始根である．

循環小数の作られ方を詳しく見てみよう.

$$\begin{aligned}
10^1 &= 3+7\cdot 1\\
10^2 &= 2+7\cdot 14\\
10^3 &= 6+7\cdot 142\\
10^4 &= 4+7\cdot 1428\\
10^5 &= 5+7\cdot 14285\\
10^6 &= 1+7\cdot 142857
\end{aligned}$$

$$\begin{aligned}
\therefore\ \frac{1}{7} &= \frac{142857}{10^6-1}\\
&= \frac{142857}{10^6}\left\{1+\frac{1}{10^6}+\frac{1}{10^{12}}+\cdots\right\}\\
&= 0.\dot{1}42857\dot{1}
\end{aligned}$$

以下は上の 7 で割った余りと商を用いて作られる.

$$\begin{aligned}
\frac{3}{7} &= \frac{10^1}{7}-1 &&= 0.\dot{4}28571\dot{4}\\
\frac{2}{7} &= \frac{10^2}{7}-14 &&= 0.\dot{2}85714\dot{2}\\
\frac{6}{7} &= \frac{10^3}{7}-142 &&= 0.\dot{8}57142\dot{8}\\
\frac{4}{7} &= \frac{10^4}{7}-1428 &&= 0.\dot{5}71428\dot{5}\\
\frac{5}{7} &= \frac{10^5}{7}-14285 &&= 0.\dot{7}14285\dot{7}
\end{aligned}$$

このうち $\dfrac{6}{7}$ はじつは

$$\frac{6}{7}+\frac{1}{7}=1=0.\dot{9}\quad \text{より}\quad 0.\dot{9}-0.\dot{1}42857\dot{1}=0.\dot{8}57142\dot{8}$$

としても求まる.

例 8.3　$n=13$ とする. 10^7 以降は不要であるが書く.

$$\begin{aligned}
10^1 &= 10+13\cdot 0\\
10^2 &= 9+13\cdot 07\\
10^3 &= 12+13\cdot 076\\
10^4 &= 3+13\cdot 0769\\
10^5 &= 4+13\cdot 07692\\
10^6 &= 1+13\cdot 076923\\
10^7 &= 10+13\cdot 0769230\\
10^8 &= 9+13\cdot 07692307\\
10^9 &= 12+13\cdot 076923076
\end{aligned}$$

$$
\begin{aligned}
10^{10} &= 3 + 13 \cdot 0769230769 \\
10^{11} &= 4 + 13 \cdot 07692307692 \\
10^{12} &= 1 + 13 \cdot 076923076923
\end{aligned}
$$

10 の法 13 に対する指数 e は 6 である.

$$
\begin{aligned}
\therefore \quad \frac{1}{13} &= \frac{076923}{10^6 - 1} \\
&= \frac{076923}{10^6} \left\{ 1 + \frac{1}{10^6} + \frac{1}{10^{12}} + \cdots \right\} \\
&= 0.\dot{0}76923\dot{}
\end{aligned}
$$

これから次の循環小数ができる.

$$
\begin{aligned}
\frac{10}{13} &= \frac{10^1}{13} - 0 &&= 0.\dot{7}69230\dot{} \\
\frac{9}{13} &= \frac{10^2}{13} - 07 &&= 0.\dot{6}92307\dot{} \\
\frac{12}{13} &= \frac{10^3}{13} - 076 &&= 0.\dot{9}23076\dot{} \\
\frac{3}{13} &= \frac{10^4}{13} - 0769 &&= 0.\dot{2}30769\dot{} \\
\frac{4}{13} &= \frac{10^5}{13} - 07692 &&= 0.\dot{3}07692\dot{}
\end{aligned}
$$

これ以外のものは次の式から出る.

$$
\begin{aligned}
2 \cdot 10^1 &= 7 + 13 \cdot 1 \\
2 \cdot 10^2 &= 5 + 13 \cdot 15 \\
2 \cdot 10^3 &= 11 + 13 \cdot 153 \\
2 \cdot 10^4 &= 6 + 13 \cdot 1538 \\
2 \cdot 10^5 &= 8 + 13 \cdot 15384 \\
2 \cdot 10^6 &= 2 + 13 \cdot 153846
\end{aligned}
$$

つまり

$$
\begin{aligned}
\frac{7}{13} &= \frac{2 \cdot 10^1}{13} - 1 &&= 0.\dot{5}38461\dot{} \\
\frac{5}{13} &= \frac{2 \cdot 10^2}{13} - 15 &&= 0.\dot{3}84615\dot{} \\
\frac{11}{13} &= \frac{2 \cdot 10^3}{13} - 153 &&= 0.\dot{8}46153\dot{} \\
\frac{6}{13} &= \frac{2 \cdot 10^4}{13} - 1538 &&= 0.\dot{4}61538\dot{} \\
\frac{8}{13} &= \frac{2 \cdot 10^5}{13} - 15384 &&= 0.\dot{6}15384\dot{} \\
\frac{2}{13} &= \frac{2 \cdot 10^5}{13} - 153846 &&= 0.\dot{1}53846\dot{}
\end{aligned}
$$

練習問題 8.4 (解答 34)　$n = 91 = 7 \cdot 13$ のとき, $\frac{1}{91}$ から $\frac{90}{91}$ を循環節が同じもので分類せよ.

8.4 演習問題

演習問題 28（解答 28） 歴史的に有名なウイルソンの定理，ライプニッツの定理を次の順に証明せよ．

(1) $f(x)$ を整数係数の n 次多項式とし p を素数とする．このとき， $f(x)$ の最高次の係数が p の倍数でないとすると，

$$f(0),\ f(1),\ \cdots,\ f(p-1)$$

のうちで， p の倍数となるものは， n 個以下であることを n に関する数学的帰納法で示せ．

(2) $f(x)$ を整数係数の n 次多項式とし p を素数とする．このとき，

$$f(0),\ f(1),\ \cdots,\ f(p-1)$$

のうちに， p の倍数となるものが $n+1$ 個以上あれば $f(x)$ の係数はすべて p の倍数であることを示せ．

(3) 任意の素数 p について，$(p-1)!+1$ は p で割り切れることを示せ．

[ヒント] 必要なら $f(x)=(x-1)(x-2)\cdots(x-p+1)-x^{p-1}+1$ を用いよ．

(4) 自然数 $p>2$ について，

$$p \text{ が素数} \quad \Longleftrightarrow \quad (p-2)!-1 \text{ が } p \text{ の倍数}$$

を示せ．

9　原始根と指数

9.1　原始根

13 を法とする剰余系から 0 を除いた各剰余のべきを縦方向に順次書いてみる．1 が出ればそこからは同じことがくり返される．それは省略している．

剰余 a	1	2	3	4	5	6	7	8	9	10	11	12
a^2		4	9	3	12	10	10	12	3	9	4	1
a^3		8	1	12	8	8	5	5	1	12	5	
a^4		3		9	1	9	9	1		3	3	
a^5		6		10		2	11			4	7	
a^6		12		1		12	12			1	12	
a^7		11				7	6				2	
a^8		9				3	3				9	
a^9		5				5	8				8	
a^{10}		10				4	4				10	
a^{11}		7				11	2				6	
a^{12}	1	1	1	1	1	1	1	1	1	1	1	1

フェルマの定理によれば p が素数で, a が p で割り切れないとき,

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

である．したがって a^{12} の段に 1 が並ぶのは当然であるが，2，6，7，11 は 12 乗してはじめて 1 と合同であり，しかも途中の $1,\ a,\ a^2,\ \cdots,\ a^{11}$ が 13 を法とする既約剰余系の代表の組となっている．p が素数の場合，既約でない剰余系は 0 のみである．そこで a が $p-1$ 乗してはじめて 1 と合同になるとき，a を p を法としての**原始根**という．略して p の原始根ともいう．

さて「原始根」という呼び名はすでに第 7 節「1 の n 乗根」で出ている．複素数全体の中で n 乗してはじめて 1 になるものを「1 の原始 (n 乗) 根」と呼んだ．今は p を法とする剰余の集合

$$K = \{0,\ 1,\ 2,\ \cdots,\ p-1\}$$

のなかで, $p-1$ 乗してはじめて 1 と合同になるものを考えている．この場合，p を法とする剰余系の代表として数 a が e 乗して 1 と合同になるなら，e は $p-1$ の約数である．はじめて 1 と合同になるとき e は a の (p を法とする) 指数というのであった．指数が $p-1$ となる場合にそれを原始根というのである．

ちなみに「群，体」の意味を知っている人のために注意すれば，上の集合 K は p 個の要素からなる有限集合であるが，立派に和・差・積・商が定まる．いわゆる「体」である．また K から 0 を除いた $K^\times$ は乗法に関して $p-1$ 個の要素からなる「群」である．

次の定理が示すように原始根の順次のべきからから, $K^\times$ のすべての要素が得られる．つまり, 原始根はこの「群を生成する」要素であるともいえる．

定理 27

素数 p を法として原始根が存在する．r をその一つとすれば,

$$1,\ r,\ r^2,\ \cdots,\ r^{p-2}$$

は既約剰余系の一組である．

証明　a を p を法とする既約剰余系の一つの代表である数とする．言いかえれば $a \not\equiv 0 \pmod{p}$ をとる． a の指数を m とする．$a^m \equiv 1 \pmod{p}$ なので

$$a^0 = 1,\ a^1,\ \cdots,\ a^{m-1} \tag{34}$$

はいずれも

$$x^m \equiv 1 \pmod{p} \tag{35}$$

の解である．これらは互いに同じ剰余系に属さない．なぜなら, $1 \leqq i \leqq m-1$ に対して

$$a^i \equiv a^j \pmod{p} \quad \Longleftrightarrow \quad a^{i-j} \equiv 1 \pmod{p}$$

である．定理 24 から $i-j$ は m の倍数である．$-m+2 \leqq i-j \leqq m-2$ なのでこれは $i=j$ のときのみである．定理 14 から (34) が (35) の解のすべてである．

さて $m = p-1$ なら a 自身が原始根である．$m < p-1$ のとき．a をもとに m より大きい指数の数を構成できることを示す.

p を法とする既約剰余系は $p-1$ 個あるので，この場合 (34) のいずれとも異なる剰余系がある．そのような剰余系に属する数 b をとる． b の指数を n とする．このとき n は m の約数でない．もし約数なら $b^m \equiv 1 \pmod{p}$ となる．したがって b も合同方程式 (35) の解となり b に関する仮定に反する．そこで

(1) $(m,\ n) = 1$ のとき． ab の指数は mn である.

なぜなら，まず $(ab)^{mn} = a^{mn}b^{mn} \equiv 1 \pmod{p}$ であるが，逆に $(ab)^x \equiv 1 \pmod{p}$ とする．このとき

$$(ab)^{mx} \equiv b^{mx} \equiv 1 \pmod{p}$$

定理 21 から mx は n の倍数であるが $(m,\ n) = 1$ から x が n の倍数である.

同様に x は m の倍数でもあり， 定理 3 から x は m と n の最小公倍数の倍数である．$(m,\ n) = 1$ から最小公倍数は mn ．ゆえに ab の指数は mn である．$mn > m$ より p を法として m より大きい指数の数が構成できた.

(2) $(m,\ n) = d > 1$ のとき．m と n の最小公倍数を l とする．このとき $l = m_0 n_0,\ (m_0,\ n_0) = 1$ で m_0 は m の約数，n_0 は n の約数となるものをとる．これはかならずできる．d を互いに素な積 $d = d_1 d_2$ に分け (一方が 1 でもよい)

$$m_0 = \frac{md_1}{d},\ n_0 = \frac{nd_2}{d}$$

とすればよい．このとき $a^{\frac{m}{m_0}},\ b^{\frac{n}{n_0}}$ はそれぞれ指数が $m_0,\ n_0$ である．$(m_0,\ n_0) = 1$ より $a^{\frac{m}{m_0}},\ b^{\frac{n}{n_0}}$ の指数は $m_0 n_0 = l$．n は m の約数ではないので $l > m$ ．やはり p を法として m より大きい指数の数が構成できた.

真に増加する指数の列ができ，しかも $p-1$ を越えないので有限回の操作で必ず指数 $p-1$ の数が構成できる．つまり原始根 r は必ず存在する．すでに見たように (34) は互いに合同でない．したがって

$$1\ ,\ r,\ r^2,\ \cdots,\ r^{p-2}$$

も互いに合同でない．つまりこれらは $p-1$ 個の既約剰余系の一組の代表である． ■

既約剰余系でみれば $(k,\ p-1) = 1$ であることが r^k が原始根であるための必要十分条件である．したがって原始根は $\varphi(p-1)$ 個ある.

例 9.1　$\varphi(13-1)=4$ なので四つある．実際 2, 6, 7, 11

練習問題 9.1 (解答 35)　$p=41$ 法とする原始根を一つ求めよ．

9.2 指数

定理 27 に述べたように r を p の原始根とすれば $a \not\equiv 0 \pmod{p}$ である任意の整数 a に対して

$$r^{\alpha} \equiv a \pmod{p}$$

となる整数 α が $0 \leqq \alpha < p-1$ の範囲に必ず，しかもただ一つ存在する．この α を r を底としての a の**指数**(index) といい，それを次のように表す．

$$\mathrm{Ind}_r(a) = \alpha$$

指数 α を $0 \leqq \alpha < p-1$ の範囲にかぎる必要はない．一般に

$$r^{s} \equiv a \pmod{p}$$

ならば

$$s \equiv \alpha \pmod{p-1}$$

この s なども指数とすれば, a の指数は $p-1$ を法として一意に定まる．

$$\mathrm{Ind}_r(a) \equiv s \pmod{p-1}$$

$a \equiv b \pmod{p}$ であることと，$\mathrm{Ind}_r(a) \equiv \mathrm{Ind}_r(b) \pmod{p-1}$ であることは同値である．

したがって指数を次のように定義することもできる．

r を p の原始根とすれば p を法とする 0 でない任意の剰余系の代表である整数 a に対して

$$r^{\alpha} \equiv a \pmod{p}$$

となる α が $p-1$ を法としてただ一つ存在する．つまり α は $p-1$ を法とする剰余系の代表となる．この剰余系を r を底としての a の「指数」といい，それを $\mathrm{Ind}_r(a)$ と表す．

意味が明白なときは等号で表す．また「$\mathrm{Ind}_r(a)$ の値」というときは，厳密には $p-1$ を法とする剰余系の一つを指すが，その剰余系のある代表値で表すこともする．底が定まっているときは省略して $\mathrm{Ind}\,.a$ とも記すことにする．

例 9.2　$p=13$ のとき．2 は原始根である．p を法とする剰余系の数 a に対する底 2 の指数 $I=\mathrm{Ind}\,.a$ は，この節の冒頭の表より次のようになる．

a	1	2	3	4	5	6	7	8	9	10	11	12
I	0	1	4	2	9	5	11	3	8	10	7	6

(36)

定理 28

素数 p を法として原始根 r を底とするとき,

$$\begin{aligned}&\mathrm{Ind}\,.ab \equiv \mathrm{Ind}\,.a + \mathrm{Ind}\,.b,\\ &\mathrm{Ind}\,.a^n \equiv n\,\mathrm{Ind}\,.a\ .\end{aligned} \qquad (\mathrm{mod}.\ p-1)$$

証明　$\mathrm{Ind}\,.a = \alpha,\ \mathrm{Ind}\,.b = \beta$ とする．つまり

$$a \equiv r^{\alpha}, \quad b \equiv r^{\beta} \qquad (\mathrm{mod}.\ p)$$

ゆえに

$$ab \equiv r^{\alpha+\beta} \quad (\mathrm{mod}.\ p)$$

$$\therefore \quad \mathrm{Ind}\,.ab \equiv \alpha+\beta \equiv \mathrm{Ind}\,.a + \mathrm{Ind}\,.b \quad (\mathrm{mod}.\ p-1)$$

また

$$\mathrm{Ind}\,.a^n = \mathrm{Ind}\,.a \cdot a^{n-1} \equiv \mathrm{Ind}\,.a + \mathrm{Ind}\,.a^{n-1} \quad (\mathrm{mod}.\ p-1)$$

より，帰納法で

$$\mathrm{Ind}\,.a^n \equiv n\,\mathrm{Ind}\,.a \quad (\mathrm{mod}.\ p-1)$$

となる．　■

『初等整数論講義』によれば，Jacobi は『Canon arithmeticus』(1839) において 1000 以下の素数を法とする指数を計算している．Jacobi は計算を楽しんだのだろう．そして Cunninghana という人がこの Jacobi の表の検算をおこない，正誤表が数学雑誌「Messenger of methematics, 46 巻」(1916) に載っているそうである．

例 9.3　$p = 13$ のとき．$7x \equiv 10 \pmod{13}$ を解こう．

$$\mathrm{Ind}\,.7 + \mathrm{Ind}\,.x \equiv \mathrm{Ind}\,.10 \quad (\mathrm{mod}.\ 12)$$

指数表から

$$11 + \mathrm{Ind}\,.x \equiv 10 \quad (\mathrm{mod}.\ 12)$$

$$\therefore \quad \mathrm{Ind}\,.x \equiv -1 \equiv 11 \quad (\mathrm{mod}.\ 12)$$

指数表から $x \equiv 7 \pmod{13}$.

指数の理論の応用として，合同方程式の解の存在に関する次の定理を得る．

定理 29

p を素数とし, $a \not\equiv 0 \pmod{p}$ とする．

二項合同方程式

$$x^n \equiv a \quad (\mathrm{mod}.\ p)$$

に解があるための必要十分条件は $f = \dfrac{p-1}{(n,\ p-1)}$ とするとき

$$a^f \equiv 1 \quad (\mathrm{mod}.\ p)$$

である．

証明　$x^n \equiv a \pmod{p}$ を解くには p を法とする原始根 r をとって

$$n \cdot \mathrm{Ind}_r\, x \equiv \mathrm{Ind}_r\, a \pmod{p-1} \tag{37}$$

を解けばよい．今 $(n,\ p-1) = e$ とする．定理 12 から，この合同方程式 37 が解を有するための必要十分条件は, $\mathrm{Ind}_r\, a$ が e で割り切れることである．$\mathrm{Ind}_r\, a = \alpha$ とすると, α が e で割り切れるとき，$\alpha = eq$ とおけば,

$$a \equiv r^{eq} \pmod{p}$$

$$\therefore \quad a^f \equiv r^{efq} = r^{(p-1)q} \equiv 1 \pmod{p}$$

逆に $a^f \equiv 1 \pmod{p}$ ならば，$r^{f\alpha} \equiv 1 \pmod{p}$ ．ゆえに $f\alpha$ は $p-1 = ef$ で割りきれる．つまり α が e で割りきれ，二項合同方程式は解をもつ．解があるとき解の数は $e = (n,\ p-1)$ 個である．　■

この定理は今日では，有限群 $K^\times$ がただ一つの元 (原始根) で生成される巡回群であること，およびその巡回群に関する二，三の補題で示される．ここでは『初等整数論講義』にしたがって，整数論らしい証明をおこなっている．

合同方程式 $x^n \equiv a \pmod{p}$ が解があるかないかにしたがって a を p の 「n **べき剰余**」，または「**非剰余**」という．もちろん，べき剰余か非べき剰余かは，同じ剰余系に属する二数では同じである．つまりべき剰余か非べき剰余かは p を法とする剰余系に関することである．0 はつねに n べき剰余である．$a \not\equiv 0 \pmod{p}$ である a について言えば，$(n,\ p-1) = 1$ のとき任意の a が n べき剰余である．$(n,\ p-1) = e > 1$ のときは, $\mathrm{Ind}\,.a$ が e の倍数となる a だけが n べき剰余である．$p-1 = ef$ とおけば，指数が $0,\ e,\ 2e,\ \cdots,\ (f-1)e$ となる数が n べき剰余である．したがって n べき剰余は p を法として $p-1$ 個の既約剰余類のなかの $f = \dfrac{p-1}{e}$ 個だけある．

例 9.4　$n = 2,\ p = 7$ とする．$e = 2,\ f = 3$ である．

実際，既約剰余系

$$1,\ 2,\ \cdots,\ 6$$

のうち，2 べき剰余 (平方剰余) は

$$1,\ 4,\ 2$$

の 3 個である．

練習問題 9.2 (解答 36)　表 9.2 を活用して $p = 13,\ r = 2$ のとき．次のものを求めよ．

(1) $\mathrm{Ind}\,.100$ の値

(2) $\mathrm{Ind}\,.(-1)$ の値

(3) $\mathrm{Ind}\,.x = 9$ となる x の値

(4) $\mathrm{Ind}\,.x = -1$ となる x の値

練習問題 9.3 (解答 37)　表 9.2 を活用して x を求めよ．

(1) $11x \equiv 5 \pmod{13}$

(2) $x^3 \equiv 5 \pmod{13}$

(3) $5x^2 + 3x - 10 \equiv 0 \pmod{13}$

練習問題 9.4 (解答 38)　$p \neq 2$ とする．底の取り方に関係なく，

$$\mathrm{Ind}\,.(-1) = \frac{p-1}{2}$$

練習問題 9.5 (解答 39)　$p \neq 2$ とする．　$a + b = p$ ならば

$$\mathrm{Ind}\,.a - \mathrm{Ind}\,.b \equiv \frac{p-1}{2} \pmod{p-1}$$

練習問題 9.6 (解答 40)

$$\mathrm{Ind}_r\ a \equiv \frac{\mathrm{Ind}_{r'}\ a}{\mathrm{Ind}_{r'}\ r} \pmod{p-1}$$

練習問題 9.7 (解答 41)　k が $p-1$ で割りきれないならば

$$1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$$

練習問題 9.8 (解答 42)　p が素数ならば

$$(p-1)! \equiv -1 \pmod{p}$$

(ウイルソンの定理の別証明)

9.3　演習問題

演習問題 29 (解答 29)　［95 京大文系後期］
自然数 n の関数 $f(n),\ g(n)$ を

$$f(n) = n \text{ を } 7 \text{ で割った余り}$$
$$g(n) = 3f\left(\sum_{k=1}^{7} k^n\right)$$

によって定める．

(1) すべての自然数 n に対して $f(n^7) = f(n)$ を示せ．

(2) あなたの好きな自然数 n を一つ決めて $g(n)$ を求めよ．その $g(n)$ の値をこの設問 (2) におけるあなたの得点とする．

10　平方剰余の相互法則

10.1　平方剰余・ルジャンドルの記号

5 を法とする剰余類は 0, 1, 2, 3, 4 であるが，それらの類の数を平方すると剰余類は順に

$$0,\ 1^2 = 1,\ 2^2 = 4,\ 3^2 \equiv 4 \pmod 5,\ 4^2 \equiv 1 \pmod 5$$

となり，2 や 3 は平方数を 5 で割った剰余の中には登場しない．1 や 4 は 5 の平方剰余，2 や 3 は平方非剰余という．

素数 5 に比べて素数 2 は特異である．2 で割った数の剰余類は 0, 1 である．それらの類の数を平方すると剰余類 0, 1 となり変わらない．

以下本節では p は 2 以外の素数とする．$x^2 \equiv a \pmod p$ が解をもつとき a を p の**平方剰余**，解がないとき**平方非剰余**という．$a \not\equiv 0 \pmod p$ である整数 a に対して a が p の平方剰余であるか非剰余であるかにしたがって

$$\left(\frac{a}{p}\right) = +1 \quad \text{または} \quad -1$$

とする．これを**ルジャンドル (Legendre) の記号**という．

p の任意の原始根を底として指数をとるとき，前節の議論から $\mathrm{Ind}\,a$ が偶数なら a は平方剰余，奇数なら非剰余であった．ゆえに

$$\left(\frac{a}{p}\right) = (-1)^{\mathrm{Ind}\,a} \tag{38}$$

ゆえに p に関する $p-1$ 個の既約類の中で半数は平方剰余のみからなり，半数は非剰余のみからなる．$x^2 \equiv (p-x)^2 \pmod p$ なので $1,\ 2,\ \cdots,\ \dfrac{p-1}{2}$ の平方が平方剰余のすべてである．また (38) から次の 2 性質が成り立つ．

(1) $a \equiv a' \pmod p$ ならば $\left(\dfrac{a}{p}\right) = \left(\dfrac{a'}{p}\right)$

(2) $\left(\dfrac{abc\cdots}{p}\right) = \left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)\left(\dfrac{c}{p}\right)\cdots$

これは例えば

$$(\text{非剰余数}) \times (\text{非剰余数}) = (\text{剰余数}),\quad (\text{剰余数}) \times (\text{非剰余数}) = (\text{非剰余数})$$

ということである．実際 $p = 5$ のとき

$$2 \times 3 \equiv 1 \pmod 5,\quad 4 \times 2 \equiv 3 \pmod 5$$

である．

定理 30 (オイラーの規準)

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

証明　a が平方剰余であるための必要十分条件は定理 29 から

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

である.

ゆえに $\left(\dfrac{a}{p}\right) = 1$ ならば, $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ で一致.

また $\left(\dfrac{a}{p}\right) = -1$ ならば, $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. ところがフェルマの小定理から $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$. したがって $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$ でやはり一致する. ■

この証明は, これまでの結果を結びつけただけであるが, より直接的な証明がディリクレの『整数論講義』にある.『初等整数論講義』に従ってそれを紹介する.

ディリクレの別証明

a を p で割り切れない数とし, 集合 A を

$$A = \{\ 1,\ 2,\ 3,\ \cdots,\ p-1\ \}$$

とする. A の任意の要素 r に対して

$$rs \equiv a \pmod{p}$$

となる A の要素 s がただ一つ存在する. この s を r の「共役」と呼ぼう.

$\left(\dfrac{a}{p}\right) = 1$ のとき. r を $x^2 \equiv a \pmod{p}$ の解とすれば, r の共役は r 自身である. $p-r$ もまた $x^2 \equiv a \pmod{p}$ の解で, $p-r$ の共役も $p-r$ である. A の要素で $x^2 \equiv a \pmod{p}$ を満たすものは定理 11 からこの二つ (p が奇数なので $p \neq p-r$) にかぎる. この二つを除いた残りの $p-3$ 個は二つずつ互いに共役で, それら $p-3$ 個の積は, $\equiv a^{\frac{p-3}{2}} \pmod{p}$ となる. $r(p-r) \equiv -r^2 \equiv -a \pmod{p}$ なので

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

$\left(\dfrac{a}{p}\right) = -1$ のときは共役と一致する数は A にないので

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

とくに $\left(\dfrac{1}{p}\right) = 1$ なので

$$(p-1)! \equiv -1 \pmod{p}$$

これがウイルソンの定理である.

これをあわせると上記の場合分けは

$$\left.\begin{array}{l} \left(\dfrac{a}{p}\right) = 1 \text{ ならば, } a^{\frac{p-1}{2}} \equiv 1 \\ \left(\dfrac{a}{p}\right) = -1 \text{ ならば, } a^{\frac{p-1}{2}} \equiv -1 \end{array}\right\} \pmod{p}.$$

これがオイラーの規準である．　■

注意 10.1　この証明ではフェルマの小定理を用いていない．$\left(\frac{a}{p}\right) = \pm 1$ にかかわらず，

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

つまりこれはフェルマの小定理の別証になっている．

例 10.1　$p = 5$ のとき．

$$2^2 \equiv 4,\ 2^3 \equiv 3,\ 2^4 \equiv 1,\ 2^2 \equiv 4 \pmod{5}$$

であるから，2 は法 5 に関する原始根であり，

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

一方．$\dfrac{p-1}{2} = 2$ なのでオイラーの規準から

$$\left(\frac{1}{5}\right) \equiv 1,\ \left(\frac{2}{5}\right) \equiv 2^2 \equiv -1,\ \left(\frac{3}{5}\right) \equiv 3^2 \equiv -1 \quad ,\ \left(\frac{4}{5}\right) \equiv 4^2 \equiv 1 \pmod{5}$$

となる．

10.2　整数を平方数の和に分解すること

平方剰余の応用として次の有名な定理を証明しよう．

定理 31

すべての正の整数 n を (0 を含む) 四つの平方数の和として表すことができる．

$$n = {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2 \quad (0 \leqq x_1,\ x_2,\ x_3,\ x_4)$$

証明　次の恒等式

$$\begin{aligned}(x_1{}^2 + x_2{}^2 + x_3{}^2 + x_4{}^2)(y_1{}^2 + y_2{}^2 + y_3{}^2 + y_4{}^2) &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ &+ (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &+ (x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2)^2 \\ &+ (x_1y_4 + x_2y_2 - x_3y_2 - x_4y_1)^2 \quad (39)\end{aligned}$$

によって，四つの平方数の和の積は，再び四つの平方数の和である．従って n が素数 p の場合に証明すれば十分である．

$n = 2$ なら $2 = 1^2 + 1^2$ で成立する．

$n = p > 2$ とする．-1 が p の平方剰余なら

$$x^2 + 1 = ph$$

とおく．

-1 つまり $p-1$ が p の平方非剰余なら $1,\ 2,\ \cdots,\ p-1$ は p の平方剰余 1 から始まって非剰余 $p-1$ に終わる系列なので，そのなかには k は平方剰余であるが, $k+1$ は非剰余であるような k が必ずある．ところがこのとき

$$\left(\frac{-k-1}{p}\right)=\left(\frac{-1}{p}\right)\left(\frac{k+1}{p}\right)=(-1)\cdot(-1)=1$$

であるから

$$\begin{aligned} {x_1}^2 &\equiv k \qquad (\text{mod. } p),\\ {x_2}^2 &\equiv -k-1 \qquad (\text{mod. } p), \end{aligned}$$

となる $x_1,\ x_2$ がある．これは

$${x_1}^2+{x_2}^2+1\equiv 0 \pmod{p}$$

つまり

$${x_1}^2+{x_2}^2+1=ph$$

とおける．

従って一般に素数 p に対して

$${x_1}^2+{x_2}^2+{x_3}^2+{x_4}^2=ph \tag{40}$$

となる $x_1,\ x_2,\ x_3,\ x_4$ と h が存在する．あえて x_4 までとるのは，後の証明で恒等式 (39) を使うからである．

ここで $h>1$ なら $x_1,\ x_2,\ x_3,\ x_4$ を適当な $x_1',\ x_2',\ x_3',\ x_4'$ にとりかえて $1\leqq h'<h$ で

$${x_1'}^2+{x_2'}^2+{x_3'}^2+{x_4'}^2=ph'$$

とできることを示す．これが示されれば, h は正の整数なので有限回の操作の後 $h=1$ にすることができ，題意が示されるからである．

式 (40) における $x_1,\ x_2,\ x_3,\ x_4$ を h で割って絶対値最小の剰余を $y_1,\ y_2,\ y_3,\ y_4$ とする．つまり

$$\begin{aligned} &x_1\equiv y_1,\ x_2\equiv y_2,\ x_3\equiv y_3,\ x_4\equiv y_4 \pmod{h}\\ &|y_i|\leqq\frac{1}{2} \quad ,\ i=1,\ 2,\ 3,\ 4 \end{aligned}$$

従って

$${y_1}^2+{y_2}^2+{y_3}^2+{y_4}^2\equiv {x_1}^2+{x_2}^2+{x_3}^2+{x_4}^2\equiv 0 \pmod{h}$$

である．

$${y_1}^2+{y_2}^2+{y_3}^2+{y_4}^2=hh'$$

とおく．これを式 (39) に代入する．

$${z_1}^2+{z_2}^2+{z_3}^2+{z_4}^2=ph^2h'$$

ただし

$$\begin{aligned} z_1 &\equiv x_1y_1+x_2y_2+x_3y_3+x_4y_4\equiv {x_1}^2+{x_2}^2+{x_3}^2+{x_4}^2\equiv 0 \qquad (\text{mod. } h)\\ z_2 &\equiv x_1y_2-x_2y_1+x_3y_4-x_4y_3\equiv x_1x_2-x_2x_1+x_3x_4-x_4x_3\equiv 0 \quad (\text{mod. } h)\\ z_2 &\equiv x_1y_3-x_2y_4-x_3y_1+x_4y_2\equiv x_1x_3-x_2x_4-x_3x_1+x_4x_2\equiv 0 \quad (\text{mod. } h)\\ z_2 &\equiv x_1y_4+x_2y_2-x_3y_2-x_4y_1\equiv x_1x_4+x_2x_2-x_3x_2-x_4x_1\equiv 0 \quad (\text{mod. } h) \end{aligned}$$

ゆえに

$$z_1 = ht_1,\ z_2 = ht_2,\ z_3 = ht_3,\ z_4 = ht_4$$

とおける．このとき

$$t_1{}^2 + t_2{}^2 + t_3{}^2 + t_4{}^2 = ph'$$

ところが

$$hh' = y_1{}^2 + y_2{}^2 + y_3{}^2 + y_4{}^2 \leqq 4\left(\frac{h}{2}\right)^2$$

ゆえに

$$h' \leqq h$$

ここでもし $h' = h$ とすれば，この等号が成立するのは $y_i = \dfrac{h}{2}$ $(i = 1,\ 2,\ 3,\ 4)$ のときである．このとき $\dfrac{h}{2}$ は整数で

$$x_i = y_i + m_i h = (2m_i + 1)\frac{h}{2}\ (i = 1,\ 2,\ 3,\ 4)$$

となる．これを式 (40) に代入すると，

$$(2m_1+1)^2\frac{h^2}{4} + (2m_2+1)^2\frac{h^2}{4} + (2m_3+1)^2\frac{h^2}{4} + (2m_4+1)^2\frac{h^2}{4} = ph$$

つまり

$$\{(2m_1+1)^2 + (2m_2+1)^2 + (2m_3+1)^2 + (2m_4+1)^2\}\frac{h}{4} = p$$

左辺は $(m_1{}^2 + m_1 + \cdots + m_4{}^2 + m_4 + 1)h$ となるが h が偶数なので p が奇素数であることと矛盾した．

$$\therefore\quad h' < h$$

つまり証明は完成した． ■

10.3　平方剰余の相互法則

2 が法 113 に関する平方剰余であるか，非剰余であるか，つまり $\left(\dfrac{2}{113}\right)$ を決定する方法はあるのか．一般に $\left(\dfrac{p}{q}\right)$ を求める方法は．これは初等整数論の基本問題である．これについてガウスが整数論の基本定理と呼んだ大変美しい定理が成り立つ．それが**平方剰余の相互法則** である．これはこの『初等整数論』全体でもいちばん山場の定理である．ぜひ数学好きの高校生に「平方剰余の相互法則」を理解しその美しさを味わってもらいたい．

定理 32 (平方剰余の相互法則)

$p,\ q$ を相異なる奇素数とする．

(1) **平方剰余の相互法則**：$\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

(2) **第一補充法則**：$\left(\dfrac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

(3) **第二補充法則**：$\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

各法則の意味は次の通りである．

(1) $\dfrac{p-1}{2}$ と $\dfrac{q-1}{2}$ のいずれもが奇数のときにかぎり $(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = -1$ である．ゆえに

$$\begin{aligned} &p \equiv 1 \pmod 4 \text{ または } q \equiv 1 \pmod 4 &&\Longrightarrow \left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \\ &p \equiv q \equiv 3 \pmod 4 &&\Longrightarrow \left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) \end{aligned}$$

(2)

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & (\ p \equiv 1 \pmod 4 \text{ のとき}) \\ -1 & (\ p \equiv 3 \pmod 4 \text{ のとき}) \end{cases}$$

(3)

$$\begin{aligned} \left(\frac{2}{p}\right) = 1 \quad &\Longleftrightarrow \quad p \equiv 1,\ 7 \pmod 8 \\ \left(\frac{2}{p}\right) = -1 \quad &\Longleftrightarrow \quad p \equiv 3,\ 5 \pmod 8 \end{aligned}$$

相互法則はすでにオイラー (Leonhard Euler，1707〜83) が多くの実例から帰納的に発見していた．ルジャンドル (Adrien Marie Legendre，1752〜1833) が定理 32 のような形式で表し，その証明を試みた．彼はその証明の中で，初項と公差が互いに素な無限等差数列 (算術級数) のなかに素数が存在することを，証明なしに用いている．そのため証明は完全ではなかった．

相互法則を最初に完全に証明したのはガウス (Karl Friedrich Gauss，1777〜1855) である．ガウスは相互法則を整数論の基本法則と名づけ，なんと七つのまったく異なる証明を与えた．「ガウスの予備定理」を用いるいちばん初等的な第三の証明法，および「ガウス和」を用いる第四の証明法によって，証明する．

まず「ガウスの予備定理」の証明からはいる．

定理 33 (ガウスの予備定理)

a が p で割り切れないならば

$$1 \cdot a,\ 2 \cdot a,\ 3 \cdot a,\ \cdots,\ \frac{p-1}{2} \cdot a, \tag{41}$$

を p で割るとき，その剰余の中に $\dfrac{p}{2}$ より大きいものが n 個あれば，

$$\left(\frac{a}{p}\right) = (-1)^n$$

例 10.2　$a = 3,\ p = 7$ のとき $\dfrac{p-1}{2} = 3$ で 3, 6, 9 を 7 で割った剰余は 3, 6, 2 である．したがって $n = 1$ で $\left(\dfrac{3}{7}\right) = -1$ ．実際，法 7 に関する平方剰余は 1, 2, 4 であり, 3, 5, 6 が非剰余である．

証明　法 p に関する剰余のうち $\dfrac{p}{2}$ より大きいものについて，それから p を引くと，絶対値において $\dfrac{p}{2}$ より小さい剰余を得る．p を法とする剰余をこのように絶対値で最小になるようにとると, n はそのうち負な剰余の個数である．(41) の数の絶対値最小な剰余は

$$\pm 1,\ \pm 2,\ \cdots,\ \pm\frac{p-1}{2}$$

の中にある．(41) のなかのどの二つの和も差も p では割りきれないので，(41) の絶対値最小剰余はすべて異なるのみでなく，(41) のなかに絶対値が等しいものもない．(41) の $\dfrac{p-1}{2}$ 個の数は絶対値をとると $1,\ 2,\ \cdots,\ \dfrac{p-1}{2}$ と一対一に対応し，そのうち n 個が負である．よって

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

すなわち

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

ゆえにオイラーの規準 (定理 30) から

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

である．ところが両辺とも ± 1 でかつ p が奇数なので

$$\left(\frac{a}{p}\right) = (-1)^n$$

■

定理 32 の証明先に二つの補充則を示さなければならない.

第一補充則の証明.

オイラーの規準を $a=-1$ で用いると得られる.

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

p は奇数であるから

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

あるいはガウスの予備定理を $a=-1$ で用いる．(41) の数は

$$-1,\ -2,\ -3,\ \cdots,\ -\frac{p-1}{2}$$

であるが，これらがすべて絶対値最小剰余である．つまり, $n=\dfrac{p-1}{2}$

$$\therefore\quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

第二補充則の証明.

ガウスの予備定理を $a=2$ で用いる．(41) の数は

$$2,\ 4,\ 6,\ \cdots,\ p-5,\ p-3,\ p-1$$

となる．このうち $\dfrac{p}{2}$ より大きいものの個数が n である． $\dfrac{p}{2}<2k$ は $p-2<\dfrac{p}{2}$ と同値であるから，その個数は $1,\ 3,\ 5\cdots$ のなかの $\dfrac{p}{2}$ より小さいものの個数でもある．$\dfrac{p-1}{2}$ が奇数ならここまで，$\dfrac{p-1}{2}$ が偶数なら $\dfrac{p-1}{2}-1$ までである．いずれにせよ，

$$n\equiv 1+3+\cdots+\left(\frac{p}{2}\text{より小さい奇数}\right)\equiv 1+2+3+\cdots+\frac{p-1}{2}\pmod 2$$

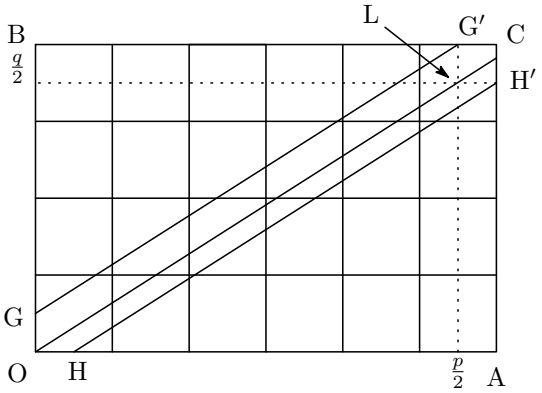
すなわち

$$n\equiv\frac{1}{2}\cdot\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)=\frac{p^2-1}{8}\pmod 2$$

$$\therefore\quad\left(\frac{2}{p}\right)=(-1)^n=(-1)^{\frac{p^2-1}{8}}$$

相互法則の証明.

xy 平面上に点 $\mathrm{A}\left(\dfrac{p+1}{2},\ 0\right)$ と $\mathrm{B}\left(0,\ \dfrac{q+1}{2}\right)$ をとり点 $\mathrm{C}\left(\dfrac{p+1}{2},\ \dfrac{q+1}{2}\right)$ とする．



直線 $y=\dfrac{q}{p}x$ を引く．点 $\mathrm{L}\left(\dfrac{p}{2},\ \dfrac{q}{2}\right)$ とする．OACB の内部で直線 OL 上に格子点はない．さて，$c=1,\ 2,\ \cdots,\ \dfrac{p-1}{2}$ として, cq を p で割った絶対値最小剰余を r とする．直線 $x=c$ と直線 OL の交点が $\mathrm{P}\left(c,\ \dfrac{cq}{p}\right)$ で, $\left|\dfrac{r}{p}\right|$ は直線 $x=c$ 上の格子点で P にもっとも近いものとの距離になり．この格子点が P より上にあるとき r は負である．

ガウスの予備定理を $a=q$ で考えると，そこにおける n は各 c に対して直線 $x=c$ 上 $\mathrm{P}\left(c,\ \dfrac{cq}{p}\right)$ より上にあり，距離が $\dfrac{1}{2}$ より小さい格子点の個数である．いま直線 OL を y 軸の正の方向に $\dfrac{1}{2}$ だけ平行移動した直線を GG′ する． n は平行四辺形 OLG′G の内部にある格子点の個数である．

同様にガウスの予備定理で $\left(\dfrac{p}{q}\right)=(-1)^m$ となる m は直線 OL を x 軸の正の方向に $\dfrac{1}{2}$ だけ平行移動した直線を HH′ とするとき，平行四辺形 OHH′L の内部にある格子点の個数である．

$\left(\dfrac{p}{q}\right)\left(\dfrac{q}{p}\right)=(-1)^{m+n}$ における $m+n$ はこの二つの平行四辺形の内部にある格子点の個数である．小四角形 LH′CG′ を付け加えて六角形 OGG′CH′H の内部の格子点の個数もやはり $m+n$ で

ある．六角形 OGG′CH′H は OC の中点 $\left(\frac{p+1}{4},\ \frac{q+1}{4}\right)$ を対象の中心として点対称である．したがって六角形 OGG′CH′H 内の格子点は $\left(\frac{p+1}{4},\ \frac{q+1}{4}\right)$ が格子点であるときはこれを除いてその他の格子点は対象の中心に関して二つずつ組になっている．

したがって $m+n$ が奇数であるか偶数であるかは，点 $\left(\frac{p+1}{4},\ \frac{q+1}{4}\right)$ 自身が格子点であるかないかによって決まる．つまり $m+n$ が奇数であるのは，$\frac{p+1}{4}, \frac{q+1}{4}$ がともに整数 $s,\ t$ となるときにかぎる．$\frac{p-1}{2} = 2s-1,\ \frac{q-1}{2} = 2t-1$ なので，これは $\frac{p-1}{2},\ \frac{q-1}{2}$ がともに奇数になることと同値である．

これで相互法則が証明された． ■

相互法則その他を活用して p と a が与えられたとき，$\left(\frac{a}{p}\right)$ の値を計算することができる．

例 10.3　$p = 23$

$$\left(\frac{1}{23}\right) = 1 \quad (\ 1 = 1^2\ )$$
$$\left(\frac{2}{23}\right) = 1 \quad (\ 23 \equiv 7 \pmod 8,\quad \text{第 2 補充法則})$$
$$\left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1 \quad (\ \text{相互法則},\quad \text{第 2 補充法則})$$
$$\left(\frac{4}{23}\right) = \left(\frac{2}{23}\right)^2 = 1$$
$$\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{-2}{5}\right) = \left(\frac{-1}{5}\right)\left(\frac{2}{5}\right) = 1(-1) = -1 \quad (\ \text{相互法則},\quad \text{第 1 ，第 2 補充法則})$$
$$\left(\frac{6}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{3}{23}\right) = 1$$
$$\left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -1 \quad (\ \text{相互法則},\quad \text{第 2 補充法則})$$
$$\left(\frac{8}{23}\right) = \left(\frac{2}{23}\right)^3 = 1$$
$$\left(\frac{9}{23}\right) = \left(\frac{3}{23}\right)^2 = 1$$
$$\left(\frac{10}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{5}{23}\right) = -1$$
$$\left(\frac{11}{23}\right) = -\left(\frac{23}{11}\right) = -\left(\frac{1}{11}\right) = -1 \quad (\ \text{相互法則})$$
$$\left(\frac{17}{23}\right) = \left(\frac{23}{17}\right) = \left(\frac{6}{17}\right) = \left(\frac{2}{23}\right)\left(\frac{3}{17}\right)$$
$$= \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1 \quad (\ \text{相互法則},\quad \text{第 2 補充法則})$$

練習問題 10.1（解答 43）　$\left(\frac{365}{1847}\right)$ を求めよ．

練習問題 10.2（解答 44）　p が $8k+1$ または $8k+3$ の形の素数であるときにかぎって

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

を示せ.

練習問題 10.3（解答 45）　p が $5k \pm 1$ の形の素数であるときにかぎって

$$\left(\frac{5}{p}\right) = 1$$

を示せ.

練習問題 10.4（解答 46）　p が $12k \pm 1$ の形の素数であるときにかぎって

$$\left(\frac{3}{p}\right) = 1$$

を示せ.

練習問題 10.5（解答 47）　p が $p \equiv 1 \pmod 4$ の形の素数のとき

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) = \sum_{0 \leqq b \leqq p \text{ の偶数}} \left(\frac{b}{p}\right) = \sum_{0 \leqq c \leqq p \text{ の奇数}} \left(\frac{c}{p}\right) = 0$$

10.4　ガウス和による証明

ここでいわゆる**ガウス和**を用いて平方剰余の相互法則 (定理 32 の (1)) の証明を行う．今日ガウス和を用いた証明は,「有限体の指標」の問題としてガロア理論を土台にして行われるが，ここではガロア理論も有限体や巡回群の理論も仮定せずに，もっとも最初になされたように初等整数論の範囲内で行う.

p を奇素数とし，α を 1 の原始 p 乗根とする．具体的には例えば

$$\alpha = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

とする．このときガウス和 G とは

$$G = \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \alpha^k$$

のことをいう．いずれの原始 p 乗根もたがいに奇数べきの違いであるから，和 G は 1 の原始 p 乗根の取り方によらない．和は p を法とする剰余系から 0 を除いた全体にわたると考えられる．この和の 2 乗 G^2 を二通りの方法で計算することによって，相互法則が示される．定理 32(1) の証明では (2) 第一補充則と (3) 第二補充則を先に示し，その結果を (1) 平方剰余の相互法則の証明に用いた．同様にここでも，(2) 第一補充則と (3) 第二補充則は示されているものとする.

ガウス和を明示的に書くために，原始根を用いる．r を p を法とする剰余系の原始根とする．定理 27 によって，原始根は存在する.

$$1,\ r,\ r^2,\ \cdots,\ r^{p-2}$$

が既約剰余系の一組になる．定理 29 の証明冒頭と同様の理由で，i が偶数か奇数にしたがって

$$\left(\frac{r^i}{p}\right) = \pm 1$$

である．ゆえにガウス和 G は原始根 r を用いれば

$$G=\sum_{j=0}^{\frac{p-3}{2}}\alpha^{r^{2j}}-\sum_{j=0}^{\frac{p-3}{2}}\alpha^{r^{2j+1}}$$

と明示的に書くことができる．

ここで

$$\beta_0=\sum_{j=0}^{\frac{p-3}{2}}\alpha^{r^{2j}}=\alpha+\alpha^{r^2}+\ldots+\alpha^{r^{p-3}}$$
$$\beta_1=\sum_{j=0}^{\frac{p-3}{2}}\alpha^{r^{2j+1}}=\alpha^{r}+\alpha^{r^3}+\ldots+\alpha^{r^{p-2}}$$

とおく．α は $\alpha^{p-1}+\alpha^{p-2}+\cdots+1=0$ であるから $\beta_0+\beta_1+1=0$ ．

$$G^2=(\beta_0-\beta_1)^2=(\beta_0+\beta_1)^2-4\beta_0\beta_1$$

であるから G^2 を計算するためには，$\beta_0\beta_1$ が確定すればよい．

例 10.4　$p=5$ のとき．3 は 5 を法とする原始根である．実際

$$3\equiv 3,\ 3^2\equiv 4,\ 3^3\equiv 2,\ 3^4\equiv 1 \pmod 5$$

α を 1 の原始 5 乗根とする．

$$\beta_0=\alpha+\alpha^{3^2}=\alpha+\alpha^4$$
$$\beta_1=\alpha^3+\alpha^{3^3}=\alpha^2+\alpha^3$$

$$\begin{aligned}\therefore\quad \beta_0\beta_1 &= (\alpha+\alpha^4)(\alpha^2+\alpha^3)\\ &= \alpha^3+\alpha^4+\alpha^6+\alpha^7=\alpha+\alpha^2+\alpha^3+\alpha^4\\ &= -1=\frac{1-5}{4}\end{aligned}$$

例 10.5　$p=7$ のとき．3 は 7 を法とする原始根である．実際

$$3^1\equiv 3,\ 3^2\equiv 2,\ 3^3\equiv 6,\ 3^{\equiv}4,\ 3^5\equiv 5,\ 3^6\equiv 1 \pmod 7$$

α を 1 の原始 7 乗根とする．

$$\beta_0=\alpha+\alpha^{3^2}+\alpha^{3^4}=\alpha+\alpha^2+\alpha^4$$
$$\beta_1=\alpha^3+\alpha^{3^3}+\alpha^{3^5}=\alpha^3+\alpha^5+\alpha^6$$

$$\begin{aligned}\therefore\quad \beta_0\beta_1 &= (\alpha+\alpha^2+\alpha^4)(\alpha^3+\alpha^5+\alpha^6)\\ &= \alpha^4+\alpha^6+\alpha^7+\alpha^5+\alpha^7+\alpha^8+\alpha^7+\alpha^9+\alpha^{10}\\ &= 3+\alpha+\alpha^2+\alpha^3+\alpha^4+\alpha^5+\alpha^6\\ &= 2=\frac{1+7}{4}\end{aligned}$$

この例を一般化して示すために 1 のべき根の性質で必要なものをまとめておく．

補題 2　α を 1 の原始 p 乗根，r を p を法とする原始根とする．

(1) 有理数 $c_1, \cdots, c_{p-1}$ を用いて

$$c_1\alpha + \cdots + c_{p-1}\alpha^{p-1} = 0$$

となるなら，$c_1 = \cdots = c_{p-1} = 0$ である．

(2) 有理数 $q_0, \cdots, q_{p-2}$ を用いて

$$F(X) = q_0X + q_1X^r + q_2X^{r^2} + \cdots + q_{p-2}X^{r^{p-2}}$$

とおく．$F(\alpha) = F(\alpha^r)$ ならば $F(\alpha)$ は有理数である．

証明

(1) $\alpha \neq 0$ より

$$c_1 + c_2\alpha + \cdots + c_{p-1}\alpha^{p-2} = 0$$

となるが，α は 1 の原始 p 乗根なので $p-2$ 以下の次数の方程式の解とはならない．ゆえに $c_1 = \cdots = c_{p-1} = 0$ である．

(2) $(\alpha^{r^i})^{r^j} = \alpha^{r^{i+j}}$ である．

$$1,\ r,\ r^2,\ \cdots,\ r^{p-2}$$

は既約剰余系で，$i \equiv j \pmod{p-1}$ なら $r^i \equiv r^j \pmod{p}$ となる．したがって

$$X,\ X^r,\ \cdots,\ X^{r^{p-2}}$$

に α を代入したものと，α^{r^i} を代入したものは，1 の p 乗根で 1 以外のものが順序が i 番ずれて現れる．(1) から既約剰余系の有理数係数の一次結合による複素数の表示は一意である．ゆえに $F(\alpha) = F(\alpha^r)$ のとき，$\alpha^{r^{p-1}} = \alpha$ より

$$q_0\alpha + q_1\alpha^r + q_2\alpha^{r^2} + \cdots + q_{p-2}\alpha^{r^{p-2}} = q_0\alpha^r + q_1\alpha^{r^2} + q_2\alpha^{r^3} + \cdots + q_{p-2}\alpha^{r^{p-1}}$$

となり，$q_0 = q_{p-2},\ q_1 = q_0,\ \cdots,\ q_{p-2} = q_{p-3}$ と，対応する係数 q_k が順次等しくなる．

$$\therefore\quad q_0 = q_1 = \cdots = q_{p-2}$$

である．

$$\therefore\quad F(\alpha) = q_0(\alpha + \alpha^2 + \cdots + \alpha^{p-1}) = -q_0$$

となり，確かに有理数である．

さて，$p = 5,\ 7$ の計算は次の結果を推測させたが，それを示そう．

定理 34

記号はこの節の通りとする．このとき

$$\beta_0\beta_1 = \begin{cases} \dfrac{1+p}{4} & (p \equiv -1 \pmod{4} \text{ のとき}) \\ \dfrac{1-p}{4} & (p \equiv 1 \pmod{4} \text{ のとき} \end{cases}$$

証明　フェルマの小定理から

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

である．ゆえに

$$r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

したがって，整数 k に対して

$$r^k + r^{k+\frac{p-1}{2}} \equiv 0 \pmod{p}$$

次に $\beta_0 \cdot \beta_1$ において α の代わりに α^r を代入すると β_0 と β_1 が入れ替わるので $\beta_0 \cdot \beta_1$ は変わらない．したがって補題から $\beta_0 \cdot \beta_1$ は有理数である．

また有理数 $c_1, \cdots, c_{p-1}$ に対して

$$c_1\alpha + \cdots + c_{p-1}\alpha^{p-1}$$

が有理数となるのは $c_1 = \cdots = c_{p-1}$ のときにかぎる．それ以外にあれば，$1 + \alpha + \cdots + \alpha^{p-1} = 0$ とあわせて α^{p-1} の項を消せば，α が $p-2$ 次以下の方程式を満たすことにあるからである．

そこで

(i) $\dfrac{p-1}{2}$ が奇数．つまり $p \equiv -1 \pmod{p}$ のとき．

$\beta_0 \cdot \beta_1 = (\alpha + \alpha^{r^2} + \ldots + \alpha^{r^{p-3}})(\alpha^r + \alpha^{r^3} + \ldots + \alpha^{r^{p-2}})$ を展開した段階でできる $\left(\dfrac{p-1}{2}\right)^2$ 個の積のうち，1 になるものが $\dfrac{p-1}{2}$ 個あり，残る $\left(\dfrac{p-1}{2}\right)^2 - \dfrac{p-1}{2} = \dfrac{(p-1)(p-3)}{4}$ 個の和は有理数なので，それら $p-1$ 個ずつ $\alpha + \cdots + \alpha^{p-1} = -1$ でまとめられ，それが $\dfrac{p-3}{4}$ 個ある．

$$\therefore \quad \beta_0 \cdot \beta_1 = 1 \cdot \frac{p-1}{2} + (-1) \cdot \frac{p-3}{4} = \frac{1+p}{4}$$

(ii) $\dfrac{p-1}{2}$ が偶数．つまり $p \equiv 1 \pmod{p}$ のとき．

$\beta_0 \cdot \beta_1$ を展開した段階でできる $\left(\dfrac{p-1}{2}\right)^2$ 個の積のうちに 1 になるものはなく，すべて $p-1$ 個ずつ $\alpha + \cdots + \alpha^{p-1} = -1$ でまとめらる．

$$\therefore \quad \beta_0 \cdot \beta_1 = (-1) \cdot \frac{p-1}{4} = \frac{p-1}{4}$$

■

これから G^2 が計算でき，他の計算と比較して相互法則が示される．

補題 3　素数 p と整数係数の多項式 $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$ に対して

$$(a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0)^p \equiv {a_n}^p x^{pn} + {a_{n-1}}^p x^{p(n-1)} + \cdots + {a_0}^p \pmod{p}$$

証明　$1 \leqq k \leqq p-1$ に対して $k_p\mathrm{C}_k = p_{p-1}\mathrm{C}_{k-1}$ より ${}_p\mathrm{C}_k$ は p の倍数.

$$\begin{aligned}
\therefore\quad (a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0)^p &= \{a_nx^n + (a_{n-1}x^{n-1} + \cdots + a_0)\}^p \\
&\equiv {a_n}^p x^{pn} + (a_{n-1}x^{n-1} + \cdots + a_0)^p \pmod{p} \\
&\equiv {a_n}^p x^{pn} + {a_{n-1}}^p x^{p(n-1)} + (a_{n-2}x^{n-2} + \cdots + a_0)^p \pmod{p} \\
&\cdots \\
&\equiv {a_n}^p x^{pn} + {a_{n-1}}^p x^{p(n-1)} + \cdots + {a_0}^p
\end{aligned}$$

■

これを証明のなかで用いる.

定理 35 (平方剰余の相互法則の別証明)
q を p と異なる奇素数とする．複合を $p \equiv \pm 1 \pmod{p}$ と同順にとって

$$\left(\frac{q}{p}\right) = \left(\frac{\pm p}{q}\right)$$

証明　$G = \beta_0 - \beta_1$ であるから，上の定理から

$$G^2 = (\beta_0 - \beta_1)^2 = (\beta_0 + \beta_1)^2 - 4\beta_0\beta_1 = 1 - (1 \mp p) = \pm p$$

オイラーの規準 (定理 30) から

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

であるから

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

つまり

$$G^q \equiv \left(\frac{\pm p}{q}\right) G \pmod{q}$$

一方

$$\begin{aligned}
G^q &= \left(\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \alpha^k\right)^q \equiv \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)^q \alpha^{kq} \pmod{q} \quad (\because \text{ 補題 3}) \\
&= \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \alpha^{kq} \quad (\because \ q \text{ は奇数}) \\
&= \left(\frac{q}{p}\right) \sum_{k=1}^{p-1} \left(\frac{kq}{p}\right) \alpha^{kq} = \left(\frac{q}{p}\right) G
\end{aligned}$$

$$\therefore \quad \left(\frac{q}{p}\right) G = \left(\frac{\pm p}{q}\right) G \pmod{q}$$

つまり

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

であるが， G において $\alpha,\ \alpha^2,\ \cdots\alpha^{p-1}$ の係数はすべて ±1 で $\left(\frac{q}{p}\right)-\left(\frac{\pm p}{q}\right)$ がすべて q の倍数になる．

これがとりうる値は $0,\ \pm2$ であるが q が奇素数なので

$$\left(\frac{q}{p}\right)=\left(\frac{\pm p}{q}\right)$$

でなければならない． ■

これはすなわち平方剰余の相互法則である．

ここではガウス和 G の平方のみを用いた． G そのものは使わなかったので， G の符号を決定する必要がなかった． G の符号を決定するのは簡単ではない．

なお，原始根による 1 の p 乗根の表示と分類は,『数学対話』「1 の 17 乗根」の理論的な背景をなしている．もう一度読み返してほしい．

10.5 三角法の補題による証明

平方剰余の相互法則のもう一つの証明を,『数論講義』(J.P,Serre，岩波書店) に沿いつつそれを初等化して行う．G.Eisenstein,F. が 1845 年に発表したもので，ある三角法の補題を用いる．ガウスの予備定理 33 は前提にする．その後の初等的な座標による証明の部分に対する別証明を与えるものである．

補題 4 (三角法の補題)

m を奇素数とする．次の等式が成り立つ．

$$\frac{\sin mx}{\sin x}=(-4)^{\frac{m-1}{2}}\prod_{j=1}^{\frac{m-1}{2}}\left(\sin^2 x-\sin^2\frac{2\pi j}{m}\right)$$

証明 ド・モアブルの定理と二項定理により,

$$\begin{aligned}
&\cos mx+i\sin mx=(\cos x+i\sin x)^m\\
=\ &\sum_{k=0}^{m}{}_m\mathrm{C}_k\cos^{m-k}x\cdot(i\sin x)^k\\
=\ &{}_m\mathrm{C}_0\cos^m x-{}_m\mathrm{C}_2\cos^{m-2}x\sin^2x+{}_m\mathrm{C}_4\cos^{m-4}x\sin^4x-\cdots\\
&+i({}_m\mathrm{C}_1\cos^{m-1}x\sin x-{}_m\mathrm{C}_3\cos^{m-3}x\sin^3x+{}_m\mathrm{C}_5\cos^{m-5}x\sin^5x-\cdots)
\end{aligned}$$

が成立する．虚数部分を比較して

$$\sin mx=\sin x\{{}_m\mathrm{C}_1\cos^{m-1}x-{}_m\mathrm{C}_3\cos^{m-3}x\sin^2x+{}_m\mathrm{C}_5\cos^{m-5}x\sin^4x-\cdots\}$$

となる． m が奇素数なので $m=2u+1$ とおくと

$$\begin{aligned}
&{}_m\mathrm{C}_1\cos^{m-1}x-{}_m\mathrm{C}_3\cos^{m-3}x\sin^2x+{}_m\mathrm{C}_5\cos^{m-5}x\sin^4x-\cdots\\
=\ &{}_m\mathrm{C}_1\cos^{2u}x-{}_m\mathrm{C}_3\cos^{2u-2}x\sin^2x+{}_m\mathrm{C}_5\cos^{2u-4}x\sin^4x-\cdots
\end{aligned}$$

$$
\begin{aligned}
&= {}_m\mathrm{C}_1(1-\sin^2 x)^u - {}_m\mathrm{C}_3(1-\sin^2 x)^{u-1}\sin^2 x + {}_m\mathrm{C}_5(1-\sin^2 x)^{u-2}\sin^4 x - \cdots \\
&= (-1)^u({}_m\mathrm{C}_1 + {}_m\mathrm{C}_3 + {}_m\mathrm{C}_5 + \cdots)\sin^{2u} x + \cdots \\
&= (-4)^{\frac{m-1}{2}}(\sin^2 x)^{\frac{m-1}{2}} + \cdots
\end{aligned}
$$

したがって，$\dfrac{\sin mx}{\sin x}$ は $\sin^2 x$ の多項式で，その次数は $\dfrac{m-1}{2}$ であり，さらに最高次数の係数は $(-4)^{\frac{m-1}{2}}$ となることがわかる．

一方，

$$
x = \pm\frac{2\pi j}{m} \quad \left(1 \leqq j \leqq \frac{m-1}{2}\right)
$$

に対して $\sin mx = 0$ であり，

$$
\pm\sin\frac{2\pi j}{m} \quad \left(1 \leqq j \leqq \frac{m-1}{2}\right)
$$

はすべて異なる．ゆえに

$$
\frac{\sin mx}{\sin x} = (-4)^{\frac{m-1}{2}} \prod_{j=1}^{\frac{m-1}{2}} \left(\sin x - \sin\frac{2\pi j}{m}\right)\left(\sin x + \sin\frac{2\pi j}{m}\right)
$$

と分解される．つまり補題が示された．

定理 32(再掲)

p と q を相異なる 2 つの奇素数とする．

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

証明

$$i = 1,\ 2,\ \cdots,\ \frac{p-1}{2}$$

に対して qi を考える．それらを p で割った余りが $\dfrac{p}{2}$ を超えるものの個数を n とする．n は

$$\sin\frac{2\pi qi}{p}\ \left(i = 1,\ 2,\ \cdots,\ \frac{p-1}{2}\right)$$

のうち負になるものの個数である．さらにこれらはガウスの予備定理 33 の証明にあるように符号を除けば

$$\sin\frac{2\pi i}{p}\ \left(i = 1,\ 2,\ \cdots,\ \frac{p-1}{2}\right)$$

と一致する．

$$\therefore\quad \prod_{i=1}^{\frac{p-1}{2}}\sin\frac{2\pi qi}{p} = (-1)^n\prod_{i=1}^{\frac{p-1}{2}}\sin\frac{2\pi i}{p}$$

ガウスの予備定理 33 より

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

なので，三角法の補題 4 を $m = q,\ x = \dfrac{2\pi i}{p}$ で用いることにより

$$\begin{aligned}\left(\frac{q}{p}\right) &= \prod_{i=1}^{\frac{p-1}{2}}\frac{\sin\dfrac{2\pi qi}{p}}{\sin\dfrac{2\pi i}{p}}\\ &= \prod_{i=1}^{\frac{p-1}{2}}(-4)^{\frac{q-1}{2}}\prod_{j=1}^{\frac{q-1}{2}}\left(\sin^2\frac{2\pi i}{p} - \sin^2\frac{2\pi j}{q}\right)\\ &= (-4)^{\frac{(p-1)(q-1)}{4}}\prod_{i=1}^{\frac{p-1}{2}}\prod_{j=1}^{\frac{q-1}{2}}\left(\sin^2\frac{2\pi i}{p} - \sin^2\frac{2\pi j}{q}\right)\end{aligned}$$

p と q を入れ替えれば

$$\left(\frac{p}{q}\right) = (-4)^{\frac{(p-1)(q-1)}{4}}\prod_{i=1}^{\frac{p-1}{2}}\prod_{j=1}^{\frac{q-1}{2}}\left(\sin^2\frac{2\pi j}{q} - \sin^2\frac{2\pi i}{p}\right)$$

ところがこの積は合計 $\dfrac{p-1}{2}\cdot\dfrac{q-1}{2}$ 個にわたるものであるから

$$\prod_{i=1}^{\frac{p-1}{2}}\prod_{j=1}^{\frac{q-1}{2}}\left(\sin^2\frac{2\pi j}{q} - \sin^2\frac{2\pi i}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}\prod_{i=1}^{\frac{p-1}{2}}\prod_{j=1}^{\frac{q-1}{2}}\left(\sin^2\frac{2\pi i}{p} - \sin^2\frac{2\pi j}{q}\right)$$

したがって

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

つまり

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

が示された. ■

10.6 演習問題

演習問題 30 (解答 30) ［98 横国大文系後期］

次の問に答えよ.

(1) $x^2+y^2+z^2=n$ を満たす整数の組 $(x,\ y,\ z)$ が存在しないような正の整数 n を小さいものから順に 5 個求めよ.

(2) 「正の整数 n を 8 で割ったときの余りが 7 ならば，$x^2+y^2+z^2=n$ を満たす整数の組 $(x,\ y,\ z)$ が存在しない」というのは，つねに正しいか理由を述べて答えよ.

11　ガウス整数

11.1　ガウス整数

ガウスは平方剰余の研究からさらにすすんで四乗剰余の相互法則を考えていった．そのなかで彼は，整数の概念を複素数の世界に拡張しなければならないことに気づいた．ガウスのこの創意は虚数の意義を決定的なものにし，現代の代数的整数論の起源となった，数学史上重大な転回点だった．

高校でもいろいろ複素数について習う．ここでガウスが考えたことの一端に触れよう．

$i = \sqrt{-1}$ を虚数単位として

$$R = \{\ a + bi \mid a,\ b\ :\ \text{整数}\ \}$$

とおく． R の二つの要素 $\alpha = a + bi,\ \beta = c + di$ に対してその和・差・積は

$$\begin{aligned} \alpha \pm \beta &= (a + bi) \pm (c + di) = (a \pm c) + (b \pm d)i \\ \alpha\beta &= (a + bi)(c + di) = (ac - bd) + (ad + bc)i \end{aligned}$$

であるからふたたび R に属する．つまり R は環である．**環** については節末の定義を参照のこと．R のことを **ガウス環** , R の要素を **ガウス整数** という．

以下「整数」と言えば「ガウス整数」のこととし，特に従来の整数を表すときは「有理整数」と言う．

R の要素 $\alpha = a + bi$ に対して $\bar{\alpha} = a - bi$ を α の共役という．これはふたたび整数で R の要素になる．ここで R の要素 $\alpha = a + bi$ に対して

$$N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2$$

と定め, α の **ノルム** と呼ぶことにする．ガウス整数 α に対してノルム $N(\alpha)$ は有理整数になる．また $N(\alpha\beta) = N(\alpha)N(\beta)$ が成り立つ．

R の二つの要素 $\alpha = a + bi,\ \beta = c + di$ に対してその商

$$\frac{\alpha}{\beta} = \frac{a + bi}{c + di} = \frac{ac + bd}{c^2 + d^2} + \frac{bc - ad}{c^2 + d^2}i$$

は必ずしも整数でない． $\dfrac{\alpha}{\beta} = \gamma$ が再び整数であるとき，α は β で割り切れると言い, α を β の倍数，β を α の約数，と言う．

有理整数で逆数もまた整数になるのは 1 と -1 であった．ガウス整数ではどのようなものになるだろうか． α が逆数 $\dfrac{1}{\alpha}$ も整数とする．このとき

$$1 = N\left(\alpha \cdot \frac{1}{\alpha}\right) = N(\alpha)N\left(\frac{1}{\alpha}\right)$$

$N(\alpha) \geqq 0$ なので $N(\alpha) = 1$ でなければならない．つまり $\alpha = a + bi$ とすれば

$$a^2 + b^2 = 1$$

a と b は有理整数なので $(a,\ b) = (1,\ 0),\ (-1,\ 0),\ (0,\ 1),\ (0,\ -1)$ である．つまりガウス整数で逆数もまた整数になるのは

$$1,\ -1,\ i,\ -i$$

の四個である．これらを R の**単数**と呼ぶ．この四数が R のノルム 1 の要素である．

$\dfrac{\alpha}{\beta}$ が単数であるとき, α と β を**同伴数**という．α の同伴数は $\alpha,\ -\alpha,\ i\alpha,\ -i\alpha$ である．

二つの整数の割れる割れないの関係は，それらの整数を同伴数に置き換えて考えても同じことになる．つまり整除の問題を考えるかぎり同伴数を同じ数のように考えて良い．これは有理整数の整除の問題では, ± 1 の因数を度外視して良いのと同じである．

定理 36 (ガウス整数環における除法の原理)

R の要素 α と β に対して

$$\alpha = \beta\gamma + \rho\ , \quad \rho = 0 \quad \text{または } N(\rho) < N(\beta)$$

となる $\gamma,\ \rho \in R$ が存在する．

証明 $\dfrac{\alpha}{\beta} = r + si$ とおく．ここに $r,\ s$ は有理数である．

この $r,\ s$ に対して整数 $m,\ n$ を $|r-m| \leqq \dfrac{1}{2},\ |s-n| \leqq \dfrac{1}{2}$ とることができる．

$\gamma = m + ni$ とおく．

$$N\left(\frac{\alpha}{\beta} - \gamma\right) \leqq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$$

なので, $\rho = \alpha - \beta\gamma$ とおくと

$$N(\rho) = N\left(\beta\left(\frac{\alpha}{\beta} - \gamma\right)\right) = N(\beta)N\left(\frac{\alpha}{\beta} - \gamma\right) \leqq \frac{N(\beta)}{2} < N(\beta)$$

■

このように除法の原理が成立する環を「**ユークリッド整域**」という．

環	用いられる大きさ		
有理整数環	絶対値 $\vert\ \ \vert$	$a = bq + r$	$0 \leqq r < \lvert b \rvert$
多項式環	次数 deg	$f(x) = g(x)q(x) + r(x)$	$0 \leqq \deg r(x) < \deg b(x)$
ガウス環	ノルム $N(\ )$	$\alpha = \beta\gamma + \rho$	$0 \leqq N(\rho) < N(\beta)$

などである．除法の原理が成立するならば，最大公約数がさだまり因数分解ができて，その一意性が成り立つ．

定理 37

$\alpha,\ \beta \in R$ に対し，集合 J を

$$J = \{\ \alpha x + \beta y \mid x,\ y \in R\ \}$$

する．このとき J はある R の要素 δ の倍数全体になる．δ は単数倍の違いを除いて一意に定まる．

証明 J の要素のノルムの値の集合を考える．それは 0 と自然数の部分集合であるからそのなかに 0 でない最小のものが存在する．そのノルムを与える要素を $\delta\alpha x_0 + \beta y_0$ とする．

J の任意の要素 $\alpha x + \beta y$ をとる．

$$\alpha x + \beta y = \delta\gamma + \rho, \quad 0 \leqq N(\rho) < N(\delta)$$

である．

$$\rho = \alpha(x - \gamma x_0) + \beta(y - \gamma y_0) \in R$$

であるから, $N(\delta)$ の最小性により $\rho = 0$ である．

他の δ' もノルム最小なら，δ と δ' はノルムが等しいので単数倍違うのみである． ■

この δ を α と β の最大公約数という．ガウス環では除法を用いてユークリッドの互除法ができ α と β の最大公約数 δ が一意に存在することをが示される．

ノルムが 1 より大きいガウス整数は，単数とそれ自身の同伴数以外の約数をもたないとき**ガウス素数**と呼ばれる．すると有理整数の場合と同様に素因数分解ができる．分解の存在はノルムに関する数学的帰納法でできる．一意性の証明は，有理整数に関する一連の性質をガウス環についておこなったうえで同様に示される．よって証明は略する．

定理 38

すべての 0 でないガウス整数は一つの単数といくつかのガウス整数の積として単数倍の違いを除いて一意的に書き表される．

ガウス環の素数はどのようなものか．

定理 39

p を奇素数とする． p は次のいずれかである．ガウス素数である．またはあるガウス素数 π のノルムである，つまり $p = \pi\bar{\pi}$ と因数分解され, π と $\bar{\pi}$ は同伴数でなく，さらにこのとき p は π と $\bar{\pi}$ とその同伴数以外のガウス素因数をもたない．

証明 p をガウス環 R で因数分解しそれを

$$p = \epsilon\pi_1\pi_2\cdots\pi_l$$

とする．ここで ϵ は単数であり，$\pi_1,\ \pi_2,\ \cdots,\ \pi_l$ は単数でないガウス素数である．

ノルムをとると

$$p^2 = N(\pi_1)N(\pi_2)\cdots N(\pi_l)$$

ここでどれかが $N(\pi_l) = p^2$ となれば他のノルムはすべて 1 で単数になったしまう．ゆえにこの場合 $l = 1$ で $p = \epsilon\pi_1$ となり, p がガウス素数である．

そうでなければ単数以外のノルムは p であり, $l = 2$

$$N(\pi_1) = \pi_l\bar{\pi}_l = p$$

となり, $\bar{\pi}_l(= \pi_2)$ もガウス素数である．

$p = \pi\bar{\pi}$ のとき π と $\bar{\pi}$ が同伴数なら $\bar{\pi}$ は $\pm\pi,\ \pm i\pi$ のどれかと一致する．$\pi x + iy$ とすれば，これは $x = 0,\ p = y^2$, $y = \pm x,\ p = 2x^2$ を意味するが, p が奇素数なのでこれはあり得ない． ■

$p = 2$ のとき，その分解は

$$2 = N(1 + i) = (1 + i)(1 - i) = i^3(1 + i)^2$$

で与えられる．四つのガウス整数 $\pm 1 \pm i$ は互いに同伴なので「単数倍を除いて一意」であることはもちろん成立している．

では奇素数 p がガウス環で分解されるか否かは何で決まるのか．

定理 40

p を奇素数とする．このとき

$$p \equiv 1 \pmod 4 \iff p = (a+bi)(a-bi) \text{ と分解される}$$
$$p \equiv 4 \pmod 4 \iff p \text{ はガウス素数である}$$

証明 p がガウス素数のノルムであれば $p = (a+bi)(a-bi) = a^2 + b^2$ となる．p が奇素数なので a と b の一方のみが偶数で他方が奇数になる．

$$\therefore \quad p \equiv 1 \pmod 4$$

逆に $p \equiv 1 \pmod 4$ のとき．平方剰余の第一補充法則から -1 は p を法とする平方剰余である．つまり

$$-1 \equiv x^2 \pmod p$$

となる x がある．ゆえに $x^2 + 1$ は p の倍数である．ところがこのとき

$$x^2 + 1 = (x+i)(x-i)$$

なので，もし p 自身がガウス素数なら p は $x+i,\ x-i$ のいずれかの約数でなければならないが明らかにそれなあり得ない．したがって p はガウス素数のノルムである．

$p \equiv 1 \pmod 4$ のときの必要十分性が示されたので，$p \equiv 3 \pmod 4$ についての命題も成立する． ■

このことから「有理素数は，2 か，または 4 を法として 1 に合同なときにかぎり，二つの平方数の和として一通りに書き表すことができる」ということがわかる．

練習問題 11.1 (解答 48)　次の数を平方数の和に書き表せ．

$$5,\ 13,\ 65,\ 5^2,\ 50,\ 13^2$$

付記：群・環・体

「ガウス環」の「環」という言葉について，ここで群や体とあわせて，最低限の定義を述べる．

加法や乗法など **演算** のもつ性質を抽出したのが，次の **群** である．

＝群＝　集合 G の要素について，演算 $\circ$ が与えられており，次の条件を満たしているとき，集合 G は演算 $\circ$ について，**群** である，という．これらの四条件を **「群の公理」** という．

集合 G に演算 $\circ$ が定義されていて，次の公理を満たすとき，G は演算 $\circ$ に関して **群である** という．

(1) $a, b \in G$ ならば $a \circ b \in G$ （演算について閉じている）

(2) $(a \circ b) \circ c = a \circ (b \circ c)$ （結合法則）

(3) 任意の $a \in G$ に対して, $a \circ e = e \circ a = a$ となる $e \in G$ が存在する.（単位元の存在）

(4) 任意の $a \in G$ に対して, $a \circ x = x \circ a = e$ となる $x \in G$ が存在する.（逆元の存在）（この x を a^{-1} と表わす）.

さらに, $a \circ b = b \circ a$ を満たすとき， **可換群**（または **アーベル群** ）であるという.

例 11.1 数の集合 N, Z, Q, R, C は加法に関して，可換群である．つまり「群構造」をもつ．N, Z, Q, R, C から 0 を除いた集合 $N^{\times}, Z^{\times}, Q^{\times}, R^{\times}, C^{\times}$ は乗法に関して，可換群である．

＝環＝ 集合 M に 2 種類の演算 $\circ$ と $*$ が定義されていて，一方の演算 $*$ については可換群であり，他の演算 $\circ$ については **結合法則** と次の **分配法則**

$$a \circ (b * c) = (a \circ b) * (a \circ c),\ (b * c) \circ a = (b \circ a) * (c \circ a)$$

が成り立つとき，集合 M は **環** であるという.

例 11.2 (1) 整数の集合 Z は，加法と乗法に関して，環になる．

(2) 有理数係数の x の多項式の全体，および実数係数の x の多項式の全体は，加法と乗法に関して，環になる．

(3) 整数係数の x の多項式の全体は，加法と乗法に関して，環になる．

(4) ベクトルの集合は，実数の乗法とベクトルの加法に関して，環である．

＝体＝ 集合 K が演算 $\circ$ と $*$ に関して環であり，さらに K から演算 $*$ の単位元を除いた集合が $\circ$ に関して可換群を作るとき，集合 K は**体** であるという.

例 11.3 (1) 有理数，実数の全体はそれぞれ加法と乗法に関して体である．

(2) 有理数または実数を係数とする有理式の全体も，加法と乗法に関して体である．

11.2 演習問題

演習問題 31 (解答 31)

$$x^2 + y^2 = z^2,\ (x,\ y) = 1$$

の正の整数解は,

$$x,\ y = m^2 - n^2,\ 2nm,\ z = m^2 + n^2$$

ただし， $(m,\ n) = 1,\ m > n > 0$ で m と n は偶数と奇数.

演習問題 32 (解答 32) ［01 京大］ p を素数，a ，b を互いに素な正の整数とするとき, $(a+bi)^p$ は実数ではないことを示せ．ただし i は虚数単位を表す.

演習問題 33 (解答 33) ［02 慶応医］

設問 (1) から (5) に答えなさい.

4 で割ると余りが 1 になるような素数 $p,\ p = 4k + 1$，を 1 つとる．これに対し，等式

$$\text{(Q)} \qquad a^2 + 4bc = p$$

を満たす自然数 3 つの組 $(a,\ b,\ c)$ の全体を考える．両辺の絶対値を比べればわかるように，このような自然数 3 つの組の可能性は有限通りしかありえない.

いま等式 (Q) を満たす自然数 3 つの組 $(a,\ b,\ c)$ から新しく自然数 3 つの組を作る手続きを次の (i)，(ii)，(iii) により定める:

(i) $a < b - c$ ならば $(a + 2c,\ c,\ b - a - c)$ を作る;

(ii) $b - c < a < 2b$ ならば $(2b - a,\ b,\ a - b + c)$ を作る;

(iii) $a > 2b$ ならば $(a - 2b,\ a - b + c,\ b)$ を作る.

(1) $(a,\ b,\ c)$ が等式 (Q) を満たす自然数の組でさらに (i) の条件 $a < b - c$ を満たすとする．このとき，上の (i) より得られる $(a + 2c,\ c,\ b - a - c)$ もまた等式 (Q) を満たすことを示しなさい.

(2) 等式 (Q) を満たす自然数の組 $(a,\ b,\ c)$ は $a = b - c$ や $a = 2b$ を満たすことはないことを示しなさい.

(3) 等式 (Q) を満たす自然数の組 $(a,\ b,\ c)$ の中には，上の手続きを施しても変化しないという性質を持つものが存在する．$p = 4k + 1$ と表すとき，この性質を持つ $(a,\ b,\ c)$ を k を用いて具体的に与え，かっそれがただ 1 組しか存在しないことを示しなさい.

(4) 等式 (Q) を満たす自然数の組 $(a,\ b,\ c)$ に対して上の手続きを 2 回繰返して施すとどうなるか，結論を簡潔に説明しなさい．また，この観察をもとに等式 (Q) を満たす自然数 3 つの組の全体の個数が偶数か奇数かを決定し，そう判断できる理由を述べなさい．ただし，等式 (Q) を満たす自然数 3 つの細から上の手続きにより新しく作られた自然数 3 つの組は (i)，(ii)，(iii) のどの場合でも再び等式 (Q) を満たすという事実についてはここでは証明なしに用いてよい.

(5) 素数 $p = 4k + 1$ をある 2っの自然数 $a,\ b$ により

$$p = a^2 + (2b)^2$$

と表すことができることを示しなさい.

12　ペル方程式の解の構造

12.1　ペル方程式の解の構造

われわれの『整数論入門』の今後の課題は「二次不定方程式」の解明である．高校数学の知識以外のことは必要なく，しかも大変美しい理論である．高木貞治著『初等整数論講義』第二章「連分数」は「二次体の整数論」という分野の準備もかねて展開されている．が，われわれの『整数論入門』はそこまでは行かない．したがってここでは「二次不定方程式」の解明という点に絞って，連分数をなじみやすい二次行列のことばに書き直して再構成する．

ペルの方程式

二次不定方程式のなかで，$x^2 - Dy^2 = \pm 1$ の形をしたものを「ペル方程式」という．ここで，D は平方数でない整数である．この方程式の意義に気づき本格的に研究したのはフェルマである．本来は「フェルマ方程式」と呼ぶべきだが，オイラーがある手紙の中で (不注意で)「ペル (J.Pell 1610-1385) 方程式」と呼んだために，今では「ペル方程式」が定着している．

ペル方程式の場合も一次不定方程式の場合と同様，研究すべきは次の三項である．

(1) ペル方程式の整数解の集合の構造

(2) ペル方程式に整数解が存在する証明

(3) ペル方程式の整数解を構成する方法

ところで，日本の大学の入学試験で「ペル方程式の整数解の集合の構造」に関する問題が過去何回か出題されている．高校生諸君の勉強の便宜を考え，材料としていくつかの入試問題を掘りさげるところから始めよう．まず，同じ 95 年に出題された二つの問題と 85 年の問題を解いてみよう．

ちなみに『ペル方程式の解の構成』まで読み進めば

$D = 1999$ のとき，

$x^2 - Dy^2 = \pm 1$ を満たす最小の正の整数解 $(P,\ Q)$ は

$P = 4027701399389138208695911951306886478800$

$Q = 90084665203202024260494303744425250249$

$k = 84$

であることがわかる! これを楽しみにして進もう．

三つの入試問題

例題 12.1　［大阪府立大 95 年］

$A = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$ に対して，

$$\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad n = 1, 2, 3, \cdots$$

とする．次の問いに答えよ．

(1) x_n と y_n を求めよ.

(2) $a=2+\sqrt{3}$, $b=2-\sqrt{3}$ とおく. a^n と b^n を x_n, y_n を用いて表せ. また, 点

$$\mathrm{P}_1(x_1,\ y_1),\ \mathrm{P}_2(x_2,\ y_2),\ \mathrm{P}_3(x_3,\ y_3),\ \cdots,\mathrm{P}_n(x_n,y_n),\ \cdots$$

はすべて同じ曲線上にある. $ab=1$ が成り立つことを利用して, その曲線の方程式を求めよ.

例題 12.2 [明治大学 95 年]

$A=\begin{pmatrix}2 & 3\\ 1 & 2\end{pmatrix}$ とする. 以下の問いに答えよ.

(1) ベクトル $\begin{pmatrix}x\\ y\end{pmatrix}$ に対し, $\begin{pmatrix}x_1\\ y_1\end{pmatrix}=A^{-1}\begin{pmatrix}x\\ y\end{pmatrix}$ とおく. $x^2-3y^2=1$ ならば $x_1^2-3y_1^2=1$ であることを示せ.

(2) 等式 $x^2-3y^2=1$ をみたす正の整数 x, y に対して, $\begin{pmatrix}x_1\\ y_1\end{pmatrix}=A^{-1}\begin{pmatrix}x\\ y\end{pmatrix}$ とおけば, $y>y_1\geqq 0$ が成り立つことを示せ.

(3) 数列 $\{a_n\}$, $\{b_n\}$ を $\begin{pmatrix}a_n\\ b_n\end{pmatrix}=A^n\begin{pmatrix}1\\ 0\end{pmatrix}$ $(n=1,2,\cdots)$ によって定めると, 等式

$$(2+\sqrt{3})^n=a_n+b_n\sqrt{3}\ (n=1,2,\cdots)$$

が成り立つことを示せ.

(4) 等式 $x^2-3y^2=1$ をみたす正の整数の組 (x,y) は (3) で与えられた整数の組 (a_n,b_n) $(n=1,2,\cdots)$ のどれかに等しいことを証明せよ.

例題 12.3 [東京工大 85 年]

二つの条件

(i) $a^2-2b^2=+1$ または $a^2-2b^2=-1$

(ii) $a+\sqrt{2}b>0$

をみたす任意の整数 a, b から得られる実数 $g=a+\sqrt{2}b$ 全体の集合を G とする. 1 より大きい G の元のうち最小のものを u とする.

(1) u を求めよ.

(2) 整数 n と G の元 g に対し, gu^n は G の元であることを示せ.

(3) G の任意の元 g は適当な整数 m によって, $g=u^m$ と書かれることを示せ.

それぞれの解答をつける.

問題 12.1

(1) $x_{n+1}-\alpha y_{n+1}=\beta(x_n-\alpha y_n)$ となる α,β を求める．

$$x_{n+1}-\alpha y_{n+1}=2x_n+3y_n-\alpha(x_n+2y_n)=\beta(x_n-\alpha y_n)$$

であるから，$2-\alpha=\beta,\ 3-2\alpha=-\alpha\beta$ となり，β を消去すると $\alpha^2=3$ となり，$\alpha=\pm\sqrt{3}$ ，したがって $\beta=2\mp\sqrt{3}$ である．

つまり，

$$\begin{cases} x_{n+1}-\sqrt{3}y_{n+1}=(2-\sqrt{3})(x_n-\sqrt{3}y_n) \\ x_{n+1}+\sqrt{3}y_{n+1}=(2+\sqrt{3})(x_n+\sqrt{3}y_n) \end{cases}$$

従って，

$$\begin{cases} x_n-\sqrt{3}y_n=(2-\sqrt{3})^{n-1}(x_1-\sqrt{3}y_1)=(2-\sqrt{3})^n \\ x_n+\sqrt{3}y_n=(2+\sqrt{3})^{n-1}(x_1+\sqrt{3}y_1)=(2+\sqrt{3})^n \end{cases}$$

これを解いて，

$$\begin{cases} x_n=\dfrac{(2+\sqrt{3})^n+(2-\sqrt{3})^n}{2} \\ y_n=\dfrac{(2+\sqrt{3})^n-(2-\sqrt{3})^n}{2\sqrt{3}} \end{cases}$$

(2) $x_n=\dfrac{a^n+b^n}{2},\ \sqrt{3}y_n=\dfrac{a^n-b^n}{2}$ である．両辺を二乗して辺々引くと

$$(x_n)^2-3(y_n)^2=a^{n-1}b^{n-1}=1$$

つまり $\mathrm{P}_n,\ n=1,2,\cdots$ はすべて，曲線 $x^2-3y^2=1$ の上にある．

注意 12.1　ここでは手短に求めたが，A^n 計算を行う方法がいくつか参考書には載っているので，それから求めても良い．

つまり，一般に二次行列はハミルトン・ケイレイの定理によって，

$$A^2+pA+qE=0$$

となる実数 p ，q があるので，

$$A^{n+2}+pA^{n+1}+qA^n=0$$

となり，三項間漸化式と同じ方法で A^n が求まる．

問題 12.2

(1) $\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}=\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}^{-1}\begin{pmatrix} x \\ y \end{pmatrix}$ より $\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}=\begin{pmatrix} x \\ y \end{pmatrix}$ である．つまり，

$$\begin{cases} x=2x_1+3y_1 \\ y=x_1+2y_1 \end{cases}$$

より，逆に解いて，

$$\begin{cases} x_1=2x-3y \\ y_1=-x+2y \end{cases}$$

である．したがって，

$$\begin{aligned} 1 &= (2x_1+3y_1)^2-3(x_1+2y_1)^2 \\ &= (4-3){x_1}^2+12x_1y_1-12x_1y_1+(9-12){y_1}^2 \\ &= {x_1}^2-3{y_1}^2 \end{aligned}$$

(2)

$$\begin{aligned} y-y_1 &= y-(-x+2y)=x-y \\ &= \frac{x^2-y^2}{x+y}=\frac{(1+3y^2)-y^2}{x+y} \\ &= \frac{1+y^2}{x+y}>0 \\ y_1 &= -x+2y \\ &= \frac{4y^2-x^2}{x+2y}=\frac{4y^2-(1+3y^2)}{x+2y} \\ &= \frac{y^2-1}{x+2y}\geqq 0 \end{aligned}$$

よって $y>y_1\geqq 0$ である．

(3) 府立大の問 1 と同様．ただし結果が与えられているので数学的帰納法で証明できる．ここでは数学的帰納法による証明をおこなおう．

$n=1$ のときは，明らかである．

$n=k$ のとき，成立するとする．すなわち $\begin{pmatrix} a_k \\ b_k \end{pmatrix}=A^k\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ で定まる (a_k,b_k) が $(2+\sqrt{3})^k=a_k+b_k\sqrt{3}$ となるとする．

すると，

$$\begin{pmatrix} a_{k+1} \\ b_{k+1} \end{pmatrix}=A^{k+1}\begin{pmatrix} 1 \\ 0 \end{pmatrix}=\begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}\begin{pmatrix} a_k \\ b_k \end{pmatrix}=\begin{pmatrix} 2a_k+3b_k \\ a_k+2b_k \end{pmatrix}$$

一方，

$$\begin{aligned} (2+\sqrt{3})^{k+1} &= (2+\sqrt{3})(a_k+b_k\sqrt{3}) \\ &= (2a_k+3b_k)+(a_k+2b_k)\sqrt{3} \\ &= a_{k+1}+b_{k+1}\sqrt{3} \end{aligned}$$

したがって，$k+1$ のときも成立する．

よってすべての自然数 n に対して成立する．

(4) $x^2-3y^2=1$ を満たす正の整数の組 (x,y) に対して，

$$\begin{cases} x_1=2x-3y \\ y_1=-x+2y \end{cases}$$

とおく.

すると (2) より $y_1 \geqq 0$ であるが，さらに

$$\begin{aligned} x_1 &= 2x - 3y \\ &= \frac{4x^2 - 9y^2}{2x + 3y} = \frac{4x^2 - 3(x^2-1)^2}{2x + 3y} \\ &= \frac{x^2 + 3}{2x + 3y} > 0 \end{aligned}$$

となるので，(x_1, y_1) は $x^2 - 3y^2 = 1$ を満たす正の整数の組である.

したがって，同じ操作を繰り返えすことができる．すなわち，順次 $(x_2, y_2), (x_3, y_3), \cdots$ を定めることができる．このとき，$y > y_1 > y_2 \cdots y_k \geqq 0$ なので，ある番号 n において $y_n = 0$ したがって $x_n = 1$ となる．すなわち $\begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^{-n} \begin{pmatrix} x \\ y \end{pmatrix}$ が $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ となる.

つまり

$$\begin{pmatrix} x \\ y \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a_n \\ b_n \end{pmatrix}$$

である.

問題 12.3

(1) 求める u を $u = a + \sqrt{2}b$ と置く． $a^2 - 2b^2 = \pm 1$ ，つまり $|(a+\sqrt{2}b)(a-\sqrt{2}b)| = 1$ である.

$u = (a + \sqrt{2}b) > 1$ だから $|a - \sqrt{2}b| < 1$.

つまり $a - \sqrt{2}b < 1$ かつ $a - \sqrt{2}b > -1$.

よって， $a + \sqrt{2}b > 1$ と辺々和と差をとることにより， $a > 0, b > 0$ が得られる.

したがって最小となるのは $a = 1, b = 1$ のときである.

(2) G の任意の二元 $g = a + \sqrt{2}b$， $g' = a' + \sqrt{2}b'$ について，$gg' \in G$ を示す.

$gg' = (aa' + 2bb') + (ab' + a'b)\sqrt{2}$ であるが，ここで,

$$\begin{aligned} (aa' + 2bb')^2 - 2(ab' + a'b)^2 &= a^2(a'^2 - 2b') - 2b^2(a'^2 - 2b') \\ &= \pm(a^2 - 2b^2) \end{aligned}$$

したがって， $gg' \in G$.

さらに， $(1 + \sqrt{2})^{-1} = (-1) + \sqrt{2} > 0$ より， G の元である．その積はつねに G に属する．G に属する元の積は再び G に属する．よってすべての整数に対して $gu^n \in G$ が示された.

(3) $g = a + \sqrt{2}b$ とする．$u > 1$ であるから u^m は m が増加すれば増加する.

今 $u^{m+1} > g \geqq u^m$ となる最大の m をとる.

したがって， $u > g \times u^{-m} \geqq 1$.

他方 (2) と同様の考察により， $g \times u^{-m} \in G$ である.

したがって u の最小性により， $g \times u^{-m} = 1$ でなければならない.

すなわち， $g = u^m$ である.

三つの問題の相互関係

大阪府立大と明治大学の問題で記号の使い方が違うが，二つの集合を

$$A = \left\{ (x_n, y_n) \,\middle|\, \begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}, n : \text{自然数} \right\}$$
$$B = \{(x, y) \mid x^2 - 3y^2 = 1, x, y \text{ 正の整数 }\}$$

と置くとき，大阪府立大の問題は，数列がペル方程式を満たすことを示せ，つまり

$$A \subset B$$

を示せといい，明治大の問題は，逆にそのペル方程式のすべての解がその数列から得られることを示せ，つまり

$$A \supset B$$

を示せといっている．

必要条件と十分条件のそれぞれが同じ年に出題されたのである．

さらに，解の集合の構造がどのようになっているかについて，観点を変えて出題したのが第三の東京工大の問題である．ここには，この問題の本質的な解法が問われている．東京工業大学の問題を一般化することでペル方程式の構造定理が得られる．

ペル方程式の解の構造

今はペル方程式に $(\pm 1,\ 0)$ 以外の解があるかどうかは，未解決である．もし解に $(\pm 1,\ 0)$ 以外の解があるなら解の集合がどのようなものになるか，これを定式化することができる．1985 年の東京工業大学の入試問題は，そのまま一般の場合の構造定理になる．さらにあわせて，数列との関係もまとめたのが次の構造定理である．

定理 41 (ペル方程式の解の構造定理)

D を平方数ではない正の整数とし，２次不定方程式 $x^2 - Dy^2 = \pm 1$ を考える．解 (x, y) の部分集合 S を次のように定める．

$$S = \{(x, y) \mid x^2 - Dy^2 = \pm 1,\ x, y \in Z,\ x + \sqrt{D}y > 0\}$$

S は $(1, 0)$ 以外の解を持つとする．

S に属し，$x + \sqrt{D}y > 1$ でかつ $x + \sqrt{D}y$ の値が最小となるものを (p, q) とする．

(1) $(x_1, y_1), (x_2, y_2) \in S$ および任意の整数 n に対し，

$$(x_1 + \sqrt{D}y_1)(x_2 + \sqrt{D}y_2)^n = s + \sqrt{D}t$$

で (s, t) を定める．$(s, t) \in S$ である．

(2) S のすべての元は，整数 n に対して，$(p + \sqrt{D}q)^n = x_n + \sqrt{D}y_n$ によって定まる (x_n, y_n) で得られる．すなわち次式が成立する．ただし，$x_1 = p, y_1 = q$ とする．

$$S = \{(x_n, y_n) \mid (p + \sqrt{D}q)^n = x_n + \sqrt{D}y_n, n \text{ は整数 }\}$$

(3) S はまた行列 $A=\begin{pmatrix} p & Dq \\ q & p \end{pmatrix}$ によって,

$$S=\left\{(x_n,y_n)\middle|\begin{pmatrix} x_n \\ y_n \end{pmatrix}=A^n\begin{pmatrix} 1 \\ 0 \end{pmatrix},\ n \text{ は整数}\right\}$$

と書ける.

証明

(1) $(x_1+\sqrt{D}y_1)(x_2+\sqrt{D}y_2)=(x_1x_2+Dy_1y_2)+(x_1y_2+x_2y_1)\sqrt{D}$

ここで,

$$\begin{aligned} & (x_1x_2+Dy_1y_2)^2-D(x_1y_2+x_2y_1)^2 \\ = \ & x_1^2x_2^2+2Dx_1x_2y_1y_2+D^2y_1^2y_2^2-Dx_1^2y_2^2-2Dx_1y_2x_2y_1-Dx_2^2y_1^2 \\ = \ & (x_1^2-Dy_1^2)(x_2^2-Dy_2^2) \\ = \ & \pm1 \end{aligned}$$

よって, $n=1$ のとき成立する.

次に, これより

$$\frac{1}{x_2+\sqrt{D}y_2}=\frac{x_2-\sqrt{D}y_2}{\pm1}=\{\pm x_2+\sqrt{D}(\mp y_2)\}\quad\text{(複号同順)}$$

$x_2+\sqrt{D}y_2>0$ であるから,

$$\frac{1}{x_2+\sqrt{D}y_2}>0$$

かつ, $(\pm x_2)^2-D(\pm y_2)^2=\pm1$ なので, $n=-1$ のときも成立し,

$$(x_1+\sqrt{D}y_1)(x_2+\sqrt{D}y_2)^{\pm1}=s+\sqrt{D}t$$

で定まる $(s,\ t)$ について,

$$(s,\ t)\in S$$

となった. そして, $(x_1,\ y_1)$, $(x_2,\ y_2)$ は任意であるから, 帰納的にすべての整数 n に対し成立する.

(2) $(s,\ t)$ を S の元で, $s+\sqrt{D}t>1$ である任意の元とする. $p+\sqrt{D}q$ の最小性により,

$$(p+\sqrt{D}q)^n\leqq s+\sqrt{D}t<(p+\sqrt{D}q)^{n+1}$$

となる n が存在する. したがって,

$$1\leqq\frac{s+\sqrt{D}t}{(p+\sqrt{D}q)^n}<p+\sqrt{D}q$$

ところが, (1) より $\dfrac{s+\sqrt{D}t}{(p+\sqrt{D}q)^n}=u+\sqrt{D}v$ で定まる $(u,\ v)$ について,

$$(u,\ v)\in S$$

である．したがって，$p+\sqrt{D}q$ の最小性により，

$$u+\sqrt{D}v=1$$

つまり，この場合ある n によって，

$$s+\sqrt{D}t=(p+\sqrt{D}q)^n$$

となった．

次に，$s+\sqrt{D}t<1$ のとき，

$$\frac{1}{s+\sqrt{D}t}>1$$

で，この $\dfrac{1}{s+\sqrt{D}t}$ について，

$$\frac{1}{s+\sqrt{D}t}=(p+\sqrt{D}q)^n$$

と表せば，

$$s+\sqrt{D}t=(p+\sqrt{D}q)^{-n}$$

となり，この場合もある整数 n によって，

$$s+\sqrt{D}t=(p+\sqrt{D}q)^n$$

となる．

逆に，$(p+\sqrt{D}q)^n=x_n+\sqrt{D}y_n$ で定まる $(x_n,\ y_n)$ は，(1) より S の元であるから，これで集合 S と集合 $\{(x_n,\ y_n)\}$ が一致することが示された．

(3)　$A=\begin{pmatrix} p & Dq \\ q & p \end{pmatrix}$ とする．

$$\begin{aligned} x_{n+1}+\sqrt{D}y_{n+1} &= (x_n+\sqrt{D}y_n)(p+\sqrt{D}q) \\ &= (x_np+Dy_nq)+\sqrt{D}(x_nq+y_np) \end{aligned}$$

よって，

$$\begin{pmatrix} x_{n+1} \\ y_{n+1} \end{pmatrix}=\begin{pmatrix} p & Dq \\ q & p \end{pmatrix}\begin{pmatrix} x_n \\ y_n \end{pmatrix}$$

となる．したがって，

$$\begin{aligned} \begin{pmatrix} x_n \\ y_n \end{pmatrix} &= A^{n-1}\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}=A^{n-1}\begin{pmatrix} p \\ q \end{pmatrix} \\ &= A^{n-1}\begin{pmatrix} p & Dq \\ q & p \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}=A^n\begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{aligned}$$

■

練習問題 12.1（解答 49）　$D=2,\ D=3$ のときに具体的に考える．

(1)　$D=2, D=3$ のとき，それぞれ上の行列 A を求めよ．

(2)　$D=3$ のとき，$x^2-3y^2=-1$ の整数解は存在しないことを示せ．

12.2 演習問題

演習問題 34 (解答 34)　［98 お茶の水女子大］

(1) 等式 $(x^2-ny^2)(z^2-nt^2)=(xz+nyt)^2-n(xt+yz)^2$ を示せ.

(2) $x^2-2y^2=-1$ の自然数解 (x,y) が無限組あることを示し，$x>100$ となる解を一組求めよ.

演習問題 35 (解答 35)　［01 滋賀医大］

xy 平面上の 2 曲線 C_+ と C_- を次の式で定義する.

$$C_+ : x^2-2y^2=1 \ (x>0,\ y>0), \quad C_- : x^2-2y^2=-1 \ (x>0,\ y>0)$$

また，点 $\mathrm{P}(x,\ y)$ に対して点 $\mathrm{Q}(u,\ v)$ を次式で定める.

$$u=-x+2y,\ v=x-y$$

点 $\mathrm{P}(x,\ y)$ は $x,\ y$ がともに整数であるとき整数点という.

(1) $\mathrm{P}(x,\ y)$ が曲線 C_+ 上の整数点ならば $\mathrm{Q}(u,\ v)$ は曲線 C_- 上の整数点であり，$\mathrm{P}(x,\ y)$ が曲線 C_- 上の整数点ならば $x=y=1$ の場合を除いて，$\mathrm{Q}(u,\ v)$ は曲線 C_+ 上の整数点であることを示せ.

(2) $\mathrm{P}(x,\ y)$ が C_+ または C_- の整数点で $y\neq 1$ ならば $0<v<y$ であることを示せ.

(3) $(\sqrt{2}+1)^n=x_n+y_n\sqrt{2}$ ($x_n,\ y_n$は整数, n は自然数) と表す．点 $\mathrm{P}(x_n,\ y_n)$ は曲線 C_+ または C_- 上にあることを示せ.

(4) 曲線 C_+ または C_- 上の整数点は $\mathrm{P}(x_n,\ y_n)$ (n は自然数) に限ることを示せ.

(5) $\displaystyle\lim_{n\to\infty}\frac{y_{n+1}-y_n}{x_{n+1}-x_n}$ を求めよ.

13　実数の近似

13.1　ディリクレの原理

ペル方程式 $x^2 - Dy^2 = \pm 1$ で解 $(\pm 1,\ 0)$ を「自明な解」という．いつでも明らかに解になるからである．そこで以下でペル方程式に自明な解以外の解が必ず存在することを証明する．存在を保証するのは，ディリクレ (P.G.Dirichlet，1805-59) によって用いられたまことに巧妙な「鳩の巣原理」と呼ばれる原理である．

鳩の巣原理

n 個の箱に $n+1$ 個のものを入れると，少なくともひとつ，2 個以上のものが入った箱が存在する．

この明快な原理によって解の存在が示される．

定理 42

ω を与えられた無理数とする．このとき

$$|x - \omega y| < \frac{1}{y}$$

となる整数 x, y が **無数に** 存在する．

証明

(i) 任意の自然数 n に対して，

$$0 < y < n,\ |x - \omega y| < \frac{1}{y}$$

となる (x, y) が少なくとも 1 組存在すること示す．

実数 $a < b$ に対して a を含み b を含まない区間を $[a, b)$ と表す．区間 $[0, 1)$ を次のように n 等分する．

$$\left[0, \frac{1}{n}\right),\ \left[\frac{1}{n}, \frac{2}{n}\right), \cdots, \left[\frac{n-1}{n}, 1\right)$$

y に $0, 1, \cdots, n$ の各値を与え，その y に対して， ωy を超えない最大の整数を x とする．

$$0 \leqq \omega y - x < 1$$

これらは全部で $n+1$ 個あるので，上の n 個のうち少なくとも一つの区間には，二つ以上の $\omega y - x$ が属する． $\omega y_1 - x_1$ ， $\omega y_2 - x_2$, $(x_1 > x_2)$ が同じ区間に属するとする．つまり

$$|(\omega y_1 - x_1) - (\omega y_2 - x_2)| < \frac{1}{n}$$

$x = x_1 - x_2$, $y = y_1 - y_2$ とおけば

$$|\omega y - x| < \frac{1}{n}$$

ところが，

$$\frac{1}{n} \leqq \frac{1}{y}$$

であるから，

$$|\omega y - x| < \frac{1}{y}$$

である．

(ii) 各自然数 n に対して少なくとも一つ $0 < y < n$ で $|\omega y - x| < \dfrac{1}{y}$ となる (x, y) が作れた．n を動かすとき，これらの (x, y) のなかに相異なるものが無数にあることを示す．

もし有限個しかなかったとする．そのなかで $|\omega y - x|$ の値が最小のものを $|\omega y_0 - x_0|$ とする．それに対して，

$$\frac{1}{n} < |\omega y_0 - x_0|$$

となる n をとる．この n に対して再び，$|\omega y - x| < \dfrac{1}{n}$ となるように (x, y) を選ぶことができる．ところが

$$|\omega y - x| < \frac{1}{n} < |\omega y_0 - x_0|$$

なので，(x_0, y_0) の最小性と矛盾した．

よって相異なるものは無数にある． ■

この定理は，鳩ノ巣原理からの帰結であった．

「近似分数が無数にあること」を示す定理 42 は，後に実数の連分数展開において，別証明を与える．

練習問題 13.1 (91 広島大学) (解答 50)　次の文章は，ある条件を満たすものが存在することを証明する際に，よく使われる「鳩の巣原理」（または，抽出（ひきだ）し論法ともいう）を説明したものである．

「 m 個のものが， n 個の箱にどのように分配されても， $m > n$ であれば，2 個以上のものが入っている箱が少なくとも一つ存在する」

この原理を用いて，次の二つの命題が成り立つことを証明せよ．

(1) 1 辺の長さが 2 の正三角形の内部に，任意に 5 個の点をとったとき，その内の 2 点で，距離が 1 より小さいものが少なくとも 1 組存在する．

(2) 座標空間で，その座標がすべて整数であるような点を格子点という．座標空間に 9 個の格子点が与えられたとき，その内の 2 点で，中点がまた格子点であるものが少なくとも 1 組存在する．

13.2　ペル方程式の解の存在

さていよいよ存在定理に進もう．ペル方程式の解の存在は後の「構成定理」からも示される．つまり，つねに解を構成する方法があることが証明されれば，結果として解の存在も示される．しかし，一般的には「存在するが一般的構成法はない」ということがある（例，五次方程式の解の公式」）ので，直接存在が示せるならばその証明は重要である．以下に直接証明を行う．

定理 43

D が正の整数で，かつ $\sqrt{D}$ が無理数であるとする．このとき方程式

$$x^2 - Dy^2 = 1$$

は，自明でない解 (X, Y), $(X > 0, Y > 0)$ をもつ．

証明　定理 42 により，

$$|x - \sqrt{D}y| < \frac{1}{y}$$

となる (x, y) $x > 0,\ y > 0$ が無数に存在する．

つまり

$$-\frac{1}{y} < x - \sqrt{D}y < \frac{1}{y}$$

従って $x + \sqrt{D} < \dfrac{1}{y} + 2\sqrt{D}y$ ．従って $|x - \sqrt{D}y| < \dfrac{1}{y}$ と乗じて，

$$|x^2 - Dy^2| < \frac{1}{y^2} + 2\sqrt{D} < 1 + 2\sqrt{D}$$

この不等式の右辺は (x, y) に無関係である．

$x^2 - Dy^2$ は $-(1 + 2\sqrt{D})$ と $(1 + 2\sqrt{D})$ の間にある (有限個の) 整数のうちのいくつかと一致する．ところが (x, y) の組は無数のあるので少なくとも一つの整数 l に対して，

$$x^2 - Dy^2 = l$$

は無数の解をもつ．

整数を l で割った余りで分類すると， l 組に分類される．整数の組 (x, y) は，l^2 個の有限個に分類される．他方 (x, y) は無数だから，分類されたどれかの組には無数の (x, y) が属する．

(s, t), (u, v) が同一の組に属するとする．

$$\begin{cases} u = s + kl \\ v = t + hl \end{cases}$$

とおく．

$tu - sv = (kt - hs)l$ である． $Y = (kt - hs)$ とおく．

一方 $s^2 - Dt^2 = l$, $u^2 - Dv^2 = l$ であるから，

$$\begin{aligned} l^2 &= (s^2 - Dt^2)(u^2 - Dv^2) \\ &= (su - Dtv)^2 - D(sv - tu)^2 \\ &= (su - Dtv)^2 - DY^2 l^2 \end{aligned}$$

つまり $(su - Dtv)^2$ が l^2 で割り切れ，したがって $(su - Dtv)$ が l で割り切れる．$su - Dtv = Xl$ と置く．

かくして

$$(Xl)^2 - D(Yl)^2 = l^2$$

つまり，

$$X^2 - DY^2 = 1$$

ゆえに解 (X,Y) は $x^2-Dy^2=l$ の解である． ■

この定理によってペル方程式はつねに自明でない解をもち，したがって前節の構造定理が空論ではないことが保証されるのである．

13.3 演習問題

演習問題 36 (解答 36) ［99 名大理系］

複素数平面において集合 $A,\ B,\ C,\ D,\ E$ を次のように定義する．

$$A=\left\{z \mid \frac{z+\bar{z}}{\sqrt{2}} \text{ は整数}\right\},\ B=\left\{z \mid \frac{z+\bar{z}}{\sqrt{3}} \text{ は整数}\right\}$$
$$C=\left\{z \mid \frac{z-\bar{z}}{\sqrt{2}i} \text{ は整数}\right\},\ D=\left\{z \mid \frac{z-\bar{z}}{\sqrt{3}i} \text{ は整数}\right\}$$
$$E=(A\cap C)\cup(A\cap D)\cup(B\cap C)\cup(B\cap D)$$

集合 E から 17 個の複素数を任意に選んでその集合を F とする．F の中に，中点が E の要素になっているような 2 点が存在することを示せ．

演習問題 37 (解答 37) ［97 京大理系］

自然数 n と n 項数列 $a_k\ (1\leqq k\leqq n)$ が与えられていて，次の条件 (i, ii) を満たしている．

(i) $a_k\ (1\leqq k\leqq n)$ はすべて正整数で，すべて 1 と $2n$ の間にある．

$$1\leqq a_k\leqq 2n$$

(ii) $s_j=\displaystyle\sum_{k=1}^{j}a_k$ とおくとき， $s_j(1\leqq j\leqq n)$ はすべて平方数である．(整数の 2 乗である数を平方数という．)

このとき

(1) $s_n=n^2$ であることを示せ．

(2) $a_k\ (1\leqq k\leqq n)$ を求めよ．

14　二次行列と実数の連分数展開

14.1　実数のメービス変換と連分数展開

メービス変換の定義

定理 7 で，一次不定方程式の解をユークリッドの互除法で構成するとき，二次行列を用いると明快な表現ができることが示された．そこで用いられた，ユークリッドの互除法を二次行列で表現する方法を再検討する．

$$a = qb + r \quad (\ 0 \leqq r < |b|\ )$$

であるとし，行列で

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r \end{pmatrix}$$

と表す．

ここで a と b の比を考えると

$$\frac{a}{b} = \frac{qb+r}{b} = \frac{q\dfrac{b}{r}+1}{\dfrac{b}{r}} = \frac{q\left(\dfrac{b}{r}\right)+1}{1\left(\dfrac{b}{r}\right)+0}$$

である．ここに q は有理数 $\dfrac{a}{b}$ の整数部分であり，$\dfrac{b}{r}$ は小数部分の逆数であることに注意しよう．

整数部分をとり，小数部分の逆数をとるという操作は，任意の実数で定義可能な操作である．この操作を行列で表現しその性質を調べることがこの節の目的である．

一般に，実数 ω に対して，成分が実数の行列 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ によって実数 $\dfrac{a\omega+b}{c\omega+d}$ を対応させる変換を**メービウス変換**と呼び，この実数を $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\omega$ と記す．これは $\omega = -\dfrac{d}{c}$ 以外のすべての実数に対して定義される．

次のことはすぐに確認される．

(1) $\begin{pmatrix} a & b \\ c & d \end{pmatrix}\left\{\begin{pmatrix} e & f \\ g & h \end{pmatrix}\omega\right\} = \left\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right\}\omega$

(2) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\omega = \omega$

(3) $\begin{pmatrix} ka & kb \\ kc & kd \end{pmatrix}\omega = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\omega$

(4) $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}\omega$　なら　$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} u = \omega$

したがって，メービウス変換をくりかえし行った結果は，各行列の積の行列によるメービウス変換の結果と一致する．これをメービウス変換の積と呼ぶ．

連分数展開

メービウス変換を用いて，実数の連分数展開が定義される．それは，実数の整数部分をとり，残された小数部分の逆数をとるという操作を繰り返すことで実現される．

ω を整数でない正の実数とする．実数 ω に対し，次の手続きを考える．

(1) ω を超えない最大の整数を q_0 とする．

(2) $\omega = q_0 + u \ \ (0 < u < 1)$ とおく．

(3) そして $\omega_1 = \dfrac{1}{u}$ する． $1 < \omega_1$ である．

このとき，

$$\omega = q_0 + \frac{1}{\omega_1} = \frac{q_0\omega_1 + 1}{\omega 1} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\omega_1$$

と，上の手続きが行列で表現される．この手続きを ω_1 に対して再び実行する．このとき，得られた q_0 と $\dfrac{1}{\omega_1}$ の番号を 1 づつ増していくと，順次 $\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}$ の型の行列と，実数 ω_{k+1} の系列が得られる．

これを ω の **連分数展開**という．すなわち $k+1$ 回この手続きを行うと，

$$\omega = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}\omega_{k+1}$$

となる．この過程で ω_{k+1} が整数になったとする．そのときはそこで展開を終えるか，または次のようにもう一つ展開して終える．

$$\omega_{k+1} = \begin{pmatrix} \omega_{k+1} - 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot 1$$

つまり，$\omega_{k+2} = 1,\ q_{k+1} = \omega_{k+1} - 1$ とする．

上の展開を「連分数展開」というのは，この手続きを一つの分数形式で書いていくと，次のようになるからである．

$$\begin{aligned} \omega &= q_0 + \frac{1}{\omega_1} \\ &= q_0 + \cfrac{1}{q_1 + \dfrac{1}{\omega_2}} \\ &= q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \dfrac{1}{q_3 + \cdots}}} \end{aligned}$$

今後，連分数展開という表現で，行列の積としてメービウス変換の積を表すこともあれば，分数形式で書いたものを表すこともある．

$(P_0,\ Q_0) = (q_0,\ 0)$ として，

$$\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}$$

で $(P_k,\ Q_k)$ を定める．$n \geqq 2$ に対して，

$$\begin{pmatrix} P_k \\ Q_k \end{pmatrix} = \begin{pmatrix} P_{k-1}q_k + P_{k-2} \\ Q_{k-1}q_k + Q_{k-2} \end{pmatrix}$$

となる．

このような展開は本質的に一意である．ω を整数でない実数とし，ω に二つの連分数展開ができたとする．

$$\begin{aligned} \omega &= \begin{pmatrix} k_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} k_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} k_n & 1 \\ 1 & 0 \end{pmatrix}\omega' \ (\omega' > 1) \\ &= \begin{pmatrix} h_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} h_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} h_m & 1 \\ 1 & 0 \end{pmatrix}\omega'' \ (\omega'' > 1) \end{aligned}$$

このとき，$n \geqq m$ であれば，

$$k_0 = h_0,\ k_1 = h_2,\ \cdots,\ k_m = h_m$$

となる．それを示すために，

$$\begin{aligned} X &= \begin{pmatrix} k_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} k_n & 1 \\ 1 & 0 \end{pmatrix}\omega' \\ Y &= \begin{pmatrix} h_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} h_m & 1 \\ 1 & 0 \end{pmatrix}\omega'' \end{aligned}$$

と置く．すると，$X > 1, Y > 1$ である．このとき，

$$\begin{aligned} \omega &= \begin{pmatrix} k_0 & 1 \\ 1 & 0 \end{pmatrix}X = k_0 + \frac{1}{X} \\ &= \begin{pmatrix} h_0 & 1 \\ 1 & 0 \end{pmatrix}Y = h_0 + \frac{1}{Y} \end{aligned}$$

となり，k_0 と h_0 は同じ実数の整数部分であるから等しい．よって $X = Y$ となるので同様の議論をくり返せば，順次

$$k_0 = h_0,\ k_1 = h_2,\ \cdots,\ k_m = h_m$$

となるからである．

また，有理数 $\dfrac{a}{b}$ の連分数展開は，ユークリッドの互除法からつくったものと一致する．

つまり，互除法による展開が次のようになったとする．

$$\begin{aligned} \begin{pmatrix} a \\ b \end{pmatrix} &= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ \text{（または）} &= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_n - 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{aligned}$$

この途中をまとめると，

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}\begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix}, k = 1, 2, \cdots, n$$

である．よって

$$\frac{a}{b} = \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} \frac{r_k}{r_{k+1}}, k = 1, 2, \cdots, n-1$$

となる．つまり, $\omega = \dfrac{a}{b}$, $\omega_{k+1} = \dfrac{r_k}{r_{k+1}}$ とおけば，実数の連分数展開と一致する．

有理数の連分数展開は必ず有限で終わるが，その長さは，最後の展開の方法の調整によって偶数・奇数のいずれのものも作ることができる．

14.2 近似分数

ω を無理数とする．ω からはじめて連分数展開をおこなっていった結果，もし $k+1$ 回の後に，ω_k が整数となって展開が終了したとすれば，それは ω が有理数であることを意味する．従って無理数の連分数展開は無限に継続される．

定理 44

ω を正の実数とする．ω の $k+1$ 回の連分数展開を,

$$\begin{aligned} \omega &= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \omega_{k+1} \\ &= \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} \omega_{k+1} \end{aligned}$$

と置く．このとき,

(1) $\dfrac{P_0}{Q_0} < \dfrac{P_2}{Q_2} < \cdots < \dfrac{P_{2k}}{Q_{2k}} < \cdots < \omega < \cdots < \dfrac{P_{2k+1}}{Q_{2k+1}} < \cdots < \dfrac{P_3}{Q_3} < \dfrac{P_1}{Q_1}$

(2) $\lim\limits_{n\to\infty} \dfrac{P_n}{Q_n} = \omega$

(3) 各 $\dfrac{P_n}{Q_n}$ は既約である．

証明

(1) $\Delta \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} = (-1)^{n+1}$ より, $P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n+1}$ ，つまり,

$$\frac{P_n}{Q_n} - \frac{P_{n-1}}{Q_{n-1}} = \frac{(-1)^{n+1}}{Q_nQ_{n-1}} \quad , \quad \frac{P_{n+1}}{Q_{n+1}} - \frac{P_n}{Q_n} = \frac{(-1)^n}{Q_nQ_{n+1}}$$

したがって

$$\frac{P_{n+1}}{Q_{n+1}} - \frac{P_{n-1}}{Q_{n-1}} = (-1)^{n+1} \frac{Q_{n+1} - Q_{n-1}}{Q_{n-1}Q_nQ_{n+1}}$$

一方, $Q_{n+1} = Q_nq_n + Q_{n-1}$ より, $Q_{n-1} < Q_n < Q_{n+1}$.

したがって

$$\frac{P_{n+1}}{Q_{n+1}} - \frac{P_{n-1}}{Q_{n-1}} = \begin{cases} > 0 & (\ n \text{ 奇数のとき}) \\ < 0 & (\ n \text{ 偶数のとき}) \end{cases}$$

また,

$$\begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix}^{-1} \omega = \left((-1)^{n+1} \begin{pmatrix} Q_{n-1} & -P_{n-1} \\ -Q_n & P_n \end{pmatrix} \right) \omega$$
$$= \frac{Q_{n-1}\omega - P_{n-1}}{-Q_n\omega + P_n} = \omega_{n+1} > 0$$

ここで $\dfrac{Q_n}{-Q_{n-1}} < 0$ を乗じて

$$\frac{\omega - \dfrac{P_{n-1}}{Q_{n-1}}}{\omega - \dfrac{P_n}{Q_n}} < 0$$

他方，明らかに $\dfrac{P_0}{Q_0} = q_1 < \omega$ ．よって

$$\frac{P_n}{Q_n} = \begin{cases} > \omega & (\ n \text{ 奇数のとき}) \\ < \omega & (\ n \text{ 偶数のとき}) \end{cases}$$

(2) N を任意の偶数とする．$\dfrac{P_N}{Q_N} < \omega < \dfrac{P_{N+1}}{Q_{N+1}}$ であるがさらに,

$$\begin{aligned} 0 &< \omega - \frac{P_N}{Q_N} < \frac{P_{N+1}}{Q_{N+1}} - \frac{P_N}{Q_N} \\ &= \frac{P_{N+1}Q_N - Q_{N+1}P_N}{Q_NQ_{N+1}} = \frac{(-1)^{N+2}}{Q_NQ_{N+1}} \\ &= \frac{1}{Q_NQ_{N+1}} < \frac{1}{Q_N^2} \end{aligned}$$

N を任意の奇数とする．同様に

$$\begin{aligned} 0 &> \omega - \frac{P_N}{Q_N} > \frac{P_{N+1}}{Q_{N+1}} - \frac{P_N}{Q_N} \\ &= \frac{P_{N+1}Q_N - Q_{N+1}P_N}{Q_NQ_{N+1}} = \frac{(-1)^{N+2}}{Q_NQ_{N+1}} \\ &= \frac{1}{Q_NQ_{N+1}} > \frac{1}{Q_N^2} \end{aligned}$$

したがって

$$0 < \left| \omega - \frac{P_N}{Q_N} \right| < \frac{1}{Q_N^2}$$

$\lim_{N\to\infty} Q_N = \infty$ だから,

$$\lim_{N\to\infty} \left| \omega - \frac{P_N}{Q_N} \right| = 0$$

である．

(3) $P_nQ_{n-1} - Q_nP_{n-1} = (-1)^{n+1}$ より，右辺は P_n, Q_n の公約数の倍数であるから，既約性は明らかである． ■

各 $\dfrac{P_n}{Q_n}$ のことを ω の **近似分数** という．無理数 ω を近似する分数 $\dfrac{P}{Q}$ が，$q < Q$ なるどんな分数 $\dfrac{p}{q}$ に対しても

$$\left|\omega - \frac{P}{Q}\right| < \left|\omega - \frac{p}{q}\right|$$

がなりたつとき，分数 $\dfrac{P}{Q}$ を無理数 ω の**最良近似分数**という．

定理 45

各 n に対して分数 $\dfrac{P_n}{Q_n}$ は最良近似分数である．

証明　一般に正の数 $A,\ B,\ C,\ D$ に対し，二つの分数 $\dfrac{A}{B},\ \dfrac{C}{D}$ で $AD - BC = 1$ であるものを考える．このとき二つの分数は既約で，両分数の差は $\dfrac{1}{BD}$ である．

この二つの分数の間にある任意の分数 $\dfrac{X}{Y}$ をとる．

$$\frac{C}{D} < \frac{X}{Y} < \frac{A}{B}$$

とする．これから $DX - CY > 0,\ AY - BX > 0$ である．

そこで

$$\begin{cases} Ax + Cy = X \\ Bx + Dy = Y \end{cases}$$

となる $x,\ y$ を求めるとこれがちょうど

$$x = DX - CY,\ y = AY - BX$$

となる．そして $x > 0,\ y > 0$ であるから

$$X > A,\ X > C,\ Y > B,\ Y > D$$

となる．

ここで分数 $\dfrac{p}{q}$ が

$$\frac{P_{2k}}{Q_{2k}} < \frac{p}{q} < \frac{P_{2k+1}}{Q_{2k+1}}$$

の範囲にあれば $P_{2k+1}Q_{2k} - Q_{2k+1}P_{2k} = 1$ なので，上の考察より $q > Q_{2k},\ Q_{2k+1}$ である．つまり，$\dfrac{P_{2k}}{Q_{2k}} < \dfrac{p}{q} < \omega$ や $\omega < \dfrac{p}{q} < \dfrac{P_{2k+1}}{Q_{2k+1}}$ となる分数 $\dfrac{p}{q}$ の分母は $Q_{2k},\ Q_{2k+1}$ より大きい．

すなわち $\dfrac{P_{2k}}{Q_{2k}},\ \dfrac{P_{2k+1}}{Q_{2k+1}}$ は最良近似分数である．　■

次の定理は，第 13 節「ペル方程式の解の存在」の中の「近似分数が無数にあること」を示す定理 42 の別証明になっている．ここで x と y の関係を定理 42 の逆にしている．定理 42 では $x^2 - \sqrt{D}y^2 = \pm 1$ との関係で $|x - \omega y|$ を考えた．ここでは無理数 ω を座標上の格子点 $(x,\ y)$ で $\omega = \dfrac{y}{x}$ と近似することを考えるので $|\omega x - y|$ を考察する．

定理 46

ω が与えられた無理数とすると

$$|\omega x - y| < \frac{1}{x}$$

となる整数 x, y が **無数に** 存在する.

証明 定理 44 の証明より,

$$|P_N - \omega Q_N| < \frac{1}{Q_N}$$

すなわち, $x = Q_N,\ y = P_N$ は条件を満たす. N は無数に取ることができ, 各近似分数は既約で $x = Q_N,\ y = P_N$ は異なるので, 実際に無数の組が存在する. ■

14.3 実数の対等

二つの実数 ω と θ が, 整数でかつ $ad - bc = \pm 1$ である $a,\ b,\ c,\ d$ によって

$$\omega = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \theta$$

となっているとき, ω と θ は **対等** であるという.

$\omega = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \theta$ なら, $\theta = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \omega$ であるから, 一方が他方に対等であれば逆も対等である.

定理 47 (対等な無理数の基本性質)

ω と θ が対等な無理数で, $\omega = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \theta$ かつ, $\theta > 1\ ,\ c > d > 0$ ならば, ω の連分数展開の途中に θ が現れる.

証明

$$\omega = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \theta\ ,\ ad - bc = e = \pm 1$$

とする, a と c は互いに素なのでそのユークリッドの互除法を

$$\begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} k_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} k_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

とする. 互いに素な整数の組の展開の個数 n は偶数奇数いずれにもできるので, $e = (-1)^{n+1}$ となる方の n にしておく.

$$\begin{pmatrix} k_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} k_n & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix}$$

とおく.

つまり

$$\begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

すると, $a=P_n,\ c=Q_n$ でさらに $P_nQ_{n-1}-Q_nP_{n-1}=e$ ，つまり $aQ_{n-1}-cP_{n-1}=e$ ．よって $ad-bc=e$ より, $a(d-Q_{n-1})=c(b-P_{n-1})$ ．ところが a と c は互いに素であるから, $d-Q_{n-1}$ は c で割り切れる．

他方 $c>d>0$ かつ $c=Q_n\geqq Q_{n-1}\geqq 0$ より, $|d-Q_{n-1}|<c$ ．したがって $d=Q_{n-1}$ ．その結果 $b=P_{n-1}$ になる．

したがって, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 自身が $\begin{pmatrix} a \\ c \end{pmatrix}$ の展開を用いて

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} k_0 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} k_n & 1 \\ 1 & 0 \end{pmatrix}$$

となる．つまり

$$\omega=\begin{pmatrix} k_0 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} k_n & 1 \\ 1 & 0 \end{pmatrix}\theta$$

となる．$\theta>1$ であるから，展開の一意性より確かに ω の連分数展開（の一部）そのものである．
■

連分数展開の途中に現れる実数は，つねに対等であることに注意しよう．

例 14.1　連分数展開によって $\sqrt{2}$ の近似分数列を求めよう．

$$\begin{aligned}
\sqrt{2} &= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\left(\frac{1}{\sqrt{2}-1}\right)=\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}(\sqrt{2}+1) \\
&= \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}(\sqrt{2}+1)=\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}(\sqrt{2}+1) \\
&= \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}(\sqrt{2}+1)=\begin{pmatrix} 7 & 3 \\ 5 & 2 \end{pmatrix}(\sqrt{2}+1) \\
&= \begin{pmatrix} 7 & 3 \\ 5 & 2 \end{pmatrix}\begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix}(\sqrt{2}+1)=\begin{pmatrix} 17 & 7 \\ 12 & 5 \end{pmatrix}(\sqrt{2}+1) \\
\cdots &\quad \cdots
\end{aligned}$$

こうして,

$$\frac{1}{1}<\frac{7}{5}<\cdots<\sqrt{2}<\cdots<\frac{17}{12}<\frac{3}{2}$$

という近似分数列が得られる．

練習問題 14.1 (解答 51)　$\sqrt{7}$ の近似分数を 5 番目まで作れ．

14.4　演習問題

演習問題 38 (解答 38)　［00 上智大後期理工］

a を正の無理数とする．$a_0=a$ とおく．a_0 に対して, a_0 を超えない最大の整数を k_0 とおき,

$$a_0=k_0+\frac{1}{a_1}$$

によって a_1 を決める. このようにして a_n まで決めたとき, この a_n に対して, a_n を超えない最大の整数を k_n とおき,

$$a_n = k_n + \frac{1}{a_{n+1}}$$

によって a_{n+1} を決める.

また, 数列 $\{P_n\}$ $(n = 0,\ 1,\ 2,\ \cdots,\ )$, $\{Q_n\}$ $(\ n = 0,\ 1,\ 2,\ \cdots,\ )$ を次の漸化式で定義する.

$$\begin{aligned} P_0 = 1,\ P_1 = k_0,\ P_{n+1} &= P_{n-1} + k_n P_n\ (n = 1,\ 2,\ \cdots) \\ Q_0 = 0,\ Q_1 = 1,\ Q_{n+1} &= Q_{n-1} + k_n Q_n\ (n = 1,\ 2,\ \cdots) \end{aligned}$$

このとき次のことが成り立つことを示せ.

(1) $P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n$ $(n = 1,\ 2,\ \cdots)$

(2) $n \geqq 1$ のとき, P_n と Q_n の最大公約数は 1 である.

(3) $a = \dfrac{P_{n-1} + P_n a_n}{Q_{n-1} + Q_n a_n}$ $(n = 1,\ 2,\ \cdots)$

(4) $\left| a - \dfrac{P_n}{Q_n} \right| < \dfrac{1}{Q_n^2}$ $(n = 1,\ 2,\ \cdots)$

15　数の幾何

15.1　格子点と近似分数

格子点

後により一般的な格子点は後に定義する．ここではまず高校数学で登場する格子点から考えはじめよう．

xy 座標平面の点で，x 座標，y 座標とも整数である点を**格子点**という.「格子」という言葉の意味を知らない人も多いと思われるので，平安時代の「格子」のある絵を紹介する．

「格子」とはもともとこのように細い角材を縦横に組み合わせて作った建具．寝殿造りの建具である蔀（しとみ）のこと.『竹取物語』に「かうし共も、人はなくしてあきぬ」などとある．さらに細い木や竹などを、縦横に間をすかして組んで、窓や戸口の外などに打ちつけたものをいう．

このような格子点を最初に研究したのはガウス (Gauss，1777-1855) である．それを引き継ぎ整数問題の各方面に応用したのが，ミンコフスキー (H.Minkowski，1864-1909) である．彼はドイツの幾何学者で，彼は幾何学的考察を整数論に適用し，いわゆる『数の幾何』なる分野を開拓した．

ミンコフスキー の定理

さて，一定の (連続な) 曲線で囲まれた平面領域が**凸形**であるとは，その領域内の任意の 2 点を結ぶ線分の全体がこの領域に含まれることをいう．Minkowski は一般的に n 次元空間での凸形の研究をし,「ミンコフスキーの定理」と呼ばれる定理を得た．それはさらに進んだ整数論で有用な定理なのであるが，ここでは二次元の場合について証明しその応用を考えよう．

定理 48 (ミンコフスキーの定理)
平面上の格子点を対称の中心とする点対称な面積 4 の凸形は，その内部あるいは境界線上に，中心の格子点以外の格子点を少なくとも一つ含む．

これを拡張した次の定理を証明する．

定理 49
s を任意の正数とする．平面上に面積 s の任意の平面図形 F がある． F に適当な平行移動をおこなって，F の内部か周に含まれる格子点の数 k を s よりも大きくすることができる．

証明　図形 F を xy 平面上に置く． m と n を任意の整数とし，図形 F を直線群 $x = m, y = n$ を引き，いくつかの一辺の長さ 1 の正方形に含まれる小領域に分割する．分割の境界は分割された双方に入れる．

小領域を含むこれらの正方形をおのおの平行に移動し，一つの正方形の上に重ねる．このとき F の面積が s であるから，一般に s より多くの小領域が重なっている点が存在する．なぜならもしどの点での重なりも s より少なければ，一辺の長さが 1 の正方形を十分細かな小片に細分して，各小片上の重なりが s より少なくできる．従ってそれらの面積の総和も s より小さくなるからである．s が整数のとき分割された境界でのみ重なりが s を越えることがあり得るが，この場合はそ

の境界上の点をとる．s が整数で，領域が正方形 s 枚ちょうどからできているときにかぎり, s 個の点の重なりしかないがこの場合ははじめから平行移動する必要がない．

従って自明な最後の場合を除き，領域の重なりが s より大きい点が存在する．そのときの重なりの個数を k とする． $s < k$ である．

この点を分割された各正方形に記し，これらの正方形を元の位置に戻す．すると F 上に点列 $\mathrm{P}_1,\ \mathrm{P}_2,\ \cdots,\ \mathrm{P}_k$ ができ，これらの任意の 2 点間の x 座標, y 座標の差はどれも整数である．P_1 が格子点に来るように平行移動させれば，$\mathrm{P}_1,\ \mathrm{P}_2,\ \cdots,\ \mathrm{P}_k$ はすべて格子点である． ■

これをもとに定理 48 を証明しよう．

証明　図形 F は，面積が 4 で，原点 O を対称の中心とするとしてよい．

O を中心に F を 長さで $\dfrac{1}{2}$ に縮小した図形を F' とする．F' は面積が 1 であるから， F' の内部あるいは周上に，2 点 $\mathrm{P}(x,\ y)$ と $\mathrm{P}'(x',\ y')$ で，その差 $x-x',\ y-y'$ がともに整数であるものが存在する．

F' も O に関して対称であるから， P の対称点 $\mathrm{Q}(-x,\ -y)$ も F' の周か内部にある．さらに F' も凸形であるから P′Q が F' に含まれ，特にその中点 $\mathrm{M}'\left(\dfrac{x'-x}{2},\ \dfrac{y'-y}{2}\right)$ も F' に含まれる．

P と P′ は異なる点なので M′ は O と異なる．

そこで OM′ を 2 倍に拡大した点を M とすれば M は F の周か内部にあり, $\mathrm{M}(x-x',\ y-y')$ であるから確かに格子点である． ■

実数を有理数で近似するという問題に関して，ミンコフスキーの定理は非常に有効である．

定理 50

$\alpha,\ \beta,\ \gamma,\ \delta$ は実数で $\Delta = \alpha\delta - \beta\gamma \neq 0$ とする．また $h,\ k$ は正数で $hk = \Delta$ とする．このとき

$$\begin{cases} |\alpha x + \beta y| \leqq h \\ |\gamma x + \delta y| \leqq k \end{cases}$$

は $x = y = 0$ 以外の整数解を有する．

証明　この連立不等式が定める領域を F とする． F に点 $(x,\ y)$ が属すれば $(-x,\ -y)$ も属するから原点対称である．

F の面積は

$$0 \leqq \alpha x + \beta y \leqq h \quad , \quad 0 \leqq \gamma x + \delta y \leqq k$$

で定まる平行四辺形の 4 倍である．この平行四辺形の一つの頂点は原点で，その両隣の頂点はそれぞれ

$$\begin{cases} \alpha x + \beta y = h \\ \gamma x + \delta y = 0 \end{cases} , \quad \begin{cases} \alpha x + \beta y = 0 \\ \gamma x + \delta y = k \end{cases}$$

の交点で，それは $\left(\dfrac{\delta h}{\Delta},\ -\dfrac{\gamma h}{\Delta}\right)$, $\left(-\dfrac{\beta k}{\Delta},\ \dfrac{\alpha k}{\Delta}\right)$ である．したがって F 面積は

$$4 \times \left| \frac{\delta h}{\Delta}\frac{\alpha k}{\Delta} - \frac{\gamma h}{\Delta}\frac{\beta k}{\Delta} \right| = 4 \times \frac{(\alpha\delta - \beta\gamma)hk}{\Delta^2} = 4$$

ゆえにミンコフスキーの定理から， F は原点以外の格子点を含む． ■

ここで，ω を与えられた無理数とする．このとき $\alpha=\omega,\ \beta=-1,\ \gamma=1,\ \delta=0$ とすれば $\Delta=1$ である．よって $h=\dfrac{1}{n},\ k=n$ とすれば，

$$|\omega x-y|\leqq\frac{1}{n},\ |x|\leqq n$$

となる原点以外の格子点 $(x,\ y)$ が任意の正数 n に対して存在する． n を消去すると

$$|\omega x-y|\leqq\frac{1}{x}$$

となる．ゆえにこれは近似定理 (定理 42) の別証明になっている．

練習問題 15.1 (解答 52)　$a,\ b,\ c$ は実数で， $a>0,\ D=b^2-4ac<0$ ならば，

$$ax^2+bxy+cy^2\leqq\frac{2\sqrt{-D}}{\pi}$$

は $(0,\ 0)$ 以外の整数解をもつ．

15.2　連分数と格子点

一般の格子点

xy 座標平面の二つの点 $\mathrm{A}(a,\ b),\ \mathrm{B}(c,\ d)$ をとる．ここで直線 OA と OB は平行でないとする．整数 $m,\ n$ に対して

$$\overrightarrow{\mathrm{OP}}=m\overrightarrow{\mathrm{OA}}+n\overrightarrow{\mathrm{OB}}$$

で定まる点 P を**格子点**という．そして基本になるベクトル $\overrightarrow{\mathrm{OA}},\ \overrightarrow{\mathrm{OB}}$ を単位として，原点から規則正しく排列された格子点，およびそれらの点を結ぶ線とそれらの線で囲まれた面の総体を「格子」という．基本ベクトル $\overrightarrow{e_1}=(1,\ 0),\ \overrightarrow{e_2}=(0,1)$ で定まる格子をとくに**正方格子**という．

ここで，$a,\ b,\ c,\ d$ を整数としさらに $ad-bc=\pm1$ であるとする．任意の整数の組 $(u,\ v)$ に対して

$$\begin{cases}u=ma+nc\\ v=mb+nd\end{cases}$$

とすると，

$$\begin{cases}m=\pm(ud-vc)\\ n=\pm(-ub+va)\end{cases}$$

と逆に解ける．

したがってこの場合，ベクトル $\overrightarrow{\mathrm{OA}},\ \overrightarrow{\mathrm{OB}}$ で定まる格子点の全体と正方格子の格子点の全体とが一致する．

連分数による実数の近似と格子

無理数 ω を近似分数で近似する過程は格子点でどのように作図されるのか.

$$\begin{aligned}\omega &= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} \omega_{k+1} \\ &= \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} \omega_{k+1}\end{aligned}$$

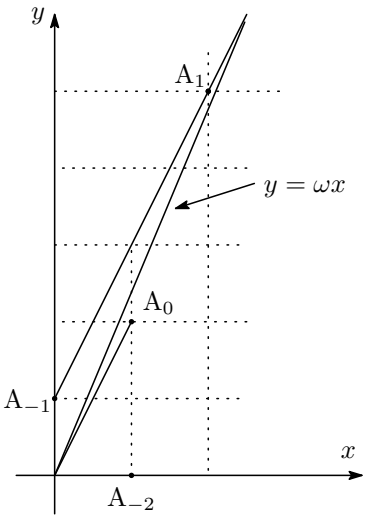
で

$$\begin{pmatrix} P_k \\ Q_k \end{pmatrix} = \begin{pmatrix} P_{k-1}q_k + P_{k-2} \\ Q_{k-1}q_k + Q_{k-2} \end{pmatrix}$$

となるのであった.

このとき点 $\mathrm{A}_k(P_k,\ Q_k)$ は次のように作図される.

xy 座標と正方格子を準備する.



まず直線 $y = \omega x$ を描く. この直線を ω線 と呼ぶ. $\mathrm{A}_{-2}(1,\ 0)$, $\mathrm{A}_{-1}(0,\ 1)$ とおく. 直線 $x = 1$ 上, $y = \omega x$ を越えない y 座標最大の格子点が $\mathrm{A}_0(1,\ q_0)$ である.

次に $\mathrm{A}_{-1}(1,\ 0)$ を通り, $\overrightarrow{\mathrm{OA}_0}$ に平行な直線

$$\begin{aligned} l_1 \quad &: \quad \overrightarrow{\mathrm{OA}_{-1}} + t\overrightarrow{\mathrm{OA}_0} \\ &= \quad (t,\ tq_0 + 1)\end{aligned}$$

を引く.

$$tq_0 + 1 \geqq \omega t \quad \Longleftrightarrow \quad \frac{1}{\omega - q_0} \geqq t$$

であるから, $\dfrac{1}{\omega - q_0} \geqq t$ を満たす最大の整数 q_1 は, この直線 ω線 を越える直前の格子点を与える整数 t であることがわかる. この t を q_1 とおく.

このときその格子点が A_1 である. つまり

$$\mathrm{A}_1(q_1,\ q_0q_1 + 1)$$

確かに

$$\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} q_0q_1 + 1 & q_0 \\ q_1 & 1 \end{pmatrix}$$

なので $P_1 = q_0q_1 + 1,\ Q_1 = q_0$ である.

$\mathrm{A_{k-2}}$, $\mathrm{A_{k-1}}$ が定まったときに直線

$$\begin{aligned} l_k &: \overrightarrow{\mathrm{OA_{k-2}}} + t\overrightarrow{\mathrm{OA_{k-1}}} \\ &= (Q_{k-2} + tQ_{k-1},\ P_{k-2} + tP_{k-1}) \end{aligned}$$

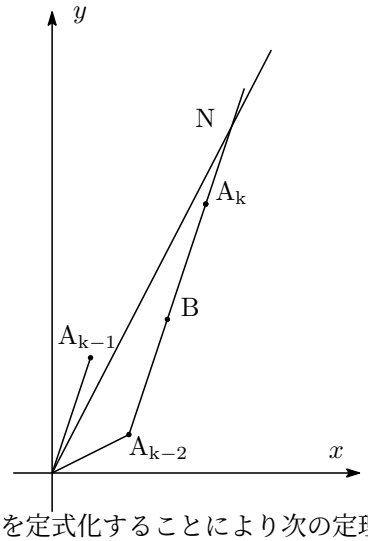
を引く．$\mathrm{A_k}$ は一般に偶数なら ω線 の下に，奇数なら ω線 の上にある．

$$\omega = \begin{pmatrix} P_{k-1} & P_{k-2} \\ Q_{k-1} & Q_{k-2} \end{pmatrix}, \quad \omega_k = \frac{\omega_k P_{k-1} + P_{k-2}}{\omega_k Q_{k-1} + Q_{k-2}}$$

であるから，

$$\begin{aligned} & \omega(Q_{k-2} + tQ_{k-1}) - P_{k-2} + tP_{k-1} > 0 \\ \Longleftrightarrow\quad & \frac{\omega_k P_{k-1} + P_{k-2}}{\omega_k Q_{k-1} + Q_{k-2}} - \frac{tP_{k-1} + P_{k-2}}{tQ_{k-1} + Q_{k-2}} > 0 \\ \Longleftrightarrow\quad & (\omega_k - t)(P_{k-1}Q_{k-2} - P_{k-2}Q_{k-1}) = (-1)^k(\omega_k - t) \end{aligned}$$

したがって，ω_k に下から (k 偶数のとき)，または上から (k 奇数のとき) もっとも近い t を決定することは，直線 l_k が ω線 を越える直前の格子点を決定することと同値になり，この格子点が $\mathrm{A_k}$ である．



$t = 1$ から $\mathrm{A_k}$ を与える t までの各 t の値に対して順次線分 $\mathrm{A_{k-2}A_k}$ 上の格子点が定まり，これ以外にはない．
このように直線 $\mathrm{A_{k-2}A_k}$ の傾きは ω線 の傾きに近づき，ω線 の両側にできる二つの折れ線 $\mathrm{A_{-2}A_0A_2A_4}\cdots$ と $\mathrm{A_{-1}A_1A_3A_5}\cdots$ の間には格子点が一つも存在しない．
格子点 $\mathrm{A_k}$ は，$\mathrm{A_k}$ と ω線 に関して同じ側にありその x 座標が $\mathrm{A_k}$ の x 座標より小さいどの格子点より，ω線 に近い．

このことを定式化することにより次の定理が得られる．

定理 51

ω は与えられた無理数, A は与えられた正の定数で，

$$0 < x \leqq A$$

とする．

(1) $\omega x - y$ を正で最小にする格子点 $(x,\ y)$ は，$Q_{2n} < A$ を満たす最大の $2n$ を k とするとき，線分 $\mathrm{A_kA_{k+2}}$ 上の格子点で x 座標が A を越えないものによって与えられる．

(2) $y - \omega x$ を正で最小にする格子点 $(x,\ y)$ は，$Q_{2n-1} < A$ を満たす最大の $2n-1$ を k とするとき，線分 $\mathrm{A_kA_{k+2}}$ 上の格子点で x 座標が A を越えないものによって与えられる．

(3) (ラグランジュの定理) $|\omega x - y|$ を最小にする x と y の整数値は

$$x = Q_n, \quad y = P_n$$

である．ただし, P_n, Q_n は ω の連分数展開から得られる近似分数 $\dfrac{P_n}{Q_n}$ で A を越えない最大分母，すなわち $Q_n \leqq A < Q_{n+1}$ となるものの分子分母である．

証明

(1) $\omega x - y$ は ω線 と格子点 $(x,\ y)$ の y 軸方向に関する距離であるがその大小と，格子点 $(x,\ y)$ と ω線 との垂直距離の大小とは一致する．このことに注意すればすでに証明は済んでいる．

(2) (1) と同様である．

(3) 図のように，線分 $\mathrm{A_{k-2}A_k}$ 上の他の格子点を B とし, $\mathrm{A_{k-2}A_k}$ と ω線 との交点を L とする．$\mathrm{OA_{k-1}}$ と $\mathrm{A_{k-2}A_k}$ は平行なので格子点 $\mathrm{A_{k-1}}$，$\mathrm{A_{k-2}}$，B，$\mathrm{A_k}$ と ω線 との距離は，$\mathrm{OA_{k-1}}$, $\mathrm{LA_{k-2}}$, LB, $\mathrm{LA_k}$ と比例している．

明らかに格子点 B から ω線 への距離は $\mathrm{A_{k-1}}$ から ω線 への距離より大きい．

したがって題意をみたす格子点は $\mathrm{A_n}$ のなかで x 座標が A を超えない最大のものによって与えられる． ■

一次形式 $x - \omega y$ で，x と y は整数値のみをとるとし，さらに $y \neq 0$ とする．このときこの一次形式の絶対値はいくらでも小さくすることができた．つまり無理数 ω は有理数 $\dfrac{P_n}{Q_n}$ で

$$\left|\omega - \frac{P_n}{Q_n}\right| < \frac{1}{{Q_n}^2}$$

と近似することができた．ところがここでもし近似有理数の分母の範囲に制限を加えるとどうなるか，というのがこの定理の趣旨である．この定理の証明は格子点の考察なしにおこなうこともできるが，格子点を用いる方がはるかに明瞭になる．

格子点の理論を用いて，無理数の近似の程度の関するさらに詳しい結果を紹介しよう．

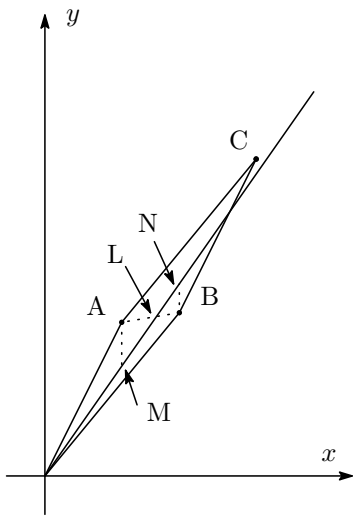
定理 52 (ヴァーレンの定理)

隣りあう二つの近似分数の少なくとも一方は

$$\left|\omega - \frac{P_n}{Q_n}\right| < \frac{1}{2{Q_n}^2}$$

を満たす.

証明



A$(Q,\ P)$ と B$(Q',\ P')$ を隣りあう二つの近似分数に対応する格子点とする．平行四辺形 OACB を作る． $Q' > Q$ とすれば B が A よりも ω線に近い (AM $>$ BN)．ゆえに AL $>$ BL が成り立つ．

$$\therefore \quad \triangle \mathrm{LAM} > \triangle \mathrm{LBN}$$

したがって

$$\triangle \mathrm{OAM} + \triangle \mathrm{OBN} < \triangle \mathrm{OBA} = \frac{1}{2}$$

ゆえに $\triangle$OAM または $\triangle$OBN のいずれかは $\dfrac{1}{4}$ より小さい．

しかるに

$$\triangle \mathrm{OAM} = \frac{1}{2}\left|Q(Q\omega - P)\right|,\ \triangle \mathrm{OBN} = \frac{1}{2}\left|Q'(Q'\omega - P')\right|$$

$$\therefore \quad \left|Q(Q\omega - P)\right| < \frac{1}{2},\ \text{または } \left|Q'(Q'\omega - P')\right| < \frac{1}{2}$$

つまり題意が示された． ■

15.3 演習問題

演習問題 39 (解答 39) ［京大過去問］

座標平面において， $x,\ y$ がともに整数であるような点 $(x,\ y)$ を格子点と呼ぶことにする．この平面上で

(1) 辺の長さが 1 で，辺が座標軸に平行な正方形 (周をこめる) は少なくとも一つの格子点を含むことを証明せよ．

(2) 辺の長さが $\sqrt{2}$ の正方形 (周をこめる) は，どんな位置にあっても，少なくとも一つの格子点を含むことを証明せよ．

演習問題 40 (解答 40) ［新潟大過去問］

$a,\ b,\ c,\ d$ は自然数で， A$(a,\ b)$, B$(a+c,\ b+d)$, C$(c,\ d)$, O$(0,\ 0)$ とする．これらを頂点とする平行四辺形 OABC の周を除いた内部を S とするとき，

(1) $ad - bc = 1$ のとき, S の中には格子点はないことを示せ．

(2) $ad - bc = 2$ のとき, S の中に格子点があれば，それは平行四辺形の対角線の交点であることを示せ．

演習問題 41 (解答 41) ［92 東大］

xy 平面において， x 座標， y 座標ともに整数であるような点を格子点と呼ぶ．格子点を頂点にもつ三角形 ABC を考える．

(1) 辺 AB, AC それぞれの上に両端をのぞいて奇数個の格子点があるとすると，辺 BC 上にも両端を除いて奇数個の格子点があることを示せ.

(2) 辺 AB, AC 上に両端をのぞいてちょうど 3 個ずつ格子点が存在するとすると，三角形 ABC の面積は 8 で割り切れる整数であることを示せ.

演習問題 42 (解答 42)　［御茶ノ水女子大改題］

(1) 平面上で，3 頂点の座標がすべて整数の組であるような三角形の面積の二倍は整数であることを示せ.

(2) 平面上で，3 頂点の座標がすべて整数の組であるような正三角形は存在するか.

(3) 平面上で，5 頂点の座標がすべて整数の組であるような正五角形は存在するか.

16　二次無理数の連分数展開

16.1　二次無理数の連分数展開

整数係数の二次方程式，$px^2+qx+r=0$ でその判別式が正かつ平方数でないとする．このときこの方程式の根を**二次（実）無理数**と呼ぶ．逆に二次無理数が満たす整係数の二次方程式を，その二次無理数の二次方程式という．

二次無理数の理論は，あまり他の知識を必要とせず理解できる大変美しい理論であるが，殘念ながら高校では習わない．ぜひ意慾的な高校生が，実際に計算をしながら学び理解してほしい．

補題 5　二次無理数の二次方程式は，定数倍を除いて一意である．

証明　なぜなら，ω が $px^2+qx+r=0$ 解であるとして，さらに $p'x^2+q'x+r'=0$ の解でもあるとする．u を有理数とし，$p'=pu$ とする．従って，$(q'-uq)\omega+(r'-ru)=0$ となるが，ω が無理数で各係数が整数なので $q'=qu$, $r'=ru$ となる．■

二次無理数 ω に対し，ω が属する二次方程式のもう一つの根を ω の共役根と呼ぶ．

定理 53 (二次無理数の展開と判別式)

(1) 二次実無理数に対等な無理数は，再び二次無理数である．

(2) 対等な二次無理数の二次方程式の判別式は等しい．

証明

(1)

$$\omega_1=\frac{a\omega_0+b}{c\omega_0+d}$$

と置く．ω_1 が $px^2+qx+r=0$ をみたすとする．この二次方程式の判別式を D とする．

$$p\left(\frac{a\omega_0+b}{c\omega_0+d}\right)^2+q\left(\frac{a\omega_0+b}{c\omega_0+d}\right)+r=0$$

分母をはらってまとめると，

$$\begin{aligned}&(pa^2+qac+rc^2)\omega_0^2\\&\quad+\{2pab+q(ad+bc)+2rcd\}\omega_0+(pb^2+qbd+rd^2)=0\end{aligned}$$

こうして，ω_0 は整数を係数とする二次方程式の解となり，たしかに二次無理数である．

(2) この二次方程式の判別式を D' とする．さらに

$$\begin{aligned}D' &= \{2pab+q(ad+bc)+2rcd\}^2\\&\quad -4(pa^2+qac+rc^2)(pb^2+qbd+rd^2)\\&= q^2(ad-bc)^2-4pr(ad-bc)^2\\&= q^2-4pr=D\end{aligned}$$

確かに二つの二次方程式の判別式は等しい．■

ここで，最も重要な論点となる定理を証明しよう．それは **二次実無理数の連分数展開は循環する** ということである．既出の例のように， $\sqrt{2}$ は第 2 項目から循環し，循環の長さは 1 である．このような循環性がすべての実二次無理数で成り立つのである．

その証明のための次の事実に注意しよう．

補題 6　整数係数の二次方程式 $px^2+qx+r=0$ で，判別式が D （一定）であって，さらに p,q,r が互いに素かつ $pr<0$ であるようなものは，有限個しかない．

証明　なぜなら，$4pr=q^2-D<0$ より $q^2<D$ ．従って q は有限個である．各 q に対して，$4pr=q^2-D<0$ を満たす整数の組 (p,r) は，右辺の因数分解を 4 と p と q に分ける場合の数なので有限個である．　■

定理 54 (実二次無理数の基本性質)

実二次無理数の連分数展開は循環する．すなわち，あるところから一定の周期をもって同じ展開が繰りかえす．また，循環のはじまる N は $\omega_N>1, -1<\omega'_N<0$ となる最初の番号である．

証明　いくつかの段階に分けて考えよう．正のもので証明できればよく，また共役なもののいずれかで証明できればよいので ω を正な二次無理数で， ω' をその共役無理数とし，$\omega>\omega'$ とする．

(i) ω の $k+1$ までの展開を次のようにおく．

$$\omega=\begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}\omega_{k+1}$$

したがって ω_{k+1} の共役をとると，

$$\omega'=\begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}\omega'_{k+1}$$

これから

$$\begin{aligned}\omega'_{k+1} &= \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}^{-1}\omega'=(-1)^{k+1}\begin{pmatrix} Q_{k-1} & -P_{k-1} \\ -Q_k & P_k \end{pmatrix}\omega' \\ &= \frac{Q_{k-1}\omega'-P_{k-1}}{Q_k\omega'-P_k}=-\frac{Q_{k-1}}{Q_k}\cdot\frac{\omega'-\dfrac{P_{k-1}}{Q_{k-1}}}{\omega'-\dfrac{P_k}{Q_k}}\end{aligned}$$

ところが,

$$\lim_{k\to\infty}\frac{P_{k-1}}{Q_{k-1}}=\omega,\ \lim_{k\to\infty}\frac{P_k}{Q_k}=\omega$$

であるから十分大きな k に対して,

$$\omega'-\frac{P_{k-1}}{Q_{k-1}}<0,\ \omega'-\frac{P_k}{Q_k}<0$$

したがって， $\omega'_{k+1}<0$ となる．

他方 ω_{k+1} は ω_k から整数部分を除いた小数部分の逆数なので $\omega_{k+1}>1$ である．

さらに $\omega'_{k+1} < 0$ とすれば

$$\omega'_{k+1} = \begin{pmatrix} q_{k+1} & 1 \\ 1 & 0 \end{pmatrix} \omega'_{k+2}$$

であるが，逆に解いて，

$$\frac{1}{\omega'_{k+1} - q_{k+1}} = \omega'_{k+2}$$

である．このとき， $q_{k+1} \geqq 1$ より $-1 < \omega'_{k+2} < 0$ である．

(ii) まとめると，

$$\omega = \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} \omega_{k+1}$$

とすれば， $\omega_{k+1}, \omega_{k+2}, \omega_{k+3}, \cdots$ はすべて同一の判別式の二次方程式の解であり，上の論証過程より共役無理数が負である．

これらの二次方程式は二つの根の積が負で判別式が同一なので，補題 6 より $\omega_{k+1}, \omega_{k+2}, \omega_{k+3}, \cdots$ の中に異なるものは有限個しかない．

ゆえにある番号 N と j があって，

$$\omega_1, \omega_2, \cdots \omega_N, \omega_{N+1}, \cdots, \omega_{N+j} = \omega_N \cdots$$

となり，以下 N と $N+j$ の間の無理数が繰り返し現れる．

(iii) このような N, j のうち j が最小となる j を k とする．すると $\omega_{N+j} = \omega_N$ なる j はすべて k の倍数である．

一般に一列に並んでいる数学的な対象が a 回毎にくり返しさらに b 回毎にくり返せば $|a-b|$ 回毎にもくり返す．なぜなら x 回目のその対象を $f(x)$ と書けば，$f(x+a) = f(x), f(x+b) = f(x)$ がつねに成立することから，

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

が成立するからである．

このことに注意して， j を k で割った余りを r とおく．

$$j = km + r$$

である．

ゆえに $r = j - km$ でもくり返すので k の最小性により， $r = 0$ ．つまり k を周期として循環する．

(iv) 循環のはじまる N は $\omega_N > 1, -1 < \omega'_N < 0$ となる最初の番号である．

N が $\omega_N > 1, -1 < \omega'_N < 0$ を満たし，かつ循環のはじまる番号 M が $N \leqq M$ であったとする．つまり $\omega_M = \omega_{M+j}$ なる ω_{M+j} がある最初の番号が M とする．よって

$$\begin{aligned} \omega_{M-1} &= \begin{pmatrix} q_{M-1} & 1 \\ 1 & 0 \end{pmatrix} \omega_M \\ \omega_{M+j-1} &= \begin{pmatrix} q_{M+j-1} & 1 \\ 1 & 0 \end{pmatrix} \omega_{M+j} = \begin{pmatrix} q_{M+j-1} & 1 \\ 1 & 0 \end{pmatrix} \omega_M \end{aligned}$$

したがって $\omega_{M-1}-\omega_{M+j-1}=q_{M-1}-q_{M+j-1}$ ． ω_{M-1} と ω_{M+j-1} は同一の判別式に属し，差が整数なので，$\omega_{M-1}=\dfrac{p+\sqrt{D}}{r}$, $\omega_{M+j-1}=\dfrac{t+\sqrt{D}}{r}$ ，とおけ，

$$\omega_{M-1}-\omega_{M+j-1}=\frac{p}{r}-\frac{t}{r}=\omega'_{M-1}-\omega'_{M+j-1}$$

すでに見たようにこの場合 $|\omega'_{M-1}-\omega'_{M+j-1}|<1$ より $|q_{M-1}-q_{M+j-1}|<1$ となって $q_{M-1}-q_{M+j-1}=0$ ． すなわち

$$\omega_{M-1}=\omega_{M+j-1}$$

これが繰り返し成り立つので $-1<\omega'_N<0$ であるがきり番号が 1 づつ減じる．つまり，循環のはじまる N は $\omega_N>1,-1<\omega'_N<0$ となる最初の番号である． ■

k のことを二次無理数の連分数展開の周期と呼ぶ.

例 16.1　$\omega_1=-3+\sqrt{29}$ のとき． $D=29$ である．

ω	二次方程式	ω'
$\omega_1=-3+\sqrt{29}=2+(\sqrt{29}-5)$	$x^2+3x-5=0$	$-3+\sqrt{29}<-1$
$\omega_2=\dfrac{1}{\sqrt{29}-5}=\dfrac{\sqrt{29}+5}{4}=2+\dfrac{\sqrt{29}-3}{4}$	$4x^2-5x-1=0$	$-1<\dfrac{-\sqrt{29}+5}{4}<0$
$\omega_3=\dfrac{4}{\sqrt{29}-3}=\dfrac{\sqrt{29}+3}{5}=1+\dfrac{\sqrt{29}-2}{5}$	$5x^2-6x-4=0$	$\dfrac{-\sqrt{29}+3}{5}$
$\omega_4=\dfrac{5}{\sqrt{29}-2}=\dfrac{\sqrt{29}+2}{5}=1+\dfrac{\sqrt{29}-3}{5}$	$5x^2-4x-5=0$	$\dfrac{-\sqrt{29}+2}{5}$
$\omega_5=\dfrac{5}{\sqrt{29}-3}=\dfrac{\sqrt{29}+3}{4}=2+\dfrac{\sqrt{29}-5}{4}$	$4x^2-6x-5=0$	$\dfrac{-\sqrt{29}+3}{4}$
$\omega_6=\dfrac{4}{\sqrt{29}-5}=\sqrt{29}+5=10+\sqrt{29}-5$	$x^2-10x-4=0$	$-\sqrt{29}+5$
$\omega_7=\dfrac{1}{\sqrt{29}-5}=\dfrac{\sqrt{29}+5}{4}=\omega_2$		

ω_2 の共役が条件を満たす最初の共役無理数である．実際 $\omega_2=\omega_7$ となり，ここから循環が始まっている．そして循環周期は $k=5$ である．

練習問題 16.1 (解答 53)　$\omega_1=4+\sqrt{13}$ について調べよ.

17　ペル方程式の解の構成

17.1　ペル方程式の解の構成

二次無理数の連分数展開の周期性を活用すると，ペル方程式 $x^2 - Dy^2 = \pm 1$ の解を構成することができる．

定理 55 (構成定理 (1))
D は平方数でない正の整数とする． $\sqrt{D}$ の連分数展開の循環の周期を k とする．

(1) k が奇数の時

(i) 偶数 m に対して, $(x,\ y) = (P_{mk-1}, Q_{mk-1})$ は $x^2 - Dy^2 = 1$ の解

(ii) 奇数 m に対して, $(x,\ y) = (P_{mk-1}, Q_{mk-1})$ は $x^2 - Dy^2 = -1$ の解

(2) k が偶数の時

(i) 整数 m に対して, $(x,\ y) = (P_{mk-1}, Q_{mk-1})$ は $x^2 - Dy^2 = 1$ の解

（注）後に示すように k が偶数のとき, $x^2 - Dy^2 = -1$ の解はない．

証明

$$\sqrt{D} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} x_1$$

とすると, $x_1 > 1$, $-1 < x_1' < 0$ （ただし x_1' は x_1 の共役な無理数）となる．

なぜなら, $x_1 > 1$ は明らかであるが, q_0 を $\sqrt{D}$ を超えない最大の整数とすれば,

$$x_1' = \frac{1}{-\sqrt{D} - q_0} = -\left(\frac{1}{\sqrt{D} + q_0}\right)$$

となるので明らかである．

したがって，定理 54 より, $\sqrt{D}$ の連分数展開の展開は第二項より始まる．この周期を k とする．

$$\begin{aligned}
\sqrt{D} &= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} x_1 \\
&= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} x_{k+1} \\
&= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} x_1 \\
&= \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} x_1 = \begin{pmatrix} P_{2k} & P_{2k-1} \\ Q_{2k} & Q_{2k-1} \end{pmatrix} x_1 \cdots = \begin{pmatrix} P_{mk} & P_{mk-1} \\ Q_{mk} & Q_{mk-1}1 \end{pmatrix} x_1
\end{aligned}$$

となる．

$\sqrt{D} = \begin{pmatrix} P_{mk} & P_{mk-1} \\ Q_{mk} & Q_{mk-1} \end{pmatrix} x_1$ に, $x_1 = \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix} \sqrt{D}$ を代入する．

$$\sqrt{D} = \begin{pmatrix} P_{mk-1} & P_{mk} - q_0 P_{k-1} \\ Q_{mk-1} & Q_{mk} - q_0 Q_{k-1} \end{pmatrix} \sqrt{D}$$

さて一般に $\sqrt{D}$ が自分自身と対等，つまり $\sqrt{D} = \begin{pmatrix} p & q \\ r & s \end{pmatrix}\sqrt{D}$ ならば，

$$\frac{p\sqrt{D}+q}{r\sqrt{D}+s} = \sqrt{D} \Longrightarrow rD - q + (s-p)\sqrt{D} = 0 \Longrightarrow rD - q = 0, s = p$$

したがって，

$$p^2 - Dr^2 = ps - rq = \Delta\begin{pmatrix} p & q \\ r & s \end{pmatrix}$$

となる．

よって

$$\begin{aligned} P_{mk-1}^2 - DQ_{mk-1}^2 &= \left|\begin{pmatrix} P_{mk} & P_{mk-1} \\ Q_{mk} & Q_{mk-1} \end{pmatrix}\right|\left|\begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}\right| \\ &= (-1)^{mk+1}\cdot(-1) \\ &= (-1)^{mk} \end{aligned}$$

したがって，

(1) k が奇数の時

(i) 偶数 m に対して，$(x,\ y) = (P_{mk-1}, Q_{mk-1})$ は $x^2 - Dy^2 = 1$ の解

(ii) 奇数 m に対して，$(x,\ y) = (P_{mk-1}, Q_{mk-1})$ は $x^2 - Dy^2 = -1$ の解

(2) k が偶数の時

(i) 整数 m に対して，$(x,\ y) = (P_{mk-1}, Q_{mk-1})$ は $x^2 - Dy^2 = 1$ の解

が示された． ■

例 17.1 $x^2 - 13y^2 = \pm 1$

$$\begin{aligned} \sqrt{13} &= \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\left(\frac{\sqrt{13}+3}{4}\right) \\ &= \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\left(\frac{\sqrt{13}+1}{3}\right) \\ &= \begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\left(\frac{\sqrt{13}+2}{3}\right) \\ &= \begin{pmatrix} 7 & 4 \\ 2 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\left(\frac{\sqrt{13}+1}{4}\right) \\ &= \begin{pmatrix} 11 & 7 \\ 3 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}(\sqrt{13}+3) \\ &= \begin{pmatrix} 18 & 11 \\ 5 & 3 \end{pmatrix}\begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix}\left(\frac{\sqrt{13}+3}{4}\right) \\ &= \begin{pmatrix} 119 & 18 \\ 33 & 5 \end{pmatrix}\left(\frac{\sqrt{13}+3}{4}\right) \end{aligned}$$

従って $k=5$ となった.

$(x,\ y)=(P_4,\ Q_4)$ が $x^2-Dy^2=-1$ の解となり $(x,\ y)=(P_9,\ Q_9)$ が $x^2-Dy^2=1$ の解となるはずである.

$(P_4,\ Q_4)=(18,\ 5)$ である. $(P_9,\ Q_9)$ を求める, $x_1=\dfrac{\sqrt{13}+3}{4}$ が次に現れるときである. その展開は $x_1=\begin{pmatrix}3&1\\1&0\end{pmatrix}^{-1}\begin{pmatrix}119&18\\33&5\end{pmatrix}x_1$ をあらためて $\begin{pmatrix}P_5&P_4\\Q_5&Q_4\end{pmatrix}x_1$ に代入する.

$$\begin{aligned}\sqrt{13} &= \begin{pmatrix}3&1\\1&0\end{pmatrix}x_1\\ &= \begin{pmatrix}119&18\\33&5\end{pmatrix}x_1=\begin{pmatrix}P_5&P_4\\Q_5&Q_4\end{pmatrix}x_1\\ &= \begin{pmatrix}119&18\\33&5\end{pmatrix}\begin{pmatrix}0&1\\1&-3\end{pmatrix}\begin{pmatrix}119&18\\33&5\end{pmatrix}x_1, \text{代入!}\\ &= \begin{pmatrix}4165&649\\1225&180\end{pmatrix}x_1=\begin{pmatrix}P_{10}&P_9\\Q_{10}&Q_9\end{pmatrix}x_1\end{aligned}$$

したがって, $(P_9,\ Q_9)=(649,\ 180)$ となる.

また, $(P_4,\ Q_4)$ に対して, $(P_9,\ Q_9)$ はその次に現れる解であるから,

$$(P_4+Q_4\sqrt{D})^2=P_9+Q_9\sqrt{D}$$

となる.

$$(18+5\sqrt{13})^2=649+180\sqrt{13}$$

である.

こうして $x^2-13y^2=\pm1$ の解が構成された.

実際,

$$18^2-13\times5^2=-1$$

$$649^2-13\times180^2=1$$

である.

前の『二次不定方程式の解－構造・存在』のなかの構造定理をふまえて次の十分性定理を証明する.

定理 56 (構成定理 (2))

$x^2-Dy^2=\pm1$ の解で $x+\sqrt{D}y>1$ であるものは, $\sqrt{D}$ の展開から得られる $(P_{mk-1},\ Q_{mk-1})$ で尽くされる. ここに k は $\sqrt{D}$ の展開の周期である.

証明 $x+\sqrt{D}y>1$ である任意の解を $(x_1,\ y_1)$ とする. $x_1^2-Dy_1^2=\pm1$, つまり $\Delta\begin{pmatrix}x_1&Dy_1\\y_1&x_1\end{pmatrix}=\pm1$ である. ここで, $x_1+\sqrt{D}y_1>1$ であるので, ペル方程式の解の構造定理 (第 12 節定理 41) の証明のなかで示したように, $x_1>0,\ y_1>0$ である.

$$\sqrt{D}=\begin{pmatrix}q_0&1\\1&0\end{pmatrix}\theta$$

とおく．$\theta > 1, 0 > \theta' > -1$ （ θ' は θ の共役）である．これを

$$\begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix}\sqrt{D} = \frac{\sqrt{D}x_1 + D\sqrt{D}y_1}{\sqrt{D}y_1 + x_1} = \sqrt{D}$$

に代入する．

$$\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\theta = \begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix}\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\theta$$

$$\begin{aligned} \therefore \quad \theta &= \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}\begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix}\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\theta \\ &= \begin{pmatrix} y_1 & x_1 \\ x_1 - q_0y_1 & Dy_1 - q_0x_1 \end{pmatrix}\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\theta \\ &= \begin{pmatrix} q_0y_1 + x_1 & y_1 \\ (D - {q_0}^2)y_1 & x_1 - q_0y_1 \end{pmatrix}\theta \end{aligned}$$

ここで $\begin{pmatrix} q_0y_1 + x_1 & y_1 \\ (D - {q_0}^2)y_1 & = \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ とおく．$\Delta\begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix} = \pm 1$ なので $ps - qr = \pm 1$ である．$ps - qr = e$ とする．

$$\epsilon = r\theta + s\,,\ \epsilon' = r\theta' + s$$

とおく．$r = (D - {q_0}^2)y_1 > 0$ で $s = x_1 - q_0y_1 > x_1 - \sqrt{D}y_1 = \dfrac{\pm 1}{x_1 + \sqrt{D}y_1} > -1$ となるから，$\theta > 1$ とあわせて，$\epsilon > 1$.

さらに，θ, θ' は $t = \begin{pmatrix} p & q \\ r & s \end{pmatrix}t$ つまり $rt^2 + (s - p)t - q = 0$ の二根である．

$$\begin{aligned} \therefore \quad \epsilon\epsilon' &= r^2\theta\theta' + (\theta + \theta')rs + s^2 \\ &= r^2\frac{(-q)}{r} - \frac{(s - p)}{r}rs + s^2 \\ &= -qr - s^2 + ps + s^2 = e = \pm 1 \end{aligned}$$

よって $|\epsilon'| < 1$ ．さらに，$s > r\theta' + s > -r + s$ つまり $s > \epsilon' > -r + s$ が成り立つ．したがって

(i) $\epsilon\epsilon' = 1\,(e = 1)$ のとき，$1 > \epsilon' > 0$ ，よって $r \geqq s > 0$.

(ii) $\epsilon\epsilon' = -1\,(e = -1)$ のとき，$0 > \epsilon' > -1$ ，よって $r > s \geqq 0$.

そこで

(1) $r > s > 0$ のとき，定理 47 により $\begin{pmatrix} p & q \\ r & s \end{pmatrix}\theta$ は θ の連分数展開から得られる．

(2) $r = s$ のとき，つまり $e = 1$ のとき，$ps - qr = 1$ より $(p - q)r = 1$, $r > 0$ なので $p - q = 1, r = 1$.

よって

$$\theta = \frac{(q + 1)\theta + q}{\theta + 1} = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\theta$$

(3) $s=0$ のとき，つまり $e=-1$ のとき, $ps-qr=-1, qr=1$ より $r>0$ なので $q=r=1$.

よって $\theta=\dfrac{p\theta+1}{\theta}=\begin{pmatrix} p & 1 \\ 1 & 0 \end{pmatrix}\theta$

いずれの場合も $\begin{pmatrix} p & q \\ r & s \end{pmatrix}\theta$ は θ 自身の連分数展開のなかに現れる.

つまり

$$\sqrt{D}=\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\theta=\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix}\theta$$

は $\sqrt{D}$ の連分数展開である.

$$\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} p & q \\ r & s \end{pmatrix}\theta=\begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix}\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\theta=\begin{pmatrix} x_1q_0+Dy_1 & x_1 \\ y_1q_0+x_1 & y_1 \end{pmatrix}\theta$$

が連分数展開であるから，ある h で

$$\begin{pmatrix} x_1q_0+Dy_1 & x_1 \\ y_1q_0+x_1 & y_1 \end{pmatrix}=\begin{pmatrix} P_h & P_{h-1} \\ Q_h & Q_{h-1} \end{pmatrix}$$

とかける．このとき $\sqrt{D}=\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\theta=\begin{pmatrix} P_h & P_{h-1} \\ Q_h & Q_{h-1} \end{pmatrix}\theta$ となり， h は 周期 k の倍数になる.
つまりある整数 m によって $h=mk$ となる.

したがって, $x_1=P_{mk-1},\ y_1=Q_{mk-1}$ となり，題意が証明された. ■

以上によって，構造定理の, $x+\sqrt{D}y>1$ のなかでの最小解 (p,q) は $p=P_{k-1}$, $q=Q_{k-1}$ であることが確定した.

周期 k が偶数の場合 $x^2-Dy^2=-1$ に解がないことも示せた.

練習問題 17.1（解答 54） $x^2-19y^2=\pm1$ の解を構成せよ.

練習問題 17.2（解答 55） $x^2-46y^2=\pm1$ の解を構成せよ.

17.2 解構成のアルゴリズム

ペル方程式の解の構成理論ができたのだから，実際にプログラムを作っていくつかの解を求めよう．そのためには，まず解を構成する手順を書き出し，適切なプログラム言語を定め，翻訳しなければならない.

D に対して $x^2-Dy^2=\pm1$ の $x+\sqrt{D}y>1$ のなかでの最小解を求める手順は次の通りである.

(1) D を決める.

(2) $\sqrt{D}$ の整数部分を q_0 ， $x_1=\dfrac{1}{\sqrt{D}-q_0}$ と置く.

(3) $P_{-1}=1, P_0=q_0, Q_{-1}=0, Q_0=1$ とし, $n\geqq 1$ に対し次の過程を繰り返す.

(i) $x_n=\dfrac{1}{x_{n-1}-q_{n-1}}$ で x_n を定め，x_n の整数部分を q_n と置く.

(ii)

$$\begin{cases} P_n = q_n \cdot P_{n-1} + P_{n-2} \\ Q_n = q_n \cdot Q_{n-1} + P_{n-2} \end{cases}$$

(4) $x_{k+1} = x_1$ となったとき，この過程を終える．その k に対して，最小解 $x = P_{k-1}, y = Q_{k-1}$ が得られる．

UBASIC によるプログラム

この手順を実行するプログラム言語を探す．高等学校の教科書に載っている BASIC は，数値が一定の桁の有効数字をもつ小数表示の近似実数である．$1/3$ や$\sqrt{2}$ と置けば, 0.33333333, 1.41421356 (有効桁まで) となる．大きい数も不動点表示になる．従ってこのままでは $x_{k+1} = x_1$ の判断ができない.

UBASIC という， BASIC を改良し，大きい整数も不動点表示をせずそのままで扱え，有理数も分母分子を（約分して）別々に保持するようにした言語がある．それを用いる．// が分数である． UBASIC でも無理数は近似数になり，そのままでは比較できないので， $x_{k+1} = x_1$ の判断をさせるために, $x_n = S + T\sqrt{D}$ と二つの有理数に分けそれぞれを比較することにする．

三項間漸化式を解くのには工夫がいる． P_n , Q_n の値を順次入れていく変数を二つずつ用意し交互に用いるようにする．

次に掲げるのは $D = 2$ から $D = 1999$ まで, $x^2 - Dy^2 = \pm 1$ の最小解を書き出すプログラムである．

```
\ 10  open "pell.txt" for output as #1
\ 20  for D=2 to 1999
\ 30  if D=(isqrt(D))^2 then 220 else 40
\ 40  Q0=isqrt(D)
\ 50  S1=Q0//(D-Q0^2):T1=1//(D-Q0^2)
\ 60  X=S1+T1*(sqrt(D)):PA=Q0:QA=1:PB=1:QB=0:S=S1:T=T1
\ 70  Q=int(X):PB=PA*Q+PB:QB=QA*Q+QB
\ 80  K=K+1
\ 90  S0=S
100  S=(Q-S)//(T^2*D-(Q-S)^2):T=T//(T^2*D-(Q-S0)^2)
110  X=S+T*(sqrt(D))
120  if S=S1 and T=T1 then goto 190 else 130
130  Q=int(X):PA=PB*Q+PA:QA=QB*Q+QA
140  K=K+1
150  S0=S
160  S=(Q-S)//(T^2*D-(Q-S)^2):T=T//(T^2*D-(Q-S0)^2)
170  X=S+T*(sqrt(D))
180  if S=S1 and T=T1 then goto 200 else 70
190  print # 1D,"&",PA,"&",QA,"&",K:goto 210
200  print # 1D,"&",PB,"&",QB,"&",K
210  K=0
```

```
220  next D
230  end
```

$D = 331$ までの 6 桁以上の解

D	P	Q	k
94	2143295	221064	16
103	227528	22419	12
109	8890182	851525	15
109	181718045	17405432	15
118	306917	28254	10
124	4620799	414960	16
127	4730624	419775	12
133	2588599	224460	16
134	145925	12606	14
139	77563250	6578829	18
149	113582	9305	9
149	2749429	225242	9
151	1728148040	140634693	20
157	4832118	385645	17
157	118531681	9459858	17
163	64080026	5019135	18
166	1700902565	132015642	22
172	24248647	1848942	16
179	4190210	313191	14
181	1111225770	82596761	21
181	29395948751	2184983663	21
191	8994000	650783	16
193	1764132	126985	13
193	47441821	3414937	13
199	16266196520	1153080099	20
201	515095	36332	14
211	278354373650	19162705353	26
213	194399	13320	12
214	695359189925	47533775646	26
217	3844063	260952	16
236	561799	36570	12
237	228151	14820	10
239	6195120	400729	12
241	71011068	4574225	17

D	P	Q	k
241	2167554245	139624443	17
244	1766319049	113076990	26
249	8553815	542076	16
251	3674890	231957	14
253	3222617399	202604220	22
259	847225	52644	10
261	192119201	11891880	16
262	104980517	6485718	14
263	139128	8579	12
268	4771081927	291440214	20
271	115974983600	7044978537	24
277	8920484118	535979945	21
277	291194190653	17496163238	21
281	1063532	63445	13
281	34844557	2078652	13
283	138274082	8219541	18
284	24220799	1437240	16
286	561835	33222	10
292	2281249	133500	10
295	2024999	117900	12
298	409557	23725	11
298	14032519	812882	11
301	5883392537695	339113108232	26
302	4276623	246092	16
307	88529282	5052633	14
309	64202725495	3652365444	26
310	848719	48204	16
311	16883880	957397	16
313	126862368	7170685	17
313	4401084661	248764013	17
317	352618	19805	11
317	12272691	689303	11
319	12901780	722361	14
329	2376415	131016	12
331	2785589801443970	153109862634573	34

18　問題解答

18.1　練習問題解答

解答 1 (問題 2.1)

(1) $n(n+1)(n+2)(n+3)$ は 4 連続数だから，この 4 個の整数の中には 2 の倍数が 2 個あり，そのうち一方は 4 の倍数．また 3 の倍数が少なくとも 1 個ある．ゆえにこれは 24 の倍数である．

(2) n が奇数なので，$n = 2k-1$ とおく．

$$n^3 - n = (n-1)n(n+1) = (2k-2)(2k-1)(2k) = 4(k-1)k(2k-1)$$

まず 3 連続数なので 3 の倍数がある．次に $(k-1)k$ は 2 連続数なので偶数．ゆえに $4(k-1)k$ は 8 の倍数．あわせて 24 の倍数であることが示せた．

(3) $n^2-1 = (n-1)(n+1)$ である．$n-1,\ n,\ n+1$ のなかには 3 の倍数があるが，n が 3 で割り切れないので，$n-1,\ n+1$ のいずれかは 3 の倍数である．また (2) と同様に $n-1,\ n+1$ のいずれかは 4 の倍数で他方も 2 の倍数である．ゆえに n^2-1 は 24 の倍数である．

(4)

$$n(n+1)(2n+1) = n(n+1)\{(n-1)+(n+2)\} = (n-1)n(n+1) + n(n+1)(n+2)$$

和の各項がともに 3 連続数で 6 の倍数なので $n(n+1)(2n+1)$ は 6 の倍数である．

(5)

$$\begin{aligned} n^3 - 3n^2 + 8n &= 2(n^3 - 3n^2 + 2n) - (n^3 - 3n^2 - 4n) \\ &= 2(n-2)(n-1)n - n(n-4)(n+1) \\ &= 2(n-2)(n-1)n - n(n-1)(n+1) + 3n(n+1) \end{aligned}$$

和の各項が 6 の倍数なので，$n^3 - 3n^2 + 8n$ は 6 の倍数である．

解答 2 (問題 2.2)

(1) ［解 1］

$$(7a+2b,\ 3a+b) = (2(3a+b)+a,\ 3a+b) = (a,\ 3a+b) = (a,\ b) = 1$$

ゆえに分数 $\dfrac{7a+2b}{3a+b}$ は既約分数である．

［解 2］

$$7a+2b = M,\ 3a+b = N$$

とおくと逆に解けて

$$a = M-2N,\ b = -3M+7N$$

したがって M と N の最大公約数を d とすれば a も b も d で割れる．a, b は互いに素なので $d=1$ ．つまり分数 $\dfrac{7a+2b}{3a+b}$ は既約分数である．

(2)

$$pa+qb=M,\ ra+sb=N$$

とおくと逆に解けて

$$a=sM-qN,\ b=-rM+pN$$

したがって M と N の最大公約数を d とすれば a も b も d で割れる．a,b は互いに素なので $d=1$ ．つまり分数 $\dfrac{pa+qb}{ra+sb}$ は既約分数である．

(3) $\dfrac{11n-42}{3n-13}$ が既約分数にならないような自然数 n を，小さい方から順に三つ求めよ．

$$(11n-42,\ 3n-13)=(4(3n-13)-n,\ 3n-13)=(-n,\ 3n-13)=13$$

分子分母が 13 の倍数になるときのみ既約でない．ゆえに $n=13,\ 26,\ 39$ ．

解答 3 (問題 3.1)

条件から $0=a-a\in A$ である．また A の任意の要素 a と整数 n に対して $na\in A$ であることを数学的帰納法で示す.

$n=1$ なら明らか． $(n-1)a\in A$ と仮定すれば

$$na=(n-1)a+a\in A$$

である．よって示された.

さて， 集合 A に含まれる正で最小の要素を k とする．A の任意の要素 x を a で割ったとき商が q， 余りが r であるとする.

$$x=kq+r,\ 0\leqq r<k$$

すると上に示したことから $kq\in A$ である．よって

$$r=x-kq\in A$$

もし $r\neq 0$ なら k より小さい正数 r が A に属することになり k の最小性に反する.

$$\therefore\quad r=0\quad \text{つまり}\quad x=kq$$

となり A の任意の要素は k の倍数であることが示された.

解答 4 (問題 3.2)

(1)

$$\begin{aligned}
& 25x+13y+15z=1\\
\iff\quad & (13+12)x+13y+(13+2)z=1\\
\iff\quad & 13(x+y+z)+12x+2z=1\\
\iff\quad & (2\cdot 6+1)(x+y+z)+(2\cdot 6+0)x+2z=1\\
\iff\quad & 2\{6(x+y+z)+6x+z\}+(x+y+z)+0x=1\\
& x=s\quad \text{とおく}
\end{aligned}$$

$$
\begin{aligned}
\iff\quad & 2\{12s+6y+7z\}+(s+y+z)=1\\
& 12s+6y+7z=1+t\\
& s+y+z=-1-2t\\
& \text{これを解いて}\\
& x=s,\ y=-8+5s-15t,\ z=7-6s+13t\\
& (s,\ t,\ \text{は任意の整数})
\end{aligned}
$$

(2)

$$
\begin{aligned}
& 2x+6y+5z+7w=1\\
\iff\quad & 2x+(2\cdot 3+0)y+(2\cdot 2+1)z+(2\cdot 3+1)w=1\\
\iff\quad & 0y+2(x+3y+2z+3w)+z+w=1\\
\iff\quad & 0y+(2\cdot 1+0)(x+3y+2z+3w)+(1+0)z+w=1\\
\iff\quad & 0y+0(x+3y+2z+3w)+0z+(2x+6y+5z+7w)=1\\
& y=s,\ x+3y+2z+3w=t,\ z=u,\ 2x+6y+5z+7w=1\\
& \text{これを解いて}\\
& x=-3-3s+7t+u,\ y=s,\ z=u,\ w=1-2t-u\\
& (s,\ t,\ u,\ \text{は任意の整数})
\end{aligned}
$$

解答 5 (問題 4.1)

(1) d を a の任意の約数とする．さらに s を d の素因数とすると，s は a の約数であり，したがって $p^{\alpha},\ q^{\beta},\ r^{\gamma},\ \cdots$ のいずれかの約数である． s が素数であるから $p,\ q,\ r,\ \cdots$ のいずれかと一致する．よって

$$d=p^{x}q^{y}r^{z}\cdots$$

と書ける．このとき $0\leqq x\leqq\alpha$ ， $0\leqq y\leqq\beta$ ，$0\leqq z\leqq\gamma,\ \cdots$ は明らか．逆にこのような数 d が約数であることは明らか.

(2) (1) の $x,\ y,\ z,\ \cdots$ のそれぞれがとりうる値の個数は $\alpha+1,\ \beta+1,\ \gamma+1,\ \cdots$ であり，約数はこれらのすべての組合せの個数だけある.

$$\therefore\quad T(a)=(1+\alpha)(1+\beta)(1+\gamma)\cdots$$

(3)

$$
\begin{aligned}
S(a) &= \sum_{0\leqq x\leqq\alpha,0\leqq y\leqq\beta,0\leqq z\leqq\gamma,\cdots} p^{x}q^{y}r^{z}\cdots\\
&= (1+p+p^{2}+\cdots+p^{\alpha})\sum_{0\leqq y\leqq\beta,0\leqq z\leqq\gamma,\cdots} p^{x}q^{y}r^{z}\cdots\\
&= \frac{p^{\alpha+1}-1}{p-1}\cdot\sum_{0\leqq y\leqq\beta,0\leqq z\leqq\gamma,\cdots} p^{x}q^{y}r^{z}\cdots\\
&= \frac{p^{\alpha+1}-1}{p-1}\cdot\frac{q^{\beta+1}-1}{q-1}\cdot\frac{r^{\gamma+1}-1}{r-1}\cdot\cdots
\end{aligned}
$$

(4) (2), (3) より $T(abc)$, $S(abc)$ ともそれぞれ素因数全体にわたる積であるから明らかである.

(5) $a = dd'$ と因数分解する. この分解で d を a の約数全体にわたり動かすと, d' も a の約数全体を動く. したがってそのように動かしたものをすべてかけあわせることにより

$$a^{T(a)} = \left(\prod d\right)^2$$

$$\therefore \quad \prod d = a^{\frac{T(a)}{2}}$$

解答 6 (問題 4.2)

［前半］

$2^n - 1$ が素数なら, その約数は 1 と $2^n - 1$. 2^{n-1} の約数は $1,\ 2,\ \cdots,\ 2^{n-1}$. したがって a の約数は

$$1,\ 2,\ \cdots,\ 2^{n-1},\ 2^n - 1,\ 2(2^n - 1),\ \cdots,\ 2^{n-1}(2^n - 1)$$

これらの和は

$$\begin{aligned} & 1 + 2 + \cdots + 2^{n-1} + (2^n - 1) + 2(2^n - 1) + \cdots + 2^{n-1}(2^n - 1) \\ = \quad & \frac{2^n - 1}{2 - 1} + (2^n - 1)\frac{2^n - 1}{2 - 1} \\ = \quad & 2^n(2^n - 1) = 2a \end{aligned}$$

したがって真の約数の和はここから a を引いて a に等しい.

［後半］(オイラーの解法)

a を偶数の完全数とする. $a = 2^{n-1}b,\ n > 1,\ (2,\ b) = 1$ とおける. a は完全数なので $S(a) = 2a$ である. 一方練習問題 1-(4) から

$$S(a) = S(2^{n-1})S(b) = (2^n - 1)S(b)$$

したがって

$$S(b) = \frac{2 \cdot 2^{n-1}b}{2^n - 1} = b + \frac{b}{2^n - 1}$$

ゆえに $\dfrac{b}{2^n - 1}$ は整数である. $n > 1$ より b よりも小さい b の約数である. つまり b のすべての約数の和 $S(b)$ が b の二つの異なる約数の和になる. したがって b は二つの約数しかもたない. つまり b は素数で, $\dfrac{b}{2^n - 1} = 1$ である. つまり $2^n - 1$ は素数である.

解答 7 (問題 4.3)

(1) $aa'a'' \cdots$ と $bb'b'' \cdots$ が互いに素でないとしてその最大公約数を d とする.

d の素因数 p をとる. p は $aa'a'' \cdots$ と $bb'b'' \cdots$ の公約数である. したがって p は $a,\ a',\ a'',\ \cdots$ のいずれか, $b,\ b',\ b'',\ \cdots$ のいずれかの約数である.

これは $a,\ a',\ a'',\ \cdots$ がおのおの $b,\ b',\ b'',\ \cdots$ と互いに素であることと矛盾する.

(2)

$$\begin{aligned} d_1 &= (a_1,\ a_2,\ \cdots,\ a_m) \\ d_2 &= (b_1,\ b_2,\ \cdots,\ b_n) \\ d_3 &= (a_1b_1,\ a_1b_2,\ \cdots,\ a_2b_1,\ \cdots,\ a_mb_n,\ ) \end{aligned}$$

とする．

d_1d_2 は a_ib_j のすべての約数なので d_1d_2 は d_3 の約数．

一方，d_1 も d_3 の約数なので $d_3 = d_1e$ とおく． d_3 は

$$a_1b_1,\ a_2b_1,\ \cdots,\ a_mb_1$$

の約数で $d_1 = (a_1,\ a_2,\ \cdots,\ a_m)$ なので， e は b_1 の約数．各 b_i について言えるので e は $b_1,\ b_2,\ \cdots,\ b_n$ の公約数．つまり e は d_2 の約数．

ゆえに $d_3 = d_1e$ は d_1d_2 の約数．

$$\therefore\quad d_1d_2 = d_3$$

(3) $a_1,\ a_2,\ \cdots,\ a_n$ の任意の公約数に現れる素因数は $p,\ q,\ \cdots$ 以外にはない．ゆえに公約数は

$$\prod^{p} p^{\beta}\ (\beta \geqq 0)$$

とおける．ここで

$$\beta \leqq \mathrm{Min}(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)$$

となり，最大公約数のときに限り

$$\beta = \mathrm{Min}(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)$$

同様に，最小公倍数はその最小性により現れる素因数は $p,\ q,\ \cdots$ 以外にはない．ゆえに次の数

$$\prod^{p} p^{\gamma}\ (\beta \geqq 0)$$

が公倍数なら

$$\gamma \geqq \mathrm{Max}(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)$$

となり，最小倍約数のときに限り

$$\gamma = \mathrm{Min}(\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n)$$

(4) (i) 各 p に対し $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n$ を並べ替えて $\alpha_1{}',\ \alpha_2{}',\ \cdots,\ \alpha_n{}'$ とおく．すると (3) より

$$d_1 = \prod^{p} p^{\alpha_1{}'}$$

以下同様に

$$d_k = \prod^{p} p^{\alpha_1{}'+\alpha_2{}'+\cdots+\alpha_k{}'}$$

したがって，$k = 2,\ \cdots n$ に対して d_k は d_{k-1} で割りきれる．

(ii)

$$\frac{d_k}{d_{k-1}} = e_k = \prod^{p} p^{\alpha_k{}'}$$

であるから

$$\frac{e_k}{e_{k-1}} = \prod^{p} p^{\alpha_k{}'-a_{k-1}{}'}$$

(iii) また

$$\begin{aligned} e_1e_2\cdots e_n &= \prod^{p} p^{{\alpha_1}'+{\alpha_2}'+\cdots+{\alpha_n}'} \\ &= \alpha_1\alpha_2\cdots\alpha_n \end{aligned}$$

(iv)

$$e_n = \prod^{p} p^{{\alpha_n}'}$$

なので (3) から e_n は $\alpha_1,\ a_2,\ \cdots,\ \alpha_n$ の最小公倍数に等しい.

(5)

$$a_k = \prod^{p} p^{\alpha_k},\ m = \prod^{p} p^{\mu}$$

とおけば，問題の等式を素因数 p に指数で見ることにより,

$$\mathrm{Max}\{\mathrm{Min}(\alpha_1,\ \mu),\ \mathrm{Min}(\alpha_2,\ \mu),\ \cdots,\ \mathrm{Min}(\alpha_n,\ \mu)\} = \mathrm{Min}(\mathrm{Max}\{\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n\},\ \mu)$$

を示せばよい.

$\mu \geqq \alpha_1,\ a_2,\ \cdots,\ \alpha_n$ なら左辺は $\mathrm{Max}(\alpha_1,\ a_2,\ \cdots,\ \alpha_n)$ ．右辺も同じ.

次に例えば $\alpha_1 > \mu$ とする．$\mathrm{Min}(\alpha_1,\ \mu) = \mu$ で，$\mathrm{Min}(\alpha_2,\ \mu),\ \cdots,\ \mathrm{Min}(\alpha_n,\ \mu)$ は μ 以下でから左辺は μ.

一方 $\mathrm{Max}\{\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n\} \geqq \alpha_1 > \mu$ より，右辺も μ になる.

(6) l の素因数分解を

$$l = p^{\alpha}q^{\beta}\cdots$$

とする． p^{α} は $a,\ b,\ c,\ \cdots$ の少なくとの一つに含まれている．a に含まれているこのような最高べき因子の積を a_0 とする．$b_0,\ c_0,\ \cdots$ をそれぞれ同様に定める．ただし，同じ素数べきが再び現れたらそれは加えないようにする.

このとき明らかに

$$l = a_0b_0c_0\cdots$$

である.

解答 8 (問題 4.4)　前半は後半の $n = 1$ の場合なので，後半を示せばよい.

$$\begin{aligned} {}_{p^n}\mathrm{C}_k &= \frac{p^n(p^n-1)\cdots(p^n-k+1)}{k(k-1)\cdots 1} \\ &= \frac{p^n}{k}\cdot {}_{p^n-1}\mathrm{C}_{k-1} \end{aligned}$$

つまり

$$k\cdot {}_{p^n}\mathrm{C}_k = p^n\cdot {}_{p^n-1}\mathrm{C}_{k-1}$$

ここで ${}_{p^n}\mathrm{C}_k,\ {}_{p^n-1}\mathrm{C}_{k-1}$ は組合せの場合の数なので正の整数.

$k = p^l\cdot q$ (q は p と互いに素) とおくと

$$q\cdot {}_{p^n}\mathrm{C}_k = p^{n-l}\cdot {}_{p^n-1}\mathrm{C}_{k-1}$$

q は p と互いに素 なので ${}_{p^n}\mathrm{C}_k$ が p^{n-l} の倍数である.

解答 9 (問題 4.5)　$n!$ に現れる素数 p の最高べきの指数を N とする．N は $n,\ n-1,\ \cdots,\ 1$ に含まれる素数 p の個数に等しい．

$$p^l \leqq n < p^{l+1}$$

とする．$k \geqq l+1$ なら $\left[\dfrac{n}{p^k}\right] = 0$ である．

$$\begin{array}{ll}
n,\ n-1,\ \cdots,\ 1 \text{ のなかでちょうど } p \text{ で割れるものの個数は} & \left[\dfrac{n}{p}\right] - \left[\dfrac{n}{p^2}\right] \\
n,\ n-1,\ \cdots,\ 1 \text{ のなかでちょうど } p^2 \text{で割れるものの個数は} & \left[\dfrac{n}{p^2}\right] - \left[\dfrac{n}{p^3}\right] \\
\cdots & \cdots \\
n,\ n-1,\ \cdots,\ 1 \text{ のなかでちょうど } p^l \text{で割れるものの個数は} & \left[\dfrac{n}{p^l}\right]
\end{array}$$

$$\begin{aligned}
\therefore\quad N &= 1\cdot\left(\left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]\right) + 2\cdot\left(\left[\frac{n}{p}\right] - \left[\frac{n}{p^2}\right]\right) + \cdots \\
&\qquad + k\cdot\left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]\right) + \cdots + l\cdot\left[\frac{n}{p^l}\right] \\
&= \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^l}\right] \\
&= \sum_{k=1}^{\infty}\left[\frac{n}{p^k}\right]
\end{aligned}$$

解答 10 (問題 4.6)

(i) 既約分数 $\dfrac{m}{n}$ が部分分数に分解できること．

$x,\ y,\ \cdots$ に関する条件を考えなければ

$$\frac{m}{n} = \frac{x}{p^\alpha} + \frac{y}{q^\beta} + \cdots \pm s$$

は

$$m = \frac{n}{p^\alpha}x + \frac{n}{q^\beta}y + \cdots \pm s$$

となり，これは $x,\ y,\ \cdots$ に関する一次不定方程式で係数は互いに素なので定理 5 によって解を持つ．

ここで x を p^α で割って

$$x = p^\alpha \cdot Q + r$$

となったとすれば s を調整して x の代わりに r を用いることで条件

$$0 < x < p^\alpha$$

にできる．$x = 0$ ならその項はいらないので，$0 < x$ としてよい．したがって題意を満たす部分分数分解が存在する．

(ii) 部分分数分解の一意性を示す．

二つの分解

$$\begin{aligned}
\frac{m}{n} &= \frac{x}{p^\alpha} + \frac{y}{q^\beta} + \cdots \pm s \\
&= \frac{x'}{p^\alpha} + \frac{y'}{q^\beta} + \cdots \pm s
\end{aligned}$$

があれば辺々引いて

$$0 = \frac{x - x'}{p^\alpha} + \frac{y - y'}{q^\beta} + \cdots \pm s \mp s'$$

両辺に n をかけて分母を払うと

$$0 = (x - x')q^\beta \cdots + (y - y')p^\alpha \cdots + \cdots$$

となり $x - x'$ が p^α で割りきれる．しかし

$$0 \leqq x < p^\alpha,\ 0 \leqq x' < p^\alpha$$

なので (一方に現れない項が他方に現れる可能性を考え等号が付いている)，

$$|x - x'| < p^\alpha$$

ゆえに $x = x'$ ．同様に $y = y'$, $\cdots$ ．その結果 $\pm s = \pm s'$.

解答 11 (問題 5.1)

$$\begin{aligned} a &= a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \\ &= a_n(9+1)^n + a_{n-1}(9+1)^{n-1} + \cdots + a_1(9+1) + a_0 \\ &\equiv a_0 + a_1 + \cdots + a_n \pmod 9 \end{aligned}$$

同様に

$$\begin{aligned} a &= a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \\ &= a_n(11-1)^n + a_{n-1}(11-1)^{n-1} + \cdots + a_1(11-1) + a_0 \\ &\equiv a_0 - a_1 + \cdots + (-1)^n a_n \pmod{11} \end{aligned}$$

解答 12 (問題 5.2)

$$\begin{aligned} 10^6 &= (7+3)^6 \\ &\equiv 3^6 \pmod 7 = (7+2)^3 \pmod 7 \\ &= 8 \equiv 1 \pmod 7. \quad \therefore \text{ 土曜日} \\ 10^{100} &= 10^{16\cdot 6+4} \\ &\equiv 10^4 \pmod 7 \equiv 3^4 \pmod 7 = 9^2 \equiv 4 \pmod 7. \quad \therefore \text{ 火曜日} \\ 3^{100} &\equiv (7+3)^{100} \equiv 4 \pmod 7. \quad \therefore \text{ 火曜日} \end{aligned}$$

解答 13 (問題 5.3)

(1)

$$\begin{aligned} 2^{65} + 1 &= 32^{13} + 1 \\ &\equiv (-1)^{13} + 1 \pmod{11} \\ &= 0 \pmod{11} \end{aligned}$$

(2)

$$\begin{aligned} 13^{2n}+6 &\equiv 36^n+6 \pmod 7 \\ &\equiv 1+6 \pmod 7 \equiv 0 \pmod 7 \end{aligned}$$

(3)

$$\begin{aligned} 3^{15} &= 27^5 \\ &\equiv 7^5 \pmod{10} \equiv 7 \pmod{10} \\ (3^{15})^{15} &\equiv 7^{15} \pmod{10} \\ &\equiv (-3)^{15} \pmod{10} \equiv -7 \pmod{10} \equiv 3 \pmod{10} \end{aligned}$$

(4)

$$\begin{aligned} (2^{100}-1)^{99} &= (1024^{10}-1)^{99} \\ &\equiv (24^{10}-1)^{99} \pmod{100} \\ &\equiv \{76^{10}-1\}^{99} \pmod{100} \\ &\equiv \{76-1\}^{99} \pmod{100} \quad \because 76^2 = 5776 \\ &\equiv 75^{11} \pmod{100} \quad \because 75^3 = 421875 \\ &\equiv 75 \pmod{100} \quad \because 75^3 = 421875 \end{aligned}$$

解答 14 (問題 5.4)

(1) $n = 7k \pm e$ $(e = 0,\ 1,\ 2,\ 3)$ とおく.

$$n^2 \equiv (\pm e)^2 \equiv 0,\ 1,\ 2^2,\ 3^2 \equiv 0,\ 1,\ 2,\ 4 \pmod 7$$

(2) $n = 10k \pm e$ $(e = 0,\ 1,\ 2,\ 3,\ 4,\ 5)$ とおく (5 は二重になっている).

$$\begin{aligned} n^5 - n &\equiv (\pm e)^5 - (\pm e) \pmod{10} \\ &= \pm e(e-1)\{(e+1)(e-2)(e+2)+5e)\} \\ &\equiv 0 \pmod{10} \end{aligned}$$

(3) $n = 2k - 1$ とおく.

$$n^2 - 1 = (2k-1-1)(2k-1+1) = 4k(k-1) \equiv 0 \pmod 8$$

(4)

$$\begin{aligned} n^4 + 2n^3 + 11n^2 + 10n &= n(n+1)(n^2+n+10) \\ &= n(n+1)\{(n+2)(n+3) - 4(n-1)\} \\ &= n(n+1)(n+2)(n+3) - 4(n-1)n(n+1) \\ &\equiv 0 \pmod{24} \end{aligned}$$

解答 15 (問題 5.5)

(1) $a = 3k + e$ $(e = 0,\ \pm 1)$ に対して

$$a^2 \equiv e^2 \equiv \begin{cases} 0 \pmod 3 & e = 0 \text{ のとき} \\ 1 \pmod 3 & e \neq 0 \text{ のとき} \end{cases}$$

である.

$a^2 + b^2 = c^2$ となる整数 c が存在するなら右辺は 3 を法として 0 か 1 に合同なので

$$a^2 + b^2 \equiv 2 \pmod 3$$

となることはできない. ところが, 左辺が $2 \pmod 3$ になるのは $a,\ b$ とも 3 の倍数でないときである. これが否定されるので題意が示された.

(2) 同様に

$$a^2 \equiv \begin{cases} 0 \pmod 5 & a \equiv 0 \pmod 5 \text{ のとき} \\ 1 \pmod 5 & a \equiv 1,\ 4 \pmod 5 \text{ のとき} \\ 4 \pmod 5 & a \equiv 2,\ 3 \pmod 5 \text{ のとき} \end{cases}$$

である.

ゆえに, 1 と 4 をどのように加えても 5 を法として 1 や 4 に合同にはならない.

つまり $a,\ b,\ c$ のうち少なくとも 1 つは 5 の倍数である.

解答 16 (問題 5.6) $a \equiv 3 \pmod{11}$ より $a^3 \equiv 5 \pmod{11}$ である. 一方 $a^3 + b \equiv 4 \pmod{11}$ なので,

$$b \equiv 4 - 5 \pmod{11} \equiv 10 \pmod{11}$$

解答 17 (問題 5.7) $(26,\ 57) = 1$ なので解が存在する. $57 = 26 \cdot 2 + 5$ より

$$\begin{aligned} & 26x \equiv 1 \pmod{57} \\ \Rightarrow\ & 52x \equiv 2 \pmod{57} \\ \Rightarrow\ & -5x \equiv 2 \pmod{57} \\ \Rightarrow\ & -25x \equiv 10 \pmod{57} \\ & \text{与えられた式と加えて} \\ & x \equiv 11 \pmod{57} \end{aligned}$$

ゆえに解があれば 11 に 57 を法として合同である. 解が存在することは分かっているので

$$x \equiv 11 \pmod{57}$$

［別解］$26x = 1 + 57y$ となる整数 y があればよい.

$57y \equiv -1 \pmod{26}$ より $5y \equiv 25 \pmod{26}$. つまり $y \equiv 5 \pmod{26}$

$y = 5 + 26t$ とおくと

$$26x = 1 + 57(5 + 26t) = 1 + (26 \cdot 2 + 5)(5 + 26t) = 26(11 + 57t)$$

$$x \equiv 11 \pmod{57}$$

解答 18 (問題 5.8)　ガウス の方法を用いる．

$$\begin{aligned} 5\cdot 7\cdot t_1 &\equiv 1 \pmod 3 \quad \text{より} \quad t_1 \equiv 2 \pmod 3 \\ 3\cdot 7\cdot t_2 &\equiv 1 \pmod 5 \quad \text{より} \quad t_2 \equiv 1 \pmod 5 \\ 3\cdot 5\cdot t_3 &\equiv 1 \pmod 7 \quad \text{より} \quad t_3 \equiv 1 \pmod 7 \end{aligned}$$

ゆえに求める数は

$$\begin{aligned} x &\equiv 1\cdot(5\cdot 7)\cdot 2 + 2\cdot(3\cdot 7)\cdot 1 + 3\cdot(3\cdot 5)\cdot 1 \pmod{3\cdot 5\cdot 7} \\ &\equiv 157 \pmod{3\cdot 5\cdot 7} \\ &\equiv 52 \pmod{3\cdot 5\cdot 7} \end{aligned}$$

解答 19 (問題 5.9)

$$\begin{aligned} & \begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases} \text{が解を持つ} \\ \iff \quad & x = a + mu = b + nv \text{ となる整数 } (u,\ v) \text{ が存在する．} \end{aligned}$$

つまり $a - b = -mu + nv$ となる整数解 $(u,\ v)$ が存在することと同値である．これは

$$a - b \equiv 0 \pmod d$$

と同値である (定理 5).

二つの解 $x_1,\ x_2$ が存在したとする．このとき

$$x_1 - x_2 \equiv 0 \pmod m, \text{ かつ } x_1 - x_2 \equiv 0 \pmod n$$

つまり $x_1 - x_2$ は m と n の最小公倍数 l で割り切れる (定理 3).

解答 20 (問題 5.10)　必要性は明らかである．よって，条件が成立しているとする．

ここで $\{m_1,\ m_2,\ \cdots,\ \}$ で $m_1,\ m_2,\ \cdots,$ の最小公倍数を表す．すると前問から

$$\begin{cases} x \equiv a_1 \pmod{m_1}, \\ x \equiv a_2 \pmod{m_1} \end{cases}$$

の解を

$$x \equiv b \pmod{\{m_1,\ m_2\}}$$

のように表すことができる．これに第三の合同式を組合わせて

$$\begin{cases} x \equiv b \pmod{\{m_1,\ m_2\}}, \\ x \equiv a_3 \pmod{m_3} \end{cases}$$

この解が $\{m_1,\ m_2,\ m_3\}$ を法としてただ一つに定まることを示す.

仮定から $b \equiv a_1 \pmod{m_1}$. ゆえに $b - a_3 \equiv a_1 - a_3 \pmod{m_1}$. すなわち

$$b - a_3 \equiv a_1 - a_3 \equiv 0 \pmod{(m_1,\ m_3)}$$

同様に

$$b - a_3 \equiv a_2 - a_3 \equiv 0 \pmod{(m_2,\ m_3)}$$

つまり $b-a_3$ は $(m_1,\ m_3)$ かつ $(m_2,\ m_3)$ で割りきれ，したがって $\{(m_1,\ m_3),\ (m_2,\ m_3)\}$ で割りきれる．

$$\{(m_1,\ m_3),\ (m_2,\ m_3)\} = \{(m_1,\ m_2),\ m_3\}$$

であるから (4 節「素数」練習問題 3-(5))，前問により x は

$$\{\{m_1,\ m_2\},\ m_3\} = \{m_1,\ m_2,\ m_3\}$$

に関してただ一つ定まる．

順次この操作を繰りかえすことにより題意が示された．

解答 21 (問題 5.11)

(1) $x^2+x+1 \equiv 3 \pmod 5$ を解く．

$$x^2+x-2 = (x+2)(x-1) \equiv 0 \pmod 5 \text{ より}$$
$$x \equiv 1,\ 3 \pmod 5$$

これを用いて解く．

$$\begin{aligned}
x &= 1+5y && \text{とおく．}\\
(1+5y)^2+(1+5y)-2 &= 25y^2+15y \equiv 15y \equiv 0 \pmod{25} && \text{より}\\
y &\equiv 0 \pmod 5\\
\therefore\quad & x \equiv 1 \pmod{25}\\
x &= 3+5y && \text{とおく．}\\
(3+5y)^2+(3+5y)-2 &= 25y^2+35y+10 \equiv 35y+10 \equiv 0 \pmod{25} && \text{より}\\
2y+2 &\equiv 0 \pmod 5\\
y &\equiv 4 \pmod 5\\
\therefore\quad & x \equiv 23 \pmod{25}
\end{aligned}$$

$$x \equiv 1,\ 23 \pmod{25}$$

(2)

$$\begin{aligned}
& x^2 \equiv 1 \pmod 3\\
\therefore\quad & x \equiv 1,\ -1 \pmod 3\\
& x^2 \equiv 1 \pmod{13}\\
\therefore\quad & x \equiv 1,\ -1 \pmod 3
\end{aligned}$$

$$x^2 \equiv 1 \pmod{39}$$

は四つの解をもつ．それらは，

$$\left.\begin{matrix} x\equiv 1\\ x\equiv 1 \end{matrix}\right\} \quad \left.\begin{matrix} x\equiv 1\\ x\equiv -1 \end{matrix}\right\} \quad \left.\begin{matrix} x\equiv -1\\ x\equiv 1 \end{matrix}\right\} \quad \left.\begin{matrix} x\equiv -1\\ x\equiv -1 \end{matrix}\right\} \begin{matrix}\pmod 3\\ \pmod{13}\end{matrix}$$

から求められる．

$$\therefore\quad x \equiv 1,\ x \equiv 25,\ x \equiv 14,\ x \equiv 38 \pmod{39}$$

解答 22 (問題 6.1)

(1) $1512 = 2^3 3^3 7$ であるから

$$\varphi(1512) = 1512\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{7}\right) = 432$$

実際

$$\begin{aligned} & 1512 - (\frac{1512}{2} + \frac{1512}{3} + \frac{1512}{7}) + (\frac{1512}{6} + \frac{1512}{14} + \frac{1512}{21}) - \frac{1512}{42} \\ = \quad & 1512 - (756 + 504 + 216) + (252 + 108 + 72) - 36 = 432 \end{aligned}$$

である.

(2) a が 1512 と互いに素なら $1512 - a$ も 1512 と互いに素である．したがって 1512 と互いに素なものを小さい順にならべると

$$1,\ 5,\ 11,\ \cdots,\ 1511$$

となる． a と $1512 - a$ を組にするとそれらの和は

$$\frac{432(1+1511)}{2} = 326592$$

解答 23 (問題 6.2)　点 $(a,\ b)$ と点 $(c,\ d)$ および原点が同一直線上にあるのは

$$\frac{b}{a} = \frac{d}{c}$$

となるときである．つまり一方の分子分母を約分して他方になるときである.

したがって，領域 $y < x$ の中にあって題意をみたす点 $(a,\ b)$ は既約分数 $\dfrac{b}{a}$ $(1 \leqq a,\ b \leqq 12)$ の個数である．分母を n に対して $\dfrac{a}{n}$ が既約なものは $\varphi(n)$ 個ある.

直線 $y = x$ 上では $(1,\ 1)$ のみが題意をみたす.

$$\therefore \quad \text{求める個数} = 1 + 2\sum_{k=2}^{12}\varphi(k) = 1 + 2(1+2+2+4+2+6+4+6+5+10+4) = 91$$

解答 24 (問題 6.3)　$a,\ b,\ c,\ \cdots$ と与えられた互いに素な数の個数に関する数学的帰納法で証明する.

a がただ一つ与えられたときは $1,\ 2,\ \cdots,\ [x]$ のなかで a の倍数は

$$1\cdot a,\ 2\cdots a,\ \cdots,\ \left[\frac{x}{a}\right]a$$

だけある.

$$\therefore \quad \Phi(x) = [x] - \left[\frac{x}{a}\right]$$

$a_1 = a,\ a_2 = b,\ \cdots,\ a_k$ が与えられたときそれらのいずれでも割り切れない数の個数を $\Phi_k(x)$ とし，これについては成立しているとする.

さらに a_{k+1} が追加されたとする．このときは，さらに a_{k+1} の倍数 ya_{k+1} $\left(y \leqq \dfrac{x}{a_{k+1}}\right)$ を除かなければならない．そのうち y が $a_1 = a,\ a_2 = b,\ \cdots,\ a_k$ で割り切れるものはすでに除かれているので，新たに除くべきものは

$$\Phi_k\left(\frac{x}{a_{k+1}}\right)$$

個ある．

$$\begin{aligned}
\therefore\quad \Phi_{k+1}(x) &= \Phi_k(x) - \Phi_k\left(\frac{x}{a_{k+1}}\right) \\
&= [x] - \left[\frac{x}{a_1}\right] - \left[\frac{x}{a_2}\right] - \left[\frac{x}{a_3}\right] - \cdots \\
&\qquad + \left[\frac{x}{a_1a_2}\right] + \left[\frac{x}{a_1a_3}\right] + \left[\frac{x}{a_2a_3}\right] - \cdots - \left[\frac{x}{a_1a_2a_3}\right] - \cdots \\
&\qquad - \left[\frac{x}{a_{k+1}}\right] + \left[\frac{x}{a_1a_{k+1}}\right] + \left[\frac{x}{a_2a_{k+1}}\right] + \left[\frac{x}{a_3a_{k+1}}\right] - \cdots \\
&\qquad - \left[\frac{x}{a_1a_2a_{k+1}}\right] - \left[\frac{x}{a_1a_3a_{k+1}}\right] - \left[\frac{x}{a_2a_3a_{k+1}}\right] - \cdots \\
&= [x] - \left[\frac{x}{a_1}\right] - \left[\frac{x}{a_2}\right] - \cdots - \left[\frac{x}{a_{k+1}}\right] \\
&\qquad + \left[\frac{x}{a_1a_2}\right] + \cdots + \left[\frac{x}{a_1a_{k+1}}\right] - \cdots \\
&\qquad - \left[\frac{x}{a_1a_2a_3}\right] - \cdots - \left[\frac{x}{a_1a_2a_{k+1}}\right] - \cdots
\end{aligned}$$

ゆえに $k+1$ のときも成立し，題意が示された．

解答 25 (問題 6.4)　$(m,\ n) = 1$ ならば，$d_1|m,\ d_2|n$ とすれば $(d_1,\ d_2) = 1,\ d_1d_2|mn$ ．

逆に，$d|mn$ なら $d = d_1d_2,\ (d_1,\ d_2) = 1$ の形に書ける．

$$\begin{aligned}
\therefore\quad G(mn) &= \sum^{d|mn} F(d) \\
&= \sum^{d_1|m,d_2|n} F(d_1d_2) = \sum^{d_1|m,d_2|n} F(d_1)F(d_2) \\
&= \sum^{d_1|m} F(d_1) \sum^{d_2|m} F(d_2) = G(m)G(n)
\end{aligned}$$

注意 18.1　これを用いれば，補題 1 の別の証明ができる．

$\mu(n)$ は明らかに乗法的関数である．$G(n) = \sum^{d|n} \mu(d)$ で $G(n)$ を定めると $G(n)$ も乗法的関数である．ゆえに $n = {p_1}^{e_1}{p_2}^{e_2}\cdots{p_k}^{e_k}$ のとき

$$G(n) = G({p_1}^{e_1})G({p_2}^{e_2})\cdots G({p_k}^{e_k})$$

ところが

$$G(p^e) = \sum^{d|p^e} \mu(d) = 1 + \mu(p) + \mu(p^2) + \cdots + \mu(p^e) = 1 + \mu(p) = 0$$

ゆえに補題が示された．

解答 26 (問題 6.5)　1 から $[nx]$ までの整数のうち，n との最大公約数が d であるものは

$$yd,\ y=1,\ \cdots,\ \left[\frac{[nx]}{d}\right],\ \text{かつ}\ \ (yd,\ n)=d$$

と書ける．ところが

$$(yd,\ n)=d \iff \left(y,\ \frac{n}{d}\right)=1, \quad \left[\frac{[nx]}{d}\right]=\left[\frac{nx}{d}\right]$$

であるからその個数は 1 から $\left[\dfrac{nx}{d}\right]$ までの整数のうち，$\dfrac{n}{d}$ と互いに素であるものの個数 $\varphi\left(\dfrac{n}{d},\ \dfrac{nx}{d}\right)$ に等しい．1 から nx を超えない最大の整数までの整数は $d|n$ に関して 1 度ずつ数えられるので，

$$[nx]=\sum^{d|n}\varphi\left(\frac{n}{d},\ \frac{nx}{d}\right)$$

d が n の正の約数を動けば $\dfrac{n}{d}$ の正の約数をすべて動くので第一式が示された．

第二式は第一式よりメービスの反転公式で得られる．

解答 27 (問題 7.1)

$$F_n(x)=\prod^{d|n}(x^{\frac{n}{d}}-1)^{\mu(d)}$$

であり，$n>1$ のとき

$$\sum^{d|n}\mu(d)=0$$

であるから，$F_n(x)$ の定数項は $n=1$ の場合以外 $+1$ である．

解答 28 (問題 7.2) $n>1$ のときすべての n 乗根の和は，$x^n-1=0$ から 0 である．従って原始 n 乗根の和を $f(n)$ をおくと，

$$\text{すべての } n \text{ 乗根の和}=\sum^{d|n}f(d)=\begin{cases}1 & n=1 \text{ のとき}\\ 0 & n>1 \text{ のとき}\end{cases}$$

整数 n と d に関する等式と見ればメービスの反転公式 (6 節) から

$$f(n)=\mu(n)\cdot 1+\mu(d)\cdot 0+\cdots+\mu(1)\cdot 0=\mu(n)$$

解答 29 (問題 7.3)　α^k はもちろん n 乗根である．

$$\alpha^i=\alpha^j \iff \alpha^{i-j}=1$$

であるが，α が原始 n 乗根なのでこれは

$$i-j\equiv 0\ (\mathrm{mod.}\ n)$$

を意味する．従って k を n に関する剰余系にとった α^k $(k=0,\ 1,\ \cdots,\ n-1)$ はすべて異なる．つまりこれらが，1 の n 乗根のすべてである．

つぎに

$$(\alpha^k)^i=1 \iff ki\equiv 0 \pmod{n}$$

$(k,\ n)=1$ なら，$i\equiv 0 \pmod{n}$ が結論されるので，このとき α^k は原始 n 乗根である．このような k は $\varphi(n)$ 個ある．定理 21 から原始 n 乗根はちょうど $\varphi(n)$ 個なので，これらが原始 n 乗根のすべてである．

解答 30 (問題 7.4)　$\alpha = \cos\dfrac{2\pi}{a} + i\sin\dfrac{2\pi}{a}$ ，$\beta = \cos\dfrac{2\pi}{b} + i\sin\dfrac{2\pi}{b}$ とおく．整数 $x,\ y$ に対して

$$\alpha^x\beta^y = \cos\frac{2(bx+ay)\pi}{ab} + i\sin\frac{2(bx+ay)\pi}{ab}$$

となる．定理 17（6 節）の証明にあるように，$x,\ y$ に $a,\ b$ を法とする剰余系の値を与えれば $bx+ay$ は ab を法とする剰余系になり，$x,\ y$ に $a,\ b$ を法とする既約剰余系の値を与えれば $bx+ay$ は ab を法とする既約剰余系になる．

解答 31 (問題 8.1)

(1)

$$r\,{}_p\mathrm{C}_r = \frac{rp!}{r!(p-r)!} = \frac{p(p-1)!}{(r-1)!\{(p-1)-(r-1)\}!} = p\,{}_{p-1}\mathrm{C}_{r-1}$$

上の等式の右辺は p の倍数であるが, r と p は互いに素なので ${}_p\mathrm{C}_r$ が p の倍数である．

(2)

$$2^p = (1+1)^p = 1 + \sum_{r=1}^{p-1} {}_p\mathrm{C}_r + 1$$

(1) より $2^p - 2$ は p の倍数である．よって余りは 2 $(p>2)$，$0(p=2)$ である．

(3) $n^p - n$ が p 倍数であると推測される．これを, 数学的帰納法で示す.

(i) $n=1$ は明らか. $n=2$ のときは (2) より成立

(ii) $n=k$ のとき成立するとする. つまり

$$k^p - k = pM \text{ と整数 } M \text{ を用いて表される.}$$

このとき

$$(1+k)^p = 1 + \sum_{r=1}^{p-1} {}_p\mathrm{C}_r k^r + k^p = 1 + \sum_{r=1}^{p-1} {}_p\mathrm{C}_r k^r + pM + k$$

ここで, $\displaystyle\sum_{r=1}^{p-1} {}_p\mathrm{C}_r k^r$ は p の倍数なのでこれを整数 N を用いて pN とおく.

$$(1+k)^p = 1 + pN + k$$
$$\therefore\quad (k+1)^p - (k+1) = pN$$

よって, $n=k+1$ のときも成立した.

(iii) したがって, すべての自然数 n に対して, n^p と n を p で割った余りは等しい.
つまり, n^p を p で割った余りは n を p で割った余りである．

解答 32 (問題 8.2)　$(k,\ e) = d$ とおき，　$k = k'd,\ e = e'd$ とする．

$$(a^k)^{e'} = a^{k'de'} = (a^e)^{k'} \equiv 1 \pmod{m}$$

逆に $(a^k)^x \equiv 1 \pmod{m}$ とする．このとき定理 24 から kx は e の倍数である．このとき $k'x$ が e' の倍数になる．ところが $(k',\ e') = 1$ だから x は e' の倍数である．

ゆえに $(a^k)^x \equiv 1 \pmod{m}$ となる最小の x が $e' = \dfrac{e}{(k,\ e)}$ である．

解答 33 (問題 8.3)　$M=(n!)^2+1$ とおく．M は $1,\cdots,n$ で割り切れないので M の 1 でない因数はすべて n より大きい．そこで M が $4n-1$ 型の素因数 p をもったとする．$p>n$ である．フェルマの小定理から

$$(n!)^p \equiv n! \pmod{p} \tag{42}$$

次に $p=4r+3$ とおき，因数分解

$$x^{2k+1}+1=(x+1)(x^{2k}-x^{2k-1}+x^{2k-2}-\cdots-a+1)$$

を $x=(n!)^2,\ k=r$ で用いる．このとき $M=x+1$ であるから因数分解は $\{(n!)^2\}^{2r+1}+1$ が M で割り切れることを示している．一方，

$$\{(n!)^2\}^{2r+1}+1=(n!)^{4r+2}=(n!)^{p-1}+1$$

である．M で割り切れるならその素因数 p でも割り切れる．

$$\therefore\quad n!\{(n!)^{p-1}+1\}=(n!)^p+n!\equiv 0 \pmod{p} \tag{43}$$

(42), (43) から

$$2n!\equiv 0 \pmod{p}$$

これは $p>n$ と矛盾した．ゆえに M は $4n-1$ 型の素因数はもたない．つまりすべての素因数は $4n+1$ 型の素数である．

任意の自然数 n に対して，M の素因数 p は必ず存在し (M 自身が素数なら M，M が合成数なら M の素因数)，p は $p>n$ である $4n+1$ 型の素数になる．つまり任意の自然数 n に対してそれより大きい $4n+1$ 型の素数がつねに存在するので $4n+1$ 型の素数は無数に存在する．

解答 34 (問題 8.4)

$$\begin{aligned}
10^1 &= 10+91\cdot 0\\
10^2 &= 9+91\cdot 01\\
10^3 &= 90+91\cdot 010\\
10^4 &= 81+91\cdot 0109\\
10^5 &= 82+91\cdot 01098\\
10^6 &= 1+91\cdot 010989
\end{aligned}$$

10 の法 91 に対する指数 e は 6 である．

$\varphi(91)=\varphi(7)\varphi(13)=72$ であるから分母が 91 の既約真分数は 72 個ある．

したがって，72 個の分数が 6 個ずつ 12 の循環節が等しい群に分かれる．

$$\begin{aligned}
\frac{1}{91} &= \frac{010989}{10^6-1}\\
&= \frac{010989}{10^6}\left\{1+\frac{1}{10^6}+\frac{1}{10^{12}}+\cdots\right\}\\
&= 0.\dot{0}10989\dot{0}
\end{aligned}$$

これから次の循環小数ができる.

$$\begin{aligned}
\frac{10}{91} &= \frac{10^1}{91} - 0 &&= 0.\dot{1}0989\dot{0}\\
\frac{9}{91} &= \frac{10^2}{91} - 01 &&= 0.\dot{0}9890\dot{1}\\
\frac{90}{91} &= \frac{10^3}{91} - 010 &&= 0.\dot{9}8901\dot{0}\\
\frac{81}{91} &= \frac{10^4}{91} - 0109 &&= 0.\dot{8}9010\dot{9}\\
\frac{82}{91} &= \frac{10^5}{91} - 01098 &&= 0.\dot{9}0109\dot{8}
\end{aligned}$$

分子と循環節は次の通り.

	分 子						循環節
1)	1	10	9	90	81	82	010989
2)	2	20	18	89	71	73	021978
3)	3	30	27	88	61	64	032967
4)	4	40	36	87	51	55	043956
5)	5	50	45	86	41	46	054945
6)	6	60	54	85	31	37	065934
7)	7	70	63	84	21	38	076923
8)	8	80	72	83	11	19	087912
9)	12	29	17	79	62	74	131868
10)	15	59	44	76	32	47	164835
11)	16	69	53	75	22	38	175824
12)	23	48	25	68	43	66	252747

解答 35 (問題 9.1)　$a = 2$ をとってみる.

$2^6 = 64 \equiv 23\,(\mathrm{mod.}\ 41)$, $2^7 \equiv 46 \equiv 5\,(\mathrm{mod.}\ 41)$, $2^8 \equiv 10\,(\mathrm{mod.}\ 41)$, $2^9 \equiv 20\,(\mathrm{mod.}\ 41)$, $2^{10} \equiv 40 \equiv -1\,(\mathrm{mod.}\ 41)$. $\therefore\quad 2^{20} \equiv 1\,(\mathrm{mod.}\ 41)$

したがって $a = 3$ は原始根でない. 今の計算に現れず a のべきと互いに素な数として $b = 3$ をとる. $3^4 = 81 \equiv -1\,(\mathrm{mod.}\ 41)$ なので $3^8 \equiv 1\,(\mathrm{mod.}\ 41)$ したがって 3 の指数は 8 である. $(20,\ 8) = 4$ なので $4 = 1 \cdot 4$ とし $m_0 = \dfrac{20}{4} = 5,\ n_0 = \dfrac{8 \cdot 4}{4} = 8$ とする.

$$2^{\frac{20}{5}} \cdot 3^{\frac{8}{8}} = 2^4 \cdot 3 = 48 \equiv 7\,(\mathrm{mod.}\ 41)$$

7 の指数が $5 \times 8 = 40$ になるので 7 は原始根である.

解答 36 (問題 9.2)

(1) $100 \equiv 9 \pmod{13}$. $\therefore\quad \mathrm{Ind}\,.100 = \mathrm{Ind}\,.9 = 8$

(2) $-1 \equiv 12 \pmod{13}$. $\therefore\quad \mathrm{Ind}\,.(-1) = \mathrm{Ind}\,.12 = 6$

(3) I の欄が 9 になるのは, a の欄が 5. $\therefore\ x \equiv 5 \pmod{13}$

(4) $-1 \equiv 11 \pmod{12}$. $I = 11$ に対する $a = 7$. $\therefore\ x \equiv 7 \pmod{13}$.

解答 37 (問題 9.3)

(1) $\mathrm{Ind}_2\, 11 = 7,\ \mathrm{Ind}_2\, 5 = 9$ なので $\mathrm{Ind}_2\, x = 2$. ゆえに $x \equiv 2\ (\mathrm{mod.}\ 13)$

(2) $3\,\mathrm{Ind}_2\, x = 9$ より $x \equiv 8\ (\mathrm{mod.}\ 13)$

(3) $5x^2 + 3x \equiv 10\ (\mathrm{mod.}\ 13)$ より $5(x-1)^2 \equiv 15\ (\mathrm{mod.}\ 13)$. つまり $(x-1)^2 \equiv 3\ (\mathrm{mod.}\ 13)$.
ここで $\mathrm{Ind}_2\, 3 = 4$ なので $\mathrm{Ind}_2(x-1) = 2$, つまり $x-1 \equiv 43\ (\mathrm{mod.}\ 13)$, $x \equiv 53\ (\mathrm{mod.}\ 13)$

解答 38 (問題 9.4)

$$\left(r^{\frac{p-1}{2}} - 1\right)\left(r^{\frac{p-1}{2}} + 1\right) = r^{p-1} - 1 \equiv 0 \pmod{p}$$

ところが r は原始根なので $r^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$. ゆえに $r^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
つまり題意が示された.

解答 39 (問題 9.5) $a \equiv -b \pmod{p}$ である. ゆえに

$$\begin{aligned} \mathrm{Ind}\, a &= \mathrm{Ind}\,(-1) + \mathrm{Ind}\, b \\ &\equiv \frac{p-1}{2} + \mathrm{Ind}\, b \pmod{p-1} \end{aligned}$$

つまり題意が示された.

解答 40 (問題 9.6) $r^{\alpha} \equiv a \pmod{p}$ とおく. さらに $s = \mathrm{Ind}_{r'} r$, つまり $r \equiv r'^{s} \pmod{p}$ とおく. あわせて

$$r'^{s\alpha} \equiv a \pmod{p} \quad \Rightarrow \quad \mathrm{Ind}_{r'}\, \alpha \equiv s\,\mathrm{Ind}_r\, \alpha$$

両辺 s で割って題意の式を得る.

解答 41 (問題 9.7) r を法 p の原始根とすれば k が $p-1$ で割りきれないので二つの集合

$$\{1^k,\ 2^k,\ \cdots,\ (p-1)^k\}$$
$$\{1,\ r^k,\ \cdots,\ r^{(p-2)k}\}$$

の各要素は互いに p を法として合同の関係で一対一に対応している. ゆえに

$$\begin{aligned} & 1^k + 2^k + \cdots + (p-1)^k \\ \equiv\ & 1 + r^k + \cdots + r^{(p-2)k} \\ \equiv\ & \frac{r^{(p-1)k} - 1}{r^k - 1} \equiv 0 \pmod{p} \end{aligned}$$

ここで分子は $r^{(p-1)k} - 1 \equiv 1^k - 1 \equiv 0 \pmod{p}$, 分母は $r^k - 1 \not\equiv 0 \pmod{p}$ であることに注意する.

解答 42 (問題 9.8)

$$\begin{aligned} (p-1)! &\equiv r^{1+2+\cdots+(p-2)} \\ &= \left(r^{\frac{p-1}{2}}\right)^{p-2} \\ &\equiv (-1)^{p-2} \equiv -1 \pmod{p} \end{aligned}$$

解答 43 (問題 10.1)

$$\begin{aligned}
\left(\frac{365}{1847}\right) &= \left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right) \\
&= \left(\frac{1847}{5}\right)\left(\frac{1847}{73}\right) && 5 \equiv 1,\ 73 \equiv 1 \pmod 4 \\
&= \left(\frac{2}{5}\right)\left(\frac{22}{73}\right) \\
&= \left(\frac{2}{5}\right)\left(\frac{2}{73}\right)\left(\frac{11}{73}\right) \\
&= -\left(\frac{11}{73}\right) && \text{(第二補充則)} \\
&= -\left(\frac{73}{11}\right) = -\left(\frac{-4}{11}\right) \\
&= -\left(\frac{-1}{11}\right)\left(\frac{2^2}{11}\right) \\
&= -\left(\frac{-1}{11}\right) \\
&= 1 && \text{(第一補充則)}
\end{aligned}$$

解答 44 (問題 10.2)

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}}$$

ここで

$$\frac{p-1}{2}+\frac{p^2-1}{8} = \frac{p^2+4p-5}{8} = p-1+\frac{p^2-4p+3}{8} \equiv \frac{(p-3)(p-1)}{8} \pmod 2$$

$p-3,\ p-1$ は隣り合う二つの偶数なのでともに 4 の倍数になることはない．ゆえに $(p-3)(p-1)$ が 16 の倍数になるのは $p-3,\ p-1$ のいずれかが 8 の倍数になるときにかぎる．

解答 45 (問題 10.3)　相互法則から

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$$

ところが法 5 については

$$3^2 \equiv 4,\ 4^2 \equiv 1 \pmod 5$$

なので

(1) $p \equiv 1,\ 4 \pmod 5$ のとき $\left(\dfrac{p}{5}\right) = 1$

(2) $p \equiv 2,\ 3 \pmod 5$ のとき $\left(\dfrac{p}{5}\right) = -1$

となり，あわせて題意が示された．

解答 46 (問題 10.4)　相互法則から

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right)$$

p を 3, 4, 12 を法とする剰余で分類して値を決める．

	mod. 4	mod. 3	mod. 12	$(-1)^{\frac{p-1}{2}}$	$\left(\frac{p}{3}\right)$	$\left(\frac{3}{p}\right)$
$p=$	1	1	1	1	1	$+1$
	-1	-1	-1	-1	-1	$+1$
	1	-1	5	1	-1	-1
	-1	1	-5	-1	1	-1

したがって確かに題意が成立している．

解答 47 (問題 10.5)

$$a^2 \equiv (p-a)^2 \pmod{p}$$

で

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

となる X は二つしかないので p を法として，

$$1^2,\ 2^2,\ \cdots,\ (p-1)^2$$

はちょうど二つずつが同じになる．したがって

$$1,\ 2,\ \cdots,\ p-1$$

のうち半分が平方剰余で半分が非剰余である．

$$\therefore \quad \sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$$

ところが第一補充法則から

$$\left(\frac{p-a}{p}\right) = \left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = \left(\frac{a}{p}\right)$$

したがって

$$\sum_{a=1}^{\frac{p-1}{2}}\left(\frac{a}{p}\right) = 0$$

また a と $p-a$ の偶数奇数は逆なので

$$\sum_{0\leqq b\leqq p \text{ の偶数}}\left(\frac{b}{p}\right) = \sum_{0\leqq c\leqq p \text{ の奇数}}\left(\frac{c}{p}\right)$$

となり，これはともに 0 である．

解答 48 (問題 11.1)

$$\begin{aligned}
5 &= N(1+2i) = 1^2+2^2\\
13 &= N(3+2i) = 9^2+2^2\\
65 &= N(1+2i)N(3+2i) = N(-1+8i) = 1^2+8^2\\
65 &= N(1+2i)N(3-2i) = N(7+4i) = 7^2+4^2\\
5^2 &= N(1+2i)^2 = N(-3+4i) = 3^2+4^2\\
50 &= N(1-i)N(1+2i)^2 = N(1+7i) = 1^2+7^2\\
13^3 &= N(3+2i)^2 = N(5+12i) = 5^2+12^2
\end{aligned}$$

解答 49 (問題 12.1)

(1) $(x,\ y) \in S$ かつ $x+\sqrt{D}y > 1$ であるものの中で最小の元を確定させなければならない. そこで, まず

$$x+\sqrt{D}y > 1 \text{ ならば, } x > 0,\ y > 0$$

を示す. $x^2 - Dy^2 = (x+\sqrt{D}y)(x-\sqrt{D}y) = \pm 1$ より,

$$|\, x-\sqrt{D}y \,| = \frac{1}{x+\sqrt{D}y} < 1$$

したがって,

$$-1 < x-\sqrt{D}y < 1$$

となる. すると, $1 < x+\sqrt{D}y,\ -1 < x-\sqrt{D}y$ より,

$$0 < 2x \qquad \therefore \quad x > 0$$

また, $1 < x+\sqrt{D}y,\ -1 < -x+\sqrt{D}y$ より,

$$0 < 2\sqrt{D}y \qquad \therefore \quad y > 0$$

以上より, $x > 0,\ y > 0$ という条件のもとで, $x+\sqrt{D}y$ の値が最小となるものを考 えればよい.

(i) $D = 2$ のとき, $(x,\ y) = (1,\ 1)$ に対して,

$$x^2 - 2y^2 = 1^2 - 2\cdot 1^2 = -1 \qquad \therefore \quad (1,\ 1) \in S$$

となり, 上の考察と合わせると, これが求めるものである. この場合,

$$A = \begin{pmatrix} p & 2q \\ q & p \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}$$

(ii) $D = 3$ のとき, $(x,\ y) = (1,\ 1),\ (2,\ 1)$ に対して,

$$(x,\ y) = (1,\ 1) \text{ のとき, } x^2 - 3y^2 = 1^2 - 3\cdot 1^2 \neq \pm 1$$
$$(x,\ y) = (2,\ 1) \text{ のとき, } x^2 - 3y^2 = 2^2 - 3\cdot 1^2 = 1 \therefore (2,\ 1) \in S$$

となり, 上の考察と合わせると, $(x,\ y) = (2,\ 1)$ が求めるものである. この場 合,

$$A = \begin{pmatrix} p & 3q \\ q & p \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 1 & 2 \end{pmatrix}$$

(2) $x^2 - 3y^2 = -1$ の解があれば, $x^2 \equiv -1 \pmod 3$ となる x が存在することになるが, オイラーの規準より

$$\left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1$$

なので, 法 3 に関して -1 は平方剰余ではないので, そのような解はない.

解答 50 (問題 13.1)

(1) 正三角形を各辺の中点を結んでさらに 1 辺の長さが 1 の小正三角形四つに分割する．小正三角形の各頂点はもとの正三角形の辺上にある．

$m = 5$ ， $n = 4$ で「鳩の巣原理」を適用すると，四つの小正三角形のうち少なくとも一つの小正三角形の内部または周上には二つの点がくる．かつ，点はもとの正三角形の内部に取るのであるから，いずれの点も小正三角形の頂点には来ない．

2 点 P, Q が三角形の内部にあれば直線 PQ と三角形の辺の交点を R, S とする．R や S が頂点でなければ R を固定し S を辺上で動かすと，S が一方の方向に動くとき RS は増加する．ゆえに S が頂点に来たときの方が長い．R についても同様．したがって，三角形の内部および周上にある 2 点間の距離は最大辺の長さを越えない．

ゆえにその距離は 1 より小さい．

(2) 2 点の中点が格子点であるためには 2 点の x, y, z 座標の和が偶数であることと同値である．和が偶数になるためには，その 2 数の偶数・奇数が一致していればよい．(偶数，奇数，偶数) のような組合せは全部で 8 通りしかない．$m = 9$ $n = 8$ で鳩の巣原理を適用すれば，少なくとも 1 組，(偶数，奇数，偶数) の型が同じであるものができる．その 2 点の中点は，格子点である．

解答 51 (問題 14.1)

$$
\begin{aligned}
\sqrt{7} &= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \left(\frac{1}{\sqrt{7}-2} \right) = \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \sqrt{7}+2 \\ 3 \end{pmatrix} \\
&= \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \left(\frac{3}{\sqrt{7}-1} \right) = \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} \sqrt{7}+1 \\ 2 \end{pmatrix} \\
&= \begin{pmatrix} 3 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \left(\frac{2}{\sqrt{7}-1} \right) = \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} \sqrt{7}+1 \\ 3 \end{pmatrix} \\
&= \begin{pmatrix} 5 & 3 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \left(\frac{3}{\sqrt{7}-2} \right) = \begin{pmatrix} 8 & 5 \\ 3 & 2 \end{pmatrix} (\sqrt{7}+2) \\
&= \begin{pmatrix} 8 & 5 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \left(\frac{1}{\sqrt{7}-2} \right) = \begin{pmatrix} 37 & 14 \\ 5 & 3 \end{pmatrix} \begin{pmatrix} \sqrt{7}+2 \\ 3 \end{pmatrix} \\
\cdots &\quad \cdots
\end{aligned}
$$

したがって

$$
\frac{2}{1} < \frac{5}{2} < \frac{37}{14} < \cdots < \sqrt{7} < \cdots < \frac{8}{3} < \frac{3}{1}
$$

解答 52 (問題 15.1)　$ax^2 + bxy + cy^2 = \dfrac{2\sqrt{-D}}{\pi}$ はちょうど面積が 4 の楕円である．これについては『数学対話』「三角形に辺の中点で内接する楕円 (シュタイナー楕円)」のなかの「一次変換」参照のこと．ゆえにミンコフスキーの定理より領域 $ax^2 + bxy + cy^2 \leqq \dfrac{2\sqrt{-D}}{\pi}$ には原点以外の格子点が含まれる．

解答 53 (問題 16.1)　$\omega_1 = 4 + \sqrt{13}$ のとき． $D = 13$ である．

ω	二次方程式	ω'
$\omega_1 = 4 + \sqrt{13} = 7 + (\sqrt{13} - 3)$	$x^2 - 8x + 3 = 0$	$4 - \sqrt{13} < -1$
$\omega_2 = \dfrac{1}{\sqrt{13} - 3} = \dfrac{\sqrt{13} + 3}{4} = 1 + \dfrac{\sqrt{13} - 1}{4}$	$4x^2 - 6x - 1 = 0$	$-1 < \dfrac{-\sqrt{13} + 3}{4} < 0$
$\omega_3 = \dfrac{4}{\sqrt{13} - 1} = \dfrac{\sqrt{13} + 1}{3} = 1 + \dfrac{\sqrt{13} - 2}{3}$	$3x^2 - 2x - 4 = 0$	$\dfrac{-\sqrt{13} + 1}{3}$
$\omega_4 = \dfrac{3}{\sqrt{13} - 2} = \dfrac{\sqrt{13} + 2}{3} = 1 + \dfrac{\sqrt{13} - 1}{3}$	$3x^2 - 4x - 3 = 0$	$\dfrac{-\sqrt{13} + 2}{3}$
$\omega_5 = \dfrac{3}{\sqrt{13} - 1} = \dfrac{\sqrt{13} + 1}{4} = 1 + \dfrac{\sqrt{13} - 3}{4}$	$4x^2 - 2x - 3 = 0$	$\dfrac{-\sqrt{13} + 1}{4}$
$\omega_6 = \dfrac{4}{\sqrt{13} - 3} = \sqrt{13} + 3 = 6 + \sqrt{13} - 4$	$x^2 - 6x - 4 = 0$	$-\sqrt{13} + 3$
$\omega_7 = \dfrac{1}{\sqrt{13} - 3} = \dfrac{\sqrt{13} + 3}{4} = \omega_2$		

解答 54 (問題 17.1)

$$
\begin{aligned}
\sqrt{19} &= \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} x_1 && x_1 = \frac{1}{\sqrt{19} - 4} = \frac{\sqrt{19} + 4}{3} \\
&= \begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} x_2 && x_2 = \frac{3}{\sqrt{19} - 2} = \frac{\sqrt{19} + 2}{5} \\
&= \begin{pmatrix} 9 & 4 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} x_3 && x_3 = \frac{5}{\sqrt{19} - 3} = \frac{\sqrt{19} + 3}{2} \\
&= \begin{pmatrix} 13 & 9 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} x_4 && x_4 = \frac{2}{\sqrt{19} - 3} = \frac{\sqrt{19} + 3}{5} \\
&= \begin{pmatrix} 48 & 13 \\ 11 & 3 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} x_5 && x_5 = \frac{5}{\sqrt{19} - 2} = \frac{\sqrt{19} + 2}{3} \\
&= \begin{pmatrix} 61 & 48 \\ 14 & 11 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} x_6 && x_6 = \frac{3}{\sqrt{19} - 4} = \sqrt{19} + 4 \\
&= \begin{pmatrix} 170 & 61 \\ 39 & 14 \end{pmatrix} \begin{pmatrix} 8 & 1 \\ 1 & 0 \end{pmatrix} x_7 && x_7 = \frac{1}{\sqrt{19} - 4} = x_1
\end{aligned}
$$

ゆえに $k = 6$ 最小解 $(x,\ y) = (170,\ 39)$.

$$170^2 - 19 \cdot 39^2 = 1$$

解答 55 (問題 17.2)

$$
\begin{aligned}
\sqrt{46} &= \begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix} x_1 && x_1 = \frac{1}{\sqrt{46}-6} = \frac{\sqrt{46}+6}{10} \\
&= \begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} x_2 && x_2 = \frac{10}{\sqrt{46}-4} = \frac{\sqrt{46}+4}{3} \\
&= \begin{pmatrix} 7 & 6 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} x_3 && x_3 = \frac{3}{\sqrt{46}-5} = \frac{\sqrt{46}+5}{7} \\
&= \begin{pmatrix} 27 & 7 \\ 4 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} x_4 && x_4 = \frac{7}{\sqrt{46}-2} = \frac{\sqrt{46}+2}{6} \\
&= \begin{pmatrix} 34 & 27 \\ 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} x_5 && x_5 = \frac{6}{\sqrt{46}-4} = \frac{\sqrt{46}+4}{5} \\
&= \begin{pmatrix} 61 & 34 \\ 9 & 5 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} x_6 && x_6 = \frac{5}{\sqrt{46}-6} = \frac{\sqrt{46}+6}{2} \\
&= \begin{pmatrix} 156 & 61 \\ 23 & 9 \end{pmatrix} \begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix} x_7 && x_7 = \frac{2}{\sqrt{46}-6} = \frac{\sqrt{46}+6}{5} \\
&= \begin{pmatrix} 997 & 156 \\ 147 & 23 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 0 \end{pmatrix} x_8 && x_8 = \frac{5}{\sqrt{46}-4} = \frac{\sqrt{46}+4}{6} \\
&= \begin{pmatrix} 2150 & 997 \\ 317 & 147 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} x_9 && x_9 = \frac{6}{\sqrt{46}-2} = \frac{\sqrt{46}+2}{7} \\
&= \begin{pmatrix} 3147 & 2150 \\ 464 & 317 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} x_{10} && x_{10} = \frac{7}{\sqrt{46}-5} = \frac{\sqrt{46}+5}{3} \\
&= \begin{pmatrix} 5297 & 3147 \\ 781 & 464 \end{pmatrix} \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} x_{11} && x_{11} = \frac{3}{\sqrt{46}-4} = \frac{\sqrt{46}+4}{10} \\
&= \begin{pmatrix} 19038 & 5297 \\ 2807 & 781 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} x_{12} && x_{12} = \frac{10}{\sqrt{46}-6} = \sqrt{46}+6 \\
&= \begin{pmatrix} 24335 & 19038 \\ 3588 & 287 \end{pmatrix} \begin{pmatrix} 12 & 1 \\ 1 & 0 \end{pmatrix} x_{13} && x_{13} = \frac{1}{\sqrt{46}-6} = x_1
\end{aligned}
$$

ゆえに $k = 12$ 最小解 $(x,\ y) = (24335,\ 3588)$.

$$24335^2 - 19 \cdot 3588^2 = 1$$

18.2 演習問題解答

1 節演習問題解答

解答 1 (問題 1)

(1) $2x^3 + 5x^2 - 3x + 7 = (x-3)(2x^2 + 11x + 30) + 97$ である.

$$\therefore \quad Q(x) = 2x^2 + 11x + 30, \quad r - 97$$

(2) (i) $F(x)$ を x の n 次の整式とし, x^n の係数が a_n であるとする.
ここで,

$$Q_1(x) = a_n x^{n-1},\ F_1(x) = F(x) - G(x)Q_1(x)$$

とおく.

$$G(x)Q_1(x) = (x-a)\cdot a_n x^{n-1} = a_n x^n - a a_n x^{n-1}$$

であるから $F_1(x)$ の次数は $n-1$ 以下であり，明らかに題意を満たす.

(ii) 一次式，つまり $F(x) = px + q$ のときは $Q(x) = p,\ r = ap + q$ とおけばよい.

1〜$n-1$ 次式のとき成立するとする.

n 次式 $F(x)$ に対して

$$F(x) = G(x)Q(x) + F_1(x)$$

を満たす x の整式 $Q_1(x),\ F_1(x)$, ただし $F_1(x)$ の次数は $F(x)$ の次数より小さい，が存在する.

帰納法の仮定から

$$F_1(x) = G(x)Q_1(x) + r$$

となる $Q_1(x)$ と r が存在する．したがって，

$$F(x) = G(x)Q(x) + F_1(x) = G(x)Q(x) + G(x)Q_1(x) + r = G(x)\{Q(x) + Q_1(x)\} + r$$

$Q(x) + Q_1(x)$ を改めて $Q(x)$ に取り直せば， n のときも題意が成立することがわかる.

したがって，任意の自然数 n に対して題意が示された.

(3)

$$F(x) = (x-a)Q(x) + r$$

となる $Q(x)$ と r が存在する．この等式に $x = a$ を代入する．$F(a) = r$ が得られる．$F(a) = 0$ より $r = 0$ ．したがって題意は示された.

(4) 方程式 $F(x) = 0$ の相異なる実数解を $\alpha_1,\ \cdots,\ \alpha_j$ とする.

$F(\alpha_1) = 0$ より

$$F(x) = (x-\alpha_1)Q_1(x)$$

とおける．$F(\alpha_2) = 0$ で $\alpha_2 - \alpha_1 \neq 0$ より $Q(\alpha_2) = 0$.

$$\therefore \quad Q_1(x) = (x-\alpha_2)Q_2(x)$$

とおける．つまり

$$F(x) = (x-\alpha_1)(x-\alpha_2)Q_2(x)$$

これを繰りかえすと，

$$F(x) = (x-\alpha_1)\cdots(x-\alpha_j)Q_j(x)$$

となる整式 $Q_j(x)$ がある.

もし $j > n$ なら右辺の次数は左辺の次数 n より大きくなり不合理．よって $j \leqq n$ ．つまり題意が示せた.

2 節演習問題解答

解答 2 (問題 2)

［注］内容的には本文の中にあるが，入試問題の解答として改めて解いておく．

(1)

	$a_1 = 1998$	$b_1 = 185$
$1998 = 185 \times 10 + 148$ より	$a_2 = 185$	$b_2 = 148$
$185 = 148 \times 1 + 37$ より	$a_3 = 148$	$b_3 = 37$
$148 = 37 \times 4 + 0$ より	$a_4 = 37$	$b_4 = 0$
	$a_5 = 37$	$b_5 = 0$

(2) $b_n \neq 0$ のとき b_{n+1} は a_n を b_n で割った余りであるから余りの定義より，

$$b_{n+1} < b_n$$

$b_n = 0$ のとき 数列 $\{b_n\}$ の定義から $b_{n+1} = b_n$ ． よって 任意の $k,\ l,\ n$ について $b_n \geqq b_{n+1}$ (等号は $b_n = 0$ のときに限る) が成立する．

(3) もし $b_n = 0$ となる n が存在しないとすると，すべての b_n は自然数でしかも

$$b_n > b_{n+1}$$

が成り立つ．このことは 集合 $\{b_n\}$ に最小値が存在しないことになり，自然数の性質と矛盾する．

(4) $(a,\ b)$ で a と b の最大公約数を表すことにする． $b_k \neq 0$ のとき

$$(a_k,\ b_k) = (b_k,\ b_{k+1})$$

を示す．

$a_k = b_k \cdot q_k + b_{k+1}$ とかける． a_k と b_k の公約数は b_{n+1} の約数になる．ゆえに $(a_k,\ b_k) \leqq (b_k,\ b_{k+1})$ ．

b_k と b_{k+1} の公約数は a_k の約数になる．ゆえに $(a_k,\ b_k) \geqq (b_k,\ b_{n+1})$ ．

$$\therefore \quad (a_k,\ b_k) = (b_k,\ b_{k+1})$$

つまり $(a_k,\ a_{k+1}) = (a_{k+1},\ a_{k+2})$ ．
(3) からある自然数 N で $b_{N-1} \neq 0,\ b_N = 0$ となるものがある．このとき

$$(k,\ l) = (a_1,\ a_2) = \cdots = (a_{N-1},\ a_N) = (a_N,\ b_N) = a_N$$

$N \leqq n$ の n で同様なので題意が示された．

解答 3 (問題 3)

(1) $r_{n-1} > 0$ のとき,

$$r_{n-2} = r_{n-1}q_{n-1} + r_n, \quad 0 \leqq r_n < r_{n-1}$$

したがって,

$$r_1 = a \geqq r_2 = b > r_3 > r_4 > \cdots \geqq 0$$

となり，各 r_n は自然数または 0 であるから，高々 $a+1$ 回この操作を繰り返すとこれは 0 となる. つまり,

$$r_{N-1} > r_N > 0 = r_{N+1}$$

となる整数 N が存在する.

(2) k についての帰納法で示す.

(i) $k = 1$ のとき,

$$r_{N+2-k} = r_{N+1} = 0,\ f_k = f_1 = 0$$

なので，不等式は成り立つ. 次に，$k = 2$ のとき,

$$r_{N+2-k} = r_N \geqq 1,\ f_k = f_2 = 1$$

よって，不等式は成り立つ.

(ii) $k = m-1$, m $(m \geqq 2)$ のときの不等式の成立，すなわち,

$$r_{N+2-(m-1)} \geqq f_{m-1}, \quad r_{N+2-m} \geqq f_m$$

を仮定する. このとき,

$$\begin{aligned} r_{N+2-(m+1)} &= r_{N+2-m} \cdot q_{N+2-m} + r_{N+2-(m-1)} \\ &\geqq f_m q_{N+2-m} + f_{m-1} \\ &\geqq f_m + f_{m-1} \quad (\text{なぜなら},\ q_{N+2-m} \geqq 1) \\ &= f_{m+1} \end{aligned}$$

となるので，$k = m+1$ のときも成立する.

(iii) よって，(i)，(ii) より，$k = 1,\ 2,\ \cdots,\ N+1$ のすべての k に対して不等式が成り立つ.

(3) n に関する帰納法で示す.

(i) $n = 1$ のとき,

$$f_{n+1} = f_2 = 1,\ \left(\frac{3}{2}\right)^{n-2} = \left(\frac{3}{2}\right)^{1-2} = \frac{2}{3}$$

$n = 2$ のとき,

$$f_{n+1} = f_3 = f_2 + f_1 = 1,\ \left(\frac{3}{2}\right)^{n-2} = \left(\frac{3}{2}\right)^{2-2} = 1$$

よって, いずれの場合も不等式は成り立つ.

(ii) $n=k-1$, k $(k \geqq 2)$ のときの不等式の成立，すなわち

$$f_k \geqq \left(\frac{3}{2}\right)^{k-3}, \quad f_{k+1} \geqq \left(\frac{3}{2}\right)^{k-2}$$

を仮定する．このとき

$$\begin{aligned} f_{(k+1)+1} &= f_{k+1}+f_k \\ &\geqq \left(\frac{3}{2}\right)^{k-2}+\left(\frac{3}{2}\right)^{k-3} \\ &= \left(\frac{3}{2}\right)^{k-3}\cdot\frac{5}{2} \\ &\geqq \left(\frac{3}{2}\right)^{k-1} \quad \left(\text{なぜなら，}\ \frac{5}{2} \geqq \frac{9}{4}\right) \\ &= \left(\frac{3}{2}\right)^{(k+1)-2} \end{aligned}$$

よって，$n=k+1$ のときも不等式は成り立つ．

(iii) よって，(i)，(ii) より，すべての自然数 n に対して不等式が成り立つ．

(4) (2) より，$k=N+1$ のとき，

$$a=r_1=r_{N+2-(N+1)} \geqq f_{N+1}$$

よって，(3) より，

$$a \geqq \left(\frac{3}{2}\right)^{N-2}$$

で，両辺の底を $\dfrac{3}{2}$ とする対数をとれば，

$$\log_{\frac{3}{2}} a \geqq N-2 \qquad \therefore \quad N \leqq 2+\log_{\frac{3}{2}} a$$

［注意］この入試問題は，ユークリッドの互除法で割り算をどれくらい行えばよいかを評価するものである．いちばん長くなるのが，割り算での商が常に 1 になるときで，あまりの列を逆にたどればいわゆるフィボナッチ数列になるときである．このことを問う本格的な問題である．

3 節演習問題解答

解答 4 (問題 4)

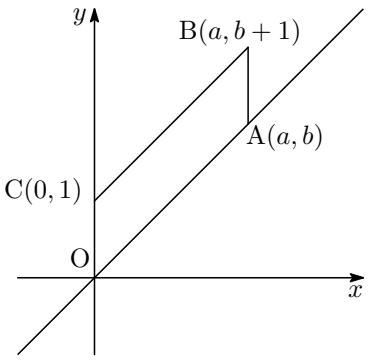
(1) a と b が互いに素であるから，$\dfrac{b}{a}x$ が整数となるのは x が a の倍数であるときにかぎる．

したがって $0<k<a$ の整数 k に対し，直線 $x=k$ と OA, CB の交点はいずれも格子点ではない．

したがって, OABC の内部にある直線 $x=k$ の上には，ちょうど一つの格子点がある．

よって，

OABC の内部には $a-1$ 個の格子点がある．



(2) OABC の内部の格子点を $\mathrm{P}_i(p_i,\ q_i)$ とおく.

$$\triangle \mathrm{OP}_i A = \frac{1}{2}|aq_i - bp_i|$$

である．$\mathrm{P}_i(p_i,\ q_i)$ は領域 $y > \dfrac{b}{a}x$ にあるので,

$$aq_i - bp_i \geqq 1$$

よって,

$$\triangle \mathrm{OP}_i A \geqq \frac{1}{2}$$

である．ここで等号が成立する i が存在することを示す.

まず，$\mathrm{P}_i(p_i,\ q_i)$ に対し，$aq_i - bp_i$ がすべて異なることを示す.

$0 < i,\ j < a$ に対して $aq_i - bp_i = aq_j - bp_j$ ならば,

$$a(q_i - q_j) = b(p_i - p_j)$$

となる．a と b が互いに素であるから，$p_i - p_j$ は a の倍数である.

ところが，$0 < p_i,\ p_j < a$ より,

$$1 - a < p_i - p_j < a - 1$$

であるから，a の倍数は $p_i - p_j = 0$ 以外にないことがわかる.

よって，$q_i = q_j$ も成り立ち，$\mathrm{P}_i = \mathrm{P}_j$ がわかる.

したがって，集合 $\{aq_i - bp_i\}$ の要素の個数は $a - 1$ である.

一方,

$$\frac{b}{a}p_i < q_i < \frac{b}{a}p_i + 1 \quad \Longleftrightarrow \quad 0 < aq_i - bp_j < a$$

なので，集合 $\{aq_i - bp_i\}$ は集合 $\{1,\ 2,\ \cdots,\ a-1\}$ に含まれ，かつ要素の個数が一致する.
よって二つの集合は一致し，かならず $aq_i - bp_i = 1$ となる番号 i がある.

したがって，求める最小値は,

$$\frac{1}{2}$$

参考

・等号成立の別証

$$J = \{aq - bp | (p,\ q) \text{ はすべての格子点 }\}$$

とする． J の要素で正で最小のものを $aq_0 - bp_0$ とする．

任意の J の要素 $aq - bp$ を $aq_0 - bp_0$ で割る．

$$aq - bp = (aq_0 - bp_0)Q + r, \quad 0 \leqq r < aq_0 - bp_0$$

ここで,

$$r = a(q - q_0Q) - b(p - p_0Q) \in J$$

であるから，$aq_0 - bp_0$ の最小性によって,

$$r = 0$$

である．つまり $aq - bp$ は，$aq_0 - bp_0$ の倍数である．

ところが

$$a = a \cdot 1 + b \cdot 0 \in J$$

同じく b も J の要素であるから,

$$aq_0 - bp_0 \text{ は } a \text{ と } b \text{ の約数}$$

となり，a と b が互いに素であるから,

$$aq_0 - bp_0 = 1$$

この $(p_0,\ q_0)$ に対して整数 n を用いて,

$$p_1 = p_0 + an, \quad q_1 = q_0 + bn$$

とおくと，$aq_1 - bp_1 = 1$ であり，n を適当にとると $0 < p_1 < a$ にできる．

このとき $q_1 = \dfrac{b}{a}p_1 + \dfrac{1}{a}$ より,

$$\frac{b}{a}p_1 < q_1 < \frac{b}{a}p_1 + 1$$

となるので，$(p_1,\ q_1)$ は, OABC の内部にある．

解答 5 (問題 5) 傾きが $\dfrac{2}{5}$ である直線 $2x - 5y - u = 0$ を l_u と表すことにする．

このとき， l_u と格子点 $(m,\ n)$ との距離は, 次の式で与えられる．

$$\frac{|2m - 5n - u|}{\sqrt{2^2 + 5^2}} \quad \cdots ①$$

$m,\ n$ が変化するとき， $2m - 5n$ は任意の整数値をとりうる．実際，任意の整数 k に対して

$$2 \cdot 3k - 5 \cdot k = k$$

が成り立つ． u を整数部分と小数部分に分けて

$$u = k + \alpha \quad (k \text{ は整数},\ 0 \leqq \alpha < 1)$$

と書くことにする．したがって上に述べたことから $m,\ n$ が変化するとき，

$$|2m-5n-u| \geqq \min(\alpha,\ 1-\alpha)$$

ゆえに① は

$$\frac{|2m-5n-u|}{\sqrt{2^2+5^2}} \geqq \min\left(\frac{\alpha}{\sqrt{29}},\ \frac{1-\alpha}{\sqrt{29}}\right)$$

そしてこの等号が成立する $m,\ n$ が必ず存在する．したがって

$$r \geqq \min\left(\frac{\alpha}{\sqrt{29}},\ \frac{1-\alpha}{\sqrt{29}}\right)$$

に円の半径をとれば，直線 l_u は円のいずれかと共有点をもつ．

u の値に関わらず共有点をもつためには u を動かしたときの $\min\left(\frac{\alpha}{\sqrt{29}},\ \frac{1-\alpha}{\sqrt{29}}\right)$ の最大値以上に r をとればよい．

明らかに

$$\frac{1}{2} \geqq \min\left(\frac{\alpha}{\sqrt{29}},\ \frac{1-\alpha}{\sqrt{29}}\right)$$

で等号は $\alpha=\dfrac{1}{2}$ のときである．

したがって

$$r \geqq \frac{1}{2}\sqrt{29}$$

であれば， u に関わらず直線 l_u は円のいずれかと共有点をもつ．求める r の最小値は

$$\frac{1}{2\sqrt{29}}$$

［注意］論証の根幹に， $m,\ n$ が変化するとき， $2m-5n$ は任意の整数値をとりうる，事実がある．

解答 6 (問題 6)

(1) (i) $(x,\ y)$ を任意の整数解とする．

$$\alpha x = \beta y$$

で $\alpha,\ \beta$ が互いに素な正の整数であるから，x は β の倍数である． $x=\beta t$ とおく．このとき $y=\alpha t$ となる．逆にこの形をしている $(x,\ y)$ は方程式を満たす．

$$x=\beta t,\ y=\alpha t \quad (t \text{ は任意の整数})$$

(ii) α を β で割り商が q 余りが r_1 とすると

$$\frac{\alpha}{\beta} = q + \frac{r_1}{\beta} \quad 0 \leqq \frac{r_1}{\beta} < 1$$

一方

$$\frac{\alpha}{\beta} = a_1 + \frac{1}{a_2+\dfrac{1}{a_3+\dfrac{1}{a_4}}}, quad 0 \leqq \frac{1}{a_2+\dfrac{1}{a_3+\dfrac{1}{a_4}}} < 1$$

正の有理数の整数部分と小数部分は一意だから

$$q = a_1,\ \frac{r_1}{\beta} = \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4}}}$$

次に

$$\frac{\beta}{r_1} = a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4}}$$

なので，同様に β を r_1 で割った商が a_2 で，余りを r_2 とすると

$$\frac{r_1}{r_2} = a_3 + \frac{1}{a_4}$$

再び同様に考えると r_1 を r_2 で割った商が a_3 で，その余りを r_3 とすると

$$\frac{r_2}{r_3} = a_4$$

つまり

$$\begin{aligned} \alpha &= a_1\beta + r_1 \\ \beta &= a_2 r_1 + r_2 \\ r_1 &= a_3 r_2 + r_3 \\ r_2 &= a_4 r_3 \end{aligned}$$

ゆえに

$$\begin{aligned} \alpha &= a_1(a_2 r_1 + r_2) + r_1 \\ &= a_1 a_2(a_3 r_2 + r_3) + a_1 r_2 + (a_3 r_2 + r_3) \\ &= a_1 a_2 a_3 a_4 r_3 + a_1 a_2 r_3 + a_1 a_4 r_3 + a_3 a_4 r_3 + r_3 \\ \beta &= a_2 a_3 a_4 r_3 + a_2 r_3 + a_4 r_3 \end{aligned}$$

α と β は互いに素なので $r_3 = 1$
(［注］ユークリッドの互除法の原理から $r_3 = 1$ であるが，ここは直接確認した．)
したがって

$$\begin{aligned} \alpha &= a_1\beta + r_1 \\ \beta &= a_2 r_1 + r_2 \\ r_1 &= a_3 r_2 + 1 \end{aligned}$$

という除法の系列ができる．
このとき

$$\begin{aligned} r_1 &= \alpha - a_1\beta \\ r_2 &= \beta - a_2 r_1 = \beta - a_2(\alpha - a_1\beta) \\ &= -a_2\alpha + (1 + a_1 a_2)\beta \\ \therefore\quad \alpha - a_1\beta &= a_3(-a_2\alpha + (1 + a_1 a_2)\beta) + 1 \end{aligned}$$

つまり

$$(1+a_2a_3)\alpha-(a_1a_2a_3+a_1+a_3)\beta=1$$
$$\therefore \quad \alpha q-\beta p=1$$

(2) 157 と 68 は互いに素である.

$$\begin{aligned} 157 &= 2\cdot 68+21 \\ 68 &= 3\cdot 21+5 \\ 21 &= 4\cdot 5+1 \end{aligned}$$

つまり

$$\frac{157}{68}=2+\cfrac{1}{3+\cfrac{1}{4+\cfrac{1}{5}}}$$

(1) より $p=2\cdot 3\cdot 4+2+4=30$, $q=3\cdot 4+1=13$ とおくと

$$157\cdot 13-68\cdot 30=1$$

したがって

$$157\cdot 39-68\cdot 90=3$$

$(x,\ y)$ を $157x-68y=3$ の任意の整数解とする.

$$157(x-39)-68(y-90)=0$$

ゆえに (1) より

$$x-39=68t,\ y-90=157t \quad (t \text{ は任意の整数})$$

と書ける.

$$\therefore \quad x=39+68t,\ y=90+157t \quad (t \text{ は任意の整数})$$

解答 7 (問題 7)

(1)

$$ax_0+by_0=c,\ al+bm=c$$

の辺々を引くと

$$a(x_0-l)+b(y_0-m)=0$$

ここで $a,\ b$ は互いに素なので, x_0-l が b の倍数. これを bu (u は整数) とおく. このとき $y_0-m=-au$ となる. つまり,

$$l=x_0+bu,\ m=y_0-au$$

を満たす整数 u が存在する.

(2) $ax+by=ab$ の整数解を考える．

$$a(x-b)+by=0$$

よりある整数で $y=au,\ x-b=-bu$，つまり $x=b(1-u)$ と書ける．ここで $x>0,\ y>0$ であるためには

$$0<u<1$$

これは u が整数であることに反する．よって， $c=ab$ のとき $ax+by=c$ を満たす正の整数の組 $(x,\ y)$ は存在しない．

(3) $c=ab$ のとき $ax+by=ab$ を満たす整数の組 $(l,\ m)$ は (1) から

$$l=x_0+bu,\ m=y_0-au$$

と書ける．
$l>0,\ m>0$ となるためには

$$l=x_0+bu>0,\ m=y_0-au>0$$

となる整数 u がとれねばならない．つまり

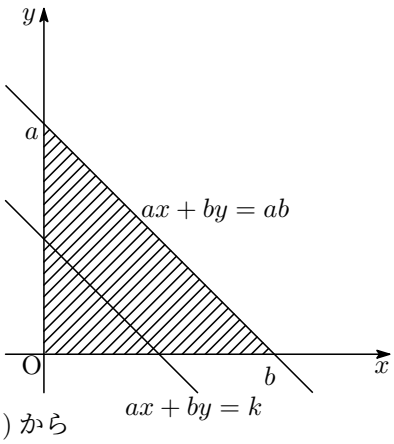
$$\frac{y_0}{a}>u>-\frac{x_0}{b}$$

ところが $c>ab$ のとき

$$\frac{y_0}{a}-\left(-\frac{x_0}{b}\right)=\frac{ax_0+by_0}{ab}=\frac{c}{ab}>1$$

従って題意を満たす整数 u が必ずとれる．つまり $c>ab$ のとき $ax+by=c$ を満たす正の整数の組 $(x,\ y)$ が存在する．

(4) $0<k<ab$ に対し二組の正の整数 $(x_0,\ y_0)$ と $(x_1,\ y_1)$ があるとする．これは図の斜線領域内の格子点である．



(1) から

$$x_1=x_0+bu,\ y_1=y_0-au$$

となる整数 u がある．ところがこのとき

$$x_1-x_0=bu,\ y_0-y_1=au$$

となり，明らかに 2 点がともに斜線領域に存在することはできない．
逆に言えば斜線領域の各格子点 $(x,\ y)$ に対する $ax+by$ の値はすべて異なる．
格子点は

$$\frac{(a-1)(b-1)}{2}$$

個あるから，正の整数の組 $(x,\ y)$ が存在しない k は

$$ab-\frac{(a-1)(b-1)}{2}=\frac{(a+1)(b+1)}{2}-1\text{（個）}$$

ある．

解答 8 (問題 8)

(1)

$$a(-ak)+(a^2+1)k=k \quad \cdots ①$$

であるから，格子点 $(-ak,\ k)$ は L 上にある．

(2) $(m,\ n)$ を L 上の任意の格子点とする．つまり

$$am+(a^2+1)n=k \quad \cdots ②$$

である．② $-$ ① をとる．

$$a(m+ak)+(a^2+1)(n-k)=0 \quad \cdots ③$$

a の約数は a^2 の約数であり，a^2+1 の約数ではありえないので a と a^2+1 は互いに素である．
したがって③ より $m+ak$ は a^2+1 の倍数である．整数 t を用いて $m+ak=(a^2+1)t$ とおける．このとき $n-k=-at$ となる．
つまり L 上の格子点は整数 t によって，

$$\begin{cases} m=-ak+(a^2+1)t \\ n=k-at \end{cases}$$

と表される．逆にこのように表されるものが L 上にあることは明らかである．
題意をみたす格子点が存在するのは，

$$\begin{cases} m=-ak+(a^2+1)t>0 \\ n=k-at>0 \end{cases}$$

をみたす t が存在することと同値である．つまり

$$\frac{k}{a}>t>\frac{ak}{a^2+1} \quad \cdots ④$$

ここで $k=a(a^2+1)$ のとき④ は

$$a^2+1>t>a^2$$

となる．よって条件をみたす整数 t が存在せず，題意をみたす L 上の格子点も存在しない．

(3) $k > a(a^2+1)$ のとき④ の左辺から右辺を引くと，

$$\frac{k}{a} - \frac{ak}{a^2+1} = \frac{k}{a(a^2+1)} > 1$$

したがって条件をみたす t がつねに存在し，題意をみたす L 上の格子点も存在する．

解答 9 (問題 9) x をひとつ固定する． $m = 2x,\ n = -x$ は $x = 3m + 5n$ を満たす．

$x = 3m + 5n$ を満たす任意の解を $(m,\ n)$ とする．

$$\begin{aligned} 3m + 5n &= x \\ 3(2x) + 5(-x) &= x \end{aligned}$$

この辺々を引いて，

$$3(m - 2x) + 5(n + x) = 0$$

3 と 5 は互いに素なので，ある整数 t によってつぎのようにおけなければならない．

$$\begin{aligned} m - 2x &= -5t \\ n + x &= 3t \end{aligned}$$

つまり x を表す $(m,\ n)$ は整数 t によって次のように表される．

$$(m,\ n) = (2x - 5t,\ -x + 3t)$$

この $(m,\ n)$ が x を表すことも明らかである．

$m = 2x - 5t \geqq 0,\ n = -x + 3t \geqq 0$ なので

$$\frac{1}{3}x \leqq t \leqq \frac{2}{5}x$$

したがってこの範囲に整数 t が存在することと， x が非負整数 $m,\ n$ を用いて表わせることが同値である．

$$\frac{2}{5}x - \frac{1}{3}x \geqq 1$$

つまり $x \geqq 15$ なら必ず条件を満たす整数 t がとれる．したがって

$$1 \leqq x \leqq 14$$

について調べればよい．

$x = 1$	$0 < \frac{1}{3} < \frac{2}{5} < 1$	なし	$x = 8$	$2 < \frac{8}{3} < 3 < \frac{16}{5}$	あり
$x = 2$	$0 < \frac{2}{3} < \frac{4}{5} < 1$	なし	$x = 9$	$\frac{9}{3} = 3$	あり
$x = 3$	$\frac{3}{3} = 1$	あり	$x = 10$	$\frac{20}{5} = 4$	あり
$x = 4$	$1 < \frac{4}{3} < \frac{4}{5} < 2$	なし	$x = 11$	$\frac{11}{3} < 4 < \frac{22}{5}$	あり
$x = 5$	$\frac{10}{5} = 2$	あり	$x = 12$	$\frac{12}{3} = 4$	あり
$x = 6$	$\frac{6}{3} = 2$	あり	$x = 13$	$\frac{13}{3} < 5 < \frac{26}{5}$	あり
$x = 7$	$2 < \frac{7}{3} < \frac{14}{5} < 3$	なし	$x = 14$	$\frac{14}{3} < 5 < \frac{28}{5}$	あり

したがって表せないものはつぎの四つである．

$$x = 1,\ 2,\ 4,\ 7$$

x を 3 で割った余りで分類して考える．

$$\begin{cases} x = 3k & x = 3\cdot k + 5\cdot 0 \text{ より} & k \geqq 0 \text{ のとき } (m,\ n) = (k,\ 0) \text{ で表せる．} \\ x = 3k+1 & x = 3\cdot (k-3) + 5\cdot 2 \text{ より} & k \geqq 3 \text{ のとき } (m,\ n) = (k-3,\ 2) \text{ で表せる．} \\ x = 3k+2 & x = 3\cdot (k-1) + 5\cdot 1 \text{ より} & k \geqq 1 \text{ のとき } (m,\ n) = (k-1,\ 1) \text{ で表せる．} \end{cases}$$

したがってのこるのは 1，2，4，7　である．ところが

$3m$ のとりうる値は 0，3，6，9，$\cdots$

$5n$ のとりうる値は 0，5，10，15，$\cdots$

であるから，明らかに 1，2，4，7 は $3m + 5n$ の形で表せない．

解答 10 (問題 10)

(1) $4m + 6n = 7$ においてどのような整数 $m,\ n$ に対しても左辺は 2 で割り切れる．一方右辺はつねに 2 で割ると 1 余る．ゆえにこの等式を満たす整数 $m,\ n$ は存在しない．

(2) $3m + 5n = 2$ を満たすひと組の $(m,\ n)$ として $(-1,\ 1)$ がとれる．

任意の解 $(m,\ n)$ に対して

$$3m + 5n = 2$$
$$3(-1) + 5(1) = 2$$

で辺々引くと，

$$3(m+1) + 5(n-1) = 0$$

3 と 5 は互いに素なので，$m+1$ が 5 の倍数．これを $m + 1 = 5t$ とおく．

このとき $n - 1 = -3t$ となる．つまり

$$(m,\ n) = (-1 + 5t,\ 1 - 3t)$$

と表される．逆にこの形をしたものがもとの方程式を満たすことは明らか．ゆえにすべての解は

$$(m,\ n) = (-1 + 5t,\ 1 - 3t) \quad (t \text{ は任意の整数})$$

(3) 背理法で示す．

$$\begin{aligned} r(k) = r(l) \quad &\Longleftrightarrow \quad ak - al \text{ が } b \text{ の倍数} \\ (a \text{ と } b \text{ は互いに素なので}) \quad &\Longleftrightarrow \quad k - l \text{ が } b \text{ の倍数} \\ \text{ところが } 1 \leqq k,\ l \leqq b-1 \text{ より} \quad &\qquad -(b-2) \leqq k - l \leqq b - 2 \\ &\therefore \qquad k - l = 0 \end{aligned}$$

ゆえに対偶が示されたので，

$$k \neq l \quad \text{ならば} \quad r(k) \neq r(l)$$

である．

(4) 二つの集合

$$A = \{1,\ 2,\ \cdots,\ b-1\}$$
$$B = \{r(k) | k = 1,\ 2,\ \cdots,\ b-1\}$$

この k に対して $r(k) = 0$ なら ak が b の倍数．a と b は互いに素なので k が b の倍数となるが，$k = 1,\ 2,\ \cdots,\ b-1$ よりあり得ない．したがって $r(k)$ は b で割った余りでしかも 0 でないので

$$B \subset A$$

一方 (3) より

$$k \neq l \quad \text{ならば} \quad r(k) \neq r(l)$$

なので，$k = 1,\ 2,\ \cdots,\ b-1$ に対して $r(k)$ はすべて異なる．つまり集合 B の個数は $b-1$ で，集合 A の個数と等しい．

$$\therefore \quad A = B$$

したがって B の要素のなかに

$$r(k) = 1$$

となるものがある．このとき

$$ak - 1 \text{ が } b \text{ の倍数}$$

つまり $ak - 1 = bl$ となる $(k,\ l)$ が存在した．

$(m,\ n) = (k,\ l)$ という解が存在した．

解答 11 (問題 11)

(1) 集合 $A = \{f(k) | k \text{ は整数}\}$ とおく．明らかに $f(k) = f(n+k)$ である．

$$\therefore \quad A = \{f(k) | k = 0,\ \cdots,\ n-1\}$$

さらに

$$f(n-k) = \left|\sin\frac{2\pi(n-k)}{n}\right| = \left|-\sin\frac{2\pi k}{n}\right| = f(k)$$

したがって

$$f(1) = (n-1),\ \cdots,\ f\left(\frac{n-1}{2}\right) = f\left(\frac{n+1}{2}\right)$$

であるから

$$A = \left\{f(k) | k = 0,\ \cdots,\ \frac{n-1}{2}\right\}$$

次に $0,\ \cdots,\ \dfrac{n-1}{2}$ で $k \neq l$ のとき

$$f(k) = f(l)$$

となるのは $\dfrac{2\pi k}{n} + \dfrac{2\pi l}{n} = \pi$ のときのみ．

このとき

$$2(k+l) = n$$

となり，n が奇数であることに反する．ゆえに $k = 0,\ \cdots,\ \dfrac{n-1}{2}$ に対して $f(k)$ はすべて異なる．

$$\therefore \quad A \text{は} \frac{n+1}{2} \text{個の要素からなる．}$$

(2) 集合

$$B = \{f(mk) | k \text{ は } 0 \leqq k \leqq \frac{n-1}{2} \text{なる整数 } \}$$

とおく．定義から

$$B \subset A$$

である．

ここで

$$\begin{aligned} f(m(k+n)) &= f(mk+mn) = f(mk) \\ f(m(n-k)) &= \left|\sin\frac{2\pi m(n-k)}{n}\right| \\ &= \left|-\sin\frac{2\pi mk}{n}\right| = f(mk) \end{aligned}$$

したがって集合 A の考察と逆に考えて

$$B = \{f(mk) | k \text{ は整数 } \}$$

である．

$$A \subset B$$

を示す．

A の任意の要素 $f(k)$ に対して $f(k) = f(mk')$ となる k' が存在すればよい．

$$\frac{2\pi k}{n} + 2l\pi = \frac{2\pi mk'}{n}$$

となる k'と l が存在すれば十分である（十分条件で成り立つ）．

これは

$$mk' = nl + k$$

となる k' と l が存在することである．

n と m は互いに素なので $mk - ml$ が n の倍数になれば $k - l$ 自身が n の倍数でなければならないので

$$m,\ m\cdot 2,\ \cdots,\ m(n-1)$$

を n で割った余りはすべて異なる．ゆえに必ず余りが k になるものが存在する．

$$\therefore \quad A \subset B$$

となり

$$A = B$$

である．つまり集合として A と B は等しく m によらず一定である．

［注意］ここは演習問題 7 とは違うやり方で $A = B$ を示した．いずれも一次不定方程式の解の存在が基本的事実である．

解答 12 (問題 12)

(1) $\mathrm{A}(k,\ l),\ \mathrm{B}(m,\ n)$ とする．

$N(\mathrm{A}) = N(\mathrm{B})$ より $kp + lq = mp + nq$ である．つまり

$$p(k-m) = q(n-l)$$

であるが，p と q が互いに素なので $k-m$ が q の倍数でなければならない．ところが $0 \leqq k,\ m < q-1$ なので

$$-(q-1) < k-m < q-1$$

である．この範囲で q の倍数は 0 しかない．つまり $k = m$.

その結果 $l = n$ となり，$\mathrm{A} = \mathrm{B}$ であることが示された．

(2) $\mathrm{A}^{\#} = \mathrm{A}$ とする．つまり

$$q-2-m = m,\ p-2-n = n$$

これから

$$q = 2m+2,\ p = 2n+2$$

となり，p と q は公約数 2 をもち互いに素であることに反する．ゆえに $\mathrm{A}^{\#} \neq \mathrm{A}$ である．

(3) 条件 $N(\mathrm{A}) \leqq pq-(p+q)$ は

$$mp + nq \leqq pq-(p+q)$$

である．他方，条件 $N(\mathrm{A}^{\#}) \geqq pq-(p+q)$ は

$$(q-2-m)p + (p-2-n)q \geqq pq-(p+q)$$

である．ここで

$$\begin{aligned} & (q-2-m)p + (p-2-n)q \geqq pq-(p+q) \\ \Longleftrightarrow\quad & pq-mp-nq-p-q \geqq 0 \\ \Longleftrightarrow\quad & pq-(p+q) \geqq mp+nq \end{aligned}$$

ゆえに 2 つの条件が同値であることが示され，題意が示された．

(4) (3) から $N(\mathrm{A}) = pq-(p+q)$ なら $N(\mathrm{A}^{\#}) = pq-(p+q)$ となる．つまり等号が成立すると $N(\mathrm{A}) = N(\mathrm{A}^{\#})$ である．(1) から $\mathrm{A} = \mathrm{A}^{\#}$ となるが，これは (2) の結果と矛盾する．ゆえに $N(\mathrm{A}) \leqq pq-(p+q)$ で等号は成立しない．

$\mathrm{A}(m,\ n)$ のとき

$$(\mathrm{A}^{\#})^{\#} = (q-2-(q-2-m),\ p-2-(p-2-n)) = (m,\ n) = \mathrm{A}$$

なので，L の元 A と $\mathrm{A}^{\#}$ は 1:1 に対応する．(4) から $N(\mathrm{A}) \leqq pq-(p+q)$ となる L の元 A の個数は L の半分である．

L は明らかに $(p-1)(q-1)$ 個からなるので，求める元の個数は

$$\frac{(p-1)(q-1)}{2}$$

4 節演習問題解答

解答 13 (問題 13)

(1)

$$\begin{aligned}
f(k)=1 \text{ となる } k \text{ は } & \left[\frac{50}{2}\right]-\left[\frac{50}{2^2}\right] && = 25-12 \text{ 個}\\
f(k)=2 \text{ となる } k \text{ は } & \left[\frac{50}{2^2}\right]-\left[\frac{50}{2^3}\right] && = 12-6 \text{ 個}\\
f(k)=3 \text{ となる } k \text{ は } & \left[\frac{50}{2^3}\right]-\left[\frac{50}{2^4}\right] && = 6-3 \text{ 個}\\
f(k)=4 \text{ となる } k \text{ は } & \left[\frac{50}{2^4}\right]-\left[\frac{50}{2^5}\right] && = 3-1 \text{ 個}\\
f(k)=5 \text{ となる } k \text{ は } & \left[\frac{50}{2^5}\right] && = 1 \text{ 個}
\end{aligned}$$

ゆえに

$$S_{50}=1\cdot(25-12)+2\cdot(12-6)+3\cdot(6-3)+4\cdot(3-1)+5\cdot 1=47$$

(2) $n=2^l$ とする．(1) と同様に

$$\begin{aligned}
S_n &= 1\cdot\left(\left[\frac{2^l}{2}\right]-\left[\frac{2^l}{2^2}\right]\right)+2\cdot\left(\left[\frac{2^l}{2^2}\right]-\left[\frac{2^l}{2^3}\right]\right)+\cdots\\
&\qquad +(l-1)\cdot\left(\left[\frac{2^l}{2^{l-1}}\right]-\left[\frac{2^l}{2^l}\right]\right)+l\cdot\left[\frac{2^l}{2^l}\right]\\
&= 2^{l-1}+2^{l-2}+\cdots+1=\frac{2^l-1}{2-1}=n-1
\end{aligned}$$

(3) $2^l \leqq n < 2^{l+1}$ とする．

$$\begin{aligned}
S_n &= 1\cdot\left(\left[\frac{n}{2}\right]-\left[\frac{n}{2^2}\right]\right)+\cdots+(l-1)\cdot\left(\left[\frac{n}{2^{l-1}}\right]-\left[\frac{n}{2^l}\right]\right)+l\cdot\left[\frac{n}{2^l}\right]\\
&= \left[\frac{n}{2}\right]+\left[\frac{n}{2^2}\right]+\cdots+\left[\frac{n}{2^{l-1}}\right]+\left[\frac{n}{2^l}\right]\\
&\quad (\ [x]\leqq x \quad \text{より})\\
&\leqq \frac{n}{2}+\frac{n}{2^2}+\cdots+\frac{n}{2^l}\\
&= \frac{n}{2}\cdot\frac{1-\frac{1}{2^l}}{1-\frac{1}{2}}<\frac{n}{2}\cdot\frac{1}{1-\frac{1}{2}}=n
\end{aligned}$$

次に

$$\begin{aligned}
S_n &\geqq S_{2^l}=2^l-1\\
&\quad (\ 2^{l+1}\geqq n+1 \quad \text{なので})\\
&\geqq \frac{n+1}{2}-1=\frac{n-1}{2}
\end{aligned}$$

以上から

$$\frac{n-1}{2}\leqq S_n<n$$

解答 14 (問題 14)

(1) （イ）⇒（ロ）を示す.

$60 = 2^2 \cdot 3 \cdot 5$ であるから n が 60 の倍数なら

$$a_1 = 1,\ a_2 = 2,\ 3_3 = 3,\ a_4 = 4,\ a_5 = 5,\ a_6 = 6 \cdots$$

である.

$$\therefore \quad \frac{1}{a_3} + \frac{1}{a_6} = \frac{1}{3} + \frac{1}{6} = \frac{1}{2} = \frac{1}{a_2}$$

(2) （ロ）⇒（イ）を示す.

条件式から $a_2a_3 + a_2a_6 = a_3a_6$ である．これを変形すると,

$$(a_3 - a_2)(a_6 - a_2) = a_2^2$$

a_2 は必ず素数だから， $a_2 = p$ とおくと， $a_3 < a_6$ より

$$a_3 - a_2 = 1,\ a_6 - a_2 = p^2 \quad \therefore \quad a_3 = p + 1,\ a_6 = p^2 + p$$

a_3 としてあり得るのは

$$a_3 = p^2,\ \text{または,}\ p \text{と異なる素数}$$

$p^2 = p + 1$ は整数解がない．よって p と異なる素数.
p と $p + 1$ がともに素数になるのは $p = 2$ のみ．このとき,

$$a_2 = 2,\ a_3 = 3,\ a_6 = 6$$

なので， $a_4 = 4,\ a_5 = 5$ 以外にない．よって n は少なくとも 3, 4, 5 を因数にもつ．つまり 60 の倍数である.

解答 15 (問題 15)

(1) $81 = 3^4$ であるから，正の約数の和は

$$1 + 3 + 3^2 + 3^3 + 3^4 = \frac{3^5 - 1}{3 - 1} = 121$$

(2) $378 = 2 \times 3^3 \times 7$ であるから約数の個数は

$$2 \times 4 \times 2 = 16$$

それらの和は

$$(1 + 2)(1 + 3 + 3^2 + 3^3)(1 + 7) = 960$$

(3) N の素因数分解の素数 p の部分が p^n であるとする．このとき和には

$$1 + p + \cdots + p^n = \frac{p^{n+1} - 1}{p - 1} \cdots ①$$

が現れる．60 の約数は

$$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 10,\ 12,\ 15,\ 20,\ 30,\ 60$$

である．このなかで① の形をしているものを調べる.

(i) $3=1+2$ このとき $60=3\cdot 20$ とすると， $20=1+19$.

$$\therefore \quad N=2\cdot 19=38$$

(ii) $3=1+2$ このとき $60=3\cdot 4\cdot 5$ とすると，5 は① の形をしていない.

(iii) $4=1+3$ このとき $60=4\cdot 15$. $15=1+2+2^2+2^3$.

$$\therefore \quad N=3\cdot 2^3=24$$

(iv) $6=1+5$ このとき $60=6\cdot 10$. 10 は① の形をしていない.

(v) $12=1+11$ このとき $60=12\cdot 5$. 5 は① の形をしていない.

(vi) $30=1+29$ このとき $60=30\cdot 2$. 2 は① の形をしていない.

(vii) $60=1+59$

$$\therefore \quad N=60$$

題意を満たす N は 24, 38, 60 の 3 個ある．そのうち 2 と 3 でできているのは 24 .

解答 16 (問題 16)

(1)

$$b(p^2+q^2)=apq \quad \cdots ①$$

左辺は b の倍数． a と b が互いに素なので pq は b の倍数である.

(2) p と q の最大公約数を g とし，

$$p=gp',\ q=gq',\ (p'\text{と}\ q'\text{は互いに素})$$

とおく．このとき① は

$$bg^2(p'^2+q'^2)=ag^2p'q'$$

となる．つまり

$$b(p'^2+q'^2)=ap'q' \quad \cdots ②$$

(1) と同様に $p'q'$ が b の倍数になる．$p'q'=bk$ とおく．このとき ② から

$$p'^2+q'^2=ak$$

ここで $k\neq 1$ なら

$$\begin{aligned}
& p'^2+q'^2 \text{と}\ p'q' \text{が互いに素でない} \\
\iff\ & p'^2+q'^2+2p'q' \text{と}\ p'q' \text{が互いに素でない} \\
\iff\ & (p'+q')^2 \text{と}\ p'q' \text{が互いに素でない} \\
\iff\ & p'+q' \text{と}\ p'q' \text{が互いに素でない} \\
\iff\ & p' \text{か}\ q' \text{の少なくともいずれかと}\ p'+q' \text{が互いに素でない} \\
\iff\ & p' \text{と}\ q' \text{が互いに素でない}
\end{aligned}$$

ゆえに $k=1$ となり， $b=p'q'$ ， $a=p'^2+q'^2$ ．つまり

$$\sqrt{a+2b}=p'+q'$$

確かに自然数である.

解答 17 (問題 17)

(1) a が奇数のとき， b も奇数と仮定する．このとき c は偶数である．

$$a = 2k+1,\, b = 2l+1,\; c = 2m$$

とおく．

$$a^2 + b^2 = 4(k^2 + k + l^2 + l) + 2,\; c^2 = 4m^2$$

となり，4 で割った余りが異なる．つまり $a^2 + b^2 = c^2$ が成り立ち得ない．

ゆえに b は偶数であり，c は奇数である．

(2) $a^2 + b^2 = c^2$ より $b^2 = (c-a)(c+a)$ となるが (1) から $c-a,\; c+a$ はともに偶数である．

$$\left(\frac{b}{2}\right)^2 = \frac{c-a}{2} \cdot \frac{c+a}{2}$$

ここで $\dfrac{c+a}{2} > \dfrac{c-a}{2} \geqq 1$ なので，p を $\dfrac{b}{2}$ の素因数の一つとすると $p > 1$.

$\dfrac{c-a}{2}$ と $\dfrac{c+a}{2}$ がともに p を因数に持てば

$$\frac{c-a}{2} = kp,\; \frac{c+a}{2} = lp$$

とおくと

$$c = (k+l)p,\; a = (l-k)p$$

となり p が a と b の公約数となる． a と b は互いに素で，$p > 1$ であるから， p は $\dfrac{c-a}{2}$ と $\dfrac{c+a}{2}$ のいずれか一方のみの素因数となる．

$\left(\dfrac{b}{2}\right)^2$ の最高べき指数は偶数であるから $\dfrac{c-a}{2}$ と $\dfrac{c+a}{2}$ のいずれもが平方数となる．

つまり

$$\frac{a+c}{2} = d^2$$

となる自然数 d が存在する．

解答 18 (問題 18)

(1) b の約数を b_i $(i = 1,\; 2,\; \cdots,\; l)$ とする．2 と b は互いに素なので $a = 2^m b$ の約数のすべては,

$$2^j b_i \quad (j = 0,\; 1,\; \cdots,\; m,\; i = 1,\; 2,\; \cdots,\; l)$$

で与えられる．

$$\begin{aligned} \therefore \quad f(a) &= \sum_{j=0,\; i=1}^{j=m,\; i=l} 2^j b_i = \sum_{j=0}^{m} 2^j \left(\sum_{i=1}^{l} b_i\right) \\ &= \left(\sum_{j=0}^{m} 2^j\right) f(b) = \frac{2^{m+1}-1}{2-1} f(b) = (2^{m+1}-1) f(b) \end{aligned}$$

(2) p が 2 以上の整数なので $pq \neq q$ である．したがって q と pq は $a = pq$ の異なる約数である．

$$\therefore \quad f(a) \geqq (p+1)q$$

等号が成り立つのは，$a = pq$ の約数が q と a のみのときである．1 とその数自身は必ず約数になるので $q = 1$ で，かつ 1 とその数自身以外の約数がないので p は素数でなければならない．

(3) (1) から

$$\begin{cases} f(a) = (2^{m+1}-1)f(r) = 2b = 2^{n+1}s \\ f(b) = (2^{n+1}-1)f(s) = 2a = 2^{m+1}r \end{cases} \quad \cdots ①$$

ここで，$2^{m+1}-1$ と 2^{n+1} は互いに素なので， s は $2^{m+1}-1$ を約数にもつ．r についも同様.

$$s = (2^{m+1}-1)s', \quad r = (2^{n+1}-1)r'$$

とおける．このとき ① から

$$f(r) = 2^{n+1}s', \quad f(s) = 2^{m+1}r' \quad \cdots ②$$

一方 (2) から

$$f(r) \geqq \{(2^{n+1}-1)+1\}r' = 2^{n+1}r', \quad f(s) \geqq \{(2^{m+1}-1)+1\}s' = 2^{m+1}s' \quad \cdots ③$$

である.

$$2^{n+1}s' \geqq 2^{n+1}r' \quad \text{かつ} \quad 2^{m+1}r' \geqq 2^{m+1}s'$$

より $r' = s'$ で③ が等号になる.

(2) より $r' = s' = 1$ なので② から

$$r = 2^{n+1}-1, \quad s = 2^{m+1}-1$$

5 節演習問題解答

解答 19 (問題 19)

$$\begin{aligned} 3^{n+1} + 4^{2n-1} &= 9 \cdot 3^{n-1} + 4 \cdot 16^{n-1} \\ &= 9 \cdot 3^{n-1} + 4 \cdot (13+3)^{n-1} \\ &\equiv 9 \cdot 3^{n-1} + 4 \cdot 3^{n-1} \,(\text{mod. } 13) \\ &= 13 \cdot 3^{n-1} \equiv 0 \,(\text{mod. } 13) \end{aligned}$$

解答 20 (問題 20)

$$\begin{aligned} 19^n + (-1)^{n-1}2^{4n-3} &= 19^n + 2 \cdot (-16)^{n-1} \\ &= (14+5)^n + 2 \cdot (5-21)^{n-1} \\ &\equiv 5 \cdot 5^{n-1} + 2 \cdot 5^{n-1} \equiv 0 \,(\text{mod. } 7) \end{aligned}$$

解答 21 (問題 21)

(1) $\alpha = \dfrac{p}{q}$ とする．ここで $p,\ q$ は互いに素とする．

$$f\left(\frac{p}{q}\right) = \left(\frac{p}{q}\right)^n + a_1\left(\frac{p}{q}\right)^{n-1} + \cdots a_{n-1}\left(\frac{p}{q}\right) + a_n = 0$$

$$\therefore \quad p^n = -(a_1 p^{n-1}q + \cdots a_{n-1}pq^{n-1} + a_n q^n)$$

右辺は q の倍数で q は p と互いに素なので $q = 1$.

つまり α は整数である．

(2) 背理法でしめす.

方程式 $f(x) = 0$ が有理数の解をもてば (1) からそれは整数である．

α を k で割って

$$\alpha = q \cdot k + r$$

とおく． $0 \leqq r < k$ である．

$$0 = f(\alpha) = f(q \cdot k + r) \equiv f(r)\,(\mathrm{mod.}\ k)$$

ゆえに k 個の整数 $f(0),\ f(1),\ \cdots,\ f(k-1)$ のどれかが k で割り切れる．

さらに

$$f(k) \equiv f(0)\,(\mathrm{mod.}\ k)$$

であるから k 個の整数 $f(1),\ f(2),\ \cdots,\ f(k)$ のどれかが k で割り切れなければならない.

これは条件と矛盾するので，題意が示された．

解答 22 (問題 22) $n^9 - n^3 = n^2(n^7 - n)$ なので n が 3 の倍数なら明らかに 9 の倍数である．

3 の倍数でないときに示す．$n = 3k \pm 1$ とおく．

$$\begin{aligned}
n^9 - n^3 &= (3k \pm 1)^3\{(3k \pm 1)^6 - 1\} \\
&= (27k^3 \pm 27k^2 + 9k \pm 1)\{(3k \pm 1)^6 - 1\} \\
&\equiv (\pm 1)\{(3k \pm 1)^6 - 1\}\,(\mathrm{mod.}\ 9) \\
&= (\pm 1)\{(9k^2 \pm 6k + 1)^3 - 1\} \\
&\equiv (\pm 1)\{(36k^2 \pm 12k + 1)(\pm 6k + 1) - 1\}\,(\mathrm{mod.}\ 9) \\
&\equiv (\pm 1)\{(\pm 3k + 1)(\pm 6k + 1) - 1\}\,(\mathrm{mod.}\ 9) \\
&= (\pm 1)(18k^2 \pm 9k + 1 - 1) \equiv 0\,(\mathrm{mod.}\ 9)
\end{aligned}$$

ゆえに $n^9 - n^3$ は 9 で割り切れる．

解答 23 (問題 23) $x = 1 + 2y$ を奇数とする．$x^2 = 1 + 4y(y+1)$ で $y(y+1)$ は偶数だから，$x^2 \equiv 1\,(\mathrm{mod.}\ 8)$.

ゆえに $\alpha \equiv 1\,(\mathrm{mod.}\ 8)$ は問題の合同式が解をもつための必要条件である．

このとき題意を e に関する数学的帰納法で示す.

$e = 3$ のとき.

解は

$$x \equiv 1,\ 3,\ 5,\ 7\,(\mathrm{mod.}\ 8)$$

である．これは確かに

$$x \equiv \pm 1,\ \pm 1 + 2^2\,(\mathrm{mod.}\ 8)$$

となっており，解の存在とその形に関して題意が成立している．

e のときの成立を仮定して $e+1$ のときの成立を示す．

つまり

$$x^2 \equiv \alpha\,(\mathrm{mod.}\ 2^{e+1}) \tag{44}$$

の解は四つあり，それは

$$\pm x_0,\ \pm x_0 + 2^e$$

であることを示す．

さて，e のときの解 x_0 を用いれば $e+1$ のときの解は

$$\pm\, x_0 + 2^e y \quad \text{または} \quad (\pm x_0 + 2^{e-1}) + 2^e y\,(\mathrm{mod.}\ 2^{e+1}) \tag{45}$$

の形をしていなければならない．そして (45) は (44) をみたすので

$$(\pm x_0 + 2^e y)^2 \equiv \alpha\,(\mathrm{mod.}\ 2^{e+1}) \tag{46}$$

$$\text{または} \quad \{(\pm x_0 + 2^{e-1}) + 2^e y\}^2 \equiv \alpha\,(\mathrm{mod.}\ 2^{e+1}) \tag{47}$$

である．

仮定から整数 t を用いて $x_0^2 = \alpha + 2^e t$ と表せる．(46) のとき．

$$2^e t \equiv 0\,(\mathrm{mod.}\ 2^{e+1})$$

したがって t が奇数なら不可能で，t が偶数なら y は任意である．$(\,\mathrm{mod}\,.\,2^{e+1})$ に関しては $y = 0,\ 1$ をとればよいので，

$$\pm x_0 \quad \text{および} \quad \pm\, x_0 + 2^e y$$

が解である．

つまり $(\mathrm{mod.}\ 2^e)$ に関する解 $\pm x_0$ から $(\mathrm{mod.}\ 2^{e+1})$ に関する解が得られないか，または四つ得られる．

次に (47) のとき． x_0 は奇数で $2n - 2 \geqq n + 1$ であるから

$$\begin{aligned}(\pm x_0 + 2^{e-1})^2 &\equiv x_0^2 \pm 2^e x_0 + 2^{2e-2} \\ &\equiv x_0^2 + 2^e\,(\mathrm{mod.}\ 2^{e+1})\end{aligned}$$

$$2^e t + 2^e \equiv 0\,(\mathrm{mod.}\ 2^{e+1})$$

これは t が偶数なら不可能で奇数なら y は任意である．ゆえに $(\mathrm{mod.}\ 2^{e+1})$ に関して

$$\pm(x_0 + 2^{e-1}) \quad \text{および} \quad \pm\,(x_0 + 2^{e-1}) + 2^e$$

が解である．

以上によって，数学的帰納法により題意が示された．

7 節演習問題解答

解答 24 (問題 24)

(1)

$$\begin{aligned} & \alpha^n = \alpha^m \\ \iff \quad & \frac{n\pi}{3} = \frac{m\pi}{3} + 2k\pi, \text{ となる整 } k \text{ が存在する} \\ \iff \quad & n \equiv m \,(\mathrm{mod.}\ 6) \end{aligned}$$

である．ゆえに 6 個.

(2) n が 6 と互いに素なら $1 \leqq i,\ j \leqq 5$ に対して

$$ni \equiv nj \,(\mathrm{mod.}\ 6) \iff i \equiv j \,(\mathrm{mod.}\ 6)$$

である．ゆえに

$$\{\alpha^n,\ \alpha^{2n},\ \alpha^{3n},\ \alpha^{4n},\ \alpha^{5n}\} = \{\alpha,\ \alpha^2,\ \alpha^3,\ \alpha^4,\ \alpha^5\}$$

となる．

一方 $n \equiv 2,\ 4\,(\mathrm{mod.}\ 6)$ のときは $\alpha^{3n} = 1$ ，$n \equiv 3\,(\mathrm{mod.}\ 6)$ のときは $\alpha^{2n} = 1$ である．

$$\therefore \quad \text{与式} = \begin{cases} 1 & n \equiv 1,\ 5(\mathrm{mod.}\ 6) \text{ のとき} \\ 0 & n \equiv 0,\ 2,\ 3,\ 4(\mathrm{mod.}\ 6) \text{ のとき} \end{cases}$$

解答 25 (問題 25)

(1) $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ は明らかに方程式 $x^n - 1 = 0$ の解である．すべて偏角が異なるので，異なる．

一方，方程式 $x^n - 1 = 0$ は n 次なので解は n 個である．

ゆえに $1, \alpha, \alpha^2, \cdots, \alpha^{n-1}$ が方程式 $x^n - 1 = 0$ の相異なる n 個の解である．

(2)

$$x^n - 1 = (x-1)(x-\alpha)(x-\alpha^2)\cdots(x-\alpha^{n-1})$$

(3) $x = -1$ を代入して

$$\begin{aligned} (-1)^n - 1 &= (-1-1)(-1-\alpha)(-1-\alpha^2)\cdots(-1-\alpha^{n-1}) \\ &= (-1)^n \cdot 2 \cdot (1+\alpha)(1+\alpha^2)\cdots(1+\alpha^{n-1}) \end{aligned}$$

$$\therefore \quad (1+\alpha)(1+\alpha^2)\cdots(1+\alpha^{n-1}) = \begin{cases} 0 & (n \text{ 偶数}) \\ 1 & (n \text{ 奇数}) \end{cases}$$

(4) m が n が互いに素な正の整数なので $1 \leqq i,\ j \leqq n-1$ に対して

$$mi \equiv mj \,(\mathrm{mod.}\ n) \iff i \equiv j \,(\mathrm{mod.}\ n)$$

である．ゆえに

$$\{\alpha^m,\ \alpha^{2m},\ \cdots,\ \alpha^{(n-1)m}\} = \{\alpha,\ \alpha^2,\ \cdots,\ \alpha^{n-1}\}$$

$$\therefore \quad (1+\alpha^m)(1+\alpha^{2m})\cdots(1+\alpha^{(n-1)m}) = \begin{cases} 0 & (n \text{ 偶数}) \\ 1 & (n \text{ 奇数}) \end{cases}$$

解答 26 (問題 26)

(1) 条件 (イ) より z_k は 1 と異なる 1 の p 乗根である.

$$\alpha = \cos\frac{2\pi}{p} + i\sin\frac{2\pi}{p}$$

とおくと, 1 と異なる 1 の p 乗根は

$$z_k = \alpha^{x_k},\ x_k \text{ は } 1 \leqq x_k \leqq p-1 \text{ の範囲の整数}$$

一意に表される.

このとき条件 (ロ) は

$$x_1 + x_2 + \cdots + x_n = (p \text{ の倍数}) \quad \cdots ①$$

となる.

a_n は ① の解

$$(x_1,\ x_2,\ \cdots,\ x_n)\ ,\ 1 \leqq x_1,\ x_2,\ \cdots,\ x_n \leqq p-1$$

の個数を表す.

$$x_n = (p \text{ の倍数}) - (x_1 + x_2 + \cdots + x_{n-1})$$

であるから, $(x_1,\ x_2,\ \cdots,\ x_{n-1})$ を $(x_1 + x_2 + \cdots + x_{n-1})$ が p の倍数でないようにさえ選べば, 一組の解が得られる.

$$\therefore \quad a_n = (p-1)^{n-1} - a_{n-1}\ (n \geqq 3)$$

ここで a_2 を求める. a_2 は $x_1 + x_2$ が p の倍数となる

$$(x_1,\ x_2) = (1,\ p-1),\ (2,\ p-2),\ \cdots,\ (p-1,\ 1)$$

$p-1$ 個である.

$$a_2 = (p-1)$$

$$\therefore \quad a_3 = (p-1)^2 - (p-1) = (p-1)(p-2)$$

(2) (1) から

$$a_{n+2} = (p-1)^{n+1} - a_{n+1}$$

(3)

$$a_{n+1} = (p-1)^n - a_n$$

を解く. $p-1 \neq 0$ なので

$$\frac{a_{n+1}}{(p-1)^{n+1}} = -\frac{1}{p-1}\cdot\frac{a_n}{(p-1)^n} + \frac{1}{p-1}$$

$$\iff \quad \frac{a_{n+1}}{(p-1)^{n+1}} - \frac{1}{p} = -\frac{1}{p-1}\left\{\frac{a_n}{(p-1)^n} + \frac{1}{p}\right\}$$

$$\therefore \quad \frac{a_n}{(p-1)^n} + \frac{1}{p} = \left(-\frac{1}{p-1}\right)^{n-2}\left\{\frac{a_2}{(p-1)^2} + \frac{1}{p}\right\}$$

これから

$$a_n = \frac{p-1}{p}\{(p-1)^{n-1} - (-1)^{n-1}\}$$

［漸化式の別解］

$$x_1 + x_2 + \cdots + x_n + x_{n+1} + x_{n+2} = (p \text{ の倍数})$$

の解を二つに分類する．

(1) $x_{n+1} + x_{n+2}$ が p の倍数のとき．この $(x_{n+1},\ x_{n+2})$ は $a_2 = p - 1$ 個あり，その各に対し結局

$$x_1 + x_2 + \cdots + x_n = (p \text{ の倍数}) - (x_{n+1} + x_{n+2}) = (p \text{ の倍数})$$

となる．この場合の個数は

$$(p-1)a_n$$

(2) $x_{n+1} + x_{n+2}$ が p の倍数でないとき． $y_{n+1} = x_{n+1} + x_{n+2}$ とおくと

$$x_1 + x_2 + \cdots + x_n + y_{n+1} = (p \text{ の倍数})$$

の解は a_{n+1} 個あり．各 y_{n+1} に対して $y_{n+1} = x_{n+1} + x_{n+2} + (p \text{ の倍数})$ となる $(x_{n+1},\ x_{n+2})$ は $p - 1$ 組ある．

なぜなら x_{n+1} は y_{n+1} と同じにはとれない (同じにとると x_{n+2} がとれない) が，逆に異なれば $y_{n+1} - x_{n+1}$ と p で割ったの余りが等しい x_{n+2} が一つ定まる．

この場合の個数は

$$(p-2)a_{n+1}$$

$$\therefore \quad a_{n+2} = (p-2)a_{n+1} + (p-1)a_n$$

解答 27 (問題 27)

(1) $\alpha = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$ とおく．

$$G = \{1,\ \alpha,\ \alpha^2,\ \cdots,\ \alpha^{n-1}\}$$

とする．この要素はすべて異なり n 次方程式 $x^n - 1 = 0$ の n 個の解の全体である．

G の任意の 2 つの要素 $\alpha^i,\ \alpha^j$ $(0 \leqq i,\ j \leqq n-1)$ に対して α^{i+j} も明らかに $x^n - 1 = 0$ の解なので，再び G の要素である．

よって G は題意を満たすちょうど n 個の複素数からなる集合である．

(2) G の要素 z に対し，そのべき $z,\ z^2,\ z^3,\ \cdots$ もすべて G の要素である．$z \in G$ とし $z = r(\cos\theta + i\sin\theta)$ とする．

$$z,\ z^2,\ z^3,\ \cdots$$

が有限集合なので，すべてが異なることはありえない．ゆえに

$$z^i = z^j \ (i < j)$$

となる $i,\ j$ がある．両辺の絶対値をとり

$$r^i = r^j \quad \therefore \quad r = 1$$

かつ

$$z^{j-i}=1$$

したがって G の要素はすべて 1 のべき根である.

$z\in G$ で $z^m=1$ なら $z^{-1}=z^{m-1}$ なので $z^{-1}\in G$ である. つまり

$z,\ w\in G$ なら $z^{-1}w\in G$ である.

G の要素 z の偏角 $\arg z$ は $0\leqq\arg z<2\pi$ でとるとする.

G の要素で偏角が正で最小であるものを α とする.

G の任意の要素 z をとる.

$$m\arg\alpha\leqq\arg z<(m+1)\arg\alpha$$

となる正整数 m がある.

このとき $z\alpha^{-m}\in G$ であるが

$$0\leqq\arg(z\alpha^{-m})<\arg\alpha$$

となる.

もし $0\neq\arg(z\alpha^{-m})$ なら偏角が正で $\arg\alpha$ の偏角より小さい要素 $z\alpha^{-m}$ が存在し, G の要素で偏角が正で最小であるものを α としたことと矛盾する.

ゆえに $0=\arg(z\alpha^{-m})$. つまり $z=\alpha^m$

ゆえに G の要素はすべて α のべきである. α のべきで初めて 1 になるものを $\alpha^m(=1)$ とすれば

$$G=\{\alpha,\ \alpha^2,\ \cdots,\ \alpha^{m-1},\ \alpha^m\}$$

となる. ゆえに $m=n$ で G は (1) で作った例と一致した.

8 節演習問題解答

解答 28 (問題 28)

(1) $n=1$ のとき. $f(x)=ax+b$ (a と p は互いに素) とおく.

$0\leqq i<j\leqq p-1$ の二つの整数 $i,\ j$ に対し

$$f(i)\equiv f(j)\pmod{p}$$

とする. $f(i)-f(j)=a(i-j)\equiv o\pmod{p}$ で $(a,\ p)=1$ なので $i\equiv j\pmod{m\ p}$.
$0<j-i<p-1$ よりこれはあり得ない.

ゆえに $\{f(0),\ f(1),\ \cdots,\ f(p-1)\}$ は p を法とする剰余系である.

$$\therefore\quad f(x)\equiv 0\pmod{p}\text{ となる }x\ (0\leqq x\leqq p-1)\text{ はただ一つである.}$$

$n=k$ のとき (1) の命題が成立しているとする.

$n=k+1$ のときの成立を背理法で示す.

$$0 \leqq i_1 < i_2 < \cdots < i_{k+2} \leqq p-1$$

で

$$f(i_u) \equiv 0 \pmod{p}\ u = 1,\ 2,\ \cdots,\ k+2$$

となったとする.

このとき $f(x) - f(i_1)$ は $x - i_1$ を因数にもつので

$$f(x) - f(i_1) = (x - i_1)g(x)$$

とおく. $f(x) = ax^n + \cdots$ なら

$$f(x) - f(i_1) = a(x^n - i_1^n) + \cdots = (x - i_1)(ax^{n-1} + \cdots)$$

となるので $g(x)$ は最高次の係数が p の倍数でない $n - 1 = k$ 次式である.

$$f(i_u) - f(i_1) = (i_u - i_1)g(i_u) \equiv 0 \pmod{p}\ u = 2,\ 3,\ \cdots k+1$$

であるが $(i_u - i_1,\ p) = 1$ なので

$$g(i_u) \equiv 0 \pmod{p}\ u = 2,\ 3,\ \cdots k+1$$

である. これは $n = k$ で (1) の命題が成立しているとの帰納法の仮定と矛盾する.

したがって対偶が示され, $n = k + 1$ 次の場合も

$$f(0),\ f(1),\ \cdots,\ f(p-1)$$

のうちで, p の倍数となるものは, $k + 1$ 個以下である.

ゆえに n に関する数学的帰納法により (1) の命題が成立する.

(2) $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots$ とおき, その係数に p の倍数ではないものがあるとする. (1) から $a_n \equiv 0 \pmod{p}$ である. n 次の方から順に見て最初に p の倍数でない係数を a_m とする.

$$f(x) = a_n x^n + \cdots + a_{m+1}x^{m+1} + g(x) \quad g(x) = a_m x^m + \cdots$$

とおく. 任意の整数 l に対して $f(l) \equiv g(l) \pmod{p}$ なので

$$g(0),\ g(1),\ \cdots,\ g(p-1)$$

のうちに, p の倍数となるものが $n+1$ 個以上ある. したがって (1) から $a_m \equiv 0 \pmod{p}$ でなければならず, a_m が n 次の方から順に見て最初に p の倍数でない係数であることと矛盾した.

したがって $f(x)$ の係数に p の倍数ではないものはない. つまり (2) が示された.

(3) $f(x) = (x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1$ は明らかに $p - 2$ 次式である. ところが $i = 1,\ 2,\ \cdots,\ p-1$ に対してフェルマの小定理より

$$f(i) = -i^{p-1} + 1 \equiv 0 \pmod{p}$$

である．(2) から $f(x)$ のすべての係数は p の倍数である． p が奇素数なら

$$f(0) = (-1)\cdots(-1+p)+1 = (p-1)!+1$$

より $(p-1)!+1$ が p の倍数． $p=2$ のときも $(p-1)!+1=2$ より成立．

(4) p が素数なら (3) から $(p-1)!+1$ は p の倍数．ところが

$$(p-1)!+1 = (p-1)!+1-p+1 = (p-1)\{(p-2)!-1\}+p$$

で $(p-1,\ p)=1$ より $(p-2)!-1$ は p の倍数．

p が素数でなければ $p=uv$ $0<u,\ v<p-1$ と因数分解される．

$(p-2)!$ は u の倍数になる．したがって $(p-2)!-1$ は u の倍数ではなく p の倍数でもない．

$$\therefore \quad p\text{が素数} \quad \Longleftrightarrow \quad (p-2)!-1 \text{が} p \text{の倍数}$$

注意 18.2　例 (3)(4) については『めざせ，数学オリンピック』(J. コフマン，現代数学社) にいくつかの計算例が載っている．

それを紹介する．

20 以下の素数 p について $(p-1)!+1$ を計算する．

$$\begin{aligned}
(2-1)!+1 &= 2\\
(3-1)!+1 &= 3\\
(5-1)!+1 &= 25 = 5^2\\
(7-1)!+1 &= 721 = 7\cdot 103\\
(11-1)!+1 &= 3628801 = 11\cdot 329891\\
(13-1)!+1 &= 479001601 = 13\cdot 2834329\\
(17-1)!+1 &= 20922789888001 = 17\cdot 61\cdot 137\cdot 139\cdot 1059511\\
(19-1)!+1 &= 6402373705728001 = 19\cdot 23\cdot 29\cdot 61\cdot 67\cdot 123610951
\end{aligned}$$

20 以下の p について $(p-2)!-1$ を計算する．

$$\begin{aligned}
(3-2)!-1 &= 0\\
(4-2)!-1 &= 1\\
(5-2)!-1 &= 5\\
(6-2)!-1 &= 23\\
(7-2)!-1 &= 119 = 7\cdot 17\\
(8-2)!-1 &= 719\\
(9-2)!-1 &= 5039\\
(10-2)!-1 &= 40319 = 23\cdot 1753\\
(11-2)!-1 &= 362879 = 11^2\cdot 2999\\
(12-2)!-1 &= 3628799 = 29\cdot 125131\\
(13-2)!-1 &= 39916799 = 13\cdot 17\cdot 23\cdot 7853
\end{aligned}$$

$$
\begin{aligned}
(14-2)!-1 &= 479001599\\
(15-2)!-1 &= 6227020799 = 1733\cdot 3593203\\
(16-2)!-1 &= 87178291199\\
(17-2)!-1 &= 1307674367999 = 17\cdot 31^2\cdot 53\cdot 1510259\\
(18-2)!-1 &= 20922789887999 = 3041\cdot 6880233439\\
(19-2)!-1 &= 355687428095999 = 19\cdot 73\cdot 256443711677\\
(20-2)!-1 &= 6402373705727999 = 59\cdot 226663\cdot 478749547
\end{aligned}
$$

9 節演習問題解答

解答 29 (問題 29)

(1) 自然数 m, n を 7 で割った商をそれぞれ m', n', 余りをそれぞれ i, j とおくと, $m=7m'+i$, $n=7n'+j$ と書けて

$$mn=(7m'+i)(7n'+j)=7(7m'n'+m'j+n'i)+ij$$

より, $f(mn)=f(ij)$ を得る. そこで, これを用いて, 自然数 n を 7 で割った余りで分類し, n^2, n^3, $\cdots$, n^7 を 7 で割った余りを順に求めていくと, 下表のようになる.

n	0	1	2	3	4	5	6
n^2	0	1	4	2	2	4	1
n^3	0	1	1	6	1	6	6
n^4	0	1	2	4	4	2	1
n^5	0	1	4	5	2	3	6
n^6	0	1	1	1	1	1	1
n^7	0	1	2	3	4	5	6

よって, すべての自然数 n に対して

$$f(n^7)=f(n)$$

［注意］これは言うまでもなく「フェルマの小定理」そのものである. 文系入試問題であるので, 実際に 7 で割った余りの表を作ることで論証した.

ほかに, n^7-n が 7 の倍数になることを, n に関する数学的帰納法で示すことができる. これについては 8 節練習問題 1 を参照のこと.

(2) (1) の結果より, すべての自然数 k に対して, k^7-k は 7 の倍数であるから

$$\sum_{k=1}^{7}k^{n+6}-\sum_{k=1}^{7}k^n=\sum_{k=1}^{7}k^{n-1}(k^7-k)=7l \quad (l \text{ は自然数})$$

$$\therefore\quad g(n+6)=g(n)$$

よって, $1 \leqq n \leqq 6$ の範囲で考えれば十分である. ここで, (1) の表を利用すると

$$g(1) = 3f(1+2+3+4+5+6+0) = 3f(21) = 0$$
$$g(2) = 3f(1+4+2+2+4+1+0) = 3f(14) = 0$$
$$g(3) = 3f(1+1+6+1+6+6+0) = 3f(21) = 0$$
$$g(4) = 3f(1+2+4+4+2+1+0) = 3f(14) = 0$$
$$g(5) = 3f(1+4+5+2+3+6+0) = 3f(21) = 0$$
$$g(6) = 3f(1+1+1+1+1+1+0) = 3f(6) = 18$$

となるから, $n = 6$ をとれば

$$g(6) = 18$$

■

10 節演習問題解答

解答 30 (問題 30)

(1) $x \leqq y \leqq z$ として良い. (2) で示されるように n が 8 で割ったときの余りが 7 なら $x^2+y^2+z^2 = n$ を満たす整数の組 $(x,\ y,\ z)$ は存在しないので, 他にあるか注意して表を作る.

x	y	z	n	x	y	z	n	x	y	z	n	x	y	z	n
(0	0	0	0)	0	2	2	8	0	0	4	16	2	2	4	24
0	0	1	1	0	0	3	9	0	1	4	17	0	3	4	25
0	1	1	2	0	1	3	10	0	3	3	18	1	3	4	26
1	1	1	3	1	1	3	11	1	3	3	19	3	3	3	27
0	0	2	4	2	2	2	12	0	2	4	20	−	−	−	28
0	1	2	5	0	2	3	13	1	2	4	21	2	3	4	29
1	1	2	6	1	2	3	14	2	3	3	22	1	2	5	30
−	−	−	7	−	−	−	15	−	−	−	23	−	−	−	31

$3^2+3^2+3^2 = 27$ なので 28 を作るためには 4 以上が入らねばならない. ところが $1^2+3^2+4^2 = 26$, $2^2+3^2+4^2 = 29$ なので, 4 までででは出来ない. 一方, $1^2+1^2+5^2 = 27$, $1^2+2^2+5^2 = 30$ なので, 5 を入れても不可能.

ゆえに 28 は表せない. $x^2+y^2+z^2 = n$ を満たす整数の組 $(x,\ y,\ z)$ が存在しないような正の整数 n は小さいものから順に

$$7,\ 15,\ 23,\ 28,\ 31$$

(2)

$$3^2 \equiv 1,\ 4^2 \equiv 0,\ 5^2 \equiv 1,\ 6^2 \equiv 4,\ 7^2 \equiv 1 \pmod 8$$

従って整数 x に対して x^2 を 8 で割った余りは $0,\ 1,\ 4$ のみ.

$x^2+y^2+z^2$ が 8 で割って 7 余るのは $x^2,\ y^2,\ z^2$ 中に奇数か奇数個なければならない. その組合せは

$$(0,\ 0,\ 1),\ (1,\ 1,\ 1),\ (0,\ 1,\ 4),\ (1,\ 4,\ 4)$$

だが，これらに対する $x^2+y^2+z^2$ はおのおの 8 を法として 1, 3, 1, となって 7 が現れない．

したがって「正の整数 n を 8 で割ったときの余りが 7 ならば，$x^2+y^2+z^2=n$ を満たす整数の組 $(x,\ y,\ z)$ が存在しない」というのは，つねに正しい．

11 節演習問題解答

解答 31 (問題 31)　z が偶数なら $x^2+y^2=z^2$ の右辺は 4 の倍数．左辺が 4 の倍数になるのは $x,\ y$ とも偶数のときにかぎる．$(x,\ y)=1$ よりこれはあり得ない．ゆえに z は奇数．

また $x+iy$ と $x-iy$ に単数以外の公約数があれば，それを α とするとその共役も公約数になり，公約数として実数 a がとれ $x+iy=a(p+qi)$ と $x-iy=a(p-qi)$ となる．ゆえに $x=ap,\ y=aq$ となって $(x,\ y)=1$ に反する．ゆえに, $x+iy$ と $x-iy$ は互いに素である．

$z^2=x^2+y^2=(x+iy)(x-iy)$ となるので単数倍を除けば $x+iy$ と $x-iy$ 自体がガウス整数の平方である．つまり

$$x+iy=\epsilon(m+in)^2\ ,\quad x-iy=\bar{\epsilon}(m-in)^2$$

とおける．ただし ϵ は単数である．

$(x,\ y)=1$ より $(m,\ n)=1$ で，さらに $x+iy$ と $x-iy$ はともに 2 の因数 $\pm1\pm i$ で割れないので，$m+in$ と $m-in$ も $\pm1\pm i$ で割れない．つまり m と n の一方が偶数で他方が奇数である．

このとき

$$x+iy=\epsilon(m^2-n^2+2imn)\ ,\ z=m^2+n^2$$

となり，題意が示された．

解答 32 (問題 32)　$p=2$ のとき．

$$(a+bi)^p=a^2-b^2+2abi$$

で, $a>0,\ b>0$ よりこれは実数とはなり得ない．

$p\geqq 3$ とする．二項定理より

$$\begin{aligned}(a+bi)^p &= \sum_{k=0}^{p}{}_p\mathrm{C}_k a^{p-k}(ib)^k \\ &= \sum_{m=0}^{\frac{p-1}{2}}(-1)^m{}_p\mathrm{C}_{2m}a^{p-2m}b^{2m}+i\left(\sum_{m=0}^{\frac{p-1}{2}}(-1)^m{}_p\mathrm{C}_{2m+1}a^{p-2m-1}b^{2m+1}\right)\end{aligned}$$

$(a+bi)^p$ が実数とすると

$$\sum_{m=0}^{\frac{p-1}{2}}(-1)^m{}_p\mathrm{C}_{2m+1}a^{p-2m-1}b^{2m+1}=0$$

である．ところが

$$\sum_{m=0}^{\frac{p-1}{2}}(-1)^m{}_p\mathrm{C}_{2m+1}a^{p-2m-1}b^{2m+1}$$

$$= pa^{p-1}b + \sum_{m=1}^{\frac{p-3}{2}} (-1)^m {}_p\mathrm{C}_{2m+1} a^{p-2m-1} b^{2m+1} + (-1)^{\frac{p-1}{2}} b^p$$

$$= pa^{p-1}b + ab^2 \left(\sum_{m=1}^{\frac{p-3}{2}} (-1)^m {}_p\mathrm{C}_{2m+1} a^{p-2m-2} b^{2m-1} \right) + (-1)^{\frac{p-1}{2}} b^p$$

ただし $p = 3$ のとき中央の項は 0 とする.

一般に $1 \leqq k \leqq p-1$ に対して

$${}_p\mathrm{C}_k = \frac{p!}{k!(p-k)!}$$

であるが, p が素数なので $k!(p-k)!$ は p と互いに素である. しかも右辺は整数なので

$$\frac{(p-1)!}{k!(p-k)!}$$

が整数. つまり ${}_p\mathrm{C}_k$ は p の倍数である. したがってある整数 N が存在して

$$pa^{p-1}b + ab^2 \cdot pN + (-1)^{\frac{p-1}{2}} b^p = 0$$

$$pa^{p-1} + ab \cdot pN + (-1)^{\frac{p-1}{2}} b^{p-1} = 0$$

となる. これからまず b が p の倍数である. そこで $b = pl$ とおく.

$$pa^{p-1} + apl \cdot pN + (-1)^{\frac{p-1}{2}} (pl)^{p-1} = 0$$

つまり

$$a^{p-1} + al \cdot pN + (-1)^{\frac{p-1}{2}} p^{p-2} l^{p-1} = 0$$

となる. これから a も p の倍数である.

a も b も p の倍数となり, a , b が互いに素であることと矛盾した.

以上から $(a+bi)^p$ は実数ではあり得ないことが示された.

解答 33 (問題 33)

(1)

$$(a+2c)^2 + 4c(b-a-c) = a^2 + 4bc$$

$(a,\ b,\ c)$ は等式 (Q) を満たすので $a^2 + 4bc = p$ である. ゆえに $(a+2c,\ c,\ b-a-c)$ もまた等式 (Q) を満たす.

(2) $a = b - c$ とする.

$$p = a^2 + 4bc = (b-c)^2 + 4bc = (b+c)^2$$

$b + c$ が自然数なので, p が素数であることに反する.

$a = 2b$ とする.

$$p = a^2 + 4bc = (2b)^2 + 4bc = 4b(b+c)$$

$b,\ b + c$ が自然数なので, p が素数であることに反する.

ゆえに, $a = b - c$ や $a = 2b$ を満たすことはない.

(3) 手続きのうち，(i) と (iii) は，必ず変化する．変化しないときは手続き (ii) で

$$2b-a=a,\ a-b+c=c$$

となるときにかぎる．これから $a=b$ ．このとき

$$p=a(a+4c)$$

p は素数，かつ $a+4c>1$ なので $a=1$ ．

このとき

$$p=1+4c=4k+1$$

から $c=k$

したがって題意をみたすものは $(a,\ b,\ c)=(1,\ 1,\ k)$ であり，これ以外には存在しない．

(4) 等式 (Q) を満たす自然数の組 $(a,\ b,\ c)$ に対して上の手続きを 1 回行ったものを $(a',\ b',\ c')$，2 回行ったものを $(a'',\ b'',\ c'')$ と記す．これらは等式 (Q) を満たす．

(i) $a<b-c$ ならば $a'=a+2c,\ b'=c,\ c'=b-a-c$．このときは $a'>2b'$ なので

$$a''=a'-2b'=(a+2c)-2c=a,\ b''=a'-b'+c'=b,\ c''=b'=c$$

(ii) $b-c<a<2b$ ならば $a'=2b-a,\ b'=b,\ c'=a-b+c$．このときは $b'-c'=2b-a-c$ なので $b'-c'<a'<2b'$ となる．ゆえに

$$a''=2b'-a'=2b-(2b-a)=a,\ b''=b'=b,\ c''=a'-b'+c'=c$$

(iii) $a>2b$ ならば $a'=a-2b,\ b'=a-b+c,\ c'=b$．このときは $a'<b'-c'$ なので

$$a''=a'+2c'=a,\ b''=c'=b,\ c''=b'-a'-c'=(a-b+c)-(a-2b)-b=c$$

したがって 2 回の操作で元の組に戻る．

したがって組の各要素はたがいにこの操作で入れ替わるものの組に分けることができる．

この操作で変わらないものはただ一つなので，その他は 2 つずつの組になる．

したがって等式 (Q) を満たす自然数 3 つの組の全体の個数は奇数である．

(5) 等式 (Q) は b と c に関して対称である．したがって組 $(a,\ b,\ c)$ が等式 (Q) を満たせば，組 $(a,\ c,\ b)$ も満たす．

(3) から等式 (Q) を満たす自然数 3 つの組は少なくとも一組は存在し，(4) からそのような組の全体の個数は奇数である．

もしすべての組が $b\neq c$ なら，2 つずつが組になってそのような組の全体の個数は偶数になる．

したがって，そのような組のなかには $b=c$ となるものが存在する．このとき

$$p=a^2+(2b)^2$$

と表される．

注意 18.3 この問題は定理 40 の別証明になっている．

出典：

D. Zagier,

A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares,

Amer. Math. Monthly 97 (1990) 144.

またこれは次の書でも紹介されている．

『数論の３つの真珠』（ヒンチン著、蟹江訳、日本評論社）p.128

12 節演習問題解答

解答 34 (問題 34)

(1)

$$\begin{aligned} & (xz+nyt)^2 - n(xt+yz)^2 \\ = \; & x^2z^2 + 2nxzyt + n^2y^2t^2 - n(x^2t^2 + 2xtyz + y^2z^2) \\ = \; & x^2(z^2-nt^2) - ny^2(z^2-nt^2) = (x^2-ny^2)(z^2-nt^2) \end{aligned}$$

(2) $x^2 - 2y^2 = -1$ の自然数解 (x, y) の集合を A とする．一組の解 $(1,\ 1)$ が存在するので A は空集合ではない．

A が有限集合であったとすると，x が最大のものが存在する．それを $(x_0,\ y_0)$ とする．

(1) で $z = t = 1,\ n = 2$ とすると

$$(x_0+2y_0)^2 - 2(x_0+y_0)^2 = (x_0^2 - 2y_0^2)(1^2 - 21^2) \pm 1$$

であるから $(x_0+2y_0,\ x_0+y_0)$ も A の要素である．ところがこの要素の値 x_0+2y_0 は明らかに値 x_0 より大きい．

$(x_0,\ y_0)$ が A の要素で値 x が最大のものであることに矛盾した．

ゆえに A は無限個の要素をもつ．

$n = 2$ で (1) を用いることにより A の二つの要素 $(x,\ y)$ と $(z,\ t)$ に対して $(xz+2yt,\ xt+yz)$ も A の要素である．

$(1,\ 1) \in A$ から $(1+2,\ 1+1) = (3,\ 2) \in A$ ．同様に $(9+2\cdot 4,\ 6+6) = (17,\ 12) \in A$ ．同様に $(17^2 + 2\cdot 12^2,\ 17\cdot 12 + 12\cdot 17) = (577,\ 408) \in A$ ．これが題意をみたしている．■

解答 35 (問題 35)

(1) $\mathrm{P}(x,\ y)$ が曲線 $C_+,\ C_-$ 上の整数点のとき，

$$\begin{aligned} u^2 - 2v^2 &= (-x+2y)^2 - 2(x-y)^2 \\ &= x^2 - 4xy + 4y^2 - 2(x^2 - 2xy + y^2) \\ &= -(x^2 - 2y^2) = -(\pm 1) = \mp 1 \\ &\quad \text{(複号同順)} \end{aligned}$$

$x = y = 1$ を除くので

$$\begin{aligned}(2y)^2 - x^2 &= 4y^2 - (2y^2 \pm 1)\\ &= 2y^2 \mp 1 > 0\\ \therefore\quad & u = -x + 2y > 0\\ x^2 - y^2 &= (2y^2 \pm 1) - y^2\\ &= y^2 \pm 1 > 0\\ \therefore\quad & v = x - y > 0\\ & \text{(複号同順)}\end{aligned}$$

ゆえに $\mathrm{Q}(u,\ v)$ は曲線 $C_-,\ C_+$ (複号同順) 上の整数点である.

(2) (1) より $u > 0,\ v > 0$ で

$$\begin{aligned}y - v &= y - (x - y)\\ &= -x + 2y = v > 0\\ \therefore\quad & 0 < v < y\end{aligned}$$

(3) 数学的帰納法で示す. $(x_1,\ y_1) = (1,\ 1)$ は C_- 上の整数点である.

$n = k$ のとき $(x_k,\ y_k)$ が $C_+,\ C_-$ 上の整数点であるとする.

$$\begin{aligned}x_{k+1} + y_{k+1}\sqrt{2} &= (\sqrt{2}+1)^{k+1}\\ &= (\sqrt{2}+1)(\sqrt{2}+1)^k\\ &= (\sqrt{2}+1)(x_k + \sqrt{2}y_k)\\ &= (x_k + 2y_k) + (x_k + y_k)\sqrt{2}\end{aligned}$$

$\sqrt{2}$ が無理数で他は整数なので

$$\begin{pmatrix} x_{k+1} \\ y_{k+1} \end{pmatrix} = \begin{pmatrix} x_k + 2y_k \\ x_k + y_k \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix}$$

これから $(x_{k+1},\ y_{k+1})$ は明らかに第 1 象限の整数点で,

$$\begin{aligned}{x_{k+1}}^2 - 2{y_{k+1}}^2 &= (x_k + 2y_k)^2 - 2(x_k + y_k)^2\\ &= -({x_k}^2 - 2{y_k}^2) = -(\pm 1) = \mp 1\end{aligned}$$

より $C_+,\ C_-$ 上の整数点である.

したがってすべての自然数 n に対し, 点 $\mathrm{P}(x_n,\ y_n)$ は曲線 C_+ または C_- 上にある.

(4) 曲線 C_+ または C_- 上の整数点で $\mathrm{P}(x_n,\ y_n)$ (n は自然数) と書き表せないもの集合 S を考える.

S が空集合であることを示せばよい. S が空集合でないと仮定し, S の要素の y 座標を考える. それは自然数の部分集合であるからその中に最小のものが存在する. それを $(X,\ Y)$ とする.

C_+ または C_- 上の整数点で $Y=1$ なら $X=1$ となり，これは $(x_1,\ y_1)$ である．したがって $Y \neq 1$ ．

(1)(2) から

$$\begin{pmatrix} U \\ V \end{pmatrix} = \begin{pmatrix} -X+2Y \\ X-Y \end{pmatrix} = \begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$$

とおくと $V<Y$ である． $(U,\ V)$ は C_+ または C_- 上の整数点であるが，S の要素で y 座標が最小である $(X,\ Y)$ より y 座標が小さいので，$(U,\ V)$ は S の要素ではない．したがって $\mathrm{P}(x_n,\ y_n)$ (n は自然数) のどれかに一致する．

$$(U,\ V) = (x_j,\ y_j),\ (j \text{ は自然数})$$

とする．

(3) から $(x_{j+1},\ y_{j+1})$ も C_+ または C_- 上にある．ところが

$$\begin{aligned} \begin{pmatrix} x_{j+1} \\ y_{j+1} \end{pmatrix} &= \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} x_j \\ y_j \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} U \\ V \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} -1 & 2 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \\ &= \begin{pmatrix} X \\ Y \end{pmatrix} \end{aligned}$$

これは $(X,\ Y)$ が $\mathrm{P}(x_n,\ y_n)$ (n は自然数) と書き表せない整数点の集合 S の要素であることと矛盾した．

したがって S は空集合であり， C_+ または C_- 上の整数点で $\mathrm{P}(x_n,\ y_n)$ (n は自然数) と書き表せないものは存在しない．

つまり曲線 C_+ または C_- 上の整数点は $\mathrm{P}(x_n,\ y_n)$ (n は自然数) に限ることが示された．

(5) $(x_{n+1},\ y_{n+1}) = (x_n+2y_n,\ x_n+y_n)$ より

$$\begin{aligned} \frac{y_{n+1}-y_n}{x_{n+1}-x_n} &= \frac{x_n}{2y_n} \\ &= \frac{1}{2}\sqrt{\frac{{x_n}^2}{{y_n}^2}} = \frac{1}{2}\sqrt{\frac{2{y_n}^2 \pm 1}{{y_n}^2}} \\ &= \frac{1}{2}\sqrt{2 \pm \frac{1}{{y_n}^2}} \end{aligned}$$

数列 $\{y_n\}$ は $y_{n+1} > y_n$ である自然数列なので $\lim_{n\to\infty} y_n = \infty$ である．

$$\therefore \quad \lim_{n\to\infty} \frac{y_{n+1}-y_n}{x_{n+1}-x_n} = \frac{\sqrt{2}}{2}$$

12 節演習問題解答

解答 36 (問題 36)　$z = x + iy$ とおく．

$$\frac{z+\bar{z}}{\sqrt{2}} = \frac{2x}{\sqrt{2}},\ \frac{z+\bar{z}}{\sqrt{3}} = \frac{2x}{\sqrt{3}},\ \frac{z-\bar{z}}{\sqrt{2}i} = \frac{2y}{\sqrt{2}},\ \frac{z-\bar{z}}{\sqrt{3}i} = \frac{2y}{\sqrt{3}},$$

ゆえに，それぞれの集合は

$$A = \left\{ z \,\middle|\, x = \frac{\sqrt{2}}{2}n \text{ , } n \text{ 整数} \right\}$$
$$B = \left\{ z \,\middle|\, x = \frac{\sqrt{3}}{2}n \text{ , } n \text{ 整数} \right\}$$
$$C = \left\{ z \,\middle|\, y = \frac{\sqrt{2}}{2}n \text{ , } n \text{ 整数} \right\}$$
$$D = \left\{ z \,\middle|\, y = \frac{\sqrt{3}}{2}n \text{ , } n \text{ 整数} \right\}$$

となる．

したがって各共通集合は

$$A \cup C = \left\{ \frac{\sqrt{2}}{2}n + i\frac{\sqrt{2}}{2}m \,\middle|\, m,\ n \text{ 整数} \right\}$$
$$A \cup D = \left\{ \frac{\sqrt{2}}{2}n + i\frac{\sqrt{3}}{2}m \,\middle|\, m,\ n \text{ 整数} \right\}$$
$$B \cup C = \left\{ \frac{\sqrt{3}}{2}n + i\frac{\sqrt{2}}{2}m \,\middle|\, m,\ n \text{ 整数} \right\}$$
$$B \cup D = \left\{ \frac{\sqrt{3}}{2}n + i\frac{\sqrt{3}}{2}m \,\middle|\, m,\ n \text{ 整数} \right\}$$

となる．

中点が E の要素になっているためには，その 2 点がともにこの四つの共通集合のなかの同じ集合の要素であって，しかも実部と虚部の n と m がそれぞれともに偶数か，ともに奇数かのときである．

この違いは合計 16 通りである．したがって，17 個の複素数よりなる集合 F の中には．四つの共通集合のなかの同じ集合に属し，しかも実部と虚部の n と m の偶数奇数がそれぞれ同じである二つの要素がある．

この 2 点の中点は再び E の要素になっている．

解答 37 (問題 37)

(1) $a_k > 0$ $(1 \leqq k \leqq n)$ なので

$$1 \leqq s_1 < s_2 < \cdots < s_n$$

ここで $s_n = m^2$ とおく．s_{n-1} は m^2 より小さい平方数なので，$s_{n-1} \leqq (m-1)^2$ ．ゆえに

$$a_n = s_n - s_{n-1} \geqq m^2 - (m-1)^2 = 2m - 1$$

$1 \leqq a_n \leqq 2n$ より $2m - 1 \leqq 2n$．つまり $2m \leqq 2n + 1$ であるが，偶数奇数を考え $2m \leqq 2n$，つまり $m \leqq n$ ．

したがって $s_n = m^2 \leqq n^2$ となる．つまり

$$1 \leqq s_1 < s_2 < \cdots < s_n \leqq n^2$$

ところが 1 から n^2 の間の平方数はちょうど n 個であるから，$s_1,\ s_2,\ \cdots,\ s_n$ が $1,\ 2^2,\ \cdots,\ n^2$ に一致しなければならない．

$$s_k = k^2 \quad (1 \leqq k \leqq n)$$

とくに $s_n = n^2$

(2) (1) から $a_k = s_k - s_{k-1} = 2k - 1\ (1 \leqq k \leqq n)$ となる．

14 節演習問題解答

解答 38 (問題 38)

(1) 条件から

$$\begin{aligned} P_{n+1}Q_n - P_nQ_{n+1} &= (P_{n-1} + k_nP_n)Q_n - P_n(Q_{n-1} + k_nQ_n) \\ &= -(P_nQ_{n-1} - P_{n-1}Q_n) \\ \therefore \quad & P_nQ_{n-1} - P_{n-1}Q_n = (-1)^{n-1}(P_1Q_0 - P_0Q_1) = (-1)^n \end{aligned}$$

(2) P_n と Q_n の最大公約数を d とし $P_n = dP'_n,\ Q_n = dQ'_n$ とする．

$$P_nQ_{n-1} - P_{n-1}Q_n = d(P'_nQ_{n-1} - P_{n-1}Q'_n) = (-1)^n$$

$$\therefore \quad d = 1$$

つまり $n \geqq 1$ のとき， P_n と Q_n の最大公約数は 1 である．

(3)

$$\frac{P_{n-1} + P_na_n}{Q_{n-1} + Q_na_n} = \frac{P_{n-1} + P_n\left(k_n + \dfrac{1}{a_{n+1}}\right)}{Q_{n-1} + Q_n\left(k_n + \dfrac{1}{a_{n+1}}\right)}$$

$$= \frac{P_{n+1} + \dfrac{P_n}{a_{n+1}}}{Q_{n+1} + \dfrac{Q_n}{a_{n+1}}} = \frac{P_n + P_{n+1}a_{n+1}}{Q_n + Q_{n+1}a_{n+1}}$$

$$\therefore \quad \frac{P_{n-1} + P_na_n}{Q_{n-1} + Q_na_n} = \frac{P_0 + P_1a_1}{Q_0 + Q_1a_1} = \frac{1 + k_0a_1}{a_1} = k_0 + \frac{1}{a_1} = a_0 = a$$

(4)

$$\begin{aligned} a - \frac{P_n}{Q_n} &= \frac{P_{n-1} + P_na_n}{Q_{n-1} + Q_na_n} - \frac{P_n}{Q_n} = \frac{(P_{n-1} + P_na_n)Q_n - P_n(Q_{n-1} + Q_na_n)}{(Q_{n-1} + Q_na_n)Q_n} \\ &= \frac{(P_{n-1}Q_n - P_nQ_{n-1}}{(Q_{n-1} + Q_na_n)Q_n} = \frac{-(-1)^n}{(Q_{n-1} + Q_na_n)Q_n} \end{aligned}$$

$$\therefore \quad \left| a - \frac{P_n}{Q_n} \right| = \frac{1}{|(Q_{n-1} + Q_n a_n) Q_n|}$$

ここで a_0 無理数なので，帰納的に定められた $\{a_n\}$ はすべて正の無理数である．また $0 < a_{n-1} - k_{n-1} = \dfrac{1}{a_n} < 1$ から $a_n > 1$.

定め方から $Q_n > 0$ $(n \geqq 1)$ なので

$$\begin{aligned} |(Q_{n-1} + Q_n a_n) Q_n| &= (Q_{n-1} + Q_n a_n) Q_n \\ &\geqq a_n Q_n^2 > Q_n^2 \end{aligned}$$

$$\therefore \quad \left| a - \frac{P_n}{Q_n} \right| < \frac{1}{Q_n^2}$$

15 節演習問題解答

解答 39 (問題 39)

(1) 四つの頂点を $(x-1,\ y-1)$, $(x,\ y-1)$, $(x,\ y)$, $(x-1,\ y)$ とする．

x を超えない最大の整数を m とする． $m \leqq x < m+1$ であるから

$$x - 1 < m \leqq x$$

つまり区間 $[x-1,\ x]$ には整数 m が存在する．

y 方向についても同様に $[y-1,\ y]$ には整数 n が存在する．

したがって，正方形 (周をこめる) には少なくとも一つの格子点 $(m,\ n)$ が存在した．

(2) 辺の長さが $\sqrt{2}$ の正方形には半径 $\dfrac{1}{\sqrt{2}}$ の円が内接している． $\dfrac{1}{\sqrt{2}}$ の円には，1 辺の長さが 1 の正方形が内接する．

したがって (1) から少なくとも一つの格子点を含むことが示された．

解答 40 (問題 40)

(1) xy 平面の点 $(x,\ y)$ に対して

$$\begin{pmatrix} u \\ v \end{pmatrix} = \begin{pmatrix} ax + cy \\ bx + dy \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}$$

で定まる点 $(u,\ v)$ を対応させる．このとき $ad - bc = 1$ なので逆に

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} du - cv \\ -bu + av \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix} \begin{pmatrix} u \\ v \end{pmatrix}$$

と解ける．

この対応で $(x,\ y)$ が格子点なら $(u,\ v)$ も格子点であり，逆も成り立つ．

S 内の任意の点 P は二つの実数 $0 \leqq s,\ t \leqq 1$ によって

$$\overrightarrow{\mathrm{OP}} = s\overrightarrow{\mathrm{OA}} + t\overrightarrow{\mathrm{OB}} = \begin{pmatrix} sa+tc \\ sb+td \end{pmatrix}$$

と表されるが

$$\begin{pmatrix} s \\ t \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}\begin{pmatrix} sa+tc \\ sb+td \end{pmatrix}$$

なので，この対応で S は $(0,\ 0),\ (1,\ 0),\ (0,\ 1),\ (1,\ 1)$ を頂点とする正方形 T に移る．

もし S の内部に格子点があれば，この対応で T 内部の格子点に移らなければならない．しかし T の内部には明らかに格子点は存在しない．

したがって S の内部にも格子点は存在しない．

(2) (1) と同様の変換を考える．

$$\begin{pmatrix} 2s \\ 2t \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}\begin{pmatrix} sa+tc \\ sb+td \end{pmatrix}$$

であり， S はこの変換で $(0,\ 0),\ (2,\ 0),\ (0,\ 2),\ (2,\ 2)$ を頂点とする正方形 U に移る． S 内部の 点 $(sa+tc,\ sb+td)$ が格子点であるとする．

$m = sa+tc,\ n = sb+td$ とおくと，

$$\begin{pmatrix} 2s \\ 2t \end{pmatrix} = \begin{pmatrix} d & -c \\ -b & a \end{pmatrix}\begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} dm-cn \\ -bm+an \end{pmatrix}$$

なので，やはり U の格子点に移る．

したがって $ad-bc=2$ のとき, S の中に格子点があれば，この対応で U 内部の格子点に移らなければならない．U 内部の格子点は正方形の対角線の交点 $(1,\ 1)$ のみである．つまり $s = \dfrac{1}{2},\ t = \dfrac{1}{2}$.

したがって S 内部の格子点は $(\dfrac{a+c}{2},\ \dfrac{b+d}{2})$ である以外になく，これは平行四辺形の対角線の交点である．

解答 41 (問題 41)

(1) 整数 $m,\ n$ をとり，点 $(x,\ y)$ に対し点 $(x+m,\ y+n)$ を対応させると，$(x,\ y)$ が格子点なら $(x+m,\ y+n)$ も格子点であり，逆もなり立つ．

したがって線分を x 方向と y 方向がともに整数分だけ平行移動してもその上にある格子点の個数は変わらない．

格子点 $(k,\ l)$ がある． k と l の最大公約数を d とし $k = dk',\ l = dl'$ とおく．

このとき原点と格子点 $(k,\ l)$ を結ぶ線分上の両端を除く格子点は

$$(k',\ l'),\ (2k',\ 2l'),\ \cdots,\ ((d-1)k',\ (d-1)l')$$

と， $d-1$ 個ある．ゆえにこの個数が奇数なら d は偶数．つまり x 座標，y 座標ともに偶数である．

三角形 ABC で A を原点に平行移動しそれを三角形 OB′C′ とする．このとき辺 AB, AC それぞれの上に両端をのぞいて奇数個の格子点があるので，点 B′, C′ の双方の x 座標と y 座標はいずれも偶数である

B′$(2s,\ 2t)$ ，C′$(2u,\ 2v)$ とおく．

B′ を原点に平行移動すると，C′ は $(2u-2s,\ 2v-2t)$ になる．

x 座標，y 座標ともに偶数であるから，線分 B′C′ 上に両端を除いて奇数個の格子点があり，辺 BC 上にも両端を除いて奇数個の格子点がある．

(2) 三角形 ABC で A を原点に平行移動しそれを三角形 OB′C′ とする．このとき辺 AB, AC それぞれの上に両端をのぞいてちょうど 3 個ずつの格子点があるので，点 B′, C′ の双方の x 座標と y 座標はいずれも 4 の倍数である

B′$(4s,\ 4t)$ ，C′$(4u,\ 4v)$ とおく．

$$\triangle \mathrm{ABC} = \frac{1}{2}|4s\cdot 4v - 4t\cdot 4u| = 8|sv-tu|$$

ゆえに，三角形 ABC の面積は 8 で割り切れる整数である．

解答 42 (問題 42)

(1) 3 頂点を $(a_1,\ b_1)$, $(a_2,\ b_2)$, $(a_3,\ b_3)$ とする．このとき面積 S は

$$S = \frac{1}{2}|(a_2-a_1)(b_3-b_1) - (a_3-a_1)(b_2-b_1)|$$

である．ゆえに $2S$ は整数である．

(2) 3 頂点の座標がすべて整数の組であるような正三角形が存在するとし，その正三角形の面積を S とする．(1) から S は有理数である．

一方正三角形の 1 辺を t をすると $t^2 = (a_2-a_1)^2 + (b_2-b_1)^2$ なので面積 S は

$$S = \frac{1}{2}\sin\frac{\pi}{3}t^2 = \frac{\sqrt{3}}{4}\{(a_2-a_1)^2 + (b_2-b_1)^2\}$$

これは無理数である．

したがって (1) の結果と矛盾した．ゆえに 3 頂点の座標がすべて整数の組であるような正三角形は存在しない．

(3) 平面上で，5 頂点の座標がすべて整数の組であるような正五角形は存在するとし，正五角形の中心を原点に平行移動する．

隣りあう二つの頂点を P, Q とする． P, Q は格子点であるから (1) と同様に △OPQ の面積は有理数である．

一方

$$S = \frac{1}{2}\sin\frac{2\pi}{5}\mathrm{OP}^2$$

ここで $\theta = \dfrac{2\pi}{5}$ とすると，$2\theta + 3\theta = \pi$ なので $\sin 2\theta = \sin 3\theta$．つまり

$$2\sin\theta\cos\theta = -4\sin^3\theta + 3\sin\theta$$

$\sin\theta \neq 0$ なので

$$2\cos\theta = -4\sin^2\theta + 3 = -4(1-\cos^2\theta) + 3$$

θ は鋭角なので $\cos\theta = \dfrac{1+\sqrt{5}}{4}$ ．ゆえに $\sin^2\theta = \dfrac{10-2\sqrt{5}}{16}$．これは無理数であり，したがって $\sin\theta$ も無理数である．

(2) と同様の矛盾が生じた．よって，平面上で 5 頂点の座標がすべて整数の組であるような正五角形は存在しない．