数論初歩

2013 年 8 月 17 日

目 次

まえがき **4**

第 1 章　数論の基礎 **5**

1.1　自然数 5
1.1.1　自然数の定義 5
1.1.2　数学的帰納法 7
1.2　整数 7
1.2.1　整数の定義 7
1.2.2　除法の原理 10
1.3　約数と倍数 11
1.3.1　最大公約数と最小公倍数 11
1.3.2　ユークリッドの互除法 13
1.4　一次不定方程式 16
1.4.1　不定方程式 16
1.4.2　一次不定方程式の解の存在 16
1.4.3　一次不定方程式の一般解と解の構成 20
1.5　素数 27
1.5.1　素数の定義 27
1.5.2　素因数分解 28
1.6　演習問題 31

第 2 章　剰余類 **39**

2.1　合同式 39
2.1.1　合同式 39
2.1.2　一次合同方程式 43
2.1.3　合同方程式の解法 46
2.2　オイラーの関数 49
2.2.1　オイラーの関数 $\varphi(n)$ 49
2.2.2　メービスの反転公式 53
2.3　1 の n 乗根 55
2.3.1　1 の n 乗根 55
2.4　フェルマの小定理 57
2.4.1　フェルマの小定理 57
2.4.2　循環小数 59
2.4.3　算術級数の定理 62
2.5　原始根と指数 65

2.5.1 原始根 65
2.5.2 指数 67
2.6 演習問題 70

第 3 章 相互法則 **78**
3.1 平方剰余 78
3.1.1 平方剰余とルジャンドルの記号 78
3.1.2 整数を平方数の和に分解すること 80
3.2 平方剰余の相互法則 83
3.2.1 相互法則とは何か 83
3.2.2 ガウスの補題による証明 84
3.3 いくつかの別証明 87
3.3.1 ガウス和を用いる証明 87
3.3.2 三角法の補題による証明 92
3.4 演習問題 94

第 4 章 除法のできる環 **96**
4.1 ユークリッド整域 96
4.2 多項式環 96
4.2.1 多項式の除法 96
4.2.2 多項式環での不定方程式 100
4.3 ガウス整数環 103
4.3.1 ガウス整数 103
4.3.2 ガウス素数 105
4.3.3 四次フェルマ問題 108
4.4 演習問題 110

第 5 章 連分数 **113**
5.1 一次不定方程式と連分数 113
5.2 二次行列と実数の連分数展開 116
5.2.1 最良近似分数 116
5.2.2 実数の対等 119
5.3 連分数と格子点 121
5.3.1 ミンコフスキーの定理 121
5.3.2 近似分数 123
5.4 演習問題 126

第 6 章 ペル方程式 **130**
6.1 解集合の構造と解の存在 130
6.1.1 ペル方程式の解の構造 130
6.1.2 ディリクレの原理 137
6.1.3 ペル方程式の解の存在 139
6.2 連分数による解の構成 140
6.2.1 二次無理数の連分数展開 140

6.2.2 ペル方程式の解の構成 144
6.2.3 解構成のアルゴリズム 150
6.3 演習問題 154

第 7 章 素数分布 **155**
7.1 素数の分布とは 155
7.2 素数が無数にあることの別証明 156
7.3 素数分布の探求 159
7.4 素数定理 164

第 8 章 存在と構成 **166**
8.1 自然数の構成 166
8.1.1 ペアノの公理 166
8.1.2 同型定理と演算 168
8.2 整数と有理数の構成 171

第 9 章 解答 **174**
9.1 演習問題解答 174
9.2 入試問題解答 203
9.3 出典と文献 253
9.3.1 入試問題出典 253
9.3.2 参考文献 254

まえがき

数えることは，言葉を話すこととともに，人間にとってもっとも基本的なことである．数は身近な第二の母語というべきものである．数はまず自然数である．この基本的な自然数の世界に，今も多くの未解決問題があることは驚きである．自然数は，整数から有理数，実数，複素数へと世界をひろげる．そのなかで整数もまた代数的整数へと拡大される．整数の理論を数論という．これは今日も発展し続けているまことに美しい理論である．

基本となるのは有理数のなかにある整数，有理整数である.『数論初歩』は有理整数の古典理論を紹介するものである．本書では，とくに断らなければ有理整数のことを単に整数という．数論は初等的な段階から数学のおもしろさ，美しさを実感することができる分野である．また，体系立てて学ぶことで，少ない原理を自由に広く応用するという，数学の大切な精神を身につけることができる．

中学生，高校生の時期に数のもつ美しい性質の一端に触れることは，その人を豊かにするとともに，現象を掘り下げて深く考える力をつける．しかし，現実に日本の高校生が出会う整数は，入学試験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切れ切れの知識が積みあげられ，小手先の方法論が先行し，単純で美しく，かつ豊かな整数の世界がかえってわかりにくくなっている．これが現状である．これはたいへん残念なことである．

このような現状を打破し，数の理論の美しさを伝えてゆく．そのための基礎作業の一つがこの『数論初歩』である．整数分野は教育数学にとっても重要な分野である．したがってこれは，教育数学を構築してゆく上での基礎作業でもある．

『数論初歩』は，実際に計算して整数に触れながらすすんでいくことに重きをおいた．整数の美しさに触れ，さらに広い世界の探索に出て行く契機となることを願っている.『数論初歩』があつかう範囲は，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 章に対応する有理整数の古典理論で，主眼は平方剰余の相互法則をいくつかの初等的な方法で証明することである．さらに素数分布について一端に触れることができるようにした．また，自然数の公理的構成から整数，有理数の構成についても最後に一章をあてた．

いくつかの節をまとめて章とし，章ごとに演習問題をつけた．演習問題はその内容を理解する助けとなる「練習問題」と関連する「入試問題」で構成した.「入試問題」は 20 世紀末から 21 世紀初頭にかけて日本に大学入学試験で実際に出題されたものである．最後に解答をつけたが，練習問題は定理やその他本文の結論を用いるようにし，逆に入試問題はできるだけそのなかで完結する方法で解くようにした．

「定理」は一般的な結果であり「系」はそれからただちに導かれる命題である.「補題」は定理の証明に必要な準備的命題を意味する．これらは通し番号になっている.「例」は材料となる具体的な例や，試しに解いてみる問題,「注意」は意味通りであり，これらは節毎に【節番号-番号】の形で番号をつけている．また■は命題の終わりを，□は証明の終わりを意味する．

第1章　数論の基礎

1.1　自然数

1.1.1　自然数の定義

自然数　「自然数」は，人が成長する過程で最初に習得する数である．3 枚の皿に 3 個のみかんをひとつずつおいていけば，皿が余ったり，みかんが余ったりすることなくちょうど 1 枚の皿にみかんが 1 つずつおける．このような経験のなかから 3 枚の皿と 3 個のみかんは何かが「同じ」だと気づく．と，ここで実はこの一文ではすでに自然数「3」が用いられていることに気づく．

朝，小屋を出すとき，羊が通るたびに石を一つずつ置いていく．夕方帰ってきたときまたその石を羊が通るたびに動かす．最後の羊が通ったとき最後の石が動けば，迷子の羊がいないことがわかる．このとき朝の羊の何と夕べの羊な何が同じなのだろうと考えた．一対一の対応がつくとき，そこで何かが同じだ．一対一対応がつかないときは違う．同じとか違うとか一体何がと考え，同じものとしての「数」という概念が生まれていった．

また，数詞が生まれても，3 個のみかんは 3 個のみかん，皿 3 枚は皿 3 枚と 3 が抽象されないまま用いられる膨大な時間があったにちがいない．そのときを経て，3 が抽象されるとともに「数」の概念が生まれていった．

このように，個別のものの形や質などに規定された具体的な量から，個別の性質を捨て一般的な「数」を抽象する力を，人間は長い時間をかけて身につけた．数の発見は，実際はもっと生産に直結した場で起こったに違いない．毎朝放牧した羊と，夕べに帰ってきた羊が同じだけあるのかどうか，数を知らなければどのように判断するか．羊が小屋を出るたびに石をひとつ並べていく．帰ってきたときは，羊が小屋に入るたびに石をひとつ除く．こうしてちょうど最後の 1 頭が戻ったとき最後の石が除かれれば，増減がなかったことがわかる．石を並べることが長く続いた後，人は数を発見したのだ．あるいは実がなるまでに月の満ち欠けがどれだけくりかえされるか，こんなところにも数の発見の起源があるかも知れない．

人間が数をつかみ，それが親から子へと伝えられて，子供は成長のなかで数を身につける．大人からの伝達の作用によって，人類の長い歴史が凝縮されて，子供のなかで反復されるのだ．みかんのように数えられるものの個数がつかまれたなら，つぎは「水がバケツに 3 杯ある」などのように連続量をはかる単位が生まれ，単位の個数として水の量をつかむことができるようになったと考えられる．

このようにして見いだされた「自然数」は，数えるという行為と一体である．数えるという行為とは，このものを認識し，その次のものを確認して，自然数によって指示される抽象的な数との間に対応をつけていく，ということにある．最後に対応した数をその集合の要素の個数と認識する，ということである．このことを定式化して自然数を改めて数学の対象として定義しなおす．

自然数とは何か．

定義 1

1 からはじめて,「1 たす」という操作だけで作られる数の集合を自然数の集合といい，その要素を

自然数という．■

「だけで作られる」というところが大切である．つまり条件を満たす最小の集合である．「たす」という操作がどのようなものであるかは問わない．その操作を記号「＋」で表す．最初の対象「1」と操作「+」とその「くりかえし」，これだけである．1 に 1 たした 1+1 を 2 と記し，2 に 1 たした 2+1 を 3 と記し，以下順次命名してゆく．このように命名された要素の集合を $\mathbb{N}$ と記す．その各要素を自然数という．

この定義から $\mathbb{N}$ は次のような構造をもつことが示される．

(i) (大小が定義される) 2 つの自然数 a と b は，a から始まって 1 たす操作を 1 回以上くりかえすことで b になるとき $a < b$ と定め，a は b より小さい，b は a より大きいという．

(ii) 自然数の集合 $\mathbb{N}$ の部分集合には最小の要素がただ一つ存在する．

(iii) (数学的帰納法の原理) $\mathbb{N}$ の部分集合 A が条件「$1 \in A$ ，かつ $x \in A$ なら $x+1 \in A$ 」を満たすなら、A は $\mathbb{N}$ 自身である．

これを証明するには，自然数の定義をもう少し厳密に定式化しなければならない．その作業はなかなか骨の折れることである．最終章「存在と構成」でその概略を示した．

最小要素の存在　自然数の性質 (ii) は，要素が自然数からなる集合には最小の要素がただ一つ存在することを主張する．これは，整数分野の諸問題で存在証明の根拠になる．

一方，整数からなる集合や有理数からなる集合では最小要素があるとはかぎらない．例えば

$$\{-5,\ -6,\ -7,\ \cdots\} = \{a \mid a \text{ は } -5 \text{ 以下の整数 }\}$$
$$\left\{\frac{1}{2},\ \frac{1}{4},\ \frac{1}{8},\ \cdots\right\} = \left\{\frac{1}{2^k} \mid k \text{ は自然数}\right\}$$

などはいずれも最小の要素がない．

整数の部分集合でも，そのうち正の要素からなる部分集合には最小の要素が存在する．これを用いた存在証明の典型は一次不定方程式に解が存在することの証明である．

自然数の演算　自然数の集合 $\mathbb{N}$ の要素 a と b には二つの演算，和 $a+b$ と積 ab が定義される．定義されるとは a と b に対して $\mathbb{N}$ の要素 $a+b$ と ab が一意に定まることを意味する．これを自然数の集合 $\mathbb{N}$ は加法と乗法で**閉じている**という．これに対して減法と除法については閉じていない．

$\mathbb{N}$ を含み減法で閉じている最小の集合が整数の集合 $\mathbb{Z}$ であり，$\mathbb{N}$ を含み除法で閉じている最小の集合が有理数の集合 $\mathbb{Q}$ である．

また整数 a にはその絶対値 $|a|$ が定義される．つまり

$$|a| = \begin{cases} a & (a \geqq 0) \\ -a & (a < 0) \end{cases}$$

である．

これらの演算の定義といくつかの演算法則の証明は，数学的帰納法による．それも最終章「存在と構成」でその概略を示した．

1.1.2 数学的帰納法

数学的帰納法の構成　自然数の性質 (iii) を数学的帰納法の原理というのはなぜか.

数学的帰納法は証明すべき対象の性質そのものであると考えられている．それは正しいのだが，数学的帰納法の証明で**すべての自然数で成り立つ**根拠は，実は自然数の性質そのもののなかにある．このことは理解しておきたい.

$p(n)$ を自然数 n を含む何らかの命題とする．$p(n)$ がすべての自然数 n で成立する，つまり真であることを証明するのに，次のような論法を用いる.

(1) $p(1)$ が真である.

(2) $p(k)$ が真なら $p(k+1)$ が真である.

(3) (1), (2) より すべての自然数 n に対して $p(n)$ が真である.

(1) と (2) から (3) が結論づけられる根拠が，自然数の性質 (iii) なのである．それはどういうことか.

数学的帰納法の根拠　数学的帰納法の論証の進展を真理集合の面から言いかえる．条件 $p(n)$ の真理集合を M とする．つまり，

$$M = \{n \mid p(n) \text{ が真}, \ n \in \mathbb{N}\}$$

である．すべての自然数 n で真であるということは，$p(n)$ が真となるような n の集合 M が自然数の集合 $\mathbb{N}$ と一致することである．数学的帰納法の (1) は $1 \in M$，(2) は $k \in M$ なら $k+1 \in M$ が成り立つことを示している．すると自然数の性質 (iii) より $M = \mathbb{N}$ となり，すべての自然数で真であることが示されるのである.

自然数の集合というのは,「1 があって k が要素であれば $k+1$ も要素である」ような集合のうちで**いちばん小さいもの**として特徴づけられる．この自然数の性質 (最小性) によって，M が $\mathbb{N}$ と一致する．条件が成立する n の集合 M が自然数全体となり，すべての自然数 n でなり立つ，つまり (3) の成立がわかる．これが数学的帰納法の論証構造である.

1.2 整数

1.2.1 整数の定義

自然数は人間にとって言葉と同じだけ古い．それに対して整数が人間のものになったのははるかに遅い．デカルト (1596 − 1650) でさえ方程式の負の根を「偽の根」と呼んでいるし，パスカル (1623 − 1662) は「ゼロから 4 を引けばゼロであることを理解できない人がいるのを知っている」といっている．0 は無であり 4 を引いてもやはり無と考えられていた．もちろんゼロや負の数を今日のように理解していた人もいたが，負数の理解は簡単でなかった.

ゼロ数，負数の導入とその加法・減法の諸法則の発見は中国が最初である.『九章算術』には「(引き算の時) 同符号は引き，異符号は加える．正を無入から引いて負とし，負を無入から引いて正とする」との一文がある.「無入」はゼロのことである．中国で発見された負の数は，インドに渡りそこで広がり，アラビアに伝わり，そして欧州にまで届いたのである.

整数の構成という問題を後で考えることにし，自然数に 0 と負整数を加えた集合を整数の集合とし $\mathbb{Z}$ で表す.

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

である.

$\mathbb{Z}$ には二つの演算，加法と乗法が定義されている．それをそれぞれ「+」「·」で表す.「定義されている」ということは，$\mathbb{Z}$ の任意の二つの要素 x と y に対し，和 $x+y$ と積 $x\cdot y$ が一意に定まり，ふたたび $\mathbb{Z}$ に属する，ということを意味する.

このとき加法と乗法について次のことが成り立つ,

I. 加法：

(i) $(x+y)+z = x+(y+z)$.

(ii) $x+y = y+x$.

(iii) すべての x に対して $x+0 = x$ となる要素 0 が存在する.

(iv) x に対し $x+y = 0$ となる y が存在する．これを $-x$ と書く.

II. 乗法：

(i) $(x\cdot y)\cdot z = x\cdot(y\cdot z)$.

(ii) $x\cdot y = y\cdot x$

(iii) すべての x に対して $x\cdot 1 = x$ となる要素 1 が存在する.

III. 分配法則：
$x\cdot(y+z) = x\cdot y + x\cdot z$.

集合 $\mathbb{Z}$ の各要素を**整数**という．実は「整数」の概念は，いま考えている整数よりはるかに広く，代数的整数といわれる世界がある．そのごく一部を後に紹介するが，広がった概念の整数の世界のなかでは，いま考えている整数を**有理整数**という．これは「有理数に含まれる整数」という意味である．区別する必要のないときは単に整数というものとする.

数学では考える対象を集合としてとらえる．あるいはある概念を構成すると，その概念に適応する対象の集合を考える．そのとき，その集合がどのような構造をもっているか，これが基本的な問題意識，探求の方向となる．代数的な対象からなる集合では，そこにどのような演算が定義されうるかによって，いくつかの構造が概念化されている．その基本的のものとして，整数の集合にかかわる群，環，体の定義をここで述べておく.

群　整数 $\mathbb{Z}$ は加法に関して可換群である．可換群とは何か．集合 G の元について，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.

(i) $a, b \in G$ ならば $a\circ b \in G$ （演算について閉じている）

(ii) $(a\circ b)\circ c = a\circ(b\circ c)$ （結合法則）

(iii) 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）

(iv) 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, $a,\ b \in G$ に対して $a \circ b = b \circ a$ を満たすとき, **可換群** (または **アーベル群**) であるという.

環 整数 $\mathbb{Z}$ は加法と乗法に関して環である. 環とは何か. 集合 M に 二種類の演算 $\circ$ と $*$ が定義されていて, 一方の演算 $\circ$ については可換群であり, 他の演算 $*$ については **結合法則** と次の **分配法則**

$$a * (b \circ c) = (a * b) \circ (a * c),\ (b \circ c) * a = (b * a) \circ (c * a)$$

が成り立つとき, 集合 M は **環** であるという.

負数の積 負数の積がなぜ正の数になるのか. これは量の構造を根拠に意味づけができる. それはそれで大切なことなのであるが, 一方 $\mathbb{Z}$ の環としての演算から示すこともできる.

$\mathbb{Z}$ の任意の要素に対して

$$(-a) \cdot (-b) = a \cdot b$$

が成り立つ.

(1)

$$a = 1 \cdot a = (0+1) \cdot a = 0 \cdot a + 1 \cdot a = 0 \cdot a + a$$

$$\therefore \quad 0 \cdot a = 0$$

(2)

$$0 = 0 \cdot a = \{1 + (-1)\} \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a$$

$$\therefore \quad (-1) \cdot a = -a$$

(3)

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

$$\therefore \quad -(-a) = a$$

ところが

$$-(-a) = (-1) \cdot \{(-1) \cdot a\} = \{(-1) \cdot (-1)\} \cdot a$$

なので

$$\{(-1) \cdot (-1)\} \cdot a = a$$

$a = 1$ とすると

$$(-1) \cdot (-1) = 1$$

よってまた

$$(-a) \cdot (-b) = (-1) \cdot a \cdot (-1) \cdot b = \{(-1) \cdot (-1)\} \cdot a \cdot b = a \cdot b$$

このように $\mathbb{Z}$ は環であるがしかし体ではない. 体とは何か.

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 $\circ$ の単位元を除いた集合が $*$ に関して可換群を作るとき，集合 K は**体** であるという．

有理数 $\mathbb{Q}$ では $\circ$ を和 $+$，$*$ を積 $\cdot$ にするとき，体になる．これを有理数体という．有理数体 $\mathbb{Q}$ は，自然数 $\mathbb{Z}$ を含む最小の体である．$\mathbb{Q}$ は整数 $\mathbb{Z}$ に成り立つ基本性質に加えて

> (iv) 0 でない任意の x に対して $x \cdot y = 1$ となる要素 y が存在する．この y を x^{-1} と表す.

を加えたものである．

このような整数環 $\mathbb{Z}$，有理数体 $\mathbb{Q}$ が実際に存在する，つまり構成できるのか．自然数の集合 $\mathbb{N}$ の存在を前提に，そこから構成することができなければならない．この問題は最終章でで考える．ここでは $\mathbb{Z}$ と $\mathbb{Q}$ の存在を前提に除法について考察を深めよう．

1.2.2　除法の原理

整数の研究の第一歩は，整数の集合のもう一つの演算である「除法」を見直し，その基本性質を明らかにすることである．$\mathbb{Z}$ の任意の要素 a と任意の正の要素 b に対して，次の定理 1 が示すように，$a = qb + r$ となる整数 q と，$0 \leqq r < b$ の範囲の整数 r がただ一つ存在する．そのとき q を a を b で割った商，r を余りという．

これはいわゆる割り算がただ一通りにできるということである．これを「除法の定理」という．有理整数で成り立つ多くの事実の根拠がここにある．この節では自然数の性質に根拠をおいて「除法の定理」を証明する．

定理 1 (除法の定理)
a を任意の整数, b は正の整数とする．このとき，

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

となる整数 q, r がただ一組存在する．　■

証明　整数 a と正整数 b に対して

$$qb \leqq |a| < (q+1)b \tag{1.1}$$

となる整数 q が存在することを示す.

$|a| < (t+1)b$ を満たす整数 t よりなる集合を A とする．A は集合 $\mathbb{N} \cup \{0\}$ の部分集合である．自然数の部分集合には最小の要素が存在するので A にも最小の数が存在する．それを q とする．$q-1$ は $|a| < (t+1)b$ を満たさないので $qb \leqq |a|$ かつ $|a| < (q+1)b$ である．つまり 1.1 を満たす整数 q が存在した.

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．$a \geqq 0$ ならこの式がただちに $a = qb + r$ である.

$a < 0$ のときは $a = -qb - r$ となる．$r = 0$ なら $-q$ を q にとりなおすことで $a = qb + r$ である．$0 < r < b$ のとき

$$a = -qb - r = (-q-1)b + (b-r)$$

$b-r$ も $0 \leqq b-r < b$ を満たす．$-q-1$ を q，$b-r$ を r にとりなおすことで $a = qb+r$ でとなり，定理 1 の等式を満たす整数 q と r が存在した．

つぎに，このような q, r が二通りあったとする．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． $q_1 < q_2$ のときも同様である．

よって $q_1 = q_2$ であり，その結果 $r_1 = r_2$ である． □

q のことを a を b で割った**商**，r のことを**余り**という．$r = 0$ であるとき，つまり

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

となる整数 q が存在するとき，a は b で割り切れるといい，$b|a$ と表す．このとき，a は b の倍数，b は a の約数である，という．

注意 1.2.1 定理 1 の r の範囲をかえて次の命題にしても成立する．

a を任意の整数, b は正の整数とする．このとき，

$$a = qb + r\ , \quad -\frac{b}{2} \leqq r < \frac{b}{2}$$

となる整数 q, r がただ一組存在する．

一般に $e \leqq r < e + b$ と幅一の半開区間を指定してもよい．

整数の集合 $\mathbb{Z}$ では除法の定理が土台になる．代数的整数といわれる世界では，この除法の定理は成り立たない．

例 1.2.1 $b = 12$ とする．

- $a = 50 : 50 = 4 \cdot 12 + 2$.
- $a = -50 : -50 = (-5) \cdot 12 + 10$.
- $a = -5 : -5 = (-1) \cdot 12 + 7$.

1.3 約数と倍数

1.3.1 最大公約数と最小公倍数

定義 2

整数 a が b の**倍数**であるとは，$a = bq$ となる整数 q が存在することと定める．このとき b は a の**約数**という．除法の定理によって，a が b の倍数であることは，a を b で割った余りが 0 であることと同値である． ■

さらに，公約数，公倍数が定義される．

定義 3

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絶対値は $a,\ b,\ c,\ \cdots$ のいずれの絶対値よりも小さくはないので，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．公約数の絶対値は $a,\ b,\ c,\ \cdots$ のいずれの絶対値よりも大きくはないので，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． ■

最大公約数が 1 であるとき，その 2 数は**互いに素**であるという．また整数 a と b の最大公約数を座標などと混同する恐れのないときは $(a,\ b)$ と書く．$(12,\ 32) = 4$ のように用いる．

定理 2

(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．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適当な整数 a' と b' を用いて，

$$l = ab' = ba'$$

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

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

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

つまり m は $a,\ b$ の公約数である．(2) より最大公約数 d の約数なので，$d = me$ 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

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

一方，$a = ma',\ b = mb'$ であるから $ma' = mea''$，$mb' = meb''$ が成り立つ．

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

その結果，

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

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

ところがこれは $\dfrac{l}{e}$ が $a,\ b$ の公倍数であることを示している．l が最小の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「除法の定理」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,「除法の定理」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 $a,\ b,\ c,\ \cdots$ の最大公約数が 1 であることを簡単に「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．

1.3.2　ユークリッドの互除法

ここで，最大公約数を求める一般的な方法であるユークリッドの互除法をまとめよう．

エウクレイデス　「エウクレイデス」のことを英語では「ユークリッド」という．最近は「マホメット」も「ムハンマド」というように，本来の読みで書くのが習わしだ．ただ,「ユークリッド」はあまりにも定着しているので，幾何学をさすときは「ユークリッド幾何学」のようにもいうことにする．

公理を立て，公理からはじめて論証を進め，新たに発見された事実を揺るぎないものとして示す，という幾何の論証はエウクレイデスにはじまる．それをまとめたものが『(幾何学) 原論』である．これは複数人の共著であり，その一人がエウクレイデスであるといわれている．

エウクレイデス（Eukleides，紀元前 365 年?〜紀元前 275 年?，英語表記 Euclid）は古代ギリシアの数学者，天文学者とされる人で，アテナイで学びプトレマイオス 1 世治下のアレクサンドリアで教えた．ちなみにプトレマイオス 1 世とは，アレクサンドロス 3 世（アレキサンダー大王）の部下であったマケドニア地方出身のギリシア人で，大王の死後，エジプトの支配を継ぎ，プトレマイオス朝を創始した．

『原論』はラテン語圏，アラビア語圏にもたらされ，その後各地で二千数百年にわたって幾何学，いや数学そのもの基本となる書物であった．この書は 13 巻から成り，1〜6 巻は平面幾何，7〜9 巻は数論，10 巻は無理量，11〜13 巻は立体幾何を取り扱っている．

図形以外では，最大公約数を求める方法であるユークリッドの互除法，素数の個数は無限であることの背理法による証明，などが書かれている.『原論』では，概念の定義から始まり，公準（要請)・公理・命題とその作図・証明・結論という形式で書かれている． 公準とは公理のように自明ではないが，公理と同様，証明不可能な命題を意味する．近代ではこれを含めて公理とすることが一般的である.「公準」と訳されるものもここでは公理に統一する．

『原論』はこのような形式で数学を論述する．自明なことをまず明らかにし，そこからはじめて厳格な論証によって数学的現象を論述していく，この学問記述の方法は，二千年以上にわたって，数学のみならず学問一般の模範であった．いまもその精神は受け継がれるべきものである．

『原論』の原典としては例えば『ユークリッド　原論 (試案)』等にある．

ユークリッドの互除法　24 と 42 の最大公約数を求めようとすれば，いずれをも割り切る素数を見い出して，順に割っていくのだ．

$$(24,\ 42) = 2 \cdot (12,\ 21) = 2 \cdot 3 \cdot (4,\ 7) = 6$$

しかしこの方法には欠点がある．暗算で見つかるような素数ならよいが，6188 と 4709 のように少し大きい素数となると，なかなか難しい．ところが，つねに最大公約数を見い出すことのできる方法がある．それがユークリッドの互除法である．その根拠は次のような除法の式からの結論である．

定理 3 (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．

(1) 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

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

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) 除法の定理から $r_k > 0$ 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 1.3.1 $(6188, 4709)$ 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 1.3.2

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

1.4 一次不定方程式

1.4.1 不定方程式

未知数が x と y，あるいは x，y，z など 2 個以上あり，係数が整数である方程式，例えば

$$2x + 3y = 1,\ xy - 2x - 3y + 1 = 0,\ \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1,\ x^2 - 3y^2 = 1$$

のようなものでは，実数の解は無数にある．解が定まらないので不定方程式という．ところが，これらの方程式を満たす整数の組となると，有限個であったり，すべてが書き下せたり，あるいは存在しなかったり，様相が一変する．

整数係数の方程式を「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で活躍したとされるギリシア時代の数学者である．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．

$2x + 4y - 3z = 5$ のような一次不定方程式の整数解を考える．その整数解の集合がどのような構造をもっているのか，これが整数の主要な問題の一つである．

まず二変数の場合に調べ，それを一般化するという方向で考えよう．a と b が互いに素なとき一次不定方程式 $ax + by = k$ に関して次の事実が成立する．

(1) 整数解が存在する．

(2) すべての解を一般的な形にかける．

(3) 解を構成するアルゴリズムがある．

本節ではこれを示すいくつかの方法をまとめた後，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，解の存在と一般解構成のアルゴリズムが存在することを示す.

1.4.2 一次不定方程式の解の存在

定理 4

a と b は互いに素な整数である．このとき，一次不定方程式 $ax + by = k$ には整数解が存在する．■

$a > b \geqq 0$ のとき解をもつことが示せれば，例えば $a < 0$ なら $(-a)(-x) + by = k$ を考えればこの場合も整数解があることがわかる．よって a と b は $a > b \geqq 0$ である互いに素な整数とする．

この定理には三通りの証明法がある．それを実行し比較検討しよう．

b についての数学的帰納法による証明　$b = 0$ のとき, $(a, b) = 1$ より $a = 1$. ゆえに方程式は $1 \cdot x + 0 \cdot y = k$ となるから，解 $(k, 0)$ をもつ.

$0 \leqq j < b$ の j と $c > j$ で j と互いに素な任意の c に対して $cx + jy = k$ が解をもつとする．このとき $ax + by = k$ $(a > b \geqq 0)$ 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 $bX + rY = k$ は解 (X_0, Y_0) をもつ．この解に対して $\begin{cases} qx_0 + y_0 = X_0 \\ x_0 = Y_0 \end{cases}$ を解くと $\begin{cases} x_0 = Y_0 \\ y_0 = X_0 - qY_0 \end{cases}$ となる.

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

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

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 $ax + by = k$ は解をもつ. □

鳩の巣原理　有限個のもののなかに，ある条件を満たすものが存在することを示す根拠としてよく用いられるのが**鳩の巣原理**とか**部屋割り論法**とかいわれる次の原理である．同等な二つの形が用いられる.

(i) m 人を n 部屋に分ける．$m > n$ なら，2 人以上入る部屋が存在する.

(ii) n 人を n 部屋に分ける．相部屋になる者がないなら，すべての部屋に入る.

「鳩の巣原理」を用いる方法　$i = 0, \cdots, b - 1$ に対して ai を b で割った余りを r_i とする．各 r_i は 0 から $b - 1$ のどれかの値をとる．$0 \leqq i,\ j \leqq b - 1$ に対して r_i と r_j が $r_i = r_j$ とする.

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

より

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

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，この範囲の b の倍数は，$i - j = 0$ 以外にない. 対偶をとると,

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

$0 \leqq i \leqq b - 1$ の b 個の i に対して，同じ範囲の値 r_i が対応し，これらのうちに同じ値がない．鳩の巣原理によって r_i $(0 \leqq i \leqq b - 1)$ は 0 から $b - 1$ の各値を一つずつとる.

k を b で割って商が q，余りが s とする．$r_i = s$ となる i が存在する．つまり

$$ai = bq_i + s$$

となる i と q_i が存在する．$s = k - bq$ なので

$$ai + b(q - q_i) = k$$

つまり $(x,\, y) = (i,\, q - q_i)$ が $ax + by = k$ の解である． □

注意 1.4.1　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．

自然数の部分集合に最小要素が存在することを用いる証明　整数からなる集合 A を

$$A = \{\ ax + by \mid x,\ y \in \mathbb{Z}\}$$

で定める．A の要素で正のものからなる集合は自然数の部分集合なので, そのなかに最小のものが存在する．それを d とし，

$$d = ax_0 + by_0$$

とする．A の任意の要素 $ax + by$ を $d\ (> 0)$ で割る．

$$ax + by = dq + r\ (0 \leqq r < d)$$

である．これから

$$r = ax + by - dq = a(x - qx_0) + b(y - qy_0)$$

なので，r も A の要素である．$r > 0$ なら d が A の要素のなかで正で最小のものであることに矛盾する．よって $r = 0$ である．

A の任意の要素は d の倍数であることが示された．逆に d の倍数 $nd = a(nx_0) + b(ny_0)$ は A の要素である．

次に $a = a \cdot 1 + b \cdot 0$ なので $a \in A$，同じく $b \in A$ も成立する．よって a と b は d の倍数，つまり d は a と b の公約数である．ところが $(a,\, b) = 1$ なので，$d = 1$ である．

ゆえに A は整数の集合と一致する．したがって任意の整数 k に対して方程式 $ax + by = k$ には解が存在する． □

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 に関する数学的帰納法を組み合わせなければならない．不可能ではないが，もっと簡明にできないか．第二の証明も未知数の個数に関する数学的帰納法が必要になる．第三の証明はどうだろうか．これは明らかに一般の場合にそのまま拡張される．

一般の場合の証明　ここでは第三の場合の証明のなかで用いられた方法を取りだして補題とし，それを用いて一般の場合を証明しよう．

補題 1
整数からなる集合 A は次の性質を持つ．

$$a,\ b \in A \Rightarrow a - b \in A$$

このとき A は A に属する正で最小の要素の倍数全体からなる集合である．　■

証明　条件から $0 = a - a \in A$ である．また $-a = 0 - a$ から $a \in A$ なら $-a \in A$ である．したがって $a,\ b \in A$ に対して

$$a + b = a - (-b) \quad \in A$$

である．

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 d とする．A の任意の要素 x を d で割ったとき商が q，余りが r であるとする．

$$x = dq + r,\ 0 \leqq r < d$$

すると上に示したことから $dq \in A$ である．よって

$$r = x - dq \in A$$

ここでもし $r \neq 0$ なら d より小さい正数 r が A に属することになり d の最小性に反する．

$$\therefore \quad r = 0$$

つまり $x = dq$ となり，A の任意の要素は d の倍数であることが示された．d の倍数が A に属することはすでに示されている．　□

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

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = k \tag{1.2}$$

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　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 の任意の 2 つの要素の差が再び J に属することは明らかである．したがって J は J に含まれる正で最小の整数 e の倍数全体からなる集合である．

e は J の要素なので

$$e = \sum_{k=1}^{n} a_k l_k \tag{1.3}$$

となる l_k $(k = 1,\ 2,\ 3,\ \cdots,\ n)$ がある．したがって $d|e$ である．

一方 $a_1 = a_1 \cdot 1 + a_2 \cdot 0 + \cdots + a_n \cdot 0$ などから $a_i \in J$ が各 i について成り立つ．それらが e の倍数なので，e は $a_1,\ a_2,\ \cdots,\ a_n$ の公約数である．つまり $e|d$ である．

$$\therefore \quad e = d$$

J が d の倍数全体の集合であることが確定したので，方程式 (1.2) が解をもつことと，k が d の倍数であることの同値性が示された． □

1.4.3 一次不定方程式の一般解と解の構成

一次不定方程式

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

の一般解と解を構成するアルゴリズムの存在について考える．

まず「一般解」を正確に定義しておこう．二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．関数 $p(x),\ q(x)$ が存在し，この不定方程式の任意の解を

$$x = p(t),\ y = q(t)$$

と表す整数 t が存在し，逆に任意の整数 t に対して $x = p(t),\ y = q(t)$ がこの不定方程式の整数解となるとき，$x = p(t),\ y = q(t)$ 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．ただし二変数の場合は任意整数を表す変数の個数は 1 個であったが，一般には変数 $x,\ y,\ \cdots$ の個数から 1 減じた個数の任意整数が必要である．

例 1.4.1

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

の一般解を求める．$(32,\ 57,\ 68)$ の最大公約数を求めるときと同様に，いちばん小さい 32 で他の二数を割る．

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

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

$$l = 8(x + y + 2z) + 6y + z = 8x + 14y + 17z,\ m = y,\ n = x + y + 2z \tag{1.4}$$

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 (1.4) 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

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

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，二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．そのためにまず二変数の場合について，確認しなければならない．

二変数の場合の個別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て一組の解を構成する一般的な方法がある．

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．

(1) $a > b$ とし，$a = bq + r, (0 \leqq r < b)$ とする．

(2) $ax+by = (bq+r)x+by = rx+b(qx+y)$ であるから，$y' = qx+y$ とおくと方程式 $ax+by = 1$ は方程式 $rx + by' = 1$ となる．

(3) $rx+by' = 1$ 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一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. これは二変数の不定方程式の解を構成する一般的な方法である.

二次行列による解の構成　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, $|A| = sv - tu$ とおくと,

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

が成り立つ. $|A|$ のことを行列 A の「行列式」という.

以上を前提に, 二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 6

(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，

$$(x,\ y) = (x_0 - bt,\ y_0 + at),\ t \in \mathbb{Z}$$

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.

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

(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) $(x_0,\ y_0)$ 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 1.4.2 $127x + 52y = 1$ 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　このように二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) 二変数の場合，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．

$$a_1X_1 + r_2X_2 + \cdots + r_nX_n = k \tag{1.5}$$

ここで (1.5) 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 (1.5) の解が構成できればよい．ところが，方程式 (1.5) 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．

1.5　素数

1.5.1　素数の定義

本節では素数に関する基礎を学ぶ．自然数はある意味では単純に定義される．和，差，積の演算も，約数，倍数の概念も自然なものである．ところが，1 とそれ自身以外には約数をもたない数として定義される素数はかぎりなく奥が深い．素数はいまもってあるいはいよいよ人間にとって神秘な世界である．実際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．高校で習う整数というのは，こういう整数の世界の大海のほんの一滴である．基本事項を練習問題として多数掲載した．

本節では整数の約数，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．

定義 4

$a > 1$ 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． ■

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 a に対して $\dfrac{1}{a}$ のことを逆数という．整数のなかで 1 と -1 は「逆数もまた整数である」という性質を持つ．逆数もまた整数である数を**単数**という．有理整数の世界では 1 と -1 の二つのみが「単数」である．

1.5.2 素因数分解

さて，合成数は素数の積として順序を除けばただ一通りに表すことができる．これが**素因数分解の一意性**といわれる基本定理である．

定理 7

2 以上の整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　2 以上の整数 n に関する数学的帰納法で示す．

(1)　$n = 2$ のとき $2 = 2$ と素数 1 個の積なので成立．

(2)　a よりも小さい 2 以上の整数については定理が成立していると仮定する．

a の分解の可能性を示す．a が素数なら a 自身が素数 1 個の積である．a が合成数のとき．

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

と分解される．数学的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．

a の分解の一意性を示す．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 2 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 $b < a$ なので数学的帰納法の仮定からこの分解は順序を除いて一意である．よって a において定理が成立する．

(3)　(1)(2) より，2 以上の任意の整数に対して定理が成立することが示された． □

因数分解の一意性の別証明　次のような除法を用いない因数分解の一意性の証明がある．『数学のたのしみ』(2006 年夏号，日本評論社) の「素数・ゼータ関数・三角関数」(黒川重信) より紹介する．ツェルメロによるものである．

これは除法を用いていない．自然数の集合には最小のものが存在することだけを用いている．因数分解の可能性は同様なので，一意性のみ別証明をおこなう．

証明　異なる素因数分解をもつ自然数の集合を考える．この集合に属する最小の自然数を n とする．n は相異なる二つの因数分解をもつ．それを

$$n = p_1 p_2 \cdots p_r \qquad (p_1 \leqq p_2 \leqq \cdots \leqq p_r)$$
$$n = q_1 q_2 \cdots q_s \qquad (q_1 \leqq q_2 \leqq \cdots \leqq q_s)$$

とする．ここに $p_1, \cdots, p_r, q_1, \cdots, q_s$ は素数である．これが異なる因数分解ということは $r \neq s$ か，または $r = s$ で $p_i \neq q_i$ となる i が存在するか，のいずれかである．

また，$p_1, \cdots, p_r$ のいずれも $q_1, \cdots, q_s$ のいずれとも異なる．なぜなら，もし $p_i = q_j$ なら，これを約せば n より小さい数で，異なる因数分解をもつ自然数が得られ，n がそのような数のなかで最小であることに反する．

$p_1 < q_1$ とする．ここで自然数 m を

$$\begin{aligned} m &= n - p_1 q_2 \cdots q_s \\ &= (q_1 - p_1) q_2 \cdots q_s \end{aligned}$$

で定める．$m < n$ である．

この m の因数分解における因数 $q_1 - p_1$ は p_1 の倍数ではない．なぜならもし p_1 の倍数なら q_1 が p_1 の倍数となり互いに異なる素数であることに反する．よってこの因数分解に p_1 は現れない．

一方 m は

$$\begin{aligned} m &= n - p_1 q_2 \cdots q_s \\ &= p_1(p_2 \cdots p_r - q_2 \cdots q_s) \end{aligned}$$

でもある．この m の因数分解には，因数 p_1 が現れている．

よって m の二つの因数分解は相異なる因数分解である．

$m < n$ なので，n が異なる二つの因数分解をもつ最小の自然数であることと矛盾した．

したがって異なる二つの因数分解をもつ自然数は存在しない． □

除法の原理自身，除法が一意に出来ることを示すためには自然数の集合に最小のものが存在することを用いた．だから，除法を使うか使わないかにかかわらず，自然数の性質が土台になっている．だから，このツェルメロの証明は，自然数の集合には最小のものが存在することをいったん除法の原理にまとめることをせず，自然数の性質から直接示す，ともいえる．

例 1.5.1　素因数分解の一意性を用いた論証の例をあげよう．(1) は次のことに注意したい．p が素数であるということは，p の約数が 1 と p 以外にないということであり，これは整数 p 自身の内在的性質である．その性質をもつ p が，二つの整数の積 ab の約数になれば，a か b 少なくとも一方の約数になっている．これは p と他の整数との関係であり，外に向かう性質である．

(1) a と b を整数，p を素数とする．ab が p で割り切れれば，a または b が p で割り切れる．

(2) $\sqrt{2}$ は有理数ではない．

それぞれ次のように素因数分解の一意性を根拠に示すことができる．

(1) a も b が p で割り切れないとする．a と b を p で割った商を q_1，q_2，余りを r_1，r_2 とする．

$$\begin{cases} a = pq_1 + r_1 & (1 \leqq r_1 < p) \\ b = pq_2 + r_2 & (1 \leqq r_2 < p) \end{cases}$$

である．これから

$$ab = (pq_1 + r_1)(pq_2 + r_2) = p^2 q_1 q_2 + p(q_1 r_2 + q_2 r_1) + r_1 r_2$$

なので，ab が p の倍数なら r_1r_2 が p の倍数となる．

$$r_1r_2 = pN$$

とおく．$1 \leqq r_1,\ r_2 \leqq p-1$ なので，左辺の素因数分解に現れる素数はすべて $p-1$ 以下である．一方，右辺には素因数 p がある．これは素因数分解の一意性と矛盾する．よって a か b の少なくとも一つは p の倍数である． □

注意 1.5.1 (1) は実は，定理 2 の (4) の直接の結果である．

ab が p の倍数で，a は p の倍数ではないとする．p の約数は 1 と p しかないので,a と p の公約数は 1，つまり a と p は互いに素である．したがって定理 2 の (4) より b が p で割りきれる．

『数論初歩』は定理 2 などを基礎に素数を定義し，因数分解の一意性を示している．したがって (1) を素因数分解の一意性を根拠に導いてもそれは循環した論法に過ぎない．

ところが整数 p 素数であることを，

任意の整数 a と b に対し「p が ab の約数なら, p は a または b の約数である」が成り立つ．

ような整数として定義することもできる．この場合は逆にこの定義から因数分解の一意性が示せる．つまり素因数分解の一意性と，(1) は同値なのである．

どのように論を構成するかという問題よりも，どのような数学的現象とどのような数学的現象が同値であるかを確認することが重要である．このような問題は整域における整除問題として，環の一般論のなかで諸定義相互の関係は明らかにされる．

(2) 有理数であるとし，$\sqrt{2} = \dfrac{n}{m}$ とおく．これから

$$2m^2 = n^2$$

右辺 n^2 の因数分解のなかに素因数 2 は偶数個ある．左辺 $2m^2$ の因数分解のなかに素因数 2 は奇数個ある．これは素因数分解の一意性と矛盾する．よって $\sqrt{2}$ は有理数ではない． □

素数は無限に存在するのだろうか．この問題の解明は本質的にはユークリッドによってなされた．ユークリッドは『原論』のなかで，素数の個数が 3 個であるとして矛盾が起こるという形で議論した．つまり背理法である．ユークリッドは歴史に残る人のなかで，はじめて背理法を用いた人である．

定理 8
素数の個数は無限である． ■

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

$$a = p_1p_2\cdots p_n + 1$$

とおく．

定理 39 より a は素数の積に分解される．一方 a は $p_1,\ p_2,\ \cdots,\ p_n$ のいずれで割っても 1 余る．つまり，$p_1,\ p_2,\ \cdots,\ p_n$ は a の約数でない．よって a の素因数分解に現れる素数は $p_1,\ p_2,\ \cdots,\ p_n$ ではあり得ず，それら以外の素数である．これは $p_1,\ p_2,\ \cdots,\ p_n$ がすべての素数という仮定と矛盾する．ゆえに素数の数は無限である． □

1.6　演習問題

練習問題 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 (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.

練習問題 3 (解答 3)　次の不定方程式の一般解を求めよ.

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

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

練習問題 4 (解答 4)
$a=p^{\alpha}q^{\beta}r^{\gamma}\cdots$ 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 5 (解答 5)

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 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 6 (解答 6)

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

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

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,

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

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, これら n 個の数から 2 数を選ぶと ${}_nC_2$ 組みできるが, 各組の数の積 $a_1a_2,\ a_1a_3,\ \cdots,\ a_{n-1}a_n$ の最大公約数を d_2 とする. 一般に $a_1,\ a_2,\ \cdots,\ a_n$ のなかから k 数選ぶと ${}_nC_k$ 組できるが, 各組の数の積をとりそれらの数の最大公約数を d_k とする. 特に $a_1a_2\cdots a_n = d_n$ である.

(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. $a,\ b,\ c,\ \cdots$ の約数で二つずつ互いに素であるような $a_0,\ b_0,\ c_0,\ \cdots$ で

$$l=a_0b_0c_0\cdots$$

となるものが存在する.

練習問題 7 (解答 7)

(1) p が素数ならば二項係数 ${}_pC_k$ $(p>k>0)$ 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, ${}_{p^n}C_k$ $(p^n>k>0)$ は p^{n-l} で割り切れることを示せ.

練習問題 8　解答 8　$n!$ 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 9 (解答 9)

$\dfrac{m}{n}$ $(m>0,\ n>1)$ 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.

関連入試問題

入試問題 1 (解答 1) [98 お茶の水女子大]

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．

入試問題 2 (解答 2) ［91 阪大理系後期］

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 $f_1=0,\ f_2=1,\ f_n=f_{n-1}+f_{n-2}(n \geqq 3$ 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) $N \leqq 2+\log_{\frac{3}{2}} a$

入試問題 3 解答 3　［80 京大文系］

互いに異なる n 個（$n \geqq 3$）の正の数の集合 $S=\{a_1,\ a_2,\ \cdots,\ a_n\}$ が次の性質をもつという．

> 「S から相異なる要素 $a_i,\ a_j$ をとれば $a_i-a_j,\ a_j-a_i$ の少なくとも一方は必ず S に属する」

このとき，$a_1,\ a_2,\ \cdots,\ a_n$ の順序を適当に変えれば等差数列になることを示せ．

入試問題 4 解答 4　［80 京大理系］

互いに異なる n 個（$n \geqq 3$）の実数の集合 $S=\{a_1,a_2,\cdots,a_n\}$ が次の性質をもつという．

> 「S から相異なる要素 $a_i,\ a_j$ をとれば $a_i-a_j,\ a_j-a_i$ の少なくとも一方は必ず S に属する」

このとき，

(1) 次の 2 つのうちのいずれか一方が成り立つことを示せ．
　（イ）$a_i \geqq 0\ (i=1,\ 2,\ \cdots,\ n)$
　（ロ）$a_i \leqq 0\ (i=1,\ 2,\ \cdots,\ n)$

(2) $a_1,\ a_2,\ \cdots,\ a_n$ の順序を適当に変えれば等差数列になることを示せ．

入試問題 5 解答 5 ［85 お茶の水女子大］

自然数を要素とする空集合でない集合 G が次の条件 (i),(ii) を満たしているとする．

(i) $m,\ n$ が G の要素ならば，$m+n$ は G の要素である．

(ii) $m,\ n$ が G の要素で $m>n$ ならば，$m-n$ は G の要素である．

このとき G の最小の要素を d とすると $G=\{kd \mid k$ は自然数 $\}$ であることを証明せよ．

入試問題 6 (解答 6) ［08 奈良県立医大］

$p,\ q$ を互いに素な正整数とする．

(1) 任意の整数 x に対して，p 個の整数 $x-q$，$x-2q$，$\cdots$，$x-pq$ を p で割った余りはすべて相異なることを証明せよ．

(2) $x>pq$ なる任意の整数 x は，適当な正整数 $a,\ b$ を用いて $x=pa+qb$ と表せることを証明せよ．

入試問題 7 (解答 7) ［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．

入試問題 8 (解答 8) ［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．

入試問題 9 (解答 9) ［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

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

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．

入試問題 10 (解答 10) ［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．

入試問題 11 (解答 11) ［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．

入試問題 12 (解答 12) ［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．

入試問題 13 (解答 13) ［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．

入試問題 14 (解答 14) ［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 $\}$ は何個の元をもつか．

(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.

入試問題 15 (解答 15) ［08 名大理系］

次の問いに答えよ.

(1) $3x + 2y \leqq 2008$ を満たす 0 以上の整数の組 $(x,\ y)$ の個数を求めよ.

(2) $\dfrac{x}{2} + \dfrac{y}{3} + \dfrac{z}{6} \leqq 10$ を満たす 0 以上の整数の組 $(x,\ y,\ z)$ の個数を求めよ.

入試問題 16 (解答 16) ［88 群馬大］

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.

入試問題 17 (解答 17) ［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.

入試問題 18 (解答 18) ［98 上智大］

(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.

入試問題 19 (解答 19) ［98 京大後期文系］

$a,\ b,\ p,\ q$ 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.

入試問題 20 (解答 20) ［99 京大文後期］

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.

入試問題 21 (解答 21) ［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.

第2章　剰余類

2.1　合同式

2.1.1　合同式

整数の合同　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**であるといい，次のように記す.

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

ここで整数の部分集合 $m\mathbb{Z}$ を

$$m\mathbb{Z} = \{mx \mid x \in \mathbb{Z}\}$$

とする．集合 $m\mathbb{Z}$ の要素の和・差・積はふたたび $m\mathbb{Z}$ に属する．合同という関係はこれを用いて

$$a \equiv b \pmod{m} \quad \Longleftrightarrow \quad a - b \in m\mathbb{Z}$$

と集合論的にとらえることができる.

定理 9
整数 a と b が m を法として合同であることと，a と b を m で割った二つの余りが等しいことは同値である. ■

証明　整数 a と b が m を法として合同であるとし，$a - b = mq$ 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 $|r_1 - r_2| < m$ である．これは矛盾である.

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

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.
　逆に a と b を m で割った余りが等しいとする.

$$a = mq_1 + r,\ b = mq_2 + r$$

より $a - b = m(q_1 - q_2)$ である．つまり a と b は m を法として合同である. □

同値関係　集合 A の要素の間に，成り立つか成り立たないかがつねに確定する関係が定義されているとする．要素 a と b の間にこの関係が成り立つことを $a\sim b$ と表す．

(i) $a\sim a$.

(ii) $a\sim b$ なら $b\sim a$.

(iii) $a\sim b$, $b\sim c$ なら $a\sim c$.

が成り立つとき，「$\sim$」を「同値関係」という．

例 2.1.1　p を整数とする．整数 a, b について関係 $a\sim b$ を

$$a-b \text{ が } p \text{ の倍数}$$

で定める．$\sim$は同値関係である．

同値類　同値関係があると，同値なものをひとつの部分集合にまとめることができる．つまり A の要素 a と同値な要素からなる A の部分集合 $\overline{a}$ が一意に確定し，A のすべての要素はいずれかただひとつの $\overline{a}$ に属する．いいかえると，任意の $\overline{a}$ と $\overline{b}$ について $\overline{a}=\overline{b}$ か $\overline{a}\cap\overline{b}=\emptyset$ のいずれか一方が成立する．

a の属する部分集合 $\overline{a}$ を a の同値類という．このようにして得られる同値類の集合

$$A/\sim\ =\{\overline{a}\mid a\in A\}$$

を，集合 A の関係$\sim$に関する**商集合**という．

合同は同値関係

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　$a\equiv b \pmod{m}$ かつ $b\equiv c \pmod{m}$ ならば $a\equiv c \pmod{m}$

反射律，対称律は明らかである．推移律も $a-b$, $b-c\in m\mathbb{Z}$ なら

$$a-c=(a-b)+(b-c)\in m\mathbb{Z}$$

より成立する．つまり合同という関係は**同値関係**である．

剰余類　$\mathbb{Z}$ において，m を法として互いに合同な整数で一つの部分集合を作り，合同でないものは異なる部分集合になるようにして，$\mathbb{Z}$ を互いに共通部分のない，いくつかの部分集合の和にすることができる．その一つ一つの部分集合を m **を法とする類**といい，類に分けることを類別という．m を法とする類とは，m を法として互いに合同なすべての数の集合である．いいかえると m で割ったとき余りの等しい整数の集合である．つまり整数を m で割った余りで類別したのである．それぞれの部分集合を剰余類という．

剰余類の集合は，整数の集合 $\mathbb{Z}$ の合同という同値関係による商集合である．これを $\mathbb{Z}/m\mathbb{Z}$ と表す．あるいは $\mathbb{Z}_m$ と表すこともある．m を法とする類別では m 個の類に類別される．したがって $\mathbb{Z}_m$ は m 個の要素からなる集合である．

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．

剰余類の間の演算

定理 10

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

ならば

$$\begin{aligned} a \pm b &\equiv a' \pm b' \pmod{m} \\ ab &\equiv a'b' \pmod{m} \end{aligned} \tag{2.1}$$

一般に

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

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

$$f(a,\ b,\ c,\ \cdots) \equiv f(a',\ b',\ c',\ \cdots) \pmod{m} \tag{2.2}$$

が成り立つ． ■

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 (2.1) が示された．

(2.1) 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 (2.1) 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 (2.2) が示された． □

$\mathbb{Z}_m$ において整数 a の属する類を $\overline{a}$ と表す．m を明示する必要があるときは $\overline{a}_m$ と表そう．本定理の意味することは，$\mathbb{Z}_m$ における和と積を

$$\overline{a} + \overline{b} = \overline{a+b},\ \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

で適切に定義することができる，ということである．つまり $\mathbb{Z}_m$ の各類からどのように整数を選んで演算を考えても同じ結果になる．選び方によらず類のみで定まる類と類の間の演算が定義される．そして，分配法則

$$\overline{c}\left(\overline{a}+\overline{b}\right)=\overline{c}\cdot\overline{a}+\overline{c}\cdot\overline{a}\overline{b}$$

も成り立つ．加法と乗法の単位元は $\overline{0}$ と $\overline{1}$ である．これによって $\mathbb{Z}_m$ は有限個 (m 個) の要素からなる環である．

例 2.1.2 $m=6$ のとき．

$$\begin{aligned}
\overline{0} &= \{\cdots,\ -12,\ -6,\ 0,\ 6,\ 12,\ \cdots\}\\
\overline{1} &= \{\cdots,\ -11,\ -5,\ 1,\ 7,\ 13,\ \cdots\}\\
\overline{2} &= \{\cdots,\ -10,\ -4,\ 2,\ 8,\ 14,\ \cdots\}\\
\overline{3} &= \{\cdots,\ -9,\ -3,\ 3,\ 9,\ 15,\ \cdots\}\\
\overline{4} &= \{\cdots,\ -8,\ -2,\ 4,\ 10,\ 16,\ \cdots\}\\
\overline{5} &= \{\cdots,\ -7,\ -1,\ 5,\ 11,\ 17,\ \cdots\}
\end{aligned}$$

$$\mathbb{Z}_6=\mathbb{Z}/6\mathbb{Z}=\{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}\}$$

演算：

$$\overline{2}+\overline{5}=\overline{7}=\overline{1},\ \overline{2}+\overline{0}=\overline{2},\ \overline{2}+\overline{4}=\overline{6}=\overline{0}$$
$$\overline{2}\cdot\overline{5}=\overline{10}=\overline{3},\ \overline{2}\cdot\overline{1}=\overline{2}$$

ただし，

$$\overline{2}\cdot\overline{3}=\overline{6}=\overline{0}$$

なので乗法の逆元が存在するとはかぎらない．

有限体　乗法の逆元が存在すれば環は体になる．有理数体，実数体，複素数体はすべて四則演算ができる体であった．これらの体は，無数の要素からなっている．それに対して有限個の要素からなる体が存在する．これはガロアの発見であるが，現代の代数学の扉を開けるものであった．

定理 11

p を素数とする．$\mathbb{Z}_p=\mathbb{Z}/p\mathbb{Z}$ は p 個の要素からなる体である．　■

証明　$\overline{0}$ でない他の $\overline{a}$ に積の逆元が存在することを示せばよい．a として 1 から $p-1$ のいずれかをとることができる．このとき p と a は互いに素になる．したがって

$$pq+ab=1$$

となる整数 b が存在する．ところが

$$\overline{a}\cdot\overline{b}=\overline{ab}=\overline{1}$$

であるから，$\overline{b}=\overline{a}^{-1}$ となり $\overline{a}$ に逆元が存在した．よって $\mathbb{Z}_p$ は体である．　□

このように，剰余類という整数の部分集合を一つの要素と見なし，剰余類にあいだの演算を考える．ここが難しいところであり，また数学が現代に飛躍するところでもあった．今後，本質的なところではこの考え方で考察をすすめるが，必ずしも本質的でないところでは，古典的な考え方でいくようにしたい．

2.1.2　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**と呼ぶ．x_0 をこの合同式を満たす一つの整数とし, $x_1 \equiv x_0$ とすれば，定理 10 より

$$f(x_1) \equiv f(x_0) \equiv 0 \pmod{m}$$

である．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．

以下，合同方程式の解とはその合同方程式を満たす m を法とする剰余類のこととする．合同方程式を解くとは，それを満たす剰余類を求めることとする．簡単に「合同式を解く」ともいう．

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 個の値を代入してみればよい．つまりどんな合同方程式の解も，有限回の計算で求めることが出来る．その意味で解を有理整数にかぎるなら，必ず解ける．そのうえで，解の存在とより少ない手順で解を構成する方法を調べよう．

まず一次合同方程式について考える．

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．■

証明　$(a,\ m) = 1$ 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．

$(a,\ m) = d > 1$ のとき．

$$ax \equiv b \pmod{m} \tag{2.3}$$

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．(2.3) は定理 11 より

$$a'x \equiv b' \pmod{m'} \tag{2.4}$$

と同値である．ここで a' と m' は互いに素であるから (2.4) 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．(2.4) の解は

$$x = x_0 + m't \quad t \text{ は任意の整数} \tag{2.5}$$

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，(2.5) で t に対して，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 (2.3) 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 (2.3) 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．

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ \cdots &\quad \cdots \\ x &\equiv a_k \pmod{m_k} \end{aligned} \tag{2.6}$$

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

$$x = a_1 + m_1 t \tag{2.7}$$

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 (2.7) 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 (2.6) 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

$$M = m_1 M_1 = m_2 M_2 = \cdots = m_k M_k \tag{2.8}$$

とおく．M_n と m_n は互いに素なので

$$M_n t_n \equiv 1 \pmod{m_n} \quad (n = 1,\ 2,\ \cdots,\ k) \tag{2.9}$$

となる解 t_n $(n = 1,\ 2,\ \cdots,\ k)$ が存在する．このとき (2.6) 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，(2.9) 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 (2.6) 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． □

2.1.3　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

$$f(x) \equiv 0 \pmod{p} \tag{2.10}$$

は n 個より多くの解を有することはない．解の数とは (2.10) を満たす p を法とする剰余類の個数である． ■

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 12 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．(2.10) 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 37) 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 (2.10) 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 (2.10) 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，m を素因数分解して各因子を法とする方程式の解から具体的に構成することが出来る．

それを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, $m = p$ のときの解から帰納的に構成することが出来ることを示す．そのために，$m = p^e$ の解から $m = p^{e+1}$ のときの解が構成できることを示す (定理 15)．この定理によって，p のときから順次解を構成してゆくことによって，$m = p^e$ のときの解が構成できる．

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

e を自然数，p を素数とする．合同方程式

$$f(x) \equiv 0 \pmod{p^{e+1}} \tag{2.11}$$

の解は

$$f(x) \equiv 0 \pmod{p^e} \tag{2.12}$$

の解から構成することが出来る．

証明　(2.11) の解は法を p^e で考えることにより (2.12) を満たす．よって x が (2.11) の解であるために，(2.12) の解 x_0 を用いて

$$x = x_0 + p^e y \tag{2.13}$$

と表されることが必要である．

逆に方程式 (2.12) の各解 x_0 に対し (2.13) の形の数 x が方程式 (2.11) の解となるように y をとることができるか否かを判断し，可能ならそれを求めることができる．

一般に整数係数の整式 $f(x)$ 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．

この x に x_0 を，y に $p^e y$ を代入することにより

$$f(x) = f(x_0 + p^e y) = f(x_0) + p^e y f'(x_0) + p^{2e} y^2 \frac{f''(x_0)}{2!} + \cdots$$

を得る．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^{e+1} で割りきれる．

この結果合同方程式 $f(x) \equiv 0 \pmod{p^{e+1}}$ は

$$f(x_0) + p^e y f'(x_0) \equiv 0 \pmod{p^{e+1}}$$

と同値である．$f(x_0)$ は p^e で割り切れるので

$$\frac{f(x_0)}{p^e} + y f'(x_0) \equiv 0 \pmod{p} \tag{2.14}$$

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 (2.14) は p を法としてただ一つの解をもつ．それを $y_0 \pmod{p}$ とする．

$$x \equiv x_0 + p^e y_0 \pmod{p^{e+1}}$$

は (2.11) の解である．

(2)　$f'(x_0) \equiv 0 \pmod{p}$ のとき．このときは (2.14) は $\dfrac{f(x_0)}{p^e}$ がさらに p で割り切れなければ解がない．$\dfrac{f(x_0)}{p^e}$ が p で割り切れるなら p の剰余系の任意の y が解になる．つまり

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

が (2.11) を満たす．すなわち $f'(x_0) \equiv 0 \pmod{p}$ となる (2.12) の解 x_0 に対して，(2.13) の形の数 x は，$f(x_0) \not\equiv 0 \pmod{p^{e+1}}$ なら y によらず (2.11) の解でなく，$f(x_0) \equiv 0 \pmod{p^{e+1}}$ なら (2.11) の p^{e+1} を法とする p 個の解を与える．　□

例 2.1.3　$p \neq 2$ 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，

$$\begin{aligned} f(x) &\equiv 0 \pmod{p^e} && (2.15)\\ f(x) &\equiv 0 \pmod{q^f} && (2.16)\\ &\cdots \end{aligned}$$

がそれぞれ l, l', $\cdots$ 個の解をもつとすれば，

$$f(x) \equiv 0 \pmod{m} \qquad (2.17)$$

は $ll' \cdots$ 個の解をもつ．それは

$$\begin{aligned} x &\equiv \alpha \pmod{p^e}\\ x &\equiv \beta \pmod{q^f} && (2.18)\\ \cdots &\quad \cdots \end{aligned}$$

から求められる．ここで α, β, $\cdots$ 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 (2.17) の解ならば (2.15)，(2.16) の解である．したがって (2.18) を満たす．

逆に (2.18) を満たす x は，(2.15)，(2.16) を満たすから，(2.17) を満たす． □

例 2.1.4

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

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，

$$\left.\begin{matrix} x \equiv 1\\ x \equiv 1 \end{matrix}\right\} \quad \left.\begin{matrix} x \equiv 1\\ x \equiv -1 \end{matrix}\right\} \quad \left.\begin{matrix} x \equiv -1\\ x \equiv 1 \end{matrix}\right\} \quad \left.\begin{matrix} x \equiv -1\\ x \equiv -1 \end{matrix}\right\} \begin{matrix}\pmod 3\\ \pmod 4\end{matrix}$$

から求められる．

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

2.2 オイラーの関数

2.2.1 オイラーの関数 $\varphi(n)$

自然数 1, 2, $\cdots$, n のなかにある n と互いに素な整数 x の個数を $\varphi(n)$ で表す．例えば，

$$\varphi(1) = 1, \qquad (x = 1)$$

$$\varphi(2) = 1, \qquad (x = 1)$$
$$\varphi(3) = 2, \qquad (x = 1,\ 2)$$
$$\varphi(4) = 2, \qquad (x = 1,\ 3)$$
$$\varphi(5) = 4, \qquad (x = 1,\ 2,\ 3,\ 4)$$
$$\varphi(6) = 2, \qquad (x = 1,\ 5)$$

$\varphi(n)$ を**オイラーの関数**という．$\varphi(n)$ 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．

n を法とする合同関係による商集合 $\mathbb{Z}_n$ は n 個の要素からなる集合であった．

$$\mathbb{Z}_n = \{\overline{0},\ \overline{1},\ \cdots,\ \overline{n-1}\}$$

である．さて，一つの $\overline{k}$ 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 $\overline{k}$ 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 $\overline{k}$ が n と互いに素である」ということが意味を持つ．n と互いに素な剰余類 $\overline{k}$ 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．既約類は $\varphi(n)$ 個ある．

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

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

が成り立つとき，**乗法的関数**という．

定理 17

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

$$\varphi(ab) = \varphi(a)\varphi(b) \tag{2.19}$$

が成り立つ． ■

証明　a を法とする既約類 $\overline{k}_a$ ，b を法とする既約類 $\overline{l}_b$ をとる．

集合

$$A = \{bx + ay \,|\, x \in \overline{k}_a,\ y \in \overline{l}_b\}$$

を考える．これは ab を法とする剰余類を定める．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 $A = \overline{bk + al}_{ab}$ 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 $\overline{k}_a$ 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 を法とする任意の既約類 $\overline{m}_{ab}$ 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 $\overline{m}_{ab}$ 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 $\overline{k}_a$ と b を法とする既約類 $\overline{l}_b$ の一組と ab を法とする既約類 $\overline{m}_{ab}$ は一対一に対応する．この組は $\varphi(a)\varphi(b)$ 個あるので (2.19) 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．なお中国の剰余定理 13 を用いれば証明は簡明である．すなわち次のようになる．

別証明 いま α_1, α_2, $\cdots$, α_m , $m = \varphi(a)$ および β_1, β_2, $\cdots$, β_n , $n = \varphi(b)$ をそれぞれ a と b を法とする既約剰余系の一組とする．$mn = \varphi(a)\varphi(b)$ 個の組合せの一つ α_i, β_j に対して

$$\gamma \equiv \alpha_i \pmod{a}\ , \quad \gamma \equiv \beta_j \pmod{b} \tag{2.20}$$

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，(2.20) となる α_i, β_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 α_i, β_j の組の間に一対一の対応が成り立つ．したがって (2.19) が示された．
□

$\varphi(n)$ は次の定理によって計算される．

定理 18
n を素数べきに分解して

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

とすると

$$\varphi(n) = n\left(1 - \frac{1}{p}\right)\left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{r}\right)\cdots \tag{2.21}$$

が成り立つ． ■

証明 定理 17 から

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

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

つまり，(2.21) が示された． □

例 2.2.1　$a=3,\ b=5$ とする．

$$
\begin{aligned}
\alpha &= 1,\ 2,\ \beta = 1,\ 2,\ 3,\ 4 \qquad \varphi(3)=2,\ \varphi(5)=4 \\
\gamma &= 1,\ 2,\ 4,\ 7,\ 8,\ 11,\ 13,\ 14 \qquad \varphi(15)=8
\end{aligned}
$$

であるが, $5\alpha+3\beta \pmod{15}$ と，別証の γ を計算すると

α	1	1	1	1	2	2	2	2
β	1	2	3	4	1	2	3	4
$5\alpha+3\beta$	8	11	14	2	13	1	4	7
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記号であった．$d=1,\ n$ のときも $d|n$ である．$\sum_{d|n}$ と書けば，和は n のすべての約数 (1 も n も含む) にわたるものとする．

定理 19

$$
\sum_{d|n}\varphi(d) = n \tag{2.22}
$$

である． ■

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 $\varphi\left(\frac{n}{d}\right)$ 個ある．

なぜなら

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

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

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ので

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

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ずつ数えられる．

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

d が n の約数全体を動くとき $\frac{n}{d}$ も n の約数全体を動くので，(2.22) が示された． □

例 2.2.2　$n = 15$ とする.

d	x	$\varphi\left(\frac{n}{d}\right)$
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

例 2.2.3　$n = 12$ とする.

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

2.2.2　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

$$\sum_{d|n} F(d) = G(n) \tag{2.23}$$

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 2.2.4

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

補題 2

$n > 1$ なら

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

である. ■

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，つまり各素数のべき指数が 2 以上のものを除くと，

$$\begin{aligned}\sum_{d|n}\mu(d) &= \mu(1)+\{\mu(p_1)+\mu(p_2)+\cdots+\mu(p_k)\}\\ &\quad +\{\mu(p_1p_2)+\mu(p_1p_3)+\cdots+\mu(p_{k-1}p_k)\}\\ &\quad +\cdots\\ &\quad +\mu(p_1p_2\cdots p_k)\\ &= 1-k+{}_k\mathrm{C}_2-{}_k\mathrm{C}_3+\cdots+(-1)^k\\ &= (1-1)^k = 0\end{aligned}$$

□

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 $F(x)$, $G(x)$ について二つの命題：

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

は同値である．■

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 が d の約数全体を動くと，$\dfrac{n}{d}$ は $\dfrac{n}{\delta}$ の約数全体を動く．したがって和の順序を逆にして

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

補題 2 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 (2.22) 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

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

2.3 1の n 乗根

2.3.1 1の n 乗根

1 の n 乗根，すなわち方程式

$$x^n - 1 = 0 \tag{2.24}$$

の根は n 個ある．それらは

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},\ (k = 0,\ 1,\ \cdots,\ n-1) \tag{2.25}$$

である．これらはすべて偏角が異なり異なる複素数である．しかも n 乗すると 1 になるので，方程式 (2.24) の解である．したがってこの n 個の複素数が n 次方程式 (2.24) の根のすべてであることがわかる．

簡単のために

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

とおく．ド・モアブルの定理より，(2.25) は

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

と表される．ここで $\alpha^n = 1$ なので，(2.25) 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 (2.25) 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 になるものを **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

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \tag{2.26}$$

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 (2.26) の $\dfrac{2k\pi}{n}$ 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．

α^k が原始 n 乗根となることと，n と互いに素な k を用いて α^k と表されることが同値であることが示された．よってその個数は $\varphi(n)$ 個である． □

ちなみに α^l は原始 n' 乗根である．これを次の定理 22 の証明に用いる．

例 2.3.1　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．$\dfrac{-1\pm\sqrt{3}i}{2}$ 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，

$$F_n(x) = \frac{(x^n-1)(x^{\frac{n}{pq}}-1)(x^{\frac{n}{qr}}-1)\cdots\cdots}{(x^{\frac{n}{p}}-1)(x^{\frac{n}{q}}-1)\cdots(x^{\frac{n}{pqr}}-1)\cdots} \tag{2.27}$$

$$= \prod_{d|n}(x^{\frac{n}{d}}-1)^{\mu(d)} \tag{2.28}$$

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 (2.28) 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 (2.28) より明らかに整数である．式 (2.27) 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 2.3.2

$$\begin{aligned} F_6(x) &= \frac{(x^6-1)(x-1)}{(x^2-1)(x^3-1)} = x^2 - x + 1 \\ F_{12}(x) &= \frac{(x^{12}-1)(x^2-1)}{(x^6-1)(x^4-1)} = x^4 - x^2 + 1 \end{aligned}$$

p が素数なら

$$\begin{aligned} F_p(x) &= \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + 1 \\ F_{p^e}(x) &= \frac{x^{p^e} - 1}{x^{p^{e-1}} - 1} = x^{p^{e-1}(p-1)} + x^{p^{e-1}(p-2)} + \cdots + 1 \end{aligned}$$

2.4　フェルマの小定理

2.4.1　フェルマの小定理

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

$$a^{\varphi(m)} \equiv 1 \pmod{m} \tag{2.29}$$

が成り立つ．

とくに $m = p$ (素数) に対しては, $(a,\ p) = 1$ のとき

$$a^{p-1} \equiv 1 \pmod{p} \tag{2.30}$$

が成り立つ．こちらの方を**フェルマの小定理**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，その集合の元にすべて a を乗じた整数の集合は確かに ax と合同な整数の全体になっており, 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

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

の各元は 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．

よって，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 (2.29) 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小定理 (2.30) が成り立つ． □

例 2.4.1

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

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 $0 \leqq r < e$ 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． □

2.4.2 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 25

$\dfrac{m}{n}$ は既約真分数で分母 n は $(10,\ n) = 1$ とする．このとき $\dfrac{m}{n}$ 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 いま

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

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 $\dfrac{m}{n}$ は循環節の桁数 e の循環小数に展開されている．

逆に $\dfrac{m}{n}$ 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，より明らか． □

$(10,\ n) = 1$ 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 $\dfrac{10^k m}{n}$ を約分して既約分数 $\dfrac{m'}{n'}$ 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， $\dfrac{m'}{n'}$ は e 桁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 2.4.2　$n = 7$ とする．

$$10^1 \equiv 3 \pmod 7,\ 10^2 \equiv 2 \pmod 7,\ 10^3 \equiv 6 \pmod 7,$$
$$10^4 \equiv 4 \pmod 7,\ 10^5 \equiv 5 \pmod 7,\ 10^6 \equiv 1 \pmod 7$$

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．

$$\begin{aligned} 10^1 &= 3 + 7 \cdot 1 \\ 10^2 &= 2 + 7 \cdot 14 \\ 10^3 &= 6 + 7 \cdot 142 \\ 10^4 &= 4 + 7 \cdot 1428 \\ 10^5 &= 5 + 7 \cdot 14285 \\ 10^6 &= 1 + 7 \cdot 142857 \end{aligned}$$

$$\begin{aligned} \therefore\ \frac{1}{7} &= \frac{142857}{10^6 - 1} \\ &= \frac{142857}{10^6}\left\{1 + \frac{1}{10^6} + \frac{1}{10^{12}} + \cdots\right\} \\ &= 0.\dot{1}42857\dot{} \end{aligned}$$

以下は上の 7 で割った余りと商を用いて作られる．

$$\begin{aligned} \frac{3}{7} &= \frac{10^1}{7} - 1 &&= 0.\dot{4}28571\dot{} \\ \frac{2}{7} &= \frac{10^2}{7} - 14 &&= 0.\dot{2}85714\dot{} \\ \frac{6}{7} &= \frac{10^3}{7} - 142 &&= 0.\dot{8}57142\dot{} \\ \frac{4}{7} &= \frac{10^4}{7} - 1428 &&= 0.\dot{5}71428\dot{} \\ \frac{5}{7} &= \frac{10^5}{7} - 14285 &&= 0.\dot{7}14285\dot{} \end{aligned}$$

このうち $\dfrac{6}{7}$ はじつは

$$\frac{6}{7} + \frac{1}{7} = 1 = 0.\dot{9} \quad \text{より} \quad 0.\dot{9} - 0.\dot{1}42857\dot{} = 0.\dot{8}57142\dot{}$$

としても求まる．

例 2.4.3　$n = 13$ とする．10^7 以降は不要であるが書く．

$$\begin{aligned}
10^1 &= 10 + 13 \cdot 0 \\
10^2 &= 9 + 13 \cdot 07 \\
10^3 &= 12 + 13 \cdot 076 \\
10^4 &= 3 + 13 \cdot 0769 \\
10^5 &= 4 + 13 \cdot 07692 \\
10^6 &= 1 + 13 \cdot 076923 \\
10^7 &= 10 + 13 \cdot 0769230 \\
10^8 &= 9 + 13 \cdot 07692307 \\
10^9 &= 12 + 13 \cdot 076923076 \\
10^{10} &= 3 + 13 \cdot 0769230769 \\
10^{11} &= 4 + 13 \cdot 07692307692 \\
10^{12} &= 1 + 13 \cdot 076923076923
\end{aligned}$$

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．

$$\begin{aligned}
\frac{10}{13} &= \frac{10^1}{13} - 0 &&= 0.\dot{7}6923\dot{0} \\
\frac{9}{13} &= \frac{10^2}{13} - 07 &&= 0.\dot{6}9230\dot{7} \\
\frac{12}{13} &= \frac{10^3}{13} - 076 &&= 0.\dot{9}2307\dot{6} \\
\frac{3}{13} &= \frac{10^4}{13} - 0769 &&= 0.\dot{2}3076\dot{9} \\
\frac{4}{13} &= \frac{10^5}{13} - 07692 &&= 0.\dot{3}0769\dot{2}
\end{aligned}$$

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

$$\begin{aligned}
\frac{7}{13} &= \frac{2\cdot 10^1}{13} - 1 &&= 0.\dot{5}3846\dot{1}\\
\frac{5}{13} &= \frac{2\cdot 10^2}{13} - 15 &&= 0.\dot{3}8461\dot{5}\\
\frac{11}{13} &= \frac{2\cdot 10^3}{13} - 153 &&= 0.\dot{8}4615\dot{3}\\
\frac{6}{13} &= \frac{2\cdot 10^4}{13} - 1538 &&= 0.\dot{4}6153\dot{8}\\
\frac{8}{13} &= \frac{2\cdot 10^5}{13} - 15384 &&= 0.\dot{6}1538\dot{4}\\
\frac{2}{13} &= \frac{2\cdot 10^5}{13} - 153846 &&= 0.\dot{1}5384\dot{6}
\end{aligned}$$

2.4.3 算術級数の定理

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.『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.

歴史的に無限等差数列のことを算術級数，無限等比数列のことを幾何級数という.

算術級数中の素数の分布　算術級数 $a+dk$ $(k=0,\ 1,\ 2,\ \cdots)$ のなかにどのように素数が分布しているのか．いくつかの実験をしてみよう．初項 a と公差 d が互いに素でなければすべてが最大公約数の倍数になるので，素数の分布を考えるときは互いに素とする.

$$\begin{aligned}
&a=1,\ d=4 && 1,\ 5,\ 9,\ 13,\ 17,\ 21,\ 25,\ 29,\ 33,\ 37,\ 41,\ \cdots\\
&a=3,\ d=4 && 3,\ 7,\ 11,\ 15,\ 19,\ 23,\ 27,\ 31,\ 35,\ 39,\ 43,\ \cdots\\
&a=1,\ d=3 && 1,\ 4,\ 7,\ 10,\ 13,\ 16,\ 19,\ 22,\ 25,\ 28,\ 31,\ \cdots\\
&a=2,\ d=3 && 2,\ 5,\ 8,\ 11,\ 14,\ 17,\ 20,\ 23,\ 26,\ 29,\ 32,\ \cdots
\end{aligned}$$

となり，初項と公差が互いに素な算術級数中には素数が無数に存在するように見える．実は次の命題が成り立つ.

定理 26 (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)．この定理の証明は簡単ではない．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．それは『数論初歩』の範囲を越える．ただ初項が $a=1$ の場合，解析的方法を用いないで証明することができる.

定理 27
m を任意の自然数とする． $1+mt$ $(t\in\mathbb{Z})$ 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．つまり，3, 7, $\cdots$, p が $4n-1$ 型の素数の全体であるとする．これら $4n-1$ 型の素数全体の積に 4 をかけ 1 を減じた数を a とする．つまり

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

a は $a \equiv -1 \pmod 4$ なので奇数である．したがってその約数はすべて奇数であるから，4 を法として 1 または -1 と合同である．$4k+1$ 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 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，3, 7, $\cdots$, p 以外の素数である．つまり 3, 7, $\cdots$, p が $4n-1$ 型の素数のすべてであるという仮定と矛盾した．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

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

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

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

a の素因数 q は奇数であるから 2 ではない．x^2+1 型の数の素因数はすべて $4n+1$ 型の素数であるから，q は $4n+1$ 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 5, 13, $\cdots$, p 以外の $4n+1$ 型の素数である．

これは 5, 13, $\cdots$, p が $4n+1$ 型の素数のすべてであるという仮定と矛盾する．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．

つまり，m を 2 以上の任意の整数とするとき，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とを証明する．

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 22 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．a を $F_m(a)\neq\pm1$ であるような任意の整数とする．このとき $F_m(a)$ の素因数は m の約数，または $mt+1$ の型のものにかぎられることを示す．

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．

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

において，$F_m(a)$, $G(a)$ は整数であるから，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

$$a^m\equiv1 \pmod{p}$$

a の指数を e とする．定理 24 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)

$$x^m-1=(x^e-1)F_m(x)H(x) \tag{2.31}$$

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．等式 (2.31) の両辺を 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 $a^e\equiv1 \pmod{p}$ を用いれば

$$f\equiv F_m(a)H(a)\equiv0 \pmod{p}$$

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，$F_m(a)\neq\pm1$ 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，$a^m\equiv1 \pmod{p}$ 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．

$F_m(a) \neq \pm 1$ を仮定したが，$F_m(a) = \pm 1$ となる a は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． □

例 2.4.4 $m = 12$ 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

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

2.5 原始根と指数

2.5.1 原始根

5 で割った余りから 0 を除いた

$$1,\ 2,\ 3,\ 4$$

のうち，2 と 3 は特別である．なぜか.

$$\begin{array}{ll} 2^1 = 2 & \\ 2^2 = 4 \equiv 4 \pmod{5} & \\ 2^3 = 8 \equiv 3 \pmod{5} & , \\ 2^4 = 16 \equiv 1 \pmod{5} & \end{array} \qquad \begin{array}{l} 3^1 = 3 \\ 3^2 = 9 \equiv 4 \pmod{5} \\ 3^3 = 27 \equiv 2 \pmod{5} \\ 3^4 = 81 \equiv 1 \pmod{5} \end{array}$$

と順にべきを取っていくと 1, 2, 3, 4 をすべて作る．1 と 4 はそうではない.

2 と 3 を「5 を法とする原始根」という.

剰余系の原始根　13 を法とする剰余系から 0 を除いた各剰余を横に並べる．それぞれ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．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「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．

上の集合 K は p 個の元からなる有限集合であるが，和・差・積・商が定まる有限体である．また K から 0 を除いた集合 $K^\times$ は乗法に関して群であり，要素の個数は $p-1$ 個である．

次の定理が示すように，一般に素数 p に対して原始根が存在し，その原始根の順次のべきから $K^\times$ のすべての元が得られる．つまり, 原始根はこの「群を生成する」元である．

定理 28

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

$$a^0 = 1,\ a^1,\ \cdots,\ a^{m-1} \tag{2.32}$$

はいずれも

$$x^m \equiv 1 \pmod{p} \tag{2.33}$$

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 (2.32) が (2.33) 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 (2.32) 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 (2.33) 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 24 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 2 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．練習問題 6 の (6) のように $l=m_0n_0$, $(m_0,\ n_0)=1$ 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 $m_0n_0=l$．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 (2.32) 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 2.5.1 $\varphi(13-1)=4$ なので四つある．実際 $2,\ 6,\ 7,\ 11$

2.5.2 指数

定理 28 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 2.5.2　$p = 13$ 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

定理 29

素数 p を法として原始根 r を底とするとき,

$$\begin{aligned} &\mathrm{Ind}\,.ab \equiv \mathrm{Ind}\,.a + \mathrm{Ind}\,.b, \\ &\mathrm{Ind}\,.a^n \equiv n\,\mathrm{Ind}\,.a\ . \end{aligned} \qquad (\mathrm{mod}.\ p-1)$$

が成り立つ. ■

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

$$ab \equiv r^{\alpha+\beta} \pmod{p}$$

$$\therefore \quad \mathrm{Ind}\,.ab \equiv \alpha+\beta \equiv \mathrm{Ind}\,.a + \mathrm{Ind}\,.b \pmod{p-1}$$

また

$$\mathrm{Ind}\,.a^n = \mathrm{Ind}\,.a \cdot a^{n-1} \equiv \mathrm{Ind}\,.a + \mathrm{Ind}\,.a^{n-1} \pmod{p-1}$$

より，帰納法で

$$\mathrm{Ind}\,.a^n \equiv n\,\mathrm{Ind}\,.a \pmod{p-1}$$

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 2.5.3 $p = 13$ のとき． $7x \equiv 10 \pmod{13}$ を解こう．底を 2 とする指数をとる．

$$\mathrm{Ind}\,.7 + \mathrm{Ind}\,.x \equiv \mathrm{Ind}\,.10 \pmod{12}$$

指数表から

$$11 + \mathrm{Ind}\,.x \equiv 10 \pmod{12}$$

$$\therefore \quad \mathrm{Ind}\,.x \equiv -1 \equiv 11 \pmod{12}$$

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 30

p を素数とし, $a \not\equiv 0 \pmod{p}$ とする．

二項合同方程式

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

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

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

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

$$n \cdot \mathrm{Ind}_r\, x \equiv \mathrm{Ind}_r\, a \pmod{p-1} \tag{2.34}$$

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 (2.34) 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．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 2.5.4　$n=2,\ p=7$ 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．

2.6　演習問題

練習問題 10 (解答 10)

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 11 (解答 11)

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 12 (解答 12)

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 13 (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 14 (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 15 (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 の倍数であることを示せ.

(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 16 (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.

練習問題 17 (解答 17)

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

を解け.

練習問題 18 (解答 18)
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 19 (解答 19)
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.

練習問題 20 (解答 20)
次の合同方程式を解け.

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

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

練習問題 21 (解答 21) 『初等整数論講義』(高木貞治著), 39 ページ〔問題 1〕より.
$\alpha\equiv 1\,(\mathrm{mod.}\ 8)$ 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 2^e を法とする解は四つあり, その一つを x_0 とすれば 4 解は

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

と表されることを示せ.

練習問題 22 (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 23 (解答 23)
xy 平面上, 不等式 $0<x\leqq 12$, $0<y\leqq 12$ で定まる領域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 24 (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 を超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.

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

を示せ. ただし $[x]$ は x を超えない最大の整数を表す.

練習問題 25 (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 2 の別証を考えよ.

練習問題 26 (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．

練習問題 27 (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 28 (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 29 (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 30 (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．

以下の練習問題は,『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 31 (解答 31)

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．

練習問題 32 (解答 32)

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．

練習問題 33 (解答 33)

因数分解

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

を活用して，任意の自然数 m に対して $(m!)^2+1$ 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．

練習問題 34 (解答 34)

$n=91=7\cdot 13$ のとき，$\dfrac{1}{91}$ から $\dfrac{90}{91}$ を循環節が同じもので分類せよ．

練習問題 35 (解答 35)

$p=41$ 法とする原始根を一つ求めよ．

練習問題 36 (解答 36)

例 2.5.2 の表を活用して $p=13,\ r=2$ 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 37 (解答 37)

例 2.5.2 の表を活用して 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 38 (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 39 (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 40 (解答 40)

$$\mathrm{Ind}_r\ a \equiv \frac{\mathrm{Ind}_{r'}\ a}{\mathrm{Ind}_{r'}\ r} \pmod{p-1}$$

練習問題 41 (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 42 (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)

関連入試問題

入試問題 22 (解答 22) ［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．

入試問題 23 (解答 23) ［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．

入試問題 24 (解答 24) ［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．

入試問題 25 (解答 25) ［01 京大文系前期］
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．

入試問題 26 (解答 26) ［06 横浜市大 2 番］

N を自然数とし，$\phi(N)$ を N より小さくかつ N と互いに素な自然数の総数とする．すなわち

$$\phi(N) = \sharp\,\{n \mid n \text{は自然数}, 1 \leqq n < N, gcd(N,\ n) = 1\ \}$$

で，オイラー関数と呼ばれている．ここに $gcd(a,\ b)$ は a と b の最大公約数を，$\sharp\ A$ は集合 A の要素の総数を意味する．例えば，

$$\phi(6) = \sharp\,\{1,5\} = 2,\ \phi(15) = \sharp\,\{1,2,4,7,8,11,13,14\} = 8$$

である．このとき以下の問いに答えよ．

(1) p と q を互いに異なる素数とし $N = pq$ とおく．

(i) N より小さい自然数 n で，$gcd(N,\ n) \neq 1$ となるものを全て求めよ．

(ii) $\phi(N)$ を求めよ．

(2) p と q を互いに異なる素数とし $N = pq$ とおく．今 N と $\phi(N)$ が**あらかじめわかつているとき**，p と q を解としてもつ二次方程式を N や $\phi(N)$ 等を用いて表せ．

(3) $N = 84773093$ および $\phi(N) = 84754668$ であるとき，$N = pq\ (p > q)$ となる素数 p および q を求めよ (求めた p および q が素数であることを示さなくてよい)．

ただし, 必要に応じて以下の数表を使つてもよい．

$$320^2 = 102400\,;\, 322^2 = 103684\,;\, 324^2 = 104976\,;$$
$$326^2 = 106276\,;\, 328^2 = 107584\,;\, 330^2 = 108900$$

入試問題 27 (解答 27) ［70 東大理系］

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．

入試問題 28 (解答 28) ［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) $\quad k = 1,\ 2,\ \cdots,\ n$ に対し, ${z_k}^p = 1$ かつ, $z_k \neq 1$

(ロ) $\quad z_1 z_2 \cdots z_n = 1$

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.

入試問題 29 (解答 29) ［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.

$$G \text{ の任意の元 } z,\ w \text{ の積 } zw \text{ は再び } G \text{ の元である.}$$

(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.

入試問題 30 (解答 30) ［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.

入試問題 31 (解答 31)　［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.

第3章　相互法則

3.1　平方剰余

3.1.1　平方剰余と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 を法とする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．

ある整数 a が整数 b を法として平方剰余であるか平方非剰余であるかということと，整数 b が整数 a を法として平方剰余であるか平方非剰余であるかということとの間には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『数論初歩』全体でもいちばん山場の定理である．

ぜひ高校生に「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

平方剰余　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

$$\left(\frac{a}{p}\right) = (-1)^{\mathrm{Ind}\,.a} \tag{3.1}$$

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 (3.1) 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 31 (オイラーの規準)
3 以上の素数 p と整数 a に対して

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

が成り立つ． ■

証明 a が平方剰余であるための必要十分条件は定理 30 から

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

である．
ゆえに $\left(\frac{a}{p}\right) = 1$ ならば，$a^{\frac{p-1}{2}} \equiv 1 \pmod p$ で一致．
また $\left(\frac{a}{p}\right) = -1$ 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 の任意の元 r に対して

$$rs \equiv a \pmod p$$

となる A の元 s がただ一つ存在する．この s を r の「共役」と呼ぼう．
$\left(\frac{a}{p}\right) = 1$ 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 の元で $x^2 \equiv a \pmod p$ を満たすものは定理 14 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

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

$\left(\frac{a}{p}\right) = -1$ 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 $\left(\frac{1}{p}\right) = 1$ なので

$$(p-1)! \equiv -1 \pmod{p}$$

これはウイルソンの定理といわれているものである.

これをあわせると上記の場合分けは

$$\left.\begin{array}{l} \left(\frac{a}{p}\right) = 1 \text{ ならば, } a^{\frac{p-1}{2}} \equiv 1 \\ \left(\frac{a}{p}\right) = -1 \text{ ならば, } a^{\frac{p-1}{2}} \equiv -1 \end{array}\right\} \pmod{p}.$$

これがオイラーの規準である. □

注意 3.1.1 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 3.1.1 $p = 5$ のとき.

$$2^1 \equiv 2,\ 2^2 \equiv 4,\ 2^3 \equiv 3,\ 2^4 \equiv 1 \pmod{5}$$

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. $\frac{p-1}{2} = 2$ 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.

3.1.2 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 32

すべての正の整数 n は

$$n = {x_1}^2 + {x_2}^2 + {x_3}^2 + {x_4}^2 \quad (0 \leqq x_1,\ x_2,\ x_3,\ x_4)$$

と，0 を許した四つの平方数の和として表すことができる. ■

証明　次の恒等式

$$(x_1{}^2+x_2{}^2+x_3{}^2+x_4{}^2)(y_1{}^2+y_2{}^2+y_3{}^2+y_4{}^2) \tag{3.2}$$

$$\begin{aligned}=\ & (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2\\ & +(x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2+(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2\end{aligned} \tag{3.3}$$

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

$$\begin{aligned}x_1{}^2&\equiv k &&(\text{mod. } p),\\ x_2{}^2&\equiv -k-1 &&(\text{mod. } p),\end{aligned}$$

となる $x_1,\ x_2$ がある．これは

$$x_1{}^2+x_2{}^2+1\equiv 0 \quad (\text{mod. } p)$$

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

$$x_1{}^2+x_2{}^2+x_3{}^2+x_4{}^2=ph \tag{3.4}$$

となる $x_1,\ x_2,\ x_3,\ x_4$ と h が存在する．あえて x_4 までとらなければならないのは，後の証明で恒等式 (3.3) 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 (3.4) 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

$$\begin{aligned}&x_1\equiv y_1,\ x_2\equiv y_2,\ x_3\equiv y_3,\ x_4\equiv y_4 \quad (\text{mod. } h)\\ &|y_i|\leqq\frac{h}{2}\quad,\ i=1,\ 2,\ 3,\ 4\end{aligned}$$

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 (3.3) に代入する.

$$z_1{}^2 + z_2{}^2 + z_3{}^2 + z_4{}^2 = ph^2h'$$

ただし

$$\begin{aligned}
z_1 &\equiv x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \equiv x_1{}^2 + x_2{}^2 + x_3{}^2 + x_4{}^2 \equiv 0 && \pmod{h}\\
z_2 &\equiv x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \equiv x_1x_2 - x_2x_1 + x_3x_4 - x_4x_3 \equiv 0 && \pmod{h}\\
z_3 &\equiv x_1y_3 - x_2y_4 - x_3y_1 + x_4y_2 \equiv x_1x_3 - x_2x_4 - x_3x_1 + x_4x_2 \equiv 0 && \pmod{h}\\
z_4 &\equiv x_1y_4 + x_2y_3 - x_3y_2 - x_4y_1 \equiv x_1x_4 + x_2x_3 - x_3x_2 - x_4x_1 \equiv 0 && \pmod{h}
\end{aligned}$$

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

$$x_i = y_i + m_ih = (2m_i + 1)\frac{h}{2}\ (i = 1,\ 2,\ 3,\ 4)$$

となる. これを式 (3.4) 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. □

3.2 平方剰余の相互法則

3.2.1 相互法則とは何か

2 が法 113 に関する平方剰余であるか，非剰余であるかを決定する方法，つまり $\left(\dfrac{2}{113}\right)$ を求める一般的な方法はあるのか．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．

定理 33 (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**：$\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

が成り立つ． ■

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)

$$\begin{aligned} \left(\frac{2}{p}\right) = 1 &\iff p \equiv 1,\ 7 \pmod 8 \\ \left(\frac{2}{p}\right) = -1 &\iff p \equiv 3,\ 5 \pmod 8 \end{aligned}$$

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 33 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．

3.2.2　ガウスの補題による証明

まず「ガウスの予備定理」の証明からはいる.

定理 34 (ガウスの予備定理)
a を p で割り切れない数とする.

$$1\cdot a,\ 2\cdot a,\ 3\cdot a,\ \cdots,\ \frac{p-1}{2}\cdot a, \tag{3.5}$$

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,

$$\left(\frac{a}{p}\right)=(-1)^n$$

が成り立つ. ■

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．(3.5) の数の絶対値最小な剰余は

$$\pm1,\ \pm2,\ \cdots,\ \pm\frac{p-1}{2}$$

の中にある．(3.5) のなかのどの二つの和も差も p では割りきれないので，(3.5) の絶対値最小剰余はすべて異なるのみでなく，(3.5) のなかに絶対値が等しいものもない．(3.5) 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

$$1a\cdot 2a\cdot 3a\cdots\frac{p-1}{2}a\equiv(-1)^n1\cdot2\cdot\cdots\cdot\frac{p-1}{2}\pmod{p}$$

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 31) 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

$$\left(\frac{a}{p}\right)=(-1)^n$$

が成り立つ. □

例 3.2.1　$a=3,\ p=7$ のとき $\dfrac{p-1}{2}=3$ である．3, 6, 9 を 7 で割った剰余は 3, 6, 2 である．$\dfrac{7}{2}$ より大きいものは 6 のみである．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.

定理 33 のガウスによる第三証明

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. (3.5) 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. (3.5) 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 $p-2k<\dfrac{p}{2}$ 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,

$$n\equiv 1+3+\cdots+\left(\frac{p}{2}\text{ より小さい奇数}\right)\equiv 1+2+3+\cdots+\frac{p-1}{2} \pmod{2}$$

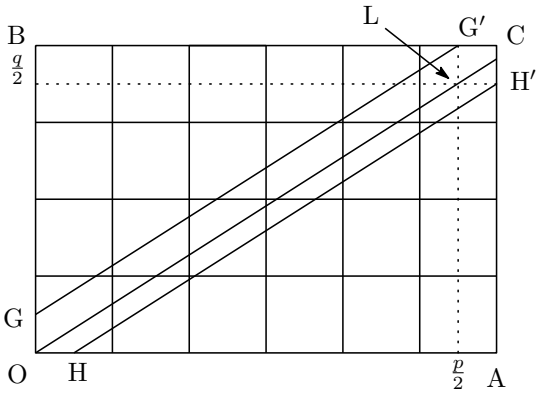
すなわち

$$n\equiv\frac{1}{2}\cdot\frac{p-1}{2}\left(\frac{p-1}{2}+1\right)=\frac{p^2-1}{8} \pmod{2}$$

$$\therefore\quad \left(\frac{2}{p}\right)=(-1)^n=(-1)^{\frac{p^2-1}{8}}$$

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 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 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 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 $\left(\dfrac{p+1}{4},\ \dfrac{q+1}{4}\right)$ 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 $\left(\dfrac{p+1}{4},\ \dfrac{q+1}{4}\right)$ 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 $\left(\dfrac{p+1}{4},\ \dfrac{q+1}{4}\right)$ 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，$\dfrac{p+1}{4},\ \dfrac{q+1}{4}$ がともに整数 $s,\ t$ となるときにかぎる．$\dfrac{p-1}{2}=2s-1,\ \dfrac{q-1}{2}=2t-1$ なので，これは $\dfrac{p-1}{2},\ \dfrac{q-1}{2}$ 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, $\left(\dfrac{a}{p}\right)$ の値を計算することができる．

例 3.2.2　$p = 23$

$$\left(\frac{1}{23}\right) = 1 \quad (\ 1 = 1^2\ )$$
$$\left(\frac{2}{23}\right) = 1 \quad (\ 23 \equiv 7 \pmod 8,\quad \text{第 2 補充法則})$$
$$\left(\frac{3}{23}\right) = -\left(\frac{23}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1 \quad (\ \text{相互法則},\quad \text{第 2 補充法則})$$
$$\left(\frac{4}{23}\right) = \left(\frac{2}{23}\right)^2 = 1$$
$$\left(\frac{5}{23}\right) = \left(\frac{23}{5}\right) = \left(\frac{-2}{5}\right) = \left(\frac{-1}{5}\right)\left(\frac{2}{5}\right) = 1(-1) = -1 \quad (\ \text{相互法則},\quad \text{第 1 , 第 2 補充法則})$$
$$\left(\frac{6}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{3}{23}\right) = 1$$
$$\left(\frac{7}{23}\right) = -\left(\frac{23}{7}\right) = -\left(\frac{2}{7}\right) = -1 \quad (\ \text{相互法則},\quad \text{第 2 補充法則})$$
$$\left(\frac{8}{23}\right) = \left(\frac{2}{23}\right)^3 = 1$$
$$\left(\frac{9}{23}\right) = \left(\frac{3}{23}\right)^2 = 1$$
$$\left(\frac{10}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{5}{23}\right) = -1$$
$$\left(\frac{11}{23}\right) = -\left(\frac{23}{11}\right) = -\left(\frac{1}{11}\right) = -1 \quad (\ \text{相互法則})$$
$$\left(\frac{17}{23}\right) = \left(\frac{23}{17}\right) = \left(\frac{6}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{3}{17}\right)$$
$$= \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right) = -1 \quad (\ \text{相互法則},\quad \text{第 2 補充法則})$$

3.3　いくつかの別証明

3.3.1　ガウス和を用いる証明

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 33 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．

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 33(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 28 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 30 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 3.3.1　$p = 5$ 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 3.3.2　$p = 7$ のとき．3 は 7 を法とする原始根である．実際

$$3^1 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1 \pmod 7$$

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 3

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 35

記号はこの節の通りとする．このとき

$$\beta_0\beta_1=\begin{cases}\dfrac{1+p}{4} & (p\equiv -1 \ \text{〔 mod . 4) のとき〕}\\ \dfrac{1-p}{4} & (p\equiv 1 \ \text{〔 mod . 4) のとき〕}\end{cases}$$

となる． ■

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なるからである．

そこで

(i) $\dfrac{p-1}{2}$ が奇数．つまり $p\equiv -1 \pmod{4}$ 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 $p\equiv 1 \pmod{4}$ 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 $\alpha+\cdots+\alpha^{p-1}=-1$ でまとめられる．

$$\therefore\quad \beta_0\cdot\beta_1=(-1)\cdot\frac{p-1}{4}=\frac{1-p}{4}$$

これで補題が示された. □

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．証明の中で用いる補題を先に証明しておく．

補題 4

素数 p と整数係数の多項式 $a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$ に対して

$$(a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0)^p \equiv {a_n}^p x^{pn} + {a_{n-1}}^p x^{p(n-1)} + \cdots + {a_0}^p \pmod{p}$$

である. ■

証明 $1 \leqq k \leqq p-1$ に対して ${}_pC_k = p_{p-1}C_{k-1}$ より ${}_pC_k$ は p の倍数.

$$\begin{aligned}
\therefore \quad & (a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0)^p \\
= \quad & \{a_nx^n + (a_{n-1}x^{n-1} + \cdots + a_0)\}^p \\
\equiv \quad & {a_n}^p x^{pn} + (a_{n-1}x^{n-1} + \cdots + a_0)^p \pmod{p} \\
\equiv \quad & {a_n}^p x^{pn} + {a_{n-1}}^p x^{p(n-1)} + (a_{n-2}x^{n-2} + \cdots + a_0)^p \pmod{p} \\
& \cdots \\
\equiv \quad & {a_n}^p x^{pn} + {a_{n-1}}^p x^{p(n-1)} + \cdots + {a_0}^p
\end{aligned}$$

である. □

定理 36 (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 $p \equiv \pm 1 \pmod{4}$ と同順にとって

$$\left(\frac{q}{p}\right) = \left(\frac{\pm p}{q}\right)$$

である. ■

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 31) 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

$$\begin{aligned}
G^q \quad = \quad & \left(\sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \alpha^k\right)^q \equiv \sum_{k=1}^{p-1} \left(\frac{k}{p}\right)^q \alpha^{kq} \pmod{q} \quad (\because \quad \text{補題 4}) \\
= \quad & \sum_{k=1}^{p-1} \left(\frac{k}{p}\right) \alpha^{kq} \quad (\because \quad q \text{ は奇数}) \\
= \quad & \left(\frac{q}{p}\right) \sum_{k=1}^{p-1} \left(\frac{kq}{p}\right) \alpha^{kq} = \left(\frac{q}{p}\right) G
\end{aligned}$$

$$\therefore \quad \left(\frac{q}{p}\right) G \equiv \left(\frac{\pm p}{q}\right) G \pmod{q}$$

つまり

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

G において $\alpha,\ \alpha^2,\ \cdots \alpha^{p-1}$ の係数はすべて ± 1 であるから，$\left(\frac{q}{p}\right) - \left(\frac{\pm p}{q}\right)$ がすべて q の倍数になる．

これがとりうる値は $0,\ \pm 2$ 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．

3.3.2 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 34 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 5 (三角法の補題)

m を奇素数とする．等式

$$\frac{\sin mx}{\sin x} = (-4)^{\frac{m-1}{2}} \prod_{j=1}^{\frac{m-1}{2}} \left(\sin^2 x - \sin^2 \frac{2\pi j}{m}\right)$$

が成り立つ． ■

証明 ド・モアブルの定理と二項定理により,

$$\begin{aligned}
& \cos mx + i \sin mx = (\cos x + i \sin x)^m \\
= \ & \sum_{k=0}^{m} {}_m\mathrm{C}_k \cos^{m-k} x \cdot (i \sin x)^k \\
= \ & {}_m\mathrm{C}_0 \cos^m x - {}_m\mathrm{C}_2 \cos^{m-2} x \sin^2 x + {}_m\mathrm{C}_4 \cos^{m-4} x \sin^4 x - \cdots \\
& \quad + i({}_m\mathrm{C}_1 \cos^{m-1} x \sin x - {}_m\mathrm{C}_3 \cos^{m-3} x \sin^3 x + {}_m\mathrm{C}_5 \cos^{m-5} x \sin^5 x - \cdots)
\end{aligned}$$

が成立する．虚数部分を比較して

$$\sin mx = \sin x \{{}_m\mathrm{C}_1 \cos^{m-1} x - {}_m\mathrm{C}_3 \cos^{m-3} x \sin^2 x + {}_m\mathrm{C}_5 \cos^{m-5} x \sin^4 x - \cdots\}$$

となる．m が奇素数なので $m=2u+1$ とおくと

$$\begin{aligned}
& {}_m\mathrm{C}_1\cos^{m-1}x-{}_m\mathrm{C}_3\cos^{m-3}x\sin^2x+{}_m\mathrm{C}_5\cos^{m-5}x\sin^4x-\cdots\\
=\ & {}_m\mathrm{C}_1\cos^{2u}x-{}_m\mathrm{C}_3\cos^{2u-2}x\sin^2x+{}_m\mathrm{C}_5\cos^{2u-4}x\sin^4x-\cdots\\
=\ & {}_m\mathrm{C}_1(1-\sin^2x)^u-{}_m\mathrm{C}_3(1-\sin^2x)^{u-1}\sin^2x+{}_m\mathrm{C}_5(1-\sin^2x)^{u-2}\sin^4x-\cdots\\
=\ & (-1)^u({}_m\mathrm{C}_1+{}_m\mathrm{C}_3+{}_m\mathrm{C}_5+\cdots)\sin^{2u}x+\cdots\\
=\ & (-4)^{\frac{m-1}{2}}(\sin^2x)^{\frac{m-1}{2}}+\cdots
\end{aligned}$$

したがって，$\dfrac{\sin mx}{\sin x}$ は $\sin^2x$ 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，

$$x=\pm\frac{2\pi j}{m}\ \left(1\leqq j\leqq\frac{m-1}{2}\right)$$

に対して $\sin mx=0$ であり，

$$\pm\sin\frac{2\pi j}{m}\ \left(1\leqq j\leqq\frac{m-1}{2}\right)$$

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 33(再掲)

p と q を相異なる 2 つの奇素数とする．

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

が成り立つ． ■

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 34 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 34 より

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

なので，三角法の補題 5 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. □

3.4 演習問題

練習問題 43 (解答 43)
$\left(\dfrac{365}{1847}\right)$ を求めよ.

練習問題 44 (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 45 (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 46 (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 47 (解答 47)

p が $p \equiv 1 \pmod 4$ の形の素数のとき

$$\sum_{a=1}^{\frac{p-1}{2}} \left(\frac{a}{p}\right) = \sum_{0 \leqq b \leqq p \text{ の偶数}} \left(\frac{b}{p}\right) = \sum_{0 \leqq c \leqq p \text{ の奇数}} \left(\frac{c}{p}\right) = 0$$

関連入試問題

入試問題 32 (解答 32) ［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.

第4章　除法のできる環

4.1　ユークリッド整域

整数環 $\mathbb{Z}$ は次のような性質がある．

(1)　$\mathbb{Z}$ の二つの要素 a, b について $ab = 0$ ならば $a = 0$ または $b = 0$ が成り立つ．いずれもが 0 ではない二つの要素 a, b で，$ab = 0$ となるものがあれば，a を左零因子，b を右零因子という．左零因子，右零因子をまとめて零因子という．

これは行列からなる環では成り立たない．二次行列の集合 A は行列の和と積で環である．行列環 A では

$$\begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

のように零因子がある．

零因子が存在しないような環を**整域**という．整数環 $\mathbb{Z}$ は整域である．

(2)　$\mathbb{Z}$ には元 a について**大きさ** $|a|$ が定義されていて，任意の $a(\neq 0)$, b について

$$b = qa + r \quad 0 \leqq r < |a|$$

となる元 q, r が一意に存在する．

環 R には，その要素 a に対して大きさといわれる 0 以上の実数が定まり，(1) と (2) の両方が成り立つなら，その環 R を**ユークリッド整域**，あるいはユークリッド環という．大きさを絶対値とすることで，整数環はユークリッド整域である．整数環は除法のできる整域である．

本節では，整数環以外に除法のできる整域を二つ考えよう．

一つは多項式からなる環である．ここで多項式は $3x$ のような単項式も含め整式と同じ意味に用いる．多項式の集合では、整数と同じく因数分解ができ，かつ素因数分解の (定数倍を除く) 一意性が成り立つ．なぜ多項式でも素因数分解の一意性がなり立つのか．それは多項式では除法の定理が成り立つからである．結局は整数の場合と同じく，除法の定理が成立することが根拠なのである．

もう一つは、実部、虚部がそれぞれ整数であるような複素数からなる集合

$$\{a + bi \mid a,\ b \in \mathbb{Z}\}$$

である．これをガウス整数環という.『数論初歩』では略してガウス環ともいうこともある．代数学の一分野の環論では，素数 (厳密には素元という) への分解が (単数を除いて) 一意である整域のことをガウス環という．

4.2　多項式環

4.2.1　多項式の除法

体を係数とする多項式の環　実数を係数とする多項式全体を考える．このような実数係数の多項式の集合を，変数を明示して $\mathbb{R}[x]$ と表そう．以下のことは $\mathbb{R}[x]$ で考えても，有理数係数にかぎっ

て $\mathbb{Q}[x]$ で考えても，また複素数で考え $\mathbb{C}[x]$ としても同じことである．そこで，体 K を有理数体 $\mathbb{Q}$，実数体 $\mathbb{R}$，複素数体 $\mathbb{C}$ のいずれかを表すものとし，これからは体 K に係数をもつ多項式の集合 $K[x]$ を考えることにする．

整数係数で考えるときはまた別の問題であることには注意したい．

x の多項式 $f(x)$ に対して $\deg f(x)$ でその次数を表すとする．$f(x)$ の大きさをその次数 $\deg f(x)$ とすると，この大きさに対して除法の定理が成り立つ．

定理 37 (多項式の除法の定理)

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

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

となる多項式 $q(x),\ r(x)$ がただ一組，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．

これが一組しかないことを示す．二組あったとする．

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

すると，

$$g(x)\cdot\{q_1(x) - q_2(x)\} = r_2(x) - r_1(x) \tag{4.1}$$

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 (4.1) 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． □

多項式の約数・倍数　整数の場合と同じように，多項式 $f(x)$ が多項式 $g(x)$ の倍数であるとは，$f(x) = q(x)g(x)$ を満たす多項式 $q(x)$ が存在することと定義する．

多項式の場合も割り算ができ，$f(x)$ を $g(x)$ に対して，$f(x)$ を $g(x)$ で割った商と余りが一意に確定することから，

> $f(x)$ が $g(x)$ の倍数であることは，$f(x)$ を $g(x)$ で割った余りが 0 であることと同値である．

因数分解は

$$x^2 + 3x + 2 = (x+1)(x+2) = \{3(x+1)\}\left\{\frac{1}{3}(x+2)\right\} = \cdots$$

のように，定数倍を除いて確定する．約数や倍数，因数分解は，定数倍の違いを除いて決まる．

$K[x]$ の中で，0 でない定数は逆数もまた多項式であるから，$K[x]$ では 0 でない定数が単数になる．

定義 5
0 および定数でない多項式 $f(x)$ は少なくとも 0 でない定数と (0 でない定数) $\times f(x)$ を約数にもつ．これら約数以外の約数を真の約数という．真の約数をもたない多項式を **既約** という．　■

既約かどうかは，定数倍しても変わらない．

$$x+1,\ 3(x+1),\ -\sqrt{2}(x+1)$$

はすべて既約である．既約な多項式というのは，整数環の素数と同じ役割を果たす．

ここで注意．既約かどうかは，係数をどこで考えるかによって異なる．

例 4.2.1 $f(x) = x^4 - 4$ は

- $\mathbb{Q}[x]$ では $f(x) = (x^2-2)(x^2+2)$ と因数分解され，$\mathbb{Q}[x]$ で $x^2-2,\ x^2+2$ は既約．
- $\mathbb{R}[x]$ では $f(x) = (x-\sqrt{2})(x+\sqrt{2})(x^2+2)$ と因数分解され，$\mathbb{R}[x]$ で $x-\sqrt{2},\ x+\sqrt{2},\ x^2+2$ は既約．
- $\mathbb{C}[x]$ では $f(x) = (x-\sqrt{2})(x+\sqrt{2})(x-\sqrt{2}i)(x+\sqrt{2}i)$ と因数分解され，$\mathbb{C}[x]$ で $x-\sqrt{2},\ x+\sqrt{2},\ x-\sqrt{2}i,\ x+\sqrt{2}i$ は既約．

となる．

既約かどうかは係数をどこにとるかで変わる．以下では係数体 K は固定されているものとする．

最小公倍数・最大公約数　さらに整数のときと同様に，公約数，公倍数が定義される．整数では ± 1 倍を除いて考えるところを，多項式では 0 でない定数倍を除いて考えることにすれば，まったく同じである．

公約数や公倍数は整数の場合と同じである．2 つの多項式 $f(x)$ と $g(x)$ に対し，その最大公約数とは，$f(x)$ と $g(x)$ の公約数のなかで次数が最も大きいものをいう．最大公約数が定数のとき，$f(x)$ と $g(x)$ は**互いに素**であるという．

最小公倍数とは，$f(x)$ と $g(x)$ の公倍数のなかで，次数が最も小さいものをいう．簡単のために，$a(x)$ や $b(x)$ などで多項式を表すことにする．

定理 38

(1) 二つ以上の多項式の公倍数は，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) $a(x)$, $b(x)$ の最小公倍数を $l(x)$ ，最大公約数を $d(x)$ とすれば $a(x)b(x) = d(x)l(x)$.

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

整数の場合の証明が，ほんの一部の手直しでそのまま使える．ここでは (1) を示す．

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

$$m(x) = q(x)l(x) + r(x), \quad \deg r(x)) < \deg l(x)$$

となる．$l(x)$ も $m(x)$ も $a(x)$ の倍数であるから $l(x) = a(x)l(x)'$, $m(x) = a(x)m(x)'$ とおくと

$$r(x) = m(x) - q(x)l(x) = a(x)\{m'(x) - q(x)l'(x)\}$$

より, $r(x)$ は $a(x)$ の倍数である．同様に $b(x)$, $c(x)$, $\cdots$ の倍数でもあり，$r(x)$ は $a(x)$, $b(x)$, $c(x)$, $\cdots$ の公倍数となる．ところが $l(x)$ は次数が最小の公倍数であったから，もし $r(x)$ が 0 でないとすると, $l(x)$ より次数が小さい公倍数があることになり, $l(x)$ の次数の最小性に反する．

$$\therefore \quad r(x) = 0$$

つまり $m(x)$ は $l(x)$ の倍数である． □

この定理の証明においても,「除法の定理」が基本定理として用いられてることがわかる．

因数分解 多項式 $f(x)$ を既約な多項式の積に分解して，

$$f(x) = p_1(x)^{e_1}p_2(x)^{e_2}\cdots p_m(x)^{e_m}$$

の形にしたものを (その体における) 素因数分解という．

$p_1(x)$, $p_2(x)$, $\cdots$, $p_m(x)$ は異なる既約な多項式，e_1, e_2, $\cdots$, e_m は正の整数である．

このとき整数と同様に次の定理が成り立つ．

定理 39

多項式は既約な多項式の積として，定数倍と順序を除けばただ一通りに表すことができる． ■

多項式の場合も**素因数分解の一意性**という．基本的な定理である．

整数の因数分解の一意性の証明にならって，多項式の場合についても，除法を用いないツェルメロの方法による別証明をしてみよう．

因数分解の一意性の別証明 相異なる因数分解をもつ多項式が存在するとする．異なる因数分解をもつ多項式の集合を考える．この集合に属する次数が最小の多項式を $f(x)$ とする．次数の集合は自然数の部分集合なので，最小値が存在する．$f(x)$ は相異なる 2 つの因数分解をもつ．それを

$$f(x) = p_1(x)p_2(x)\cdots p_r(x) \qquad (\deg p_1(x) \leqq \cdots \leqq \deg p_r(x))$$
$$f(x) = q_1(x)q_2(x)\cdots q_s(x) \qquad (\deg q_1(x) \leqq \cdots \leqq \deg q_s(x))$$

とする．ここに $p_1(x)$, $\cdots$, $p_r(x)$, $q_1(x)$, $\cdots$, $q_s(x)$ は既約である．これが異なる因数分解ということは $r \neq s$ か，または $r = s$ で異なる $p_i(x)$ と $q_i(x)$ が存在するか，のいずれかである．ただし，ここで因数が異なるとは，どのような定数を一方に乗じても $p_i(x)$ と $q_j(x)$ は一致しないことをいう．

また，$p_1(x)$, $\cdots$, $p_r(x)$ のいずれも $q_1(x)$, $\cdots$, $q_s(x)$ のいずれとも異なる．なぜなら，もし $p_i(x) = q_j(x)$ なら，これを約せば $f(x)$ より小さい次数で，異なる因数分解をもつ多項式が得られ，$f(x)$ がそのような多項式のなかで次数最小であることに反する．

$\deg p_1(x) < \deg q_1(x)$ とする．$n = \deg q_1(x) - \deg p_1(x)$ とすると，適当な定数 a を

$$\deg\{q_1(x) - ax^n p_1(x)\} < \deg q_1(x)$$

となるようにとる．

ここで多項式 $g(x)$ を

$$\begin{aligned} g(x) &= f(x) - ax^n p_1(x)q_2(x)\cdots q_s(x) \\ &= \{q_1(x) - ax^n p_1(x)\}q_2\cdots q_s \end{aligned}$$

で定める．$\deg g(x) < \deg f(x)$ である．

この $g(x)$ の因数分解における因数 $q_1(x) - ax^n p_1(x)$ は $p_1(x)$ の倍数ではない．なぜならもし $p_1(x)$ の倍数なら $q_1(x)$ が $p_1(x)$ の倍数となり，互いに異なる既約な多項式であることに反する．よってこの因数分解に $p_1(x)$ は現れない．

一方 $g(x)$ は

$$\begin{aligned} g(x) &= f(x) - ax^n p_1(x)q_2(x)\cdots q_s(x) \\ &= p_1(x)\{p_2(x)\cdots p_r(x) - ax^n q_2(x)\cdots q_s(x)\} \end{aligned}$$

でもある．この $g(x)$ の因数分解には，因数 $p_1(x)$ が現れている．

よって $g(x)$ の 2 つの因数分解は相異なる因数分解である．

$\deg g(x) < \deg f(x)$ なので，$f(x)$ が異なる 2 つの因数分解をもつ次数最小の多項式であることと矛盾した．したがって異なる 2 つの因数分解をもつ多項式は存在しない． □

4.2.2 多項式環での不定方程式

一次不定方程式が多項式環でも考えられる．

そのために，整数の場合と同様に，証明に除法が使われる基本定理を紹介しよう．

定理 40

$K[x]$ の部分集合 H が空でなく $\{0\}$ のみでもなく，次の性質をもつとする．

$$\begin{aligned} f(x),\ g(x) \in H \quad &\Rightarrow \quad f(x) - g(x) \in H \\ f(x) \in K[x],\ g(x) \in H \quad &\Rightarrow \quad f(x)g(x) \in H \end{aligned}$$

このとき集合 H はある多項式 $d(x)$ の倍数の全体と一致する．つまり

$$H = \{\ d(x)f(x) \mid f(x) \in K[x]\}$$

である． ■

証明　条件から $0 = f(x) - f(x) \in H$ である．その結果，$f(x) \in H$ なら $-f(x) = 0 - f(x) \in H$ である．そこで H の要素のうち，次数最小の多項式 $d(x)$ をとる．

H の任意の要素 $f(x)$ をとり，それを $d(x)$ で割る．

$$f(x) = d(x)Q(x) + R(x) \quad \deg(r(x)) < \deg(d(x))$$

とおく．$d(x) \in H$ より $Q(x)d(x) \in H$ である．よって

$$R(x) = f(x) - Q(x)d(x) \in H$$

ここでもし $R(x) \neq 0$ なら $d(x)$ が次数最小の要素であることに反する．よって $R(x) = 0$，つまり H の任意の要素 $f(x)$ は $d(x)$ の倍数である．したがって $H = \{\ d(x)f(x) \mid f(x) \in K[x]\}$ が示せた．　□

注意 4.2.1　整数環 $\mathbb{Z}$ の場合は，差がふたたび属する部分集合 A で考えた．この場合はこの条件から，$x \in \mathbb{Z}$, $a \in A$ に対して $xa \in A$ が導けた．しかし多項式環の場合は，別に条件として立てることが必要である．

一般に整域 R の部分集合 A に対し，

(i)　A は加法に関して可換群である．

(ii)　$x \in R$, $a \in A$ ならば $xa \in A$.

の二つが成り立つとき，A を R の**イデアル**という．

整数環，多項式環ではイデアルはすべてある要素の倍数全体になる．このような整域を単項イデアル整域という．

不定方程式の解の存在　定理 40 を用いると次のことが示される．

定理 41

$p(x)$ と $q(x)$ を互いに素な多項式とする．このとき

$$p(x)u(x) + q(x)v(x) = 1$$

を満たす多項式 $u(x)$ と $v(x)$ が存在する．　■

証明

$$H = \{\ p(x)u(x) + v(x)g(x) \mid u(x),\ v(x) \in K[x]\}$$

とおく．

$f(x) = p(x)u_1(x) + q(x)v_1(x)$，$g(x) = p(x)u_2(x) + q(x)v_2(x)$ が H に属せば

$$f(x) - g(x) = p(x)\{u_1(x) - u_2(x)\} + q(x)\{v_1(x) - v_2(x)\} \in H$$

である．

したがって定理 40 より H は，H に属するある多項式 $d(x)$ の倍数の全体である．$d(x) = p(x)u_0(x) + q(x)v_0(x)$ とする．

一方

$$p(x) = p(x) \cdot 1 + q(x) \cdot 0 \in H,\ q(x) = p(x) \cdot 0 + q(x) \cdot 1 \in H$$

なので，$p(x)$ も $q(x)$ も $d(x)$ の倍数である．つまり $d(x)$ は $p(x)$ と $q(x)$ の公約数である．$p(x)$ と $q(x)$ は互いに素なので，$d(x)$ は定数である．しかも，H は 0 のみではないので $d \neq 0$ である．

つまり

$$p(x)u_0(x) + q(x)v_0(x) = d \text{ (定数)}$$

より $\dfrac{1}{d}u_0(x),\ \dfrac{1}{d}v_0(x)$ は $p(x)u(x) + q(x)v(x) = 1$ を満たす． □

ユークリッドの互除法　ユークリッドの互除法も同じようにできる．簡単のために多項式 $f(x),\ g(x)$ の最大公約数を $(f(x),\ g(x))$ と書く．

定理 42

(1) 任意の多項式 $q(x)$ に対し，$(f(x), g(x)) = (f(x) - q(x) \cdot g(x), g(x))$.

(2) $f(x)$ を $g(x)$ で割った余り $r(x)$ に対し，$(f(x), g(x)) = (r(x), g(x))$. ■

証明

(1)　$(f(x), g(x)) = d_1(x)$, $(f(x) - q(x) \cdot g(x), g(x)) = d_2(x)$ とする．

$f(x)) = d_1(x)f_1(x), g(x)) = d_1(x)g_1(x)$．また $f(x) - q(x) \cdot g(x) = d_2(x)h(x), g(x) = d_2(x)g_2(x)$ とする．

$$f(x) = q(x) \cdot g(x) + d_2(x)h(x) = d_2(x)\{q(x)g_2(x) + h(x)\}$$

より $d_2(x)$ は $f(x)$ と $g(x)$ の公約数である．$f(x)$ と $g(x)$ の最大公約数が $d_1(x)$ なので，定理 38(2) より，$d_2(x)$ は $d_1(x)$ の約数である．

一方

$$f(x) - q(x) \cdot g(x) = d_1(x)\{f_1(x) - q(x) \cdot g_1(x)\}$$
$$g(x) = d_1(x)g_1(x)$$

より，$d_1(x)$ は $f(x) - q(x) \cdot g(x)$ と $g(x)$ の公約数である．したがって同様の理由から $d_1(x)$ は $d_2(x)$ の約数である．

つまり $d_1(x) = d_2(x)$ が示された．

(2)　$f(x)$ を $g(x)$ で割った商を $q(x)$ とすると，余りが $r(x)$ なので

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

したがって，(1) から

$$(f(x), g(x)) = (f(x) - q(x) \cdot g(x),\ g(x)) = (r(x), g(x))$$

となる． □

例 4.2.2

$$(x^3 + 2x^2 - 4x - 8,\ 2x^2 + 6x + 4) = (x^3 + 2x^2 - 4x - 8,\ x^2 + 3x + 2)$$

である．$x^3 + 2x^2 - 4x - 8$ を $x^2 + 3x + 2$ で割ることにより，

$$x^3 + 2x^2 - 4x - 8 = (x^2 + 3x + 2)(x - 1) - 3x - 6$$

(2) から

$$(x^3+2x^2-4x-8,\ 2x^2+6x+4)=(-3x-6,\ x^2+3x+2)=(x+2,\ x^2+3x+2)$$

$x^2+3x+2=(x+1)(x+2)$ なので

$$(x^3+2x^2-4x-8,\ 2x^2+6x+4)=x+2$$

注意 4.2.2　節末にいくつかの大学入試問題を紹介した．これらの入試問題は，多項式関数として解くこともでき，また多項式の整数論として解くこともできる．

整式は，一方で多項式関数として x に値を代入し因数定理や剰余定理によって，式の除法や倍数や約数の議論をおこない因数分解の論証をすることができる．一方，有理数の一部である整数と同じように因数分解ができ，かつ素因数分解の (定数倍を除く) 一意性が成り立つ．根拠はいずれも除法の基本性質なのであるが，証明の進め方はずいぶん異なる．

実際に二通りに解いてみてほしい．

4.3　ガウス整数環

4.3.1　ガウス整数

$i=\sqrt{-1}$ を虚数単位として

$$R=\{\ a+bi\mid a,\ b\in\mathbb{Z}\}$$

とおく．R の二つの元 $\alpha=a+bi,\ \beta=c+di$ 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．R のことを **ガウス整数環** , R の元を **ガウス整数** という．略してガウス環ということもある．以下この節で「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 の元 $\alpha=a+bi$ 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 の元になる．ここで R の元 $\alpha=a+bi$ 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 の二つの元 $\alpha=a+bi,\ \beta=c+di$ 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 は逆数 $\dfrac{1}{\alpha}$ も整数であるとする．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 の元である．

$\dfrac{\alpha}{\beta}$ 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く，多項式環では 0 でない定数倍の違いを度外視して良いのと同じである．

定理 43 (ガウス整数環における除法の存在)

R の元 α と β $(\beta \neq 0)$ に対して

$$\alpha = \beta\gamma + \rho\ , \quad 0 \leqq N(\rho) < N(\beta)$$

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

$$N(\rho) = N\left(\beta\left(\frac{\alpha}{\beta} - \gamma\right)\right) = N(\beta)N\left(\frac{\alpha}{\beta} - \gamma\right) \leqq \frac{N(\beta)}{2} < N(\beta)$$

よって条件を満たすガウス整数 γ と ρ が存在した． □

このように除法の定理が成立する環を**ユークリッド整域**というのだった．これで，整数環，整式環，ガウス環と三種のユークリッド整域を学んできたことになる．それらのカギになるのは，除法との関連で次のような「大きさ」が定義できたことであった．

環	用いられる大きさ		
有理整数環	絶対値 $\lvert\ \rvert$	$a = bq + r$	$0 \leqq r < \lvert b \rvert$
多項式環	次数 deg	$f(x) = g(x)q(x) + r(x)$	$0 \leqq \deg r(x) < \deg g(x)$
ガウス環	ノルム $N(\ )$	$\alpha = \beta\gamma + \rho$	$0 \leqq N(\rho) < N(\beta)$

である．この大きさによって除法の定理が成立するのであった．

定理 44
$\alpha,\ \beta \in R$ 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 の元 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 の元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元を $\delta = \alpha x_0 + \beta y_0$ とする．
J の任意の元 $\alpha x + \beta y$ 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．よって J の元はすべて δ の倍数である．
逆に δ の倍数 $z\delta = \alpha(zx_0) + \beta(zy_0)$ が J に属することは明らかである．
また他の δ' もノルム最小の元なら，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 が単数倍の違いを除いて一意に存在することをが示された．
これによって整数環，多項式環の場合と同様に，ガウス環もまた単項イデアル整域である．

4.3.2　ガウス素数

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．よってその証明は略する．代わって、ツェルメロの証明をガウス素数の場合に行う．

定理 45
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．■

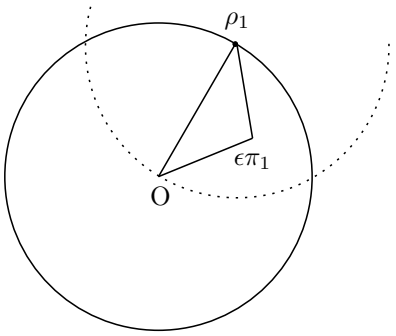
証明　異なる素因数分解をもつガウス整数の集合を考える．この集合に属するノルム最小のガウス整数を α とする．α は相異なる二つの因数分解をもつ．それを

$$n = \pi_1\pi_2\cdots\pi_r \qquad (N(\pi_1) \leqq N(\pi_2) \leqq \cdots \leqq N(\pi_r))$$
$$n = \rho_1\rho_2\cdots\rho_s \qquad (N(\rho_1) \leqq N(\rho_2) \leqq \cdots \leqq N(\rho_s))$$

とする．ここに $\pi_1,\ \cdots,\ \pi_r,\ \rho_1,\ \cdots,\ \rho_s$ はガウス素数である．これが異なる因数分解ということは $r \neq s$ か，または $r = s$ で π_i と ρ_i が同伴数でない i が存在するか，のいずれかである．
また，$\pi_1,\ \cdots,\ \pi_r$ のいずれも $\rho_1,\ \cdots,\ \rho_s$ のいずれとも同伴でない. なぜなら，もし π_i と ρ_j が同伴なら，これを約せば α よりノルムが小さいガウス整数で，異なる素因数分解をもつものが得

られ，α がそのような数のなかでノルム最小であることに反する．

$N(\pi_1) < N(\rho_1)$ とする．π_1 と同伴な 4 数 π_1，$i\pi_1$，$-\pi_1$，$-i\pi_1$ のうちには，ρ_1 との偏角の差が $\dfrac{\pi}{4}$ 以下のものがある．それを $\epsilon\pi_1$ とする．このとき，$N(\rho_1 - \epsilon\pi_1) < N(\rho_1)$ が成り立つ．



ここでガウス整数 β を

$$\beta = \alpha - \epsilon\pi_1\rho_2\cdots\rho_s = (\rho_1 - \epsilon\pi_1)\rho_2\cdots\rho_s$$

で定める．

$$N(\beta) = N(\rho_1 - \epsilon\pi_1)N(\rho_2\cdots\rho_s) < N(\rho_1)N(\rho_2\cdots\rho_s) = N(\alpha)$$

である．

β の因数分解における因数 $\rho_1 - \epsilon\pi_1$ は π_1 の倍数ではない．なぜならもし π_1 の倍数なら ρ_1 が π_1 の倍数となり互いに異なる素数であることに反する．よってこの因数分解に π_1 は現れない．

一方 β は

$$\begin{aligned}\beta &= \alpha - \epsilon\pi_1\rho_2\cdots\rho_s \\ &= \pi_1(\pi_2\cdots\pi_r - \epsilon\rho_2\cdots\rho_s)\end{aligned}$$

でもある．この β の因数分解には，因数 π_1 が現れている．

よって β の二つの因数分解は相異なる因数分解である．

$N(\beta) < N(\alpha)$ なので，α が異なる二つの因数分解をもつ最小の自然数であることと矛盾した．

したがって異なる二つの因数分解をもつ自然数は存在しない． □

ガウス環の素数はどのようなものか．

定理 46

p を奇素数とする． p は次のいずれかである．

(1) ガウス素数である．つまり R のなかでも因数分解されない．

(2) あるガウス素数 π のノルムである，つまり R において $p = \pi\bar{\pi}$ 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，π_1, π_2, $\cdots$, π_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 で単数になる．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，π は虚数なので $\bar{\pi}=\pi$ はない．$\bar{\pi}=-\pi$ なら $x=0$ で，このとき $p=y^2$ となり，$\bar{\pi}=\pm i\pi$ なら $y=\pm x$ で，このとき $p=2x^2$ となる．しかし，p は奇素数なのでこれらはあり得ない. □

$p=2$ のとき，その分解は

$$2=N(1+i)=(1+i)(1-i)=i^3(1+i)^2 \tag{4.2}$$

で与えられる．四つのガウス整数 $1+i$, $1-i$, $-1+i$, $-1-i$ は，もし単数でない二数に分解されれば，そのノルムも素数でない．よってこれら四整数は素数であり，

$$1-i=-i(1+i),\ -1+i=i(1+i),\ -1-i=-(1+i)$$

より，互いに同伴である．従ってまた因数分解 (4.2) で「単数倍を除いて一意」であることは成立している.

補題 6

ガウス整数 $\alpha=a+bi$ が $\lambda=1-i$ で割りきれるための必要十分条件は，$a\equiv b \pmod 2$ である. ■

証明 a, b ともに偶数なら，$\alpha=a+bi$ が 2 で割り切れ，λ でも割り切れる．ともに奇数なら $a+bi-(1-i)$ が 2 で割り切れ，これから $a+bi$ が λ で割り切れる．十分性が示せた.

一方が奇数で他方が偶数のとき，$a+bi-1$ において $a-1$ と b の偶奇が一致するので，$a+bi-1$ が λ で割り切れ，$\alpha=a+bi$ は λ で割り切れない．必要性が示せた. □

$\lambda=1-i$ で割り切れるか割り切れないかによって「偶数」,「奇数」と読ぶ．ガウス整数の 2 での剰余類は

$$0,\ 1,\ i,\ 1+i$$

で代表され，そのうち 0 と $1+i$ が偶数，1 と i が奇数である.

補題 7

ガウス整数 α が $\lambda=1-i$ で割りきれなければ，α^4-1 は 8 の倍数である. ■

証明 ガウス整数 α が $\lambda=1-i$ で割りきれないので，補題 6 より $\alpha-1$ または $\alpha-i$ が 2 の倍数である．それぞれ $\alpha+1$ または $\alpha+i$ も 2 の倍数なので，α^2-1 または α^2+1 が 4 の倍数であり，他方も 2 の倍数である．よって α^4-1 は 8 の倍数である. □

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 47

p を奇素数とする．このとき

$$\begin{aligned} p\equiv 1 \pmod 4 \quad &\Longleftrightarrow \quad p=(a+bi)(a-bi) \text{ と分解される.} \\ p\equiv 3 \pmod 4 \quad &\Longleftrightarrow \quad p \text{ はガウス素数である.} \end{aligned}$$

が成り立つ. ■

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，明らかにそれはあり得ない．

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．

本定理は平方剰余の第一補充法則を用いた．これを用いない初等的な大学入試問題がある．それを紹介しておきたい．2002 年慶応大医学部問題 (問題 41) である．

4.3.3　四次フェルマ問題

ガウス環の整数論を応用して，四次のフェルマー問題を解こう．

定理 48
不定方程式

$$x^4+y^4=z^2$$

はガウス整数環のなかに $xyz \neq 0$ の解をもたない．をもたない．

証明　背理法で示す．$(x,\ y,\ z) \neq (0,\ 0,\ 0)$ の解 $(\alpha,\ \beta,\ \gamma)$ があるとする．

$$\alpha^4+\beta^4=\gamma^2$$

α と β の最大公約数を δ とすると，γ^2 は δ^4 の倍数となり，これから γ は δ^2 の倍数となり，

$$\left(\frac{\alpha}{\delta}\right)^4+\left(\frac{\beta}{\delta}\right)^4=\left(\frac{\gamma}{\delta^2}\right)^2$$

つまり $\left(\dfrac{\alpha}{\delta},\ \dfrac{\beta}{\delta},\ \dfrac{\gamma}{\delta^2}\right)$ も解である．よってはじめから α と β は互いに素，この結果 α と γ，β と γ も互いに素としてよい．以下の証明で α や β は適宜その同半数に代えてもよいことに注意する．

$\alpha,\ \beta$ がともに $\lambda=1-i$ の倍数でないとする．補題 7 より，$\alpha^4-1,\ \beta^4-1$ はともに 8 の倍数なので，$\alpha^4+\beta^4-2=\gamma^2-2$ は 8 の倍数である．$\gamma^2-2=8\eta$ とおくと $\gamma^2=2(1+4\eta)$ となり γ^2 が従って γ は素数 $\lambda=1-i$ の倍数である．$\gamma=\lambda\mu$ とおくと $\gamma^2=-2i\mu^2$ となり，μ^2 と 2，つまりは μ と λ は互いに素である．

一方，$\gamma^2-2=-2i\mu^2-2$ は 8 の倍数である．つまり $-i\mu^2-1=-i(\mu^2-i)$ より μ^2-i が 4 の倍数となる．補題 7 より μ^2-1 または μ^2+1 が 4 の倍数であり，この結果 $1-i$ または $1+i$ が 4 の倍数となって，矛盾である．

よって α と β の一方のみが $\lambda=1-i$ の倍数である．α と β について対称なので

$$\alpha=\lambda^k x,\ k \text{は正整数},$$
$$x,\ \beta,\ \gamma\text{は}\lambda\text{と互いに素}.$$

として良い．このとき

$$\lambda^{4k}x^4+\beta^4=\gamma^2$$

である．このような x, β, γ が存在しないことを示す．ここで証明すべきことを強め，

$$\epsilon\lambda^{4k}x^4+\beta^4=\gamma^2,\ \epsilon \text{は単数} \tag{4.3}$$

をみたす x, β, γ が存在しないことを示す．等式 (4.3) より

$$(\gamma+\beta^2)(\gamma-\beta^2)=\epsilon\lambda^{4k}x^4$$

である．$\gamma+\beta^2$, $\gamma-\beta^2$ の公約数を d とする．β^2 と γ はともに奇数なので和と差は偶数である．一方 d は $\gamma+\beta^2$, $\gamma-\beta^2$ の和と差，つまり 2γ, $2\beta^2$ の公約数である．β と γ は互いに素でともに奇数なので d は 2 の約数である．つまり $\gamma+\beta^2$, $\gamma-\beta^2$ はともに $\lambda=1-i$ の倍数である．

ここで $\gamma+\beta^2=\gamma-\beta^2+2\beta^2$ なので，$\gamma+\beta^2$ が $\lambda^2=-2i$ の倍数であることと $\gamma-\beta^2$ が λ^2 の倍数であることは同値である．よって等式 (4.3) となるためにはともに $\lambda^2=-2i$ の倍数でなければならない．つまり $d=2$ である．よってまた $\gamma+\beta^2$ が λ^2 の倍数であるが λ^3 の倍数ではなく，$\gamma-\beta^2$ が λ^{4k-2} の倍数であるとして良い．逆の場合は β に代えて $i\beta$ で考えればよい．よって等式 (4.3) より

$$\gamma+\beta^2=\epsilon_1\lambda^2y^4,\quad \gamma-\beta^2=\epsilon_2\lambda^{4k-2}z^4$$
$$\epsilon_1,\ \epsilon_2\text{は単数},\ y\text{ と }z,\ y\text{ と}\lambda,\ z\text{ と}\lambda\text{はそれぞれ互いに素}.$$

と表せる．この結果

$$2\beta^2=\epsilon_1\lambda^2y^4-\epsilon_2\lambda^{4k-2}z^4$$

$\lambda^2=-2i$ なので

$$\beta^2=-i\epsilon_1y^4+i\epsilon_2\lambda^{4k-4}z^4$$

$-i\epsilon_1$, $i\epsilon_2$ を改めて ϵ_1, ϵ_2 と置けば

$$\beta^2=\epsilon_1y^4+\epsilon_2\lambda^{4k-4}z^4 \tag{4.4}$$

となる．

$k>1$ を示す．$k=1$ とする．このとき等式 (4.5) の右辺の各項は奇数なので和は偶数，つまり λ の倍数となる．これは β が λ と互いに素であることに反する．よって $k>1$ である．

等式 (4.5) において $k>1$ であるから $\beta^2-\epsilon_1y^4$ は λ^4 の倍数．つまり 4 の倍数である．

一方，β も y も λ の倍数ではないので，補題 7 とその証明より β^2+1 または β^2-1 が 4 の倍数で，y^4-1 は 8 の倍数である．β^2+1 が 4 の倍数のときは $(i\beta)^2-1$ が 4 の倍数になる．よって β^2-1 が 4 の倍数としてよく，このとき ϵ_1-1 が 4 の倍数になる．ϵ_1 は単数なので $\epsilon_1=1$ である．このとき等式 (4.5) は単数 ϵ_2 をもちいて

$$\beta^2=y^4+\epsilon_2\lambda^{4(k-1)}z^4 \tag{4.5}$$

となる．ところがこの等式は等式 (4.3) の k を $k-1$ に代えただけである．つまり等式 (4.3) をみたす $x,\ \beta,\ \gamma$ が k のとき存在すれば $k-1$ でも存在する．

よって帰納的に $k=1$ でも成立するが，これは $k>1$ という先に示した結果と矛盾する．よって等式 (4.3) をみたす $x,\ \beta,\ \gamma$ は存在しない． □

この定理からただちに次の結論が導かれる．

系 48.1

$$x^4+y^4=z^4$$

をみたすガウス整数は存在しない． ■

証明　もしあれば $x^4+y^4=(z^2)^2$ より $x^4+y^4=Z^2$ にガウス整数の解が存在することになるからである． □

4.4　演習問題

練習問題 48 (解答 48)

次の数を平方数の和に書き表せ．

$$5,\ 13,\ 65,\ 5^2,\ 50,\ 13^2$$

練習問題 49 (解答 49)

$$x^2+y^2=z^2,\ (x,\ y)=1$$

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．

練習問題 50 (解答 50)

有理整数 $p,\ q,\ r$ を係数にもつ 3 次方程式 $x^3+px^2+qx+r=0$ が，有理数 $u,\ v$ によって $\alpha=u+vi$ と表される虚数解をもつなら，α はガウス整数であることを示せ．

関連入試問題

入試問題 33 (解答 33) ［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．

入試問題 34 解答 34　［90 京都教育大］

まず整式に関する用語の確認をする．

- 整式 $f(x)$ が整式 $g(x)$ の約数であるとは $f(x)p(x)=g(x)$ を満たす整式 $p(x)$ が存在することをいう．
- 整式 $d(x)$ が 2 つの整式 $f(x)$，$g(x)$ の公約数であるとは，$d(x)$ が $f(x)$ の約数であり，かつ，$g(x)$ の約数でもあることをいう．
- 整式 $d(x)$ が 2 つの整式 $f(x)$，$g(x)$ の最大公約数であるとは，$d(x)$ が $f(x)$，$g(x)$ の公約数の中で次数が最大のものであることをいう．($f(x)=g(x)=0$ の場合は除く)．

これらの用語に注意して, 次の問に答えよ．

(1) 整式 $f(x)$ は $f(x)$ の約数であることを示せ．

(2) 0 と異なる整式 $f(x)$ が整式 $g(x)$ の約数であれば，$f(x)$ は $f(x)$，$g(x)$ の最大公約数であることを示せ．

(3) $f(x)$ が 0 とは異なる整式で，整式 $g(x)$ を $f(x)$ で割った余りが $r(x)$ であるとする．いま，整式 $d(x)$ が $r(x)$，$f(x)$ の最大公約数であるとすれば，$d(x)$ は $f(x)$，$g(x)$ の最大公約数でもあることを示せ．

入試問題 35 解答 35　［02 中部大改題］

$f(x)=x-1$, $g(x)=(x+1)^3$ であるとき，

$$p(x)f(x)+q(x)g(x)=1$$

を満たす整式 $p(x)$, $q(x)$ の組のなかで，$p(x)$ の次数が最小である組，および $p(x)$ の最高次数の係数が 1 であるなかで次数が最小の組，をそれぞれ求めよ．

入試問題 36 解答 36　［06 京大文理系前期 1 番 3 番］

$Q(x)$ を 2 次式とする．整式 $P(x)$ は $Q(x)$ では割り切れないが，$\{P(x)\}^2$ は $Q(x)$ で割り切れるという．このとき 2 次方程式 $Q(x)=0$ は重解を持つことを示せ．

入試問題 37 解答 37　［06 京大文理系後期 1 番 3 番］

1 次式 $A(x)$，$B(x)$，$C(x)$ に対して $\{A(x)\}^2+\{B(x)\}^2=\{C(x)\}^2$ が成り立つとする．このとき $A(x)$ と $B(x)$ はともに $C(x)$ の定数倍であることを示せ．

入試問題 38 解答 38　［00 お茶の水女子大］

$f(x)$ を x についての整数係数の整式とし，$g(y)$ を y についての整数係数の整式とする．$xy=1$ のとき常に $f(x)g(y)=1$ となるような $f(x)$, $g(y)$ をすべて求めよ．

入試問題 39 (解答 39)　［00 京大理系前期］

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.

入試問題 40 (解答 40)　［07 一橋前期 01 番］

m を整数とし，$f(x)=x^3+8x^2+mx+60$ とする．

(1) 整数 a と 0 ではない整数 b で，$f(a+bi)=0$ を満たすものが存在するような m をすべて求めよ．ただし，i は虚数単位である．

(2) (1) で求めたすべての m に対して，方程式 $f(x)=0$ を解け.

入試問題 41 (解答 41)　［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 つの組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つの自然数 $a,\ b$ 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.

第5章　連分数

5.1　一次不定方程式と連分数

メービス変換の定義　定理 6 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．b は 0 でないとする．整数 a を b で割って余りが r，つまり

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

であるとする．この除法の式は行列で

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} b \\ r \end{pmatrix}$$

と表される．ここで a と b の比を考えると，$r \neq 0$ のとき

$$\frac{a}{b} = \frac{qb + r}{b} = \frac{q\left(\dfrac{b}{r}\right) + 1}{1\left(\dfrac{b}{r}\right) + 0}$$

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，小数部分が 0 でないかぎり実行可能な操作である．この操作を行列で表現し，古典的な連分数との関連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　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が二次行列の積のメービス変換で表される．

ω を整数でない正の実数とする．また実数 x に対し $[x]$ は x を越えない最大の整数を表す．実数 ω に対し，次の手続きを考える．

(i) $q_0 = [\omega]$ とする．

(ii) $\omega = q_0 + u \ \ (0 < u < 1)$ とおく．

(iii) そして $\omega_1 = \dfrac{1}{u}$ とする．$1 < \omega_1$ 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，上の手続きが二次行列で表現される．

数列 $\{w_n\}$ と数列 $\{k_n\}$ を，$k = 1,\ 2,\ \cdots$ に対して

$$\begin{aligned} &\omega_0 = \omega,\ q_0 = [\omega], \\ &\omega_k = \frac{1}{\omega_{k-1} - q_{k-1}},\ q_k = [\omega_k] \end{aligned}$$

で定める．ただし，ω_k が整数となればいったんそこでやめるものとする．

これを ω の **連分数展開**という．k 回この手続きを行うと，

$$\omega = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_{k-1} & 1 \\ 1 & 0 \end{pmatrix}\omega_k$$

となる．ここで ω_k 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．

$$\omega_k = \begin{pmatrix} \omega_k - 1 & 1 \\ 1 & 0 \end{pmatrix} \cdot 1$$

つまり，$\omega_{k+1} = 1,\ q_k = \omega_k - 1$ 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．

$$\begin{aligned} \omega &= q_0 + \frac{1}{\omega_1} \\ &= q_0 + \cfrac{1}{q_1 + \dfrac{1}{\omega_2}} \\ &= q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cdots}}} \end{aligned}$$

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．

展開の一意性　$k \geqq 1$ に対して

$$\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_{k-1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}$$

で $(P_k,\ Q_k)$ を定める．このとき $k \geqq 1$ に対して，

$$\begin{pmatrix} P_{k+1} \\ Q_{k+1} \end{pmatrix} = \begin{pmatrix} P_k q_k + P_{k-1} \\ Q_k q_k + Q_{k-1} \end{pmatrix}$$

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,

$$k_0 = h_0,\ k_1 = h_1,\ \cdots,\ k_m = h_m$$

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．この結果 $X = Y$ となる．同様の議論をくり返せば，順次

$$k_0 = h_0,\ k_1 = h_1,\ \cdots,\ k_m = h_m$$

となるからである．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．ある数の連分数展開における違いは，この違いのみである．

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,

$$\begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_{k-1} & 1 \\ 1 & 0 \end{pmatrix}$$

$$\begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix} = \begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

とおくと,

$$\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}\begin{pmatrix} r_k \\ r_{k+1} \end{pmatrix} (k = 1, 2, \cdots, n)$$

である．よって

$$\frac{a}{b} = \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}\frac{r_k}{r_{k+1}} (k = 1, 2, \cdots, n)$$

となる．つまり, $\omega = \dfrac{a}{b}$, $\omega_k = \dfrac{r_k}{r_{k+1}}$ とおけば，実数の連分数展開と一致する．

5.2 二次行列と実数の連分数展開

5.2.1 最良近似分数

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 49

ω を正の実数とする．ω の k 回の連分数展開を,

$$\begin{aligned} \omega &= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_{k-1} & 1 \\ 1 & 0 \end{pmatrix}\omega_k \\ &= \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}\omega_k \end{aligned}$$

と置く．このとき,

(1) $\dfrac{P_1}{Q_1} < \dfrac{P_3}{Q_3} < \cdots < \dfrac{P_{2k-1}}{Q_{2k-1}} < \cdots < \omega < \cdots < \dfrac{P_{2k}}{Q_{2k}} < \cdots < \dfrac{P_4}{Q_4} < \dfrac{P_2}{Q_2}$

(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 数列 $\{P_n\}$, $\{Q_n\}$ の定義から

(1)

$$\begin{vmatrix} P_n & P_{n-1} \\ Q_n & Q_{n-1} \end{vmatrix} = \begin{vmatrix} q_0 & 1 \\ 1 & 0 \end{vmatrix}\cdots\begin{vmatrix} q_{n-1} & 1 \\ 1 & 0 \end{vmatrix} = (-1)^n$$

である．つまり，

$$\frac{P_n}{Q_n}-\frac{P_{n-1}}{Q_{n-1}}=\frac{(-1)^n}{Q_nQ_{n-1}}\quad,\quad \frac{P_{n+1}}{Q_{n+1}}-\frac{P_n}{Q_n}=\frac{(-1)^{n+1}}{Q_nQ_{n+1}}$$

したがって

$$\frac{P_{n+1}}{Q_{n+1}}-\frac{P_{n-1}}{Q_{n-1}}=(-1)^n\frac{Q_{n+1}-Q_{n-1}}{Q_{n-1}Q_nQ_{n+1}}$$

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，

$$\begin{aligned}\begin{pmatrix} P_n & P_{n-1}\\ Q_n & Q_{n-1}\end{pmatrix}^{-1}\omega &= \left((-1)^n\begin{pmatrix} Q_{n-1} & -P_{n-1}\\ -Q_n & P_n\end{pmatrix}\right)\omega\\ &= \frac{Q_{n-1}\omega-P_{n-1}}{-Q_n\omega+P_n}=\omega_n>0\end{aligned}$$

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 $\dfrac{P_1}{Q_1}=q_0<\omega$．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 を任意の奇数とする．$\dfrac{P_N}{Q_N}<\omega<\dfrac{P_{N+1}}{Q_{N+1}}$ であるがさらに，

$$\begin{aligned}0 &< \omega-\frac{P_N}{Q_N}<\frac{P_{N+1}}{Q_{N+1}}-\frac{P_N}{Q_N}\\ &= \frac{P_{N+1}Q_N-Q_{N+1}P_N}{Q_NQ_{N+1}}=\frac{(-1)^{N+1}}{Q_NQ_{N+1}}\\ &= \frac{1}{Q_NQ_{N+1}}<\frac{1}{Q_N^2}\end{aligned}$$

N を任意の偶数とする．同様に

$$\begin{aligned}0 &> \omega-\frac{P_N}{Q_N}>\frac{P_{N+1}}{Q_{N+1}}-\frac{P_N}{Q_N}\\ &= \frac{P_{N+1}Q_N-Q_{N+1}P_N}{Q_NQ_{N+1}}=\frac{(-1)^{N+1}}{Q_NQ_{N+1}}\\ &= \frac{-1}{Q_NQ_{N+1}}>-\frac{1}{Q_N^2}\end{aligned}$$

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) $P_nQ_{n-1} - Q_nP_{n-1} = (-1)^n$ より右辺は P_n, Q_n の公約数の倍数で，それが ± 1 であるから P_n, Q_n は互いに素．つまり $\dfrac{P_n}{Q_n}$ は既約である． □

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．これより小さい分母でよりよい近似が得られないという意味である．

定理 50

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 $\frac{p}{q}$ が

$$\frac{P_{2k-1}}{Q_{2k-1}} < \frac{p}{q} < \frac{P_{2k}}{Q_{2k}}$$

の範囲にあれば $P_{2k}Q_{2k-1} - Q_{2k}P_{2k-1} = (-1)^{2k} = 1$ なので，上の考察より $q > Q_{2k-1}$, Q_{2k} である．つまり，$\frac{P_{2k-1}}{Q_{2k-1}} < \frac{p}{q} < \omega$ や $\omega < \frac{p}{q} < \frac{P_{2k}}{Q_{2k}}$ となる分数 $\frac{p}{q}$ の分母は Q_{2k-1}, Q_{2k} より大きい．

すなわち $\frac{P_{2k-1}}{Q_{2k-1}}$, $\frac{P_{2k}}{Q_{2k}}$ は最良近似分数である． □

次の定理は「ペル方程式の解の存在」の定理 58 に対する別証明になっている．ここで x と y の関係を定理 58 の逆にしている．定理 58 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 $\omega = \frac{y}{x}$ と近似することを考えるので $|\omega x - y|$ を考察する．

定理 58(再掲)　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 49 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． □

5.2.2　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．対等もまた同値関係である．

定理 51 (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

$$\begin{pmatrix} a \\ c \end{pmatrix} = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

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．

$$\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}=\begin{pmatrix} P_{n+1} & P_n \\ Q_{n+1} & Q_n \end{pmatrix}$$

とおく．つまり

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

すると, $a=P_{n+1}$, $c=Q_{n+1}$ でさらに $P_{n+1}Q_n-Q_{n+1}P_n=(-1)^{n+1}=e$, つまり $aQ_n-cP_n=e$. よって $ad-bc=e$ より, $a(d-Q_n)=c(b-P_n)$. ところが a と c は互いに素であるから, $d-Q_n$ は c で割り切れる．

他方 $c>d>0$ かつ $c=Q_{n+1}\geqq Q_n\geqq 0$ より, $|d-Q_n|<c$. したがって $d=Q_n$ である．その結果 $b=P_n$ 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

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}=\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}$$

となる．つまり

$$\omega=\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_n & 1 \\ 1 & 0 \end{pmatrix}\theta$$

となる．

$\theta>1$ であるから，展開の一意性より 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 5.2.1　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,

$$\frac{1}{1}<\frac{7}{5}<\cdots<\sqrt{2}<\cdots<\frac{17}{12}<\frac{3}{2}$$

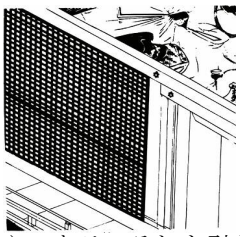
という近似分数列が得られる．

5.3　連分数と格子点

5.3.1　ミンコフスキーの定理

格子点　より一般的な格子点は後に定義する．**格子点**は座標平面と整数をつなぐ概念だ．

「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あり，幾何学的考察を整数論に適用して『数の幾何』なる分野を開拓した．

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．

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 52 (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 53
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 52 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 $\mathrm{P'Q}$ 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 54

$\alpha,\ \beta,\ \gamma,\ \delta$ 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． □

系 54.1

ω を与えられた無理数とする．

$$|\omega x-y|<\frac{1}{x}$$

となる整数 $x,\ y$ が無数に存在する． ■

証明　定理 54 において，$\alpha = \omega,\ \beta = -1,\ \gamma = 1,\ \delta = 0$ 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 を変化させることで

$$|\omega x - y| \leqq \frac{1}{x}$$

となる無数の x と y が得られる．ω が無理数なので，等号が成立することはない．　□

注意 5.3.1　これは後で示す近似定理 (定理 58) の別証明になっている．

5.3.2　近似分数

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 $m,\ n$ に対してベクトル

$$\overrightarrow{\mathrm{OP}} = m\overrightarrow{\mathrm{OA}} + n\overrightarrow{\mathrm{OB}}$$

で定まる点 P を**格子点**という．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 (ベクトル $\overrightarrow{\mathrm{OA}},\ \overrightarrow{\mathrm{OB}}$ で定まる**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**正方格子**という．

ここで, $a,\ b,\ c,\ d$ を整数としさらに $ad - bc = \pm 1$ であるとする．正方格子の格子点

$$\overrightarrow{\mathrm{OP}} = u\overrightarrow{e_1} + v\overrightarrow{e_2} = (u,\ v) \quad (u,\ v \in \mathbb{Z})$$

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，点 P は $\overrightarrow{\mathrm{OA}},\ \overrightarrow{\mathrm{OB}}$ で定まる格子点

$$m\overrightarrow{\mathrm{OA}} + v\overrightarrow{\mathrm{OB}}$$

と一致する．逆も成り立つ．つまり格子点が一対一に対応し，ベクトル $\overrightarrow{\mathrm{OA}},\ \overrightarrow{\mathrm{OB}}$ で定まる格子と正方格子の格子が一致する．

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．

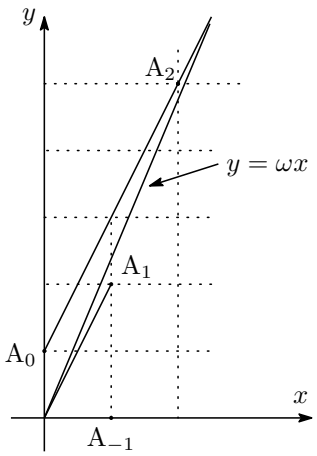
$$\omega = \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} q_{k-1} & 1 \\ 1 & 0 \end{pmatrix} \omega_k = \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} \omega_k$$

で

$$\begin{pmatrix} P_{k+1} \\ Q_{k+1} \end{pmatrix} = \begin{pmatrix} P_k q_k + P_{k-1} \\ Q_k q_k + Q_{k-1} \end{pmatrix}$$

となるのであった．このとき点 $\mathrm{A}_k(Q_k,\ P_k)$ とすると，点 A_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．$\mathrm{A}_{-1}(1,\ 0)$，$\mathrm{A}_0(0,\ 1)$ 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 $\mathrm{A}_1(1,\ q_0)$ である．　次に $\mathrm{A}_0(0,\ 1)$ を通り，$\overrightarrow{\mathrm{OA}_1}$ に平行な直線

$$l_1\ :\ \overrightarrow{\mathrm{OA}_0} + t\overrightarrow{\mathrm{OA}_1} = (t,\ tq_0 + 1)$$

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_2 である．つまり

$$\mathrm{A}_2(q_1,\ q_0q_1 + 1)$$

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 $P_2 = q_0q_1 + 1,\ Q_2 = q_1$ である．

A_{k-1}，A_k が定まったときに直線

$$\begin{aligned} l_k \quad &: \quad \overrightarrow{\mathrm{OA}_{k-1}} + t\overrightarrow{\mathrm{OA}_k} \\ &= \quad (Q_{k-1} + tQ_k,\ P_{k-1} + tP_k) \end{aligned}$$

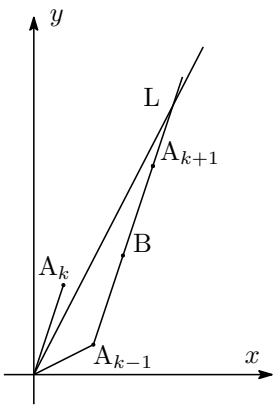
を引く．A_k は一般に奇数なら ω線 の下に，偶数なら ω線 の上にある．

$$\omega = \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}\omega_k$$

つまり $\omega = \dfrac{\omega_kP_k + P_{k-1}}{\omega_kQ_k + Q_{k-1}}$ であるから，

$$\begin{aligned} & \omega(Q_{k-1} + tQ_k) - (P_{k-1} + tP_k) > 0 \\ \Longleftrightarrow \quad & \frac{\omega_kP_k + P_{k-1}}{\omega_kQ_k + Q_{k-1}} - \frac{tP_k + P_{k-1}}{tQ_k + Q_{k-1}} > 0 \\ \Longleftrightarrow \quad & (\omega_k - t)(P_kQ_{k-1} - P_{k-1}Q_k) = (-1)^k(\omega_k - t) > 0 \end{aligned}$$

したがって，ω_k に下から (k 奇数のとき)，または上から (k 偶数のとき) 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 A_k である．



$t=1$ から A_k を与える t までの各 t の値に対して順次線分 $A_{k-1}A_{k+1}$ 上の格子点が定まり，これ以外にはない．

このように直線 $A_{k-1}A_{k+1}$ 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 $A_{-1}A_1A_3A_5\cdots$ と $A_0A_2A_4A_6\cdots$ の間には格子点が一つも存在しない．

格子点 A_k は，A_k と ω線 に関して同じ側にありその x 座標が 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 55

ω は与えられた無理数, A は与えられた 2 より大きい正の定数であり，整数 x は $0<x\leqq A$ にあるとする．

(1) $\omega x-y$ 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 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，$Q_{2n}<A$ を満たす最大の $2n$ を k とするとき，線分 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) 上図のように，線分 $A_{k-1}A_{k+1}$ 上の他の格子点を B とし, $A_{k-1}A_{k+1}$ と ω線 との交点を L とする．OA_k と $A_{k-1}A_{k+1}$ は平行なので格子点 A_k, A_{k-1}, B, A_{k+1} と ω線 との距離は，OA_k, LA_{k-1}, LB, LA_{k+1} と比例している．

線分 BA_{k+1} の長さは線分 OA_k の長さの整数倍であるから，

$$(\text{LB の長さ})\geqq(\text{OA}_k\text{の長さ})$$

となり，この結果，格子点 B から ω線 への距離は A_k から ω線 への距離以上である．

したがって題意をみたす格子点は 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 $x-\omega y$ において 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に関するさらに詳しい結果を紹介しよう．

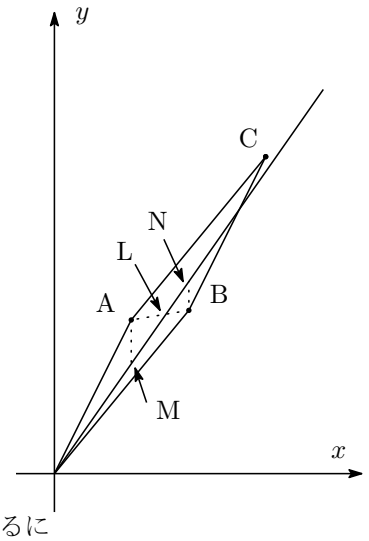
定理 56 (ヴァーレンの定理)

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. □

5.4 演習問題

練習問題 51 (解答 51)　$\sqrt{7}$ の近似分数を 5 番目まで作れ.

練習問題 52 (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．

関連入試問題

入試問題 42 (解答 42) ［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．

入試問題 43 (解答 43) ［04 名古屋大理系後期］

自然数 n に対して，a_n と b_n を

$$(3+2\sqrt{2})^n=a_n+b_n\sqrt{2}$$

を満たす整数とする．このとき以下の問に答えよ．

(1) $n\geqq 2$ のとき，a_n および b_n を a_{n-1} と b_{n-1} を用いて表せ．

(2) ${a_n}^2-2{b_n}^2$ を求めよ．

(3) (2) を用いて，$\sqrt{2}$ を誤差 $\dfrac{1}{10000}$ 未満で近似する有理数を 1 つ求めよ．

入試問題 44 (解答 44) ［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) $\left| a - \dfrac{P_n}{Q_n} \right| < \dfrac{1}{Q_n^2}$ $(n = 1,\ 2,\ \cdots)$

入試問題 45 (解答 45) ［71 京大理系］

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.

入試問題 46 (解答 46) ［新潟大過去問］

$a,\ b,\ c,\ d$ は自然数で, $\mathrm{A}(a,\ b)$, $\mathrm{B}(a + c,\ b + d)$, $\mathrm{C}(c,\ d)$, $\mathrm{O}(0,\ 0)$ 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.

入試問題 47 (解答 47) ［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.

入試問題 48 (解答 48)　［お茶の水女子大改題］

(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.

入試問題 49 (解答 49)

(1) $\sqrt{3}$ は無理数であることを証明せよ.

(2) ω が無理数，a, b が有理数で a が 0 でないとき，$a\omega + b$ が無理数であることを証明せよ.

(3) 座標平面上に 2 点 A$(p,\ q)$，B$(r,\ s)$ をとり，原点を O とする．△OAB が正三角形となるとき，$p,\ q,\ r,\ s$ のうち少なくとも 1 つは有理数とならないことを証明せよ.

第6章　ペル方程式

6.1　解集合の構造と解の存在

6.1.1　ペル方程式の解の構造

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．

(i) ペル方程式の整数解の集合の構造

(ii) ペル方程式に整数解が存在する証明

(iii) ペル方程式の整数解を構成する方法

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
$P = 4027701399389138208695911951306886478800$
$Q = 90084665203202024260494303744425250249$
であることがわかる! これを楽しみにして進もう．

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．

三つの入試問題

例 6.1.1

［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 6.1.2　［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 6.1.3　［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．

例 6.1.1

(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

$$(x_n)^2-3(y_n)^2=a^nb^n=1$$

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 6.1.1　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．

例 6.1.2 の解

(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)

$$\begin{aligned} y - y_1 &= y - (-x + 2y) = x - y \\ &= \frac{x^2 - y^2}{x + y} = \frac{(1 + 3y^2) - y^2}{x + y} \\ &= \frac{1 + 2y^2}{x + y} > 0 \\ y_1 &= -x + 2y \\ &= \frac{4y^2 - x^2}{x + 2y} = \frac{4y^2 - (1 + 3y^2)}{x + 2y} \\ &= \frac{y^2 - 1}{x + 2y} \geqq 0 \end{aligned}$$

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

$$\begin{aligned} x_1 &= 2x - 3y \\ &= \frac{4x^2 - 9y^2}{2x + 3y} = \frac{4x^2 - 3(x^2 - 1)}{2x + 3y} \\ &= \frac{x^2 + 3}{2x + 3y} > 0 \end{aligned}$$

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． □

例 6.1.3 の解

(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，

$$\begin{aligned} (aa' + 2bb')^2 - 2(ab' + a'b)^2 &= a^2(a'^2 - 2b'^2) - 2b^2(a'^2 - 2b'^2) \\ &= \pm(a^2 - 2b^2) \end{aligned}$$

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

$$A = \left\{ (x_n, y_n) \;\middle|\; \begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}, n \in \mathbb{N} \right\}$$
$$B = \{(x, y) \mid x^2 - 3y^2 = 1, x, y \in \mathbb{N}\}$$

とおくとき，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　ペル方程式に $(\pm 1,\ 0)$ 以外の解があることをこの節の最後に証明する．まず，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．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 57 (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，二次不定方程式 $x^2 - Dy^2 = \pm 1$ を考える．解 (x, y) の部分集合 S を次のように定める．

$$S = \left\{ (x, y) \;\middle|\; x^2 - Dy^2 = \pm 1,\ x, y \in \mathbb{Z},\ x + \sqrt{D}y > 0 \right\}$$

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．

$$S = \left\{ (x_n, y_n) \;\middle|\; (p + \sqrt{D}q)^n = x_n + \sqrt{D}y_n, \in \mathbb{Z} \right\}$$

(3) S はまた行列 $A = \begin{pmatrix} p & Dq \\ q & p \end{pmatrix}$ によって，

$$S = \left\{ (x_n, y_n) \left| \begin{pmatrix} x_n \\ y_n \end{pmatrix} = A^n \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ \in \mathbb{Z} \right. \right\}$$

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,

$$\begin{aligned} & (x_1x_2 + Dy_1y_2)^2 - D(x_1y_2 + x_2y_1)^2 \\ = \;& x_1^2x_2^2 + 2Dx_1x_2y_1y_2 + D^2y_1^2y_2^2 - Dx_1^2y_2^2 - 2Dx_1y_2x_2y_1 - Dx_2^2y_1^2 \\ = \;& (x_1^2 - Dy_1^2)(x_2^2 - Dy_2^2) \\ = \;& \pm 1 \end{aligned}$$

よって，$n=1$ のとき成立する．

次に，これより

$$\frac{1}{x_2+\sqrt{D}y_2}=\frac{x_2-\sqrt{D}y_2}{\pm 1}=\pm x_2\mp\sqrt{D}y_2 \quad \text{(複号同順)}$$

$x_2+\sqrt{D}y_2>0$ であるから，

$$\frac{1}{x_2+\sqrt{D}y_2}>0$$

かつ，$(\pm x_2)^2-D(\pm y_2)^2=\pm 1$ なので，$n=-1$ のときも成立し，

$$(x_1+\sqrt{D}y_1)(x_2+\sqrt{D}y_2)^{\pm 1}=s+\sqrt{D}t$$

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,

$$\begin{aligned} \begin{pmatrix} x_n \\ y_n \end{pmatrix} &= A^{n-1}\begin{pmatrix} x_1 \\ y_1 \end{pmatrix}=A^{n-1}\begin{pmatrix} p \\ q \end{pmatrix} \\ &= A^{n-1}\begin{pmatrix} p & Dq \\ q & p \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix}=A^{n}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \end{aligned}$$

□

6.1.2 ディリクレの原理

ペル方程式 $x^2-Dy^2=\pm1$ で解 $(\pm1,\ 0)$ 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

補題 8

(1) 自然数 n と k に対し，n 人の人を k 個の部屋に入れることを考える．n を k で割った商を q，余りを r とおく．もし $r>0$ ならば，少なくとも 1 つ，q 人より多くの人が入った部屋が存在する.

(2) 整数 $a_1,\ a_2,\ \cdots,\ a_n$ は，すべて $1\leqq a_1,\ a_2,\ \cdots,\ a_n\leqq n$ を満たし，さらにすべて異なる．このとき $a_1,\ a_2,\ \cdots,\ a_n$ は $1\sim n$ の値を一回ずつとる. ■

証明

(1) もしどの部屋も q 人以下なら，合計人数は qk 人以下になり $n-qk=r>0$ に反する．ゆえに q 人より多くの人が入った部屋が存在する．

(2) もし $a_1,\ a_2,\ \cdots,\ a_n$ のなかに，1〜n でとらない値があったとする．その値を除く数を記した箱を用意する．箱の数は $n-1$ 個以下になる．数 $a_1,\ a_2,\ \cdots,\ a_n$ をその値にしたがってこれらの箱に入れる．鳩の巣原理によって同じ箱に入るものが少なくとの一組できる．これは $a_1,\ a_2,\ \cdots,\ a_n$ の値がすべて異なることに矛盾する．ゆえに $a_1,\ a_2,\ \cdots,\ a_n$ は 1〜n の値を一回ずつとる． □

この明快な原理によって次のディリクレによる定理が示され，これをもとにペル方程式の解の存在が示される．次の定理はすでに無理数の連分数展開を用いて系 54.1 で示されているのであるが，次のように直接に示すことができる．

定理 58
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，

$$0<y\leqq n,\ |x-\omega y|<\frac{1}{n}$$

となる整数 (x, y) が少なくとも一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．

$$0\leqq \omega y-x<1$$

である．これらは全部で $n+1$ 個あるので，

鳩の巣原理によって上の 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．ωy_1-x_1，ωy_2-x_2，$(y_1\neq y_2)$ が同じ区間に属するとする．つまり

$$|(\omega y_1-x_1)-(\omega y_2-x_2)|<\frac{1}{n}$$

$y_1>y_2$ とし，$x=x_1-x_2,\ y=y_1-y_2$ とおく．この $(x,\ y)$ に対して

$$|\omega y-x|<\frac{1}{n}$$

である．

(ii) 各自然数 n に対して $0 < y \leqq n$ で $|\omega y - x| < \dfrac{1}{n}$ となる (x, y) が存在した．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．アルキメデスの原則 (『解析基礎』参照) によりこのような n は存在する．

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．$\dfrac{1}{n} \leqq \dfrac{1}{y}$ なので

$$|\omega y - x| < \frac{1}{y}$$

となる $(x,\ y)$ が無数にあることが示された． □

6.1.3 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 59

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，自明でない整数解 (X, Y), $(X > 0, Y > 0)$ をもつ． ■

証明　定理 58 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 $x + \sqrt{D}y < \dfrac{1}{y} + 2\sqrt{D}y$ ．$|x - \sqrt{D}y| < \dfrac{1}{y}$ と乗じて，

$$|x^2 - Dy^2| < \frac{1}{y^2} + 2\sqrt{D} \leqq 1 + 2\sqrt{D}$$

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，

$$\begin{aligned} l^2 &= (s^2-Dt^2)(u^2-Dv^2) \\ &= (su-Dtv)^2-D(sv-tu)^2 \\ &= (su-Dtv)^2-DY^2l^2 \end{aligned}$$

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．

6.2 連分数による解の構成

6.2.1 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，残念ながら高校では習わない．ぜひ意欲的な高校生が，実際に計算をしながら学び理解してほしい．

補題 9

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．

$$\begin{cases} p\omega^2+q\omega+r=0 \\ pu\omega^2+q'\omega+r'=0 \end{cases}$$

となる．第一式に u を乗じて第二式を引くことにより，$(q'-uq)\omega+(r'-ru)=0$ となる．ω が無理数で各係数が有理数なので $q'=qu$, $r'=ru$ である．つまり二つの二次方程式は，定数倍を除いて一意である．　□

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 60 (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．$D>0$ で D は平方数ではない．

$$p\left(\frac{a\omega_0+b}{c\omega_0+d}\right)^2+q\left(\frac{a\omega_0+b}{c\omega_0+d}\right)+r=0$$

分母をはらってまとめると，

$$\begin{aligned}&(pa^2+qac+rc^2)\omega_0^2 \\ &\quad+\{2pab+q(ad+bc)+2rcd\}\omega_0+(pb^2+qbd+rd^2)=0\end{aligned}$$

D が平方数ではないので，整数 $a,\ b,\ c,\ d$ に対して $pt^2+qt+r=0,\ p+qt+rt^2=0$ はいずれも有理数解をもたないので，$pa^2+qac+rc^2\neq 0,\ pb^2+qbd+rd^2\neq 0$ である．ゆえに，ω_0 は整数を係数とする二次方程式の解となり，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 5.2.1 のように，$\sqrt{2}$ は第二項目から循環し，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 10

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 r に分ける場合の数なので有限個である． □

定理 61 (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，実二次無理数 ω の $k+1$ までの展開を

$$\omega=\begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix}\omega_{k+1} \tag{6.1}$$

とすると，ω_{k+1} はあるところから一定の周期をもって同じ展開を繰りかえす．また，循環のはじまる番号 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) k を十分大きくとれば $-1<\omega'_k<0$ となることを示す．

等式 6.1 で 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．

(1) 十分大きい k をとり $-1 < \omega'_k < 0$ となっているとする.

$$\omega = \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} \omega_{k+1}$$

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，共役無理数が負である.

これら無理数の二次方程式は補題 9 より，係数の定数倍を除いて一意なので，係数は互いに素としてよい．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 10 の条件を満たす．補題 10 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.

(ii) 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.

それを示す．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.

(2) 循環のはじまる N は $\omega_N > 1, -1 < \omega'_N < 0$ となる最小の番号であることを示す.

N を循環のはじまる番号とし，番号 M は $N \leqq M$ とする．番号 M は循環部分にあるので，つまり $\omega_M = \omega_{M+j}$ なる ω_{M+j} が存在する．また，$\omega_M > 1, -1 < \omega'_M < 0$ も成立している.

さて,

$$\begin{aligned} \omega_{M-1} &= \begin{pmatrix} q_{M-1} & 1 \\ 1 & 0 \end{pmatrix} \omega_M \\ \omega_{M+j-1} &= \begin{pmatrix} q_{M+j-1} & 1 \\ 1 & 0 \end{pmatrix} \omega_{M+j} = \begin{pmatrix} q_{M+j-1} & 1 \\ 1 & 0 \end{pmatrix} \omega_M \end{aligned}$$

したがって $\omega_{M-1} - \omega_{M+j-1} = q_{M-1} - q_{M+j-1}$．ここで 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

$$\omega_{M-1} = \omega_{M+j-1}$$

この操作は $-1 < \omega_M < 0$ であるかぎり繰り返せ，番号が 1 ずつ減じる.

逆に十分大きい k では $-1 < \omega'_k < 0$ となるので，循環する部分は $-1 < \omega'_k < 0$ を満たしていなければならない.

よって，循環のはじまる 番号 N は $\omega_N > 1, -1 < \omega'_N < 0$ となる最小の番号である. □

k のことを二次無理数の連分数展開の周期と呼ぶ.

例 6.2.1 $\omega_1 = -3 + \sqrt{29}$ のとき. $D = 29$ である.

ω	二次方程式	ω'
$\omega_1 = -3 + \sqrt{29} = 2 + (\sqrt{29} - 5)$	$x^2 + 6x - 20 = 0$	$-3 - \sqrt{29} < -1$
$\omega_2 = \dfrac{1}{\sqrt{29} - 5} = \dfrac{\sqrt{29} + 5}{4} = 2 + \dfrac{\sqrt{29} - 3}{4}$	$4x^2 - 10x - 1 = 0$	$-1 < \dfrac{-\sqrt{29} + 5}{4} < 0$
$\omega_3 = \dfrac{4}{\sqrt{29} - 3} = \dfrac{\sqrt{29} + 3}{5} = 1 + \dfrac{\sqrt{29} - 2}{5}$	$5x^2 - 6x - 4 = 0$	$\dfrac{-\sqrt{29} + 3}{5}$
$\omega_4 = \dfrac{5}{\sqrt{29} - 2} = \dfrac{\sqrt{29} + 2}{5} = 1 + \dfrac{\sqrt{29} - 3}{5}$	$5x^2 - 4x - 5 = 0$	$\dfrac{-\sqrt{29} + 2}{5}$
$\omega_5 = \dfrac{5}{\sqrt{29} - 3} = \dfrac{\sqrt{29} + 3}{4} = 2 + \dfrac{\sqrt{29} - 5}{4}$	$4x^2 - 6x - 5 = 0$	$\dfrac{-\sqrt{29} + 3}{4}$
$\omega_6 = \dfrac{4}{\sqrt{29} - 5} = \sqrt{29} + 5 = 10 + \sqrt{29} - 5$	$x^2 - 10x - 4 = 0$	$-\sqrt{29} + 5$
$\omega_7 = \dfrac{1}{\sqrt{29} - 5} = \dfrac{\sqrt{29} + 5}{4} = \omega_2$		

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.

6.2.2 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 62 (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) 正の偶数 m に対して，$(x,\ y) = (P_{mk-1}, Q_{mk-1})$ は $x^2 - Dy^2 = 1$ の解である.

(ii) 正の奇数 m に対して，$(x,\ y) = (P_{mk-1}, Q_{mk-1})$ は $x^2 - Dy^2 = -1$ の解である.

(2) k が偶数の時

(i) 正整数 m に対して，$(x,\ y) = (P_{mk-1}, Q_{mk-1})$ は $x^2 - Dy^2 = 1$ の解である.

である．■

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 61 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．

$$\begin{aligned}
\sqrt{D} &= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix} x_1 \\
&= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} x_{k+1} \\
&= \begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix} x_1 \\
&= \begin{pmatrix} P_k & P_{k-1} \\ Q_k & Q_{k-1} \end{pmatrix} x_1 = \begin{pmatrix} P_{2k} & P_{2k-1} \\ Q_{2k} & Q_{2k-1} \end{pmatrix} x_1 \cdots = \begin{pmatrix} P_{mk} & P_{mk-1} \\ Q_{mk} & Q_{mk-1} \end{pmatrix} x_1
\end{aligned}$$

となる．ただし，

$$\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\left(\begin{pmatrix} q_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\begin{pmatrix} q_k & 1 \\ 1 & 0 \end{pmatrix}\right)^m = \begin{pmatrix} P_{mk} & P_{mk-1} \\ Q_{mk} & Q_{mk-1} \end{pmatrix}$$

とおいている．

$\sqrt{D} = \begin{pmatrix} P_{mk} & P_{mk-1} \\ Q_{mk} & Q_{mk-1} \end{pmatrix} x_1$ に，$x_1 = \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}\sqrt{D}$ を代入する．

$$\sqrt{D} = \begin{pmatrix} P_{mk-1} & P_{mk} - q_0 P_{mk-1} \\ Q_{mk-1} & Q_{mk} - q_0 Q_{mk-1} \end{pmatrix}\sqrt{D}$$

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，

$$p^2 - Dr^2 = ps - rq = \begin{vmatrix} p & q \\ r & s \end{vmatrix}$$

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. □

$$A = \begin{pmatrix} P_{k-1} & P_k - q_0 P_{k-1} \\ Q_{k-1} & Q_k - q_0 Q_{k-1} \end{pmatrix}$$

とおくと, $\sqrt{D} = A\sqrt{D}$ であり, 証明のなかで示しているように

$$A = \begin{pmatrix} P_{k-1} & DQ_{k-1} \\ Q_{k-1} & P_{k-1} \end{pmatrix}$$

となる. そして,

$$\begin{aligned} A^m &= \begin{pmatrix} P_{mk-1} & P_{mk} - q_0 P_{mk-1} \\ Q_{mk-1} & Q_{mk} - q_0 Q_{mk-1} \end{pmatrix} \\ &= \begin{pmatrix} P_{mk-1} & DQ_{mk-1} \\ Q_{mk-1} & P_{mk-1} \end{pmatrix} \end{aligned}$$

である. これからまた

$$(P_{k-1} + Q_{k-1}\sqrt{D})^m = P_{mk-1} + Q_{mk-1}\sqrt{D}$$

となることも (数学的帰納法で) 示される.

これでペル方程式の解の構造定理に現れる行列 $\begin{pmatrix} p & Dq \\ q & p \end{pmatrix}$ との関連も明確である.

例 6.2.2 $x^2 - 13y^2 = \pm 1$

$$\begin{aligned} \sqrt{13} &= \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \left(\frac{\sqrt{13}+3}{4} \right) \\ &= \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \left(\frac{\sqrt{13}+1}{3} \right) \\ &= \begin{pmatrix} 4 & 3 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \left(\frac{\sqrt{13}+2}{3} \right) \\ &= \begin{pmatrix} 7 & 4 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \left(\frac{\sqrt{13}+1}{4} \right) \\ &= \begin{pmatrix} 11 & 7 \\ 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} (\sqrt{13}+3) \end{aligned}$$

$$= \begin{pmatrix} 18 & 11 \\ 5 & 3 \end{pmatrix}\begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} \frac{\sqrt{13}+3}{4} \end{pmatrix}$$
$$= \begin{pmatrix} 119 & 18 \\ 33 & 5 \end{pmatrix}\begin{pmatrix} \frac{\sqrt{13}+3}{4} \end{pmatrix}$$

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.

$$\begin{aligned}
\sqrt{13} &= \begin{pmatrix} 3 & 1 \\ 1 & 0 \end{pmatrix}x_1 \\
&= \begin{pmatrix} 119 & 18 \\ 33 & 5 \end{pmatrix}x_1 = \begin{pmatrix} P_5 & P_4 \\ Q_5 & Q_4 \end{pmatrix}x_1 \\
&= \begin{pmatrix} 119 & 18 \\ 33 & 5 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}\begin{pmatrix} 119 & 18 \\ 33 & 5 \end{pmatrix}x_1, \text{代入！} \\
&= \begin{pmatrix} 4165 & 649 \\ 1189 & 180 \end{pmatrix}x_1 = \begin{pmatrix} P_{10} & P_9 \\ Q_{10} & Q_9 \end{pmatrix}x_1
\end{aligned}$$

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 $x^2 - 13y^2 = \pm 1$ の解が構成された. 実際,

$$18^2 - 13 \times 5^2 = -1$$

$$649^2 - 13 \times 180^2 = 1$$

である.

残された最後の問題は, ペル方程式の正の解がすべて P_{mk-1}, Q_{mk-1} から得られることを示すことである. この証明を一般の場合に示す.

定理 63 (構成定理 2)

$x^2 - Dy^2 = \pm 1$ 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 $\begin{vmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{vmatrix}=\pm1$ 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 57 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

$$\begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix}\sqrt{D}=\frac{\sqrt{D}x_1+Dy_1}{\sqrt{D}y_1+x_1}=\sqrt{D}$$

に代入する．

$$\begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix}\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\theta=\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\theta$$

$$\begin{aligned}\therefore\quad \theta &= \begin{pmatrix} 0 & 1 \\ 1 & -q_0 \end{pmatrix}\begin{pmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{pmatrix}\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\theta \\ &= \begin{pmatrix} y_1 & x_1 \\ x_1-q_0y_1 & Dy_1-q_0x_1 \end{pmatrix}\begin{pmatrix} q_0 & 1 \\ 1 & 0 \end{pmatrix}\theta \\ &= \begin{pmatrix} q_0y_1+x_1 & y_1 \\ (D-{q_0}^2)y_1 & x_1-q_0y_1 \end{pmatrix}\theta\end{aligned}$$

ここで $\begin{pmatrix} q_0y_1+x_1 & y_1 \\ (D-{q_0}^2)y_1 & x_1-q_0y_1 \end{pmatrix}=\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ とおく．

$\begin{vmatrix} x_1 & Dy_1 \\ y_1 & x_1 \end{vmatrix}=\pm1$ なので $ps-qr=\pm1$ である．$ps-qr=e$ とし，

$$\epsilon=r\theta+s,\quad \epsilon'=r\theta'+s$$

とおく．

$r=(D-{q_0}^2)y_1>0$ で $s=x_1-q_0y_1>x_1-\sqrt{D}y_1=\dfrac{\pm1}{x_1+\sqrt{D}y_1}>-1$ となるから，$\theta>1$ とあわせて，$\epsilon>1$ である．

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．

$$\begin{aligned}\therefore\quad \epsilon\epsilon' &= r^2\theta\theta'+(\theta+\theta')rs+s^2 \\ &= r^2\frac{(-q)}{r}-\frac{(s-p)}{r}rs+s^2 \\ &= -qr-s^2+ps+s^2=e=\pm1\end{aligned}$$

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 51 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． □

注意 6.2.1　ペル方程式の解の構造定理 57 を踏まえれば，$x + \sqrt{D}y > 1$ のなかでの最小解 (p, q) が $p = P_{k-1}, q = Q_{k-1}$ であることが確定した．

注意 6.2.2　周期 k が偶数の場合，すべての正整数 m に対して $(x,\ y) = (P_{mk-1}, Q_{mk-1})$ が $x^2 - Dy^2 = 1$ を満たし，この他に解がない．よって $x^2 - Dy^2 = -1$ には整数解がないことも示せた．

注意 6.2.3　これは二次体の数論になるのであるが，ペル方程式は次のような意味をもつ．

有理数体 $\mathbb{Q}$ に二次無理数 $\sqrt{D}$ をつけ加え四則演算で得られる数の集合は体をなす．これを $\mathbb{Q}(\sqrt{D})$ と書く．このなかで二次の項の係数が 1 である整数係数の二次方程式の解となっている数を $\mathbb{Q}(\sqrt{D})$ の整数といい，その集合を整数環という．

ペルの方程式は，この整数環の単数を求めることに関連している．したがってペル方程式の数論的な性質を解明するためには二次体の数論が必要なのである．しかしそれは『数論初歩』の範囲を越えるので，これを指摘するにとどめる．

6.2.3 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 $x^2 - Dy^2 = \pm 1$ 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)

$$\begin{cases} P_n = q_n \cdot P_{n-1} + P_{n-2} \\ Q_n = q_n \cdot Q_{n-1} + Q_{n-2} \end{cases}$$

(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 create 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 #1,"&",PA,"&",QA,"&",K:goto 210
200  print #1,"&",PB,"&",QB,"&",K
210  K=0
220  next D
230  end
```

$D = 331$ までの 6 桁以上の解　こうして得られた最小解のなかで 6 桁以上になるものを以下に掲げ，最後に $D = 1999$ を載せる．

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

また，1999 は素数で，

$P = 402770139938913820869591195130688647880 0$

$Q = 900846652032020242604943037444252502 49$

$k = 84$

である．

6.3 演習問題

練習問題 53 (解答 53)
$D = 2$, $D = 3$ のときに解の構造定理 57 を具体的に考える.

(1) $D = 2,\ D = 3$ のとき，それぞれ行列 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.

練習問題 54 (解答 54)
$\omega_1 = 4 + \sqrt{13}$ について循環がはじまるまで展開せよ.

練習問題 55 (解答 55)
$x^2 - 19y^2 = \pm 1$ の解を構成せよ.

練習問題 56 (解答 56)
$x^2 - 46y^2 = \pm 1$ の解を構成せよ.

関連入試問題

入試問題 50 (解答 50)　［98 お茶の水女子大後期］

(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.

入試問題 51 (解答 51)　［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) $\lim_{n\to\infty} \dfrac{y_{n+1} - y_n}{x_{n+1} - x_n}$ を求めよ.

第7章　素数分布

7.1　素数の分布とは

素数を 1 から 100 までのなかで書くと

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47$$
$$53,\ 59,\ 61,\ 67,\ 71,\ 73,\ 79,\ 83,\ 89,\ 97$$

の 25 個ある．ところが 5900 から 6000 のなかでは

$$5903,\ 5923,\ 5927,\ 5939,\ 5953,\ 5981,\ 5987$$

の 7 個しかない．5900 から 6000 の間の数 N が $N = mn$ と因数分解できて $m \leqq n$ とすると，$N = mn \geqq m^2$ となるが

$$73^2 = 5329,\ 79^2 = 6241$$

なので，小さい方の素因数は 73 以下である．73 までの素数で順に割って割り切れるものを除くことで 5900 から 6000 の間の素数はこれだけであることがわかる．

正整数 n が素数であるかどうかを判定したければ，$p^2 \leqq n$ の範囲の素数 p で割ってみればよい．いずれでも割り切れなければ素数と判定してよい．

例 7.1.1　1999 は素数である．

$43^2 = 1849$，$47^2 = 2209$ なので，2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 で割れるかどうかを調べればよい．いずれでも割り切れないので素数であることがわかる．

エラトステネスのふるい　このように，順に素数で割って割り切れる数をふるいにかけて除く．N までの数に対して $\sqrt{N}$ 以下の素数まで調べる．そのいずれでも割りきれずに残ったものが N 以下の素数である．

これが素数の選別法として有名な**エラトステネスの篩 (ふるい)** である．エラトステネス（Eratosthenēs，紀元前 276 頃〜前 192 頃) は古代ギリシアの数学者，天文学者，地理学者だった．はじめて赤道の周囲を測量し、約 45000 km と算出した人でもある．主著は「地理学」である．

ところで「篩 (ふるい)」とは何か.「候補をふるいにかける」とか,「一次試験でふるい落とされる」などの言い方は残っているが「篩 (ふるい)」そのものはなかなか見かけない．

1831 年 (天保 2) に薩摩藩主島津重豪 (しまづしげひで) が曾槃・白尾国柱らに命じて作らせた農業書『成形図説』に図が載っているので紹介しよう．この書は農事・五穀・疎菜・薬草・草木・鳥類などについて，和漢洋の諸書で考証し，さらに綿密な図を掲げ，編纂させた百科全書である．全 100 巻の大部なものだ．和語，漢語，オランダ語の名前を記し，説明を付けている．

このような木製や竹製ではない現代のふるいは，工事しているところで小石を除くのに使われている．鉄製で電気で振動させている．

どのように素数が分布しているのかということを，素数の分布に関する問題という．これを考えるために，正の実数 x を越えない素数の個数を $\pi(x)$ と表そう．

$$\pi(100) = 24,\ \pi(6000) - \pi(5900) = 7$$

である．

7.2 素数が無数にあることの別証明

定理 8 によって

$$\lim_{x\to\infty} \pi(x) = \infty$$

である．$\pi(x)$ は確かにいくらでも大きくなるのだが，しかしその大きさの程度は x よりもずっと小さく

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0$$

である．この二つを統一的な方法で示し，定理 8 の別解を作る．それは解析的な方法である．

定理 64

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

(2) $\lim_{x\to\infty} \dfrac{\pi(x)}{x} = 0$

この証明のために次の等式を補題としてあらかじめ示しておこう．

補題 11

$p_1,\ p_2,\ p_3,\ \cdots,\ p_r$ を相異なる素数とする．実数 x を越えない自然数のなかで $p_1,\ p_2,\ p_3,\ \cdots,\ p_r$ のいずれでも割り切れないものの個数 N は次式で与えられる．

$$\begin{aligned} N &= [x] - \left[\frac{x}{p_1}\right] - \left[\frac{x}{p_2}\right] - \cdots - \left[\frac{x}{p_r}\right] \\ &\quad + \left[\frac{x}{p_1p_2}\right] + \left[\frac{x}{p_1p_3}\right] + \cdots + \left[\frac{x}{p_{r-1}p_r}\right] - \cdots + (-1)^r \left[\frac{x}{p_1p_2\cdots p_r}\right] \end{aligned} \tag{7.1}$$

ただし $[x]$ は x を超えない最大の整数を表す． ■

証明 r に関する数学的帰納法で証明する．

$r = 1$ のときは $1,\ 2,\ \cdots,\ [x]$ のなかで p_1 の倍数は

$$1\cdot p_1,\ 2\cdot p_1,\ \cdots,\ \left[\frac{x}{p_1}\right] p_1$$

だけある．したがって実数 x を越えない自然数のなかで p_1 で割り切れないものの個数は

$$[x] - \left[\frac{x}{p_1}\right]$$

となり，等式 (7.1) は成立する．

$r=k$ のとき ① が成立するとする．$r=k+1$ とし，さらに p_{k+1} が追加されたとする．このときは，さらに p_{k+1} の倍数 yp_{k+1} $\left(y \leqq \dfrac{x}{p_{k+1}}\right)$ を除かなければならない．そのうち y が $p_1,\ p_2,\ \cdots,\ p_k$ 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の個数は，$\dfrac{x}{p_{k+1}}$ を越えない整数のなかで $p_1,\ p_2,\ \cdots,\ p_k$ で割り切れないものの個数である．ゆえに求める個数 N_{k+1} は

$$\begin{aligned} N_{k+1} &= [x]-\left[\frac{x}{p_1}\right]-\left[\frac{x}{p_2}\right]-\cdots+\left[\frac{x}{p_1p_2}\right]+\left[\frac{x}{p_1p_3}\right]+\cdots+(-1)^k\left[\frac{x}{p_1p_2\cdots p_k}\right] \\ &\quad -\left\{\left[\frac{x}{p_{k+1}}\right]-\left[\frac{x}{p_1p_{k+1}}\right]-\left[\frac{x}{p_2p_{k+1}}\right]-\cdots+(-1)^k\left[\frac{x}{p_1p_2\cdots p_{k+1}}\right]\right\} \\ &= [x]-\left[\frac{x}{p_1}\right]-\left[\frac{x}{p_2}\right]-\cdots-\left[\frac{x}{p_{k+1}}\right]+\left[\frac{x}{p_1p_2}\right]+\cdots+\left[\frac{x}{p_1p_{k+1}}\right] \\ &\quad -\left[\frac{x}{p_1p_2p_3}\right]-\cdots-\left[\frac{x}{p_1p_2p_{k+1}}\right]+\cdots+(-1)^{k+1}\left[\frac{x}{p_1p_2\cdots p_{k+1}}\right] \end{aligned}$$

ゆえに $k+1$ のときも成立し，題意が示された． □

さらに微積から補題をもう一つ．

補題 12

$$\lim_{n\to\infty}\sum_{k=1}^{n}\frac{1}{k}=+\infty$$

である． ■

証明　関数 $\dfrac{1}{x}$ は単調減少なので区間 $[k,\ k+1]$ で

$$\int_k^{k+1}\frac{1}{x}\,dx<\frac{1}{k}$$

$$\therefore\quad \sum_{k=1}^{n}\int_k^{k+1}\frac{1}{x}\,dx<\sum_{k=1}^{n}\frac{1}{k}$$

つまり

$$\int_1^{n+1}\frac{1}{x}\,dx=\log(n+1)<\sum_{k=1}^{n}\frac{1}{k}$$

$\lim\limits_{n\to\infty}\log(n+1)=+\infty$ より

$$\sum_{k=1}^{\infty}\frac{1}{k}=+\infty$$

□

以上の準備をして定理 64 を証明しよう．

定理 64 の証明

(1) x 以下の素数にわたる積

$$\prod_{p\leqq x}\frac{1}{1-\dfrac{1}{p}}=\prod_{p\leqq x}\left(1-\frac{1}{p}\right)^{-1}$$

を考える．

$$\frac{1}{1-\frac{1}{p}} = 1 + \frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + \cdots$$

であるから

$$\prod_{p \leqq x} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \leqq x} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots\right)$$

は，x 以下の素数とそのべきのみを因数にもつような数 k 全体にわたる和

$$\sum \frac{1}{k}$$

である．x 以下の正整数 n はもちろん x 以下の素数とそのべきのみを因数にもつような数であるから

$$\prod_{p \leqq x} \left(1 - \frac{1}{p}\right)^{-1} \geqq \sum_{n \leqq x} \frac{1}{n} \tag{7.2}$$

となる．

ここで補題 12 より，$x \to \infty$ のとき 7.2 の右辺は発散する．

もし $\lim_{x\to\infty} \pi(x)$ が有限であれば，$x \to \infty$ のとき 7.2 の左辺は有限個の素数にわたる和となり収束する．これは矛盾なので $\lim_{x\to\infty} \pi(x) = \infty$ が示された．

(2) $p_1 = 2,\ p_2 = 3,\ \cdots$ と小さい方から r 個の素数が与えられているとする．これらの素数は x より小さいものとする．x 以下の素数は，この r 個の素数と x 以下の数でこれら r 個の素数で割り切れない数をあわせた数の一部である．したがって

$$\begin{aligned}\pi(x) \quad \leqq \quad & r + [x] - \left[\frac{x}{p_1}\right] - \left[\frac{x}{p_2}\right] - \cdots - \left[\frac{x}{p_r}\right] \\ & + \left[\frac{x}{p_1p_2}\right] + \left[\frac{x}{p_1p_3}\right] + \cdots + \left[\frac{x}{p_{r-1}p_r}\right] - \cdots + (-1)^r \left[\frac{x}{p_1p_2\cdots p_r}\right]\end{aligned}$$

補題 11 の和の項数は 2^r である．$[x] < x,\ -[x] \leqq -x + 1$ なので，あわせて $\pm[x] < \pm x + 1$ がなりたつ．したがって

$$\begin{aligned}& [x] - \left[\frac{x}{p_1}\right] - \left[\frac{x}{p_2}\right] - \cdots - \left[\frac{x}{p_r}\right] \\ & \quad + \left[\frac{x}{p_1p_2}\right] + \left[\frac{x}{p_1p_3}\right] + \cdots + \left[\frac{x}{p_{r-1}p_r}\right] - \cdots + (-1)^r \left[\frac{x}{p_1p_2\cdots p_r}\right] \\ < \quad & 2^r + x - \frac{x}{p_1} - \frac{x}{p_2} - \cdots - \frac{x}{p_r} \\ & \quad + \frac{x}{p_1p_2} + \frac{x}{p_1p_3} + \cdots + \frac{x}{p_{r-1}p_r} - \cdots + (-1)^r \frac{x}{p_1p_2\cdots p_r} \\ = \quad & 2^r + x \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)\end{aligned}$$

となる．$r + 2^r < 2^{r+1}$ であるから

$$\pi(x) < 2^{r+1} + x \prod_{k=1}^{r} \left(1 - \frac{1}{p_k}\right)$$

$$\therefore \quad \frac{\pi(x)}{x} < \frac{2^{r+1}}{x} + \prod_{k=1}^{r}\left(1-\frac{1}{p_k}\right)$$

ここで r を $2^{r+1} \leqq \sqrt{x}$ である最大のものにとる．このとき

$$\frac{\pi(x)}{x} \leqq \frac{1}{\sqrt{x}} + \prod_{k=1}^{r}\left(1-\frac{1}{p_k}\right)$$

$x \to \infty$ のとき $r \to \infty$ である．したがって (1) で示したように

$$\lim_{x\to\infty} \prod_{k=1}^{r}\left(1-\frac{1}{p_k}\right)^{-1} = \infty$$

つまり

$$\lim_{x\to\infty} \prod_{k=1}^{r}\left(1-\frac{1}{p_k}\right) = 0$$

$\lim_{x\to\infty} \frac{1}{\sqrt{x}} = 0$ とあわせて

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = 0$$

が示された． □

7.3 素数分布の探求

その上で x を越えない素数の個数を表す関数 $\pi(x)$ はどのような性質をもっているのかを考えよう．このような場合，まず実験して，x の一定の範囲にある素数の個数を求めていくことが大切だ．自分でプログラムを組んで，書き出していくのがいちばんよい．エラチステネスのふるいの方法はプログラムを書く練習のいちばん初歩の問題だ．

個数関数のグラフ　そのうえでアメリカテネシー大学が展開している The Prime Pages に載っている表を参考にする．そのなかの How Many Primes Are There?には，段階を区切って素数の個数が表になっている．このページを見るときは，ブラウザソフトの表示文字種「エンコード」を「Unicode(UTF-7)」にするときれいになる．ここでは多くの結果が証明なしに紹介されている．

100 までだと規則性があるようには見えない．1000 になると少し上に凸な曲線に見え，1000000 となるとやや上に凸なきれいな曲線である．この曲線は対数のグラフに似ているではないか．このようなことをふまえて多くの人が $\pi(x)$ の性質を研究した．

実験的推測　$\pi(x)$ で $x = 10,\ 100,\ 1000,\ 10000$ のときの表に次の値を書き加える．

x	$\pi(x)$	$\log_{10} x$	$\pi(x)\log_{10} x$
10	4	1	4
100	25	2	50
1000	168	3	504
10000	1229	4	4916

$\frac{1}{2}x$ の値がおよそ $\pi(x)\log_{10}x$ になる．ということは

$$\frac{1}{2}x = \pi(x)\log_{10}x \quad \Longleftrightarrow \quad \frac{x}{\log x} = \pi(x)\frac{2}{\log 10}$$

なので，$\dfrac{x}{\log x}$ の値がほぼ $\pi(x)\dfrac{2}{\log 10}$ になるということである．

このようなことを昔の人はいろいろ調べた．計算機のない時代には手計算で調べた．$\log 10$ は約 2.30 なのでこの計算では $\dfrac{x}{\log x}$ はほぼ $0.868\pi(x)$ ということになる．もっと x を大きくとるとどのような値に収束するか，これをいろいろと推測したのだ．その結果 1801 年にルジャンドルは

$$\pi(x) \sim \frac{x}{\log x}$$

であろうと予想した．ただしここで $x > 0$ で定義された 2 つの関数 $f(x)$ と $g(x)$ が

$$f(x) \sim g(x)$$

であるとは，

$$\lim_{x\to\infty}\frac{f(x)}{g(x)} = 1$$

となることとする．さらにこれとは独立にガウスは

$$\pi(x) \sim \int_0^x \frac{dt}{\log t}$$

を予想した．このあたりは先のページにも載っている．

この分野で実質的に最初の前進をしたのがロシアのチェビシェフである．かれは 1850 年に次のことを示した．先のページには次のように書かれている．

> Tchebycheff made the first real progress toward a proof of the prime number theorem in 1850, showing there exist positive constants $a < 1 < b$ such that
>
> $$\frac{ax}{\log x} < \pi(x) < \frac{bx}{\log x}$$
>
> and that if $\dfrac{\pi(x)}{\dfrac{x}{\log x}}$ had a limit, then its value must be one.

ここで述べられているチェビシェフの定理の前半は，初等的に示すことができる．

定理 65
正の定数 $c_1 < 1 < c_2$ で，$x \geqq 2$ に対して

$$c_1\frac{x}{\log x} < \pi(x) < c_2\frac{x}{\log x}$$

となるものが存在する． ■

これを示すためにひとつ補題を証明する．

補題 13
自然数 $n!$ の素因数分解に含まれる素数 p の個数は,

$$\sum_{l=1}^{[\log_p n]} \left[\frac{n}{p^l}\right]$$

である. ■

証明 $[\log_p n]$ は $p^k \leqq n$ となる最大の k の値である.
1 から n までの自然数のなかでちょうど p^l で割り切れるものの個数は

$$\left[\frac{n}{p^l}\right] - \left[\frac{n}{p^{l+1}}\right]$$

である. $l \geqq [\log_p n] + 1$ に対しては $\dfrac{n}{p^l} < 1$ となり $\left[\dfrac{n}{p^l}\right] = 0$ である. したがって求める個数は

$$\begin{aligned}
&\sum_{l=1}^{[\log_p n]} l\left(\left[\frac{n}{p^l}\right] - \left[\frac{n}{p^{l+1}}\right]\right) \\
= &\sum_{l=1}^{[\log_p n]} \left(l\left[\frac{n}{p^l}\right] - (l+1)\left[\frac{n}{p^{l+1}}\right]\right) + \sum_{l=1}^{[\log_p n]} \left[\frac{n}{p^{l+1}}\right] \\
= &\sum_{l=1}^{[\log_p n]} \left[\frac{n}{p^l}\right]
\end{aligned}$$

である. □

定理 65 の証明

$$c_1 \frac{x}{\log x} < \pi(x)$$

となる正の定数の存在を示す.
m を正整数として, 整数

$${}_{2m}\mathrm{C}_m = \frac{(2m)!}{m!m!}$$

の大きさを 2 通りの方法で評価する.
$p \leqq 2m$ である素数に対して $\dfrac{(2m)!}{m!m!}$ の素因数分解に含まれる素数 p の個数は, 補題 13 より

$$\sum_{l=1}^{[\log_p(2m)]} \left(\left[\frac{2m}{p^l}\right] - 2\left[\frac{m}{p^l}\right]\right)$$

である. m を p^l で割った余りを r とするとき

$$\left[\frac{2m}{p^l}\right] - 2\left[\frac{m}{p^l}\right] = \begin{cases} 0 & \left(0 \leqq r < \dfrac{p^l}{2}\right) \\ 1 & \left(\dfrac{p^l}{2} \leqq r < p^l\right) \end{cases}$$

である. したがって

$$\sum_{l=1}^{[\log_p(2m)]} \left(\left[\frac{2m}{p^l}\right] - 2\left[\frac{m}{p^l}\right]\right) \leqq \left[\log_p(2m)\right]$$

これから

$$\frac{(2m)!}{m!m!} \leqq \prod_{p \leqq 2m} p^{[\log_p(2m)]}$$

一方，$p^{[\log_p(2m)]} \leqq 2m$ であるから

$$\prod_{p \leqq 2m} p^{[\log_p(2m)]} \leqq (2m)^{\pi(2m)}$$

つまり

$$\frac{(2m)!}{m!m!} \leqq (2m)^{\pi(2m)}$$

となる．ところが

$$\begin{aligned} \frac{(2m)!}{m!m!} &= \frac{(2m)(2m-1)\cdots(m+1)}{m(m-1)\cdots 1} \\ &= \frac{(m+m)(m+m-1)\cdots(m+1)}{m(m-1)\cdots 1} = (1+1)\left(\frac{m}{m-1}+1\right)\cdots(m+1) \\ &\geqq 2\cdot 2\cdots 2 = 2^m \end{aligned}$$

なので，上の結果より

$$2^m \leqq (2m)^{\pi(2m)}$$

対数をとって

$$m\log 2 \leqq \pi(2m)\log(2m)$$

つまり

$$\frac{\log 2}{2}\cdot\frac{2m}{\log(2m)} \leqq \pi(2m)$$

次に $m \geqq 1$ に対して

$$\frac{2m}{2m+1} \geqq \frac{2}{3}$$

であるから

$$\begin{aligned} &\pi(2m+1)\log(2m+1) > \pi(2m)\log(2m) \geqq \frac{\log 2}{2}(2m) \\ > \quad &\frac{\log 2}{2}\cdot\frac{2}{3}(2m+1) \end{aligned}$$

つまり

$$\frac{\log 2}{3}\cdot\frac{2m+1}{\log(2m+1)} \leqq \pi(2m+1)$$

したがって整数 $[x]$ に対して

$$\frac{\log 2}{3}\cdot\frac{[x]}{\log[x]} \leqq \pi([x]) \leqq \pi(x)$$

が成り立つ．ここで $[x] > x-1$ なので

$$\begin{aligned} \frac{[x]}{\log[x]} &> \frac{x-1}{\log(x-1)} > \frac{x-1}{\log x} \\ &= \frac{x}{\log x}\left(1-\frac{1}{x}\right) \geqq \frac{1}{2}\cdot\frac{x}{\log x} \end{aligned}$$

したがって

$$\frac{\log 2}{6} \cdot \frac{x}{\log x} < \pi(x)$$

$c_1 = \dfrac{\log 2}{6}$ とおけばよい.

次に,

$$\pi(x) < c_2 \frac{x}{\log x}$$

となる c_2 の存在を示す.

$m < p \leqq 2m$ の範囲の素数は $\dfrac{(2m)!}{m!m!}$ の分母を割らない. よって $\dfrac{(2m)!}{m!m!}$ は $\displaystyle\prod_{m<p\leqq 2m} p$ で割り切れる. つまり

$$m^{\pi(2m)-\pi(m)} < \prod_{m<p\leqq 2m} p \leqq \frac{(2m)!}{m!m!}$$

これから

$$(\pi(2m) - \pi(m)) \log m < \log \frac{(2m)!}{m!m!}$$

ところが

$${}_{2m}\mathrm{C}_m < \sum_{k=0}^{2m} {}_{2m}\mathrm{C}_k = 2^{2m}$$

より

$$\log \frac{(2m)!}{m!m!} < 2m \log 2$$

$$\therefore \quad (\pi(2m) - \pi(m)) < 2 \log 2 \frac{m}{\log m}$$

$y \geqq 2$ に対して

$$[2y] \leqq 2y < 2[y] + 2$$

なので

$$\begin{aligned} \pi(2y) - \pi(y) &= \pi([2y]) - \pi([y]) \\ &\leqq \pi(2[y]+2) - \pi([y]) < \pi(2[y]) + 2 - \pi([y]) \\ &< 2 \log 2 \frac{[y]}{\log [y]} + 2 < (2 \log 2 + 2) \frac{y}{\log y} \end{aligned}$$

ここで x に対して $2^{l+1} \leqq x < 2^{l+2}$ となる l をとり y に $\dfrac{x}{2}, \cdots, \dfrac{x}{2^l}$ を順次代入する.

$$\pi\left(\frac{x}{2^{j-1}}\right) - \pi\left(\frac{x}{2^j}\right) < (2 \log 2 + 2) \frac{\dfrac{x}{2^j}}{\log x - j \log 2} < (2 \log 2 + 2) \frac{\dfrac{x}{2^j}}{\log x}$$

$j = 1, \ldots, l$ について辺々加えることにより

$$\begin{aligned} & \pi(x) - \pi\left(\frac{x}{2^l}\right) \\ < \quad & (2 \log 2 + 2) \frac{x}{\log x} \left(\frac{1}{2} + \cdots + \frac{1}{2^l}\right) \\ < \quad & (2 \log 2 + 2) \frac{x}{\log x} \end{aligned}$$

$$\pi(x) < (2\log 2 + 2)\frac{x}{\log x} + \pi\left(\frac{x}{2^l}\right)$$

$2 \leqq \dfrac{x}{2^l} < 4$ なので $\pi\left(\dfrac{x}{2^l}\right) \leqq 2$ で，さらに $x \geqq 2$ のとき $1 < \dfrac{x}{\log x}$ であるから

$$\pi(x) < (2\log 2 + 4)\frac{x}{\log x}$$

つまり $c_2 = (2\log 2 + 4)$ とすればよい. □

定理 65 は定理 64 の (2) の別証明になっている．実際,

$$\frac{c_1}{\log x} < \frac{\pi(x)}{x} < \frac{c_2}{\log x}$$

なので $x \to \infty$ のとき，はさみうちの原理によって $\dfrac{\pi(x)}{x} \to 0$ である.

チェビシェフはさらにこの c_1, c_2 を調べ,

$$0.92\frac{x}{\log x} < \pi(x) < 1.11\frac{x}{\log x}$$

まで示した．またもし $\lim\limits_{x\to\infty} \dfrac{\pi(x)\log x}{x}$ が収束するならば，それは 1 であることも示した.

7.4 素数定理

チェビシフのこの証明からさらの半世紀後，1896 年になってフランスの数学者アダマール (J.Hadamard) とプーサン (C.de la Vallée Poussin) によってほとんど同時に独立に

定理 66 (素数定理)

$$\pi(x) \sim \frac{x}{\log x}$$

が示されたのだ．その証明には次の関数が本質的に用いられた.

リーマンの ζ 関数　数 s に対して

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

を**リーマンの ζ 関数**という．リーマンの ζ 関数は実数 s が $s > 1$ にあれば収束する．すべての自然数はただ一つの素因数分解をもつのであるから $s > 1$ のとき $\zeta(s)$ は

$$\zeta(s) = \prod_p \frac{1}{1 - \dfrac{1}{p^s}}$$

と素数にわたる積で表される．この積を**オイラー積**という．逆にリーマンの ζ 関数がオイラー積と一致するということが，素因数分解の一意的な存在を示している.

定理 64 の証明は $\zeta(1)$ が発散することから，素数が無数に存在することを示したのである.

自然数全体にわたる和が，素数全体にわたる積と一致する．このことは素数の分布を調べることと，ζ 関数の性質を調べることのあいだに深い関係がることを意味している．

$$\begin{aligned}\zeta(2) &= 1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\cdots=\frac{\pi^2}{6}\\ \zeta(4) &= 1+\frac{1}{2^4}+\frac{1}{3^4}+\frac{1}{4^4}+\cdots=\frac{\pi^4}{90}\end{aligned}$$

などの特別な値は初等的に知ることができる．この証明などは『数学対話』「円周率を表す」にある．

リーマンは ζ 関数を，複素関数として研究し時代を画する論文を残した．その中には今日もまだ未解決の問題が提起されている．ζ は整数論できわめて重要であるばかりでなく，その他の分野でも頻繁に登場する．彼らの素数定理の証明はこのリーマンの ζ 関数を本質的に用いる．1949 年になってセルバーグ (A.Selberg) が ζ 関数を用いない初等的な方法で示した．これらについては『数論初歩』の範囲をこえる．

青空学園では 2005 年〜2007 年に数論の読者会をした．そこで『解析的整数論』(末綱恕一，岩波書店) に載っている素数定理の証明を紹介した．読書会に使った『数論 I』の定理 7.3 までは用いる．その他は出来るかぎり完結的に整理した．といっても，関数を中心に複素関数論を使うので，理解は難しい．それは『数学対話』「素数の分布」をたどれば読める．

素数については今日もまだ未解決な問題がたくさんあることを指摘し本節を終えなければならない．それにしても，この世界に素数があるということはなんと不思議なことなのだろう．

第8章　存在と構成

存在するのか，という問い　自然数の集合は本当に存在するのか.「存在するのか」と問うのが近代である．ではどのようなことが示せれば存在するといえるのか．自然数の集合が存在するとは，自然数の公理を満たす集合が構成でき，かつその公理が互いに矛盾しないこととととらえる．さらに自然数の公理を満たす集合が二つあれば，その二つの集合の間には一対一の対応が存在し，その対応で演算の結果も対応する，つまり代数的な構造物として互いに同型であることが示せれば，数学の対象として確定する.

自然数を構成することが可能であることを確認することは，数学の基礎を確認するという意味において大変重要なのであるが，公理を満たす自然数の存在を前提として進んでいく整数の論証のうえでは必要でない．従って本節と次節，および整数と有理数の構成問題は最後においた.

8.1　自然数の構成

8.1.1　ペアノの公理

自然数の構成　自然数は数のなかでもっとも根源的なものであるから，あらゆる数の存在を前提とせずに構成しなければならない．そしてそれは可能なのだ．近代数学では集合とその構造を定義することで，数学としての対象を定義する．それが次に紹介するペアノ (G.Peano,1858-1932) による「公理」である.

定義 6 (ペアノの公理)

次の性質を持つ集合 $\mathbb{N}$ を考える.

(i) 1 という要素がある.

(ii) 集合 $\mathbb{N}$ の要素 x に対し集合 $\mathbb{N}$ の要素 $x+1$ を対応させる規則が定まっている.

(iii) $x+1=y+1$ ならば $x=y$ である.

(iv) 要素 $x+1=1$ となる要素 x は存在しない.

(v) 集合 $\mathbb{N}$ は (i)(ii)(iii)(iv) を満たす最小の集合である．つまり $\mathbb{N}$ のどのような真部分集合も (i)(ii)(iii)(iv) を満たさない.

このとき $\mathbb{N}$ を自然数の集合といい，$\mathbb{N}$ の要素を自然数という.　■

1 と記号+と (　) が組み合わさったものを要素とする集合

$$\{1,\ 1+1,\ (1+1)+1,\ ((1+1)+1)+1,\ \cdots\}$$

がまさに $\mathbb{N}$ である．ここで $(\quad)+1$ は，上の公理で作られた $\mathbb{N}$ の要素を $(\quad)$ 内に記し，さらにそれに (ii) の対応を施すことを意味する．これは要するに，1 が最初で，その後はつねに次の要素があって，それ以外の余分なものはない集合を自然数という，ということである．

$1,\ 1+1,\ (1+1)+1,\ ((1+1)+1)+1, \cdots$ を表記の簡単のために

$$1,\ 2,\ 3,\ \cdots$$

と書くのである．

この公理は，人間の「数える」という行為をそのまま定式化したものであるが，これが自然数論の基礎となるには色んな検証が必要である．数学基礎論では，この公理体系は矛盾が起こらないことが示されている．さらにこの公理はわれわれの自然数に対する素朴な理解と合致し，同型なものはひとつしかないことが示される．無矛盾性の証明は難しい．ここでは数学的帰納法の原理を含む自然数の基本性質がペアノの公理で構成された集合で成立することと，同型の意味を再確認したうえで自然数の体系はすべて同型であることを示そう．体系に矛盾がないことと，同じ型をしたものがただひとつであること，これで数学研究の対象が明確に定義できたのである．

自然数の基本性質　ここで定理の記述と証明のために「昇列」を定義する．$\mathbb{N}$ の部分集合 K で

$$x \in K \quad \Rightarrow \quad x+1 \in K$$

が成り立つとき K を「昇列」という．$\mathbb{N}$ の要素 a を含むすべての昇列の共通部分を $K(a)$ とする．

定理 67

自然数の集合 $\mathbb{N}$ は次の性質をもつ．

(1) 1 を含む昇列はひとつしかなく $\mathbb{N} = K(1)$ である．

(2) **数学的帰納法の原理** 自然数の集合 $\mathbb{N}$ の部分集合 M において

(i) $1 \in M$

(ii) $k \in M \Rightarrow k+1 \in M$

が成り立てば $N = M$ である．

(3) 1 以外のすべての要素 x は $x = z+1$ となる要素 z をただ一つもつ．この z を $x-1$ と表す．

(4) $\mathbb{N}$ の任意の空でない部分集合 M には，$m \in M$ で $M \subset K(m)$ となるものがただひとつある．これを M の最小要素という． ■

証明

(1)　1 を含む任意の昇列 K に対し，$\mathbb{N}$ において x に $x+1$ を対応させる規則を K に制限した規則を考える．定義より，$k \in K$ のとき $k+1 \in K$ であるから，これは K の要素 k に $k+1$ を対応させる規則となる．この対応の規則によって，K は 自然数の公理 (i)(ii)(iii)(iv) を満たす．$\mathbb{N}$ の最小性から $\mathbb{N} = K$ である．よってまた 1 を含む昇列はすべて $\mathbb{N}$ に一致する．

(2)　M は 1 を含む昇列である．ゆえに (1) から $\mathbb{N} = M$.

(3)　$\mathbb{N}$ において，a にはじまり $+1$ の操作を繰り返して b に至る系列はただひとつである．二つあれば，そのいずれかの系列を定めその中にのみ存在する要素を $\mathbb{N}$ から取り除いても，$\mathbb{N}$ は 1 を

含む昇列となり $\mathbb{N}$ の最小性に反するからである. $\mathbb{N}$ の要素 a で 1 でなく，しかも $a = x + 1$ となる要素 x が存在しない要素の集合を Q とする.

$$N' = N - Q$$

とする. N' の任意の要素 x に対して $x + 1 \notin Q$ つまり $x + 1 \in N'$ である. ゆえに N' は 1 を含む昇列であるから $N' = N$. つまり Q は空集合であり，1 以外で直前の要素の存在しない要素はない.

次に $z \neq z'$ かつ $z + 1 = z' + 1$ となるものがあるとする. 二つの系列

$$\begin{aligned} l &: 1 \to 1+1 \to \cdots \to z \to z+1 \\ l' &: 1 \to 1+1 \to \cdots \to z' \to z'+1 = z+1 \end{aligned}$$

が存在し，系列の唯一性に反する. ゆえに直前の要素はただひとつある.
(4) $1 \in M$ なら $M = K(1)$ なので $1 \notin M$ とする.

$$R = \{x | M \subset K(x)\}$$

とおく. $1 \in R$ なので R は空でない. $a \in R$ であるが $a + 1 \notin R$ であるような要素 a が R に存在する. なぜなら，もしなければ R が $\mathbb{N}$ 自身になる. ところが $x \in N$ に対して $x \notin K(x + 1)$ だから $\bigcap_{x \in N} K(x) = \emptyset$ である. つまり

$$M \subset \bigcap_{x \in N} K(x) = \emptyset$$

となって M が空集合になるのである. $M \not\subset K(a + 1)$ なので $m \in M$, $m \notin K(a + 1)$ が存在する. つまり

$$m \in K(a),\ m \notin K(a+1)$$

となり $a = m$, つまり $M \subset K(m)$ となる m が存在した. m と m' と二つあれば $m \in K(m')$ かつ $m' \in K(m)$ となり，m から m' をへて m にいたる系列ができる. m から m にいたる系列が 2 つでき，系列がただ一つであることに反する. □

8.1.2 同型定理と演算

自然数の和・積 この自然数の集合には，和と積という演算が定義される.

定理 68 (自然数の和・積)
$x,\ y \in N$ に対して， $x + y$ を次のように帰納的に定める.

(1) $y = 1$ なら $x + y = x + 1$ とする.

(2) $y > 1$ のとき. $x + (y - 1)$ まで定まったとすると

$$x + y = (x + (y - 1)) + 1$$

とする.

このとき $x + y$ がただ一通りに決まり次の性質を持つ.

(i) 結合法則：$(x+y)+z=x+(y+z)$.

(ii) 交換法則：$x+y=y+x$.

(iii) $x<y$ なら $x+z<y+z$.

$x\cdot y$ を次のように帰納的に定める.

(1) $y=1$ なら $x\cdot y=x$.

(2) $y>1$ のとき．$x\cdot(y-1)$ まで定まったとすると

$$x\cdot y=(x\cdot(y-1))+x$$

とする.

このとき $x\cdot y$ がただ一通りに決まり次の性質を持つ.

(i) 結合法則：$(x\cdot y)\cdot z=x\cdot(y\cdot z)$.

(ii) 交換法則：$x\cdot y=y\cdot x$.

(iii) $x<y$ なら $x\cdot z<y\cdot z$.

(iv) 分配法則：$x\cdot(y+z)=x\cdot y+x\cdot z$.

(v) $a<b$ 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. ■

証明　これらの証明は，難しくはないが煩雑ではある．例えば和の結合法則：$(x+y)+z=x+(y+z)$ を証明してみよう.

数学的帰納法にもとづく和の定義より

$$x+y-1=x+(y-1)$$

である．そこで $(x+y)+z=x+(y+z)$ を z に関する数学的帰納法で示す.

$z=1$ のとき．$(x+y)+1=x+(y+1)$ は x と $y+1$ の和の定義より成立する.

$z-1$ で成立するとする.

$$\begin{aligned}(x+y)+z &=\{(x+y)+z-1\}+1 && :\text{和の定義}\\ &=[x+\{y+(z-1)\}]+1 && :\text{帰納法の仮定}\\ &=[x+\{(y+z)-1\}]+1 && :\text{和の定義}\\ &=x+(y+z) && :\text{和の定義}\end{aligned}$$

z でも成立し，すべての z で成立する.

以下順次自然数と自然数の和・積が厳密に定義される.

また

$$a+x=b+x \quad\Rightarrow\quad a=b,\ a\cdot x=b\cdot x \quad\Rightarrow\quad a=b$$

なども成立する．これらの証明は省略する.

大小と差　$x,\ y \in \mathbb{N}$ にに対して，

$$x = y + z \quad z \in \mathbb{N}$$

のとき，$x > y$ と定める．

$x > 1$ のとき，

$$y + 1 = x$$

となる y がある．この y を $x-1$ と記し，x の直前の要素という．以下帰納的に $x-j$ $(j = 1,\ 2,\ \cdots,\ x-1)$ が定まる．これらを差という．

一意性　自然数の公理を満たすものがいくつもあっては困る．しかし実は一つしかないことが示される．

定理 69
自然数の集合 $\mathbb{N}$ はすべて同型である．つまり二つの自然数の集合 $\mathbb{N}$ と $\mathbb{N}'$ があるとする．$\mathbb{N}$ と $\mathbb{N}'$ のあいだの一対一対応 $f(x)$ で

(1) $f(1) = 1$

(2) $f(x+1) = f(x) + 1$

となるものがある． ■

証明　$\mathbb{N}_n = \{1,\ 2,\ \cdots,\ n\}$ の $\mathbb{N}'$ への写像 $f_n(x)$ を n についての数学的帰納法で定める．

(i) $n = 1$ のとき $f_1(1) = 1$ とする．

(ii) $f_k(x)$ が定まったとき

$$f_{k+1}(x) = f_k(x)\ (x = 1,\ 2,\ \cdots,\ k),\ f_{k+1}(k+1) = f_k(k) + 1$$

とする．

この $f_n(x)$ $(n = 1,\ 2,\ 3, \cdots)$ を用いて

$$f(x) = f_x(x) \quad x \in \mathbb{N}$$

と定める．作り方から $f(\mathbb{N})$ は $\mathbb{N}'$ における 1 を含む昇列である．

$$\therefore \quad f(\mathbb{N}) = \mathbb{N}'$$

このとき

$$f(x+1) = f_{x+1}(x+1) = f_x(x) + 1 = f(x) + 1$$

は成立する．

$i,\ j > 1$ で $f(i) = f(j)$ となるとする．

$$f(i-1) + 1 = f(j-1) + 1$$

より $f(i-1) = f(j-1)$．ここに $i-1,\ j-1$ は i と j の直前の要素である．もし $i > j$ ならこれを繰りかえして $f(i-j+1) = f(1) = 1$．f の作り方から $i - j + 1 = 1$．よって $i = j$ となり，これが一対一写像であることもわかる． □

8.2　整数と有理数の構成

ではこのような整数は，自然数をもとに構成することが出来るのか．それを論じよう．整数と有理数を自然数を用いて構成することが可能であることは重要なことなのであるが，構成された整数の性質の研究にとっては前提であっても論証上必要ということではない．従って本節はとりあえず置いて先に進んでもよい．

自然数の集合 $\mathbb{N}$ を基礎に，整数の集合 $\mathbb{Z}$ と有理数の集合 $\mathbb{Q}$ を構成することができる．その道筋を考えよう．そのために，今後も必要になる**集合の同値関係による類別**を明確にしておく．これは後に整数の類別においても基礎的な概念となるものである．

整数の構成　自然数 $\mathbb{N}$ に対し，直積集合 $\mathbb{N}\times\mathbb{N}$ を

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

とする．ここに関係〜を

$$(a,\ b)\sim(c,\ d)\quad\Longleftrightarrow\quad a+d=b+c$$

で定める．これは $\mathbb{N}\times\mathbb{N}$ の同値関係である．実際 (i)，(ii) は明らかである．$(a,\ b)\sim(c,\ d)$，$(c,\ d)\sim(e,\ f)$ とする．それぞれの関係より

$$a+d=b+c,\ c+f=d+e$$

これから

$$a+d+c+f=b+c+d+e\quad\text{よって}\ a+f=b+e$$

つまり $(a,\ b)\sim(e,\ f)$ となり (iii) も成立する．

この同値関係による商集合 $\mathbb{N}\times\mathbb{N}\,/\sim$ に和「+」と積「·」という二つの演算を定義する．$\mathbb{N}\times\mathbb{N}\,/\sim$ の二つの要素 $\overline{(a,\ b)}$，$\overline{(c,\ d)}$ をとる．

$$\begin{aligned}\overline{(a,\ b)}+\overline{(c,\ d)}&=\overline{(a+c,\ b+d)}\\ \overline{(a,\ b)}\cdot\overline{(c,\ d)}&=\overline{(ac+bd,\ ad+bc)}\end{aligned}$$

$\overline{(a,\ b)}$ をとったがこの類が $\mathbb{N}\times\mathbb{N}$ の他の要素 $(a_1,\ b_1)$ を用いて表されていたとする．このとき $(a,\ b)\sim(a_1,\ b_1)$ であるが，こちらを用いて，$\mathbb{N}\times\mathbb{N}\,/\sim$ の和を作ると $\overline{(a_1+c,\ b_1+d)}$ となる．このとき，$(a+c,\ b+d)$ と $(a_1+c,\ b_1+d)$ は同値である．実際 $a+b_1=b+a_1$ であるので $a+c+b_1+d=b+d+a_1+c$ が成り立つ．従って和は同じ類に属するいずれの要素を用いても同じ類を定める．このことを**和は適切に定義される**という．積についても同様に確かめられる．さらに，$\overline{(a,\ a)}$ が和の単位元，$\overline{(a+1,\ a)}$ が積の単位元，$\overline{(a,\ x+a)}$ が $\overline{(a+x,\ a)}$ 和に関する逆元であることが確認でき，これによって $\mathbb{N}\times\mathbb{N}\,/\sim$ が環をなすことが確認できる．

この環を整数の集合 (整数環)$\mathbb{Z}$ いう．

$\mathbb{N}$ から $\mathbb{N}\times\mathbb{N}\,/\sim$ への写像を自然数 a を用いて

$$\mathbb{N}\to\mathbb{N}\times\mathbb{N}\,/\sim\ :x\mapsto\overline{(x+a,\ a)}$$

で定める．これは a によらず定義され，単射でありこれによって自然数は $\mathbb{N}\times\mathbb{N}\,/\sim$ に埋め込まれる．これを同一視し，$x=\overline{(x+a,\ a)}$ のように書く．自然数 $x,\ a$ で定まる $\mathbb{N}\to\mathbb{N}\times\mathbb{N}\,/\sim$ の要素 $\overline{(a,\ x+a)}$ を $-x$，$\overline{(a,\ a)}$ を 0 と書くことにする．いいかえると

自然数だけを用いて整数を構成しようとした．そのために自然数の組に $(5,\ 2)$〜$(6,\ 3)$ のような同値関係を入れ，同値なものを同一視したのである．$(2,\ 5)$ が整数の -3 に，$(2,\ 2)$ が整数の 0 になるわけである．

有理数の構成　このように構成された整数環 $\mathbb{Z}$ を用いて有理数体 $\mathbb{Q}$ を構成しよう．

$\mathbb{Z}$ を整数の集合とする．次のような整数の組の集合を考える．

$$\mathbb{Z}\times\mathbb{Z}=\{\ (a,\ b)\mid a,b\in\mathbb{Z},\ b\neq 0\}$$

この集合の二つの要素 $(p,\ q)$，$(a,\ b)$ に対し，同値関係を，

$$(p,\ q)\text{〜}(a,\ b)\quad\Longleftrightarrow\quad p\cdot b=q\cdot a$$

で定める．このとき

$$(p,\ q)\text{〜}(a,\ b)\text{ かつ }(a,\ b)\text{〜}(s,\ t)\quad\Rightarrow\quad(p,\ q)\text{〜}(s,\ t)$$

が成り立つ．実際

$$p\cdot b=q\cdot a\text{ かつ }a\cdot t=b\cdot s\quad\Rightarrow\quad p\cdot t\cdot a\cdot b=q\cdot s\cdot a\cdot b$$

$a\cdot b\neq 0$ なので $p\cdot t=q\cdot a$ である．また，$a\neq 0$ に対して

$$(a\cdot p,\ a\cdot q)=(p,\ q)$$

も成り立つ．従って「〜」は同値関係である．

集合 $\mathbb{Z}\times\mathbb{Z}$ のこの関係での商集合 $\mathbb{Z}\times\mathbb{Z}\ /\text{〜}$ に和「$+$」と積「$\cdot$」を定める．

$$\begin{aligned}\overline{(a,\ b)}+\overline{(c,\ d)}&=\overline{(a\cdot d+b\cdot c,\ b\cdot d)}\\ \overline{(a,\ b)}\cdot\overline{(c,\ d)}&=\overline{(a\cdot c,\ b\cdot d)}\end{aligned}$$

これは適切に定義される．例えば和についていえば

$$\begin{aligned}&(a,\ b)\text{〜}(a',\ b')\text{ かつ }(c,\ d)\text{〜}(c',\ d')\\ \Rightarrow\quad&(a,\ b)+(c,\ d)\text{〜}(a',\ b')+(c',\ d')\\ \Longleftrightarrow\quad&(a\cdot d+b\cdot c,\ b\cdot d)\text{〜}(a'\cdot d'+b'\cdot c',\ b'\cdot d')\end{aligned}$$

を示さなければならない，ところが

$$(a\cdot d+b\cdot c)\cdot b'\cdot d'-(a'\cdot d'+b'\cdot c')b\cdot d=(a\cdot b'-a'\cdot b)\cdot d\cdot d'=0$$

なので成立する．積についても確認される．加法と乗法の単位元は

$$\begin{aligned}(a,\ b)+(0,\ 1)&=(a+0\cdot b,\ b)=(a,\ b)\\ (a,\ b)\cdot(1,\ 1)&=(a,\ b)\end{aligned}$$

から，$\overline{(0,\ 1)}$ と $\overline{(1,\ 1)}$ である．加法と乗法の逆元は

$$\begin{aligned}(a,\ b)+(-a,\ b)&=(ab-ab,\ b^2)=0\\ (a,\ b)\cdot(b,\ a)&=(ab,\ ab)=(1,\ 1)=1\end{aligned}$$

などから

$$-\overline{(a,\ b)} = \overline{(-a,\ b)},\ \overline{(a,\ b)}^{-1} = \overline{(b,\ a)}$$

である．分配法則も同様に示される．これらの演算で $\mathbb{Z} \times \mathbb{Z} \diagup \sim$ が体であることが確認される．

この体をを有理数体 $\mathbb{Q}$ という．

さらに

$$\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z} \diagup \sim : x \mapsto \overline{(x,\ 1)}$$

によって整数 $\mathbb{Z}$ は $\mathbb{Q}$ に埋め込まれる．そして $\overline{(a,\ b)}$ のことを $\dfrac{a}{b}$ と記すのである．

以下，有理数体の積で文字の場合，積の記号 $\cdot$ は約すかまたは紛らわしくなるときは $\cdot$ で書こう．

こうして自然数の集合 $\mathbb{N}$，整数環 $\mathbb{Z}$，有理数体 $\mathbb{Q}$ が順次構成されるのである．

第9章　解答

9.1　演習問題解答

解答 1 (問題 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)

(1)

解法 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)

$$\begin{aligned}11n-42&=3(3n-13)+2n-3\\3n-13&=2n-3+n-10\\2n-3&=2(n-10)+17\end{aligned}$$

より

$$(11n-42,\ 3n-13)=(3n-13,\ 2n-3)=(2n-3,\ n-10)=(n-10,\ 17)$$

よって分子分母に 1 より大きい公約数があればそれは 17 である. その条件は $n-10$ が 17 の倍数になることである. $n=17k+10$ よりゆえに $n=10,\ 27,\ 44$.

解答 3 (問題 3)

(1)

$$\begin{aligned}&25x+13y+15z=1\\\iff\quad&(13+12)x+13y+(13+2)z=1\\\iff\quad&13(x+y+z)+12x+2z=1\\\iff\quad&(2\cdot6+1)(x+y+z)+(2\cdot6+0)x+2z=1\\\iff\quad&2\{6(x+y+z)+6x+z\}+(x+y+z)+0x=1\\&x=s\quad\text{とおく}\\\iff\quad&2\{12s+6y+7z\}+(s+y+z)=1\\&12s+6y+7z=1+t\\&s+y+z=-1-2t\end{aligned}$$

これを解いて

$x = s,\ y = -8 + 5s - 15t,\ z = 7 - 6s + 13t$

($s,\ t,$ は任意の整数)

(2)

$$
\begin{aligned}
& 2x + 6y + 5z + 7w = 1 \\
\iff\quad & 2x + (2\cdot 3 + 0)y + (2\cdot 2 + 1)z + (2\cdot 3 + 1)w = 1 \\
\iff\quad & 0y + 2(x + 3y + 2z + 3w) + z + w = 1 \\
\iff\quad & 0y + (2\cdot 1 + 0)(x + 3y + 2z + 3w) + (1 + 0)z + w = 1 \\
\iff\quad & 0y + 0(x + 3y + 2z + 3w) + 0z + (2x + 6y + 5z + 7w) = 1
\end{aligned}
$$

$y = s,\ x + 3y + 2z + 3w = t,\ z = u,\ 2x + 6y + 5z + 7w = 1$

これを解いて

$x = -3 - 3s + 7t + u,\ y = s,\ z = u,\ w = 1 - 2t - u$

($s,\ t,\ u,$ は任意の整数)

解答 4 (問題 4)

(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

$$a^{T(a)} = \left(\prod_{d|a} d\right)^2$$

$$\therefore \quad \prod_{d|a} d = a^{\frac{T(a)}{2}}$$

解答 5 (問題 5)

［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 $2^n - 1$ は 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．これから $a = 2^{n-1}(2^n - 1)$ となり，$2^n - 1 = b$ は素数である．

解答 6 (問題 6)

(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

$$\prod_p p^{\beta(p)}\ (\beta(p) \geqq 0)$$

とおける．ここで

$$\beta(p) \leqq \mathrm{Min}(\alpha_1(p),\ \alpha_2(p),\ \cdots,\ \alpha_n(p))$$

となり，最大公約数のときに限り

$$\beta(p) = \mathrm{Min}(\alpha_1(p),\ \alpha_2(p),\ \cdots,\ \alpha_n(p))$$

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

$$\prod_p p^{\gamma(p)}\ (\gamma(p) \geqq 0)$$

が公倍数なら

$$\gamma(p) \geqq \mathrm{Max}(\alpha_1(p),\ \alpha_2(p),\ \cdots,\ \alpha_n(p))$$

となり，最小倍約数のときに限り

$$\gamma(p) = \mathrm{Min}(\alpha_1(p),\ \alpha_2(p),\ \cdots,\ \alpha_n(p))$$

(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 $a,\ b,\ c,\ \cdots$ の少なくとも一つに含まれている．p を因子に含む $a,\ b,\ c,\ \cdots$ うち，べき指数が最高のものが含まれている $a,\ b,\ c,\ \cdots$ を指定する．同じ指数のものがあるときはそのうちのいずれかをとる．a が指定された a に含まれる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．このとき $a_0,\ b_0,\ c_0,\ \cdots$ のどの 2 つも互いに素で

$$l = a_0b_0c_0\cdots$$

である.

解答 7 (問題 7)　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である.

$k = p^l \cdot q$ (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 8 (問題 8)　$n!$ 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 9 (問題 9)

(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 10 (問題 10)

$$\begin{aligned} a &= a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_1 10 + a_0 \\ &= a_n (9+1)^n + a_{n-1}(9+1)^{n-1} + \cdots + a_1(9+1) + a_0 \\ &\equiv a_0 + a_1 + \cdots + a_n \pmod 9 \end{aligned}$$

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 11 (問題 11)

$$\begin{aligned} 10^6 &= (7+3)^6 \\ &\equiv 3^6 \pmod 7 = (7+2)^3 \pmod 7 \\ &= 8 \equiv 1 \pmod 7. \quad \therefore \quad \text{土曜日} \\ 10^{100} &= 10^{16\cdot 6+4} \\ &\equiv 10^4 \pmod 7 \equiv 3^4 \pmod 7 = 9^2 \equiv 4 \pmod 7. \quad \therefore \quad \text{火曜日} \\ 3^{100} &\equiv (7+3)^{100} \equiv 4 \pmod 7. \quad \therefore \quad \text{火曜日} \end{aligned}$$

解答 12 (問題 12)　ガウス の方法を用いる.

$$5\cdot 7\cdot t_1 \equiv 1 \pmod 3 \quad より \quad t_1 \equiv 2 \pmod 3$$
$$3\cdot 7\cdot t_2 \equiv 1 \pmod 5 \quad より \quad t_2 \equiv 1 \pmod 5$$
$$3\cdot 5\cdot t_3 \equiv 1 \pmod 7 \quad より \quad t_3 \equiv 1 \pmod 7$$

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 13 (問題 13)

(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 14)

(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 15)

(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 16) $a \equiv 3 \pmod{11}$ 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 17)　$(26,\ 57) = 1$ なので解が存在する．$57 = 26 \cdot 2 + 5$ より

$$\begin{aligned} & 26x \equiv 1 \pmod{57} \\ \Rightarrow\quad & 52x \equiv 2 \pmod{57} \\ \Rightarrow\quad & -5x \equiv 2 \pmod{57} \\ \Rightarrow\quad & -25x \equiv 10 \pmod{57} \\ & \text{与えられた式と加えて} \\ & x \equiv 11 \pmod{57} \end{aligned}$$

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．

$$57y \equiv -1 \pmod{26} \text{ より } 5y \equiv 25 \pmod{26}. \text{ つまり } y \equiv 5 \pmod{26}$$

$y = 5 + 26t$ 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 18)

$$\begin{aligned} & \begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases} \text{が解を持つ} \\ \iff\quad & x = a + mu = b + nv \text{ となる整数 } (u,\ v) \text{ が存在する．} \end{aligned}$$

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 2).

解答 19 (問題 19)　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 (練習問題 6 の (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 20 (問題 20)

(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 21 (問題 21) $x = 1 + 2y$ を奇数とする．$x^2 = 1 + 4y(y+1)$ で $y(y+1)$ は偶数だから，$x^2 \equiv 1 \pmod{8}$.

ゆえに $\alpha \equiv 1 \pmod{8}$ は α が奇数であるときに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

$$x \equiv 1,\ 3,\ 5,\ 7 \pmod{8}$$

である．このいずれを x_0 としても，この 4 数は

$$x \equiv \pm x_0,\ \pm x_0 + 2^2 \pmod{8}$$

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

$$x^2 \equiv \alpha \pmod{2^{e+1}} \tag{9.1}$$

の解は四つあり，そのうちの一つを x_0 とすれば 4 解は

$$\pm x_0,\ \pm x_0 + 2^e$$

と表されることを示す.

さて，e のときの解 x_0 を用いれば $e+1$ のときの解は

$$\pm x_0 + 2^e y \quad \text{または} \quad (\pm x_0 + 2^{e-1}) + 2^e y \pmod{2^{e+1}} \tag{9.2}$$

の形をしていなければならない．そして (9.2) が (9.1) を満たさなければならないので

$$(\pm x_0 + 2^e y)^2 \equiv \alpha \pmod{2^{e+1}} \tag{9.3}$$

$$\{(\pm x_0 + 2^{e-1}) + 2^e y\}^2 \equiv \alpha \pmod{2^{e+1}} \tag{9.4}$$

のいずれかが成立する y から $e+1$ のときの解が求まる.

仮定から整数 t を用いて $x_0^2 = \alpha + 2^e t$ と表せる．これを用いると (9.3) は

$$2^e t \equiv 0 \,(\mathrm{mod.}\ 2^{e+1})$$

となり，これは t が奇数ならつねに成立せず，t が偶数ならつねに成立する．

次に (9.4) について．x_0 は奇数で $2n-2 \geqq n+1$ であるから

$$\begin{aligned}(\pm x_0 + 2^{e-1})^2 &\equiv x_0^2 \pm 2^e x_0 + 2^{2e-2} \\ &\equiv x_0^2 + 2^e \,(\mathrm{mod.}\ 2^{e+1})\end{aligned}$$

よって (9.4) は

$$2^e t + 2^e \equiv 0 \,(\mathrm{mod.}\ 2^{e+1})$$

となる．これは t が偶数ならつねに成立せず，t が奇数ならつねに成立する．

つねに成立するとき y は任意なので，mod. 2^{e+1} に関しては $y = 0,\ 1$ をとることができる．

よって t が偶数なら

$$\pm x_0 \quad \text{および} \quad \pm\, x_0 + 2^e$$

の四つが解である．

t が奇数なら

$$\pm(x_0 + 2^{e-1}) \quad \text{および} \quad \pm\,(x_0 + 2^{e-1}) + 2^e$$

の四つが解である．

以上によって，数学的帰納法により題意が示された．

解答 22 (問題 22)

(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

$$\begin{aligned}& 1512 - (\frac{1512}{2} + \frac{1512}{3} + \frac{1512}{7}) + (\frac{1512}{6} + \frac{1512}{14} + \frac{1512}{21}) - \frac{1512}{42} \\ = \ & 1512 - (756 + 504 + 216) + (252 + 108 + 72) - 36 = 432\end{aligned}$$

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 23)　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 24)　$a,\ b,\ c,\ \cdots$ 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

$$1\cdot a,\ 2\cdot a,\ \cdots,\ \left[\frac{x}{a}\right]a$$

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 25)　$(m,\ n)=1$ 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 9.1.1　これを用いれば，補題 2 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 26)　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

$$(yd,\ n)=d \iff \left(y,\ \frac{n}{d}\right)=1,\qquad \left[\frac{[nx]}{d}\right]=\left[\frac{nx}{d}\right]$$

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 27)

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

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 28) $n>1$ 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 29)　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

$$i-j \equiv 0 \pmod{n}$$

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 30)　$\alpha = \cos\dfrac{2\pi}{a} + i\sin\dfrac{2\pi}{a}$ ，$\beta = \cos\dfrac{2\pi}{b} + i\sin\dfrac{2\pi}{b}$ 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 31)　$(k,\ e)=d$ 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 32 (問題 32)

(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) $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots$ 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．

$$f(x)=a_nx^n+\cdots+a_{m+1}x^{m+1}+g(x)\quad g(x)=a_mx^m+\cdots$$

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 9.1.2　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．

$$\begin{aligned}
(3-2)!-1 &= 0\\
(4-2)!-1 &= 1\\
(5-2)!-1 &= 5\\
(6-2)!-1 &= 23\\
(7-2)!-1 &= 119=7\cdot 17\\
(8-2)!-1 &= 719\\
(9-2)!-1 &= 5039
\end{aligned}$$

$$
\begin{aligned}
(10-2)!-1 &= 40319 = 23\cdot 1753\\
(11-2)!-1 &= 362879 = 11^2\cdot 2999\\
(12-2)!-1 &= 3628799 = 29\cdot 125131\\
(13-2)!-1 &= 39916799 = 13\cdot 17\cdot 23\cdot 7853\\
(14-2)!-1 &= 479001599\\
(15-2)!-1 &= 6227020799 = 1733\cdot 3593203\\
(16-2)!-1 &= 87178291199\\
(17-2)!-1 &= 1307674367999 = 17\cdot 31^2\cdot 53\cdot 1510259\\
(18-2)!-1 &= 20922789887999 = 3041\cdot 6880233439\\
(19-2)!-1 &= 355687428095999 = 19\cdot 73\cdot 256443711677\\
(20-2)!-1 &= 6402373705727999 = 59\cdot 226663\cdot 478749547
\end{aligned}
$$

解答 33 (問題 33)　$M=(m!)^2+1$ とおく．M は $1,\cdots,m$ で割り切れないので M の 1 でない因数はすべて m 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．$p>m$ である．フェルマの小定理から

$$(m!)^p\equiv m! \pmod{p} \tag{9.5}$$

次に $p=4r+3$ とおき，因数分解

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

を $x=(m!)^2$, $k=r$ で用いる．このとき $M=x+1$ であるから因数分解は $\{(m!)^2\}^{2r+1}+1$ が M で割り切れることを示している．一方,

$$\{(m!)^2\}^{2r+1}+1=(m!)^{4r+2}+1=(m!)^{p-1}+1$$

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．

$$\therefore\quad m!\{(m!)^{p-1}+1\}=(m!)^p+m!\equiv 0 \pmod{p} \tag{9.6}$$

(9.5), (9.6) から

$$2m!\equiv 0 \pmod{p}$$

これは $p>m$ 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 m 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 $p>m$ である $4n+1$ 型の素数になる．つまり任意の自然数 m 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 34)

$$
\begin{aligned}
10^1 &= 10+91\cdot 0\\
10^2 &= 9+91\cdot 01\\
10^3 &= 90+91\cdot 010\\
10^4 &= 81+91\cdot 0109\\
10^5 &= 82+91\cdot 01098\\
10^6 &= 1+91\cdot 010989
\end{aligned}
$$

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 35)　$a = 2$ をとってみる.

$2^6 = 64 \equiv 23\,(\mathrm{mod.}\ 41)$ ， $2^7 \equiv 46 \equiv 5\,(\mathrm{mod.}\ 41)$ ， $2^8 \equiv 10\,(\mathrm{mod.}\ 41)$ ， $2^9 \equiv 20\,(\mathrm{mod.}\ 41)$ ，$2^{10} \equiv 40 \equiv -1\,(\mathrm{mod.}\ 41)$ ． $\therefore\ \ 2^{20} \equiv 1\,(\mathrm{mod.}\ 41)$

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 36)

(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. $\therefore \quad x \equiv 5 \pmod{13}$

(4) $-1 \equiv 11 \pmod{12}$. $I = 11$ に対する $a = 7$. $\therefore \quad x \equiv 7 \pmod{13}$.

解答 37 (問題 37)

(1) $\mathrm{Ind}_2\, 11 = 7,\ \mathrm{Ind}_2\, 5 = 9$ なので $\mathrm{Ind}_2\, x \equiv 2 \pmod{12}$. ゆえに $x \equiv 4 \pmod{13}$.

(2) $3\,\mathrm{Ind}_2\, x \equiv 9 \pmod{12}$ より $\mathrm{Ind}_2\, x \equiv 3 \pmod{4}$. 表から $x \equiv 7,\ 8,\ 11 \pmod{13}$.

(3) $5x^2 + 3x \equiv 10 \pmod{13}$ より $5(x-1)^2 \equiv 15 \pmod{13}$. 5 と 13 は互いに素なので $(x-1)^2 \equiv 3 \pmod{13}$. 表から $\mathrm{Ind}_2\, 3 = 4$ なので $2\,\mathrm{Ind}_2(x-1) \equiv 4 \pmod{12}$. これより $\mathrm{Ind}_2(x-1) \equiv 2 \pmod{6}$. 表から $x - 1 \equiv 4,\ 9 \pmod{13}$. よって $x \equiv 5,\ 10 \pmod{13}$.

解答 38 (問題 38)

$$\left(r^{\frac{p-1}{2}} - 1\right)\left(r^{\frac{p-1}{2}} + 1\right) = r^{p-1} - 1 \equiv 0 \pmod{p}$$

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 39) $a \equiv -b \pmod{p}$ 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 40) $r^\alpha \equiv a \pmod{p}$ 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 41) 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

$$\{1^k,\ 2^k,\ \cdots,\ (p-1)^k\}$$
$$\{1,\ r^k,\ \cdots,\ r^{(p-2)k}\}$$

の各元は互いに 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 42)

$$\begin{aligned}(p-1)! &\equiv r^{1+2+\cdots+(p-2)} \\ &= \left(r^{\frac{p-1}{2}}\right)^{p-2} \\ &\equiv (-1)^{p-2} \equiv -1 \pmod{p}\end{aligned}$$

解答 43 (問題 43)

$$\begin{aligned}\left(\frac{365}{1847}\right) &= \left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right) \\ &= \left(\frac{1847}{5}\right)\left(\frac{1847}{73}\right) && 5 \equiv 1,\ 73 \equiv 1 \pmod{4} \\ &= \left(\frac{2}{5}\right)\left(\frac{22}{73}\right) \\ &= \left(\frac{2}{5}\right)\left(\frac{2}{73}\right)\left(\frac{11}{73}\right) \\ &= -\left(\frac{11}{73}\right) && \text{(第二補充則)} \\ &= -\left(\frac{73}{11}\right) = -\left(\frac{-4}{11}\right) \\ &= -\left(\frac{-1}{11}\right)\left(\frac{2^2}{11}\right) \\ &= -\left(\frac{-1}{11}\right) \\ &= 1 && \text{(第一補充則)}\end{aligned}$$

解答 44 (問題 44)

$$\left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}+\frac{p^2-1}{8}}$$

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 45)　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 $\left(\frac{p}{5}\right) = 1$

(2) $p \equiv 2,\ 3 \pmod{5}$ のとき $\left(\frac{p}{5}\right) = -1$

となり，あわせて題意が示された．

解答 46 (問題 46)　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 47)

$$a^2 \equiv (p-a)^2 \pmod{p}$$

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 48)

$$\begin{aligned}
5 &= N(1+2i) = 1^2+2^2 \\
13 &= N(3+2i) = 9^2+2^2 \\
65 &= N(1+2i)N(3+2i) = N(-1+8i) = 1^2+8^2 \\
65 &= N(1+2i)N(3-2i) = N(7+4i) = 7^2+4^2 \\
5^2 &= N(1+2i)^2 = N(-3+4i) = 3^2+4^2 \\
50 &= N(1-i)N(1+2i)^2 = N(1+7i) = 1^2+7^2 \\
13^3 &= N(3+2i)^2 = N(5+12i) = 5^2+12^2
\end{aligned}$$

解答 49 (問題 49)　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．

注意 9.1.3 これはガウス環を用いてピタゴラス数の一般解を求めるものである．

解答 50 (問題 50)　3 次方程式の他の解は実数なのでこれを β とおく．解と係数の関係から

$$\begin{aligned}
&u+vi+u-vi+\beta=-p \\
&(u+vi)(u-vi)+\beta(u+vi)+\beta(u-vi)=q \\
&(u+vi)(u-vi)\beta=-r
\end{aligned}$$

となる．これを整理して

$$\begin{aligned}
&2u+\beta=-p \\
&u^2+v^2+2u\beta=q \\
&(u^2+v^2)\beta=-r
\end{aligned}$$

である．

まず u がある整数 a を用いて $\dfrac{a}{2}$ と表せること示す．第 2 式から

$$(u^2+v^2)\beta+2u\beta^2=q\beta$$

ここに第 1 式, 第 3 式を用いて β と u^2+v^2 を消去する.

$$-r+2u(-2u-p)^2=q(-2u-p)$$

整理して

$$8u^3+8pu^2+2(p^2+q)u+pq-r=0$$

ここで有理数 u を互いに素な整数 a と b を用いて $u=\dfrac{a}{b}$ $(b>0)$ とおく. 方程式に代入して b^3 を乗じ一部移項する.

$$8a^3=-b\{8pa^2+2(p^2+q)ab+(pq-r)b^2\}$$

右辺は b の倍数である. 左辺も b の倍数であるが a^3 と b は互いに素なので, 8 が b の倍数, つまり b が 8 の約数となることが必要である.

$b=8$ なら代入して 8 で割ると

$$a^3=-\{8pa^2+16(p^2+q)a+64(pq-r)\}$$

これから a が偶数となり a と b が互いに素に反する.

$b=4$ なら代入して 8 で割ると

$$a^3=-\{4pa^2+4(p^2+q)a+84(pq-r)\}$$

これから a が偶数となり a と b が互いに素に反する.

よって $b=1,\ 2$. つまり u は整数 a を用いて $u=\dfrac{a}{2}$ とおける.

この結果, $\beta=-p-2u$ が整数となりさらに $u^2+v^2=q-2u\beta$ も整数である.

$$v^2=-u^2+q-2u=\frac{-a^2+4q-4a}{4}$$

なので有理数 v も整数 c を用いて $v=\dfrac{c}{2}$ とおける. そして

$$u^2+v^2=\frac{a^2+c^2}{4}$$

が整数. そのためには分子が偶数でなければならないので $a,\ c$ がともに偶数かともに奇数であることが必要. ともに奇数の場合 $a=2k+1,\ c=2l+1$ とすると

$$a^2+c^2=4(k^2+k+l^2+l)+2$$

となり $\dfrac{a^2+c^2}{4}$ が整数でない.

よって a も c も偶数となり, その結果 u と v が整数となる.

注意 9.1.4　ガウスによる有理整数係数の多項式に関する定理 :

> 整数係数多項式 $f(x)$ が有理数の範囲で因数分解されれば, 有理整数の範囲で因数分解される.

を用いると，α が x^2 の係数が 1 の有理整数係数の二次方程式の根であることがわかる．この二次方程式を $x^2+lx+m=0$ とおくと，

$$\alpha=\frac{-l\pm\sqrt{4m-l^2}i}{2}$$

となる．これから $\sqrt{4m-l^2}$ が整数とならねばならず，$4m-l^2=b^2$ とおく．b が奇数とすると l も奇数であるが，このとき両辺 4 で割った余りが異なるので，これはない．かくして b, l が偶数となり，題意が示される．

注意 9.1.5　最高次の項の係数が 1 である整数係数の代数方程式の解となる数を「(代数的) 整数」と呼ぶ．ガウス整数 $a+bi$ $(a,\ b\in\mathbb{Z})$ は二次方程式 $x^2-2ax+a^2+b^2=0$ の解なので代数的整数である．

ガウス整数環に対してその商環

$$\left\{\frac{c+di}{a+bi}\middle|\ a,\ b,\ c,\ d\in\mathbb{Z},\ a+bi\neq0\right\}$$

は体である．ガウス商体といおう．これは分母を実数化することで

$$\{u+vi\mid u,\ v\in\mathbb{Q}\}$$

と同じものになる．

本問はガウス商体の元で代数的整数であるものの集合は，ちょうどガウス整数環になることを示している．

代数的整数の理論が 19 世紀末から 20 世紀にかけて大発展した.『数論初歩』に引き続く分野である．高木貞治はこの分野で「類体論」と呼ばれる決定的な仕事をした．

解答 51 (問題 51)

$$\begin{aligned}
\sqrt{7} &= \begin{pmatrix}2&1\\1&0\end{pmatrix}\left(\frac{1}{\sqrt{7}-2}\right)=\begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}\sqrt{7}+2\\3\end{pmatrix}\\
&= \begin{pmatrix}2&1\\1&0\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\left(\frac{3}{\sqrt{7}-1}\right)=\begin{pmatrix}3&2\\1&1\end{pmatrix}\begin{pmatrix}\sqrt{7}+1\\2\end{pmatrix}\\
&= \begin{pmatrix}3&2\\1&1\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\left(\frac{2}{\sqrt{7}-1}\right)=\begin{pmatrix}5&3\\2&1\end{pmatrix}\begin{pmatrix}\sqrt{7}+1\\3\end{pmatrix}\\
&= \begin{pmatrix}5&3\\2&1\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}\left(\frac{3}{\sqrt{7}-2}\right)=\begin{pmatrix}8&5\\3&2\end{pmatrix}(\sqrt{7}+2)\\
&= \begin{pmatrix}8&5\\3&2\end{pmatrix}\begin{pmatrix}4&1\\1&0\end{pmatrix}\left(\frac{1}{\sqrt{7}-2}\right)=\begin{pmatrix}37&8\\14&3\end{pmatrix}\begin{pmatrix}\sqrt{7}+2\\3\end{pmatrix}\\
&\cdots\quad\cdots
\end{aligned}$$

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 52)　$ax^2+bxy+cy^2=\dfrac{2\sqrt{-D}}{\pi}$ 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 53)

(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 54 (問題 54)　$\omega_1=4+\sqrt{13}$ 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 55 (問題 55)

$$\begin{aligned}
\sqrt{19} &= \begin{pmatrix}4&1\\1&0\end{pmatrix}x_1 && x_1=\frac{1}{\sqrt{19}-4}=\frac{\sqrt{19}+4}{3}\\
&= \begin{pmatrix}4&1\\1&0\end{pmatrix}\begin{pmatrix}2&1\\1&0\end{pmatrix}x_2 && x_2=\frac{3}{\sqrt{19}-2}=\frac{\sqrt{19}+2}{5}\\
&= \begin{pmatrix}9&4\\2&1\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}x_3 && x_3=\frac{5}{\sqrt{19}-3}=\frac{\sqrt{19}+3}{2}\\
&= \begin{pmatrix}13&9\\3&2\end{pmatrix}\begin{pmatrix}3&1\\1&0\end{pmatrix}x_4 && x_4=\frac{2}{\sqrt{19}-3}=\frac{\sqrt{19}+3}{5}\\
&= \begin{pmatrix}48&13\\11&3\end{pmatrix}\begin{pmatrix}1&1\\1&0\end{pmatrix}x_5 && x_5=\frac{5}{\sqrt{19}-2}=\frac{\sqrt{19}+2}{3}\\
&= \begin{pmatrix}61&48\\14&11\end{pmatrix}\begin{pmatrix}2&1\\1&0\end{pmatrix}x_6 && x_6=\frac{3}{\sqrt{19}-4}=\sqrt{19}+4\\
&= \begin{pmatrix}170&61\\39&14\end{pmatrix}\begin{pmatrix}8&1\\1&0\end{pmatrix}x_7 && x_7=\frac{1}{\sqrt{19}-4}=x_1
\end{aligned}$$

ゆえに $k=6$ 最小解 $(x,\ y)=(170,\ 39)$.

$$170^2-19\cdot 39^2=1$$

解答 56 (問題 56)

$$
\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 $(x,\ y) = (24335,\ 3588)$.

$$24335^2 - 19 \cdot 3588^2 = 1$$

9.2 入試問題解答

解答 1 (問題 1)

(1)

$$
\begin{aligned}
& && a_1 = 1998,\ b_1 = 185 \\
1998 &= 185 \times 10 + 148 \text{ より} && a_2 = 185,\ b_2 = 148 \\
185 &= 148 \times 1 + 37 \text{ より} && a_3 = 148,\ b_3 = 37 \\
148 &= 37 \times 4 + 0 \text{ より} && a_4 = 37,\ b_4 = 0 \\
& && a_5 = 37,\ b_5 = 0
\end{aligned}
$$

(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，

$$0 \leqq b_{n+1} < b_n$$

$b_n = 0$ 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 $\{b_n \mid n = 1,\ 2,\ \cdots\}$ に最小値が存在しないことになり，自然数の部分集合にはつねに最小値が存在するという，自然数の基本性質と矛盾する．よって $b_n = 0$ となる n が存在する．

(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 を b_k で割った商を q_k とおくと，$a_k = b_k \cdot q_k + b_{k+1}$ とかける． これから a_k と b_k の公約数は b_{k+1} の約数になり，b_k と b_{k+1} の公約数である．b_k と b_{k+1} の公約数で最大のものが最大公約数 $(b_k,\ b_{k+1})$ である．ゆえに $(a_k,\ b_k) \leqq (b_k,\ b_{k+1})$．また b_k と b_{k+1} の公約数は a_k の約数になる．同様に考え $(a_k,\ b_k) \geqq (b_k,\ b_{k+1})$ である．

$$\therefore \quad (a_k,\ b_k) = (b_k,\ b_{k+1})$$

これをいいかえると $(a_k,\ a_{k+1}) = (a_{k+1},\ a_{k+2})$．(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 で同様の等式が成り立つので題意が示された.

解答 2 (問題 2)

(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 9.2.1 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．

解答 3 問題 3 S に属する最小の数を d とする．S の任意の要素 a をとり，a を d で割り商が q，余りが r とする．

$$a = dq + r$$

$r > 0$ とする．$a-d \in S$ であり，自然数 $1 \leqq j < q$ に対して $a-jd \in S$ なら $a-jd-d = a-(j+1)d \in S$ なので，数学的帰納法で $r = a - dq \in S$ である．d が S に属する正で最小の整数という仮定に反する．よって $r = 0$ である．S のすべての要素は d の倍数である．

S に属する最大の要素を md とおく，$1 < j \leqq m$ の整数に対して $jd \in S$ なら $jd-d = (j-1)d \in S$ なので

$$md,\ (m-1)d,\ \cdots,\ d$$

はすべて S に属する．要素の個数を考え $m = n$ であり

$$S = \{nd,\ (n-1)d,\ \cdots,\ d\}$$

となる．$a_1,\ a_2,\ \cdots,\ a_n$ の順序を適当に変えれば初項 d，公差 d の等差数列になる．
※　大小の順で並べ替えて示してもよい．

解答 4 問題 4

(1) （イ），（ロ）とも成り立たないとする．S の属する最大の数を M，最小の数を m とする．このとき $m < 0 < M$ が成り立っている．$M - m$ か $m - M$ は S に属するので，$M < M - m$ または $m - M < m$ が成り立つ．これは M の最大性または m の最小性に矛盾する．よって（イ），（ロ）のうちいずれか一方が成立する．

(2) （イ）が成り立っているとする．S の要素で正で最小のものを d とする．

S の d と異なる正の任意の要素 a をとる．

$$qd \leqq a < (q+1)d$$

となる自然数 q をとる．$r = a-qd$ とおく．$r > 0$ とする．$a-d \in S$ であり，自然数 $1 \leqq j < q$ に対して $a-jd \in S$ なら $a-jd-d = a-(j+1)d \in S$ なので，数学的帰納法で $r = a-dq \in S$

である．d が S の要素で正で最小のものであるという仮定に反する．よって $r = 0$ である．S のすべての要素は d の倍数である．

S に属する最大の要素を md とおく，$1 < j \leqq m$ の整数に対して $jd \in S$ なら $jd - d = (j-1)d \in S$ なので

$$md,\ (m-1)d,\ \cdots,\ d$$

はすべて S に属する．要素の個数は，0 が S にあるかどうかを考え $m = n$ か $m = n-1$ であり

$$S = \{nd,\ (n-1)d,\ \cdots,\ d\},\ \{(n-1)d,\ (n-2)d,\ \cdots,\ d,\ 0\}$$

のいずれかである．$a_1,\ a_2,\ \cdots,\ a_n$ の順序を適当に変えれば初項が d または 0，公差 d の等差数列になる．

（ロ）の場合，すべての要素の絶対値をとって考えれば同様である．

※　大小の順で並べ替えて示してもよい．

解答 5 問題 5

自然数 j に対して $jd \in G$ なら $d + jd = (j+1)d \in G$ なので，数学的帰納法によって

$$\{kd \mid k \text{ は自然数 }\} \subset G$$

G の任意の要素 a をとり，a を d で割り商が q，余りが r とする．

$$a = dq + r$$

$dq \in G$ なので $r = a - dq \in S$ である．ここで $r > 0$ とすると d が G に属する正で最小の整数という仮定に反する．よって $r = 0$ である．G のすべての要素は d の倍数である．

$$G \subset \{kd \mid k \text{ は自然数 }\}$$

が示され，題意が証明された．

解答 6 (問題 6)

(1) $1 \leqq i,\ j \leqq p$ の範囲の i と j に対して $x - iq$ と $x - jq$ を p で割った余りが相等しいとする．それぞれの商を $l_1,\ l_2$ とし，余りを r とすると

$$x - iq = pl_1 + r, \quad x - jq = pl_2 + r$$

辺々引いて

$$(j-i)q = p(l_1 - l_2)$$

右辺は p の倍数であるが，p と q が互いに素なので，$j - i$ が p の倍数でなければならない．

ところが i と j の動く範囲より

$$-1 + p \leqq j - i \leqq p - 1$$

この範囲にある p の倍数は 0 のみ．つまり $j - i = 0$.

対偶をとって

$$i \neq j \quad \text{ならば} \quad x - iq \text{ と } x - jq \text{ を } p \text{ で割った余りは異なる.}$$

ことが示された．つまり p 個の整数 $x-q$，$x-2q$，$\cdots$，$x-pq$ を p で割った余りはすべて相異なる．

(2) $x-q$，$x-2q$，$\cdots$，$x-pq$ を p で割った余りは $0,\ 1,\ 2,\ \cdots,\ p-1$ の p 個のうちのいずれかであり，しかもすべて異なる．よって $x-q$，$x-2q$，$\cdots$，$x-pq$ を p で割った余りは $0,\ 1,\ 2,\ \cdots,\ p-1$ の各値を一つずつとる．

従ってこのなかに p で割った余りが 0，つまり p の倍数となるものが存在する．

それを $x-bq$ とし，$x-bq=ap$ とおく．$1 \leqq b \leqq p$ より b は正である．

$$ap = x - bq > (p-b)q \geqq 0$$

より $a > 0$ である．

よって，$x > pq$ なる任意の整数 x は，適当な正整数 $a,\ b$ を用いて $x = pa + qb$ と表せることが示された．

解答 7 (問題 7)

(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

$$\begin{aligned} &3m+5n=2 \\ &3(-1)+5(1)=2 \end{aligned}$$

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 の元のなかに

$$r(k) = 1$$

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 8 (問題 8)

(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

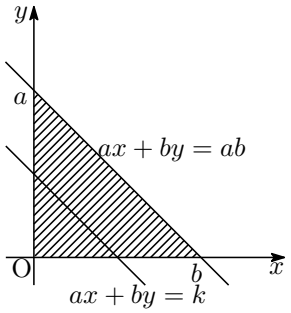
$$\frac{y_0}{a} > u > -\frac{x_0}{b}$$

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 9 (問題 9)

(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

$$\begin{aligned} & (q-2-m)p+(p-2-n)q \geqq pq-(p+q) \\ \iff\ & pq-mp-nq-p-q \geqq 0 \\ \iff\ & pq-(p+q) \geqq mp+nq \end{aligned}$$

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

$$\frac{(p-1)(q-1)}{2}$$

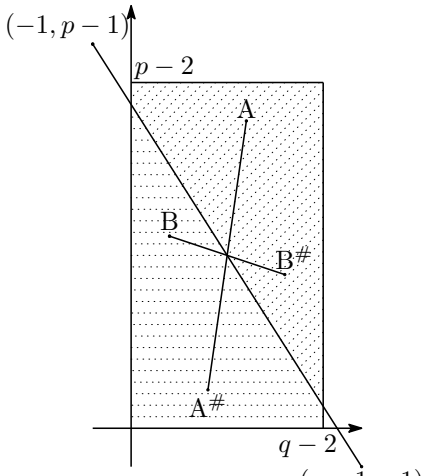
注意　条件 $mp+nq \leqq pq-(p+q)$ は書きかえると

$$\frac{m+1}{q}+\frac{n+1}{p} \leqq 1$$

である.

(4) の解答中にあるように，直線 $\dfrac{x+1}{q}+\dfrac{y+1}{p}=1$ 上には格子点がないので，この直線が L の格子点を二分することがわかる.

A と $\mathrm{A}^{\#}$ の対応は，この二分された二つの領域の中の格子点の一対一対応である.



解答 10 (問題 10) 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 11 (問題 11)

(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，

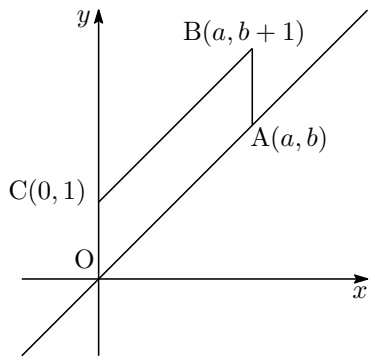
$$\frac{k}{a} - \frac{ak}{a^2+1} = \frac{k}{a(a^2+1)} > 1$$

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 12 (問題 12)

(1)

a と b が互いに素であるから，$\dfrac{b}{a}x$, $\dfrac{b}{a}x+1$ が整数となるのは x が a の倍数であるときにかぎる．直線 OA，CB の方程式が $y = \dfrac{b}{a}x$, $y = \dfrac{b}{a}x+1$ なので，$0 < k < a$ の範囲の整数 k に対し，直線 $x = k$ と直線 OA, CB の交点はいずれも格子点ではない．したがって，直線 $x = k$ の OABC の内部にある部分には，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 $\{aq_i - bp_i\}$ の元の個数は $a - 1$ 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，かつ元の個数が一致する．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 の元で正で最小のものを $aq_0 - bp_0$ とする.

任意の J の元 $aq - bp$ 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,

$$r = a(q - q_0 Q) - b(p - p_0 Q) \in J$$

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 の元であるから,

$$aq_0 - bp_0 \text{ は } a \text{ と } b \text{ の約数}$$

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 13 (問題 13) 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 $\min\left(\dfrac{\alpha}{\sqrt{29}},\ \dfrac{1-\alpha}{\sqrt{29}}\right)$ 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 9.2.2 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 14 (問題 14)

(1) 集合 $A=\{f(k)|k$ 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．

$$\therefore \quad A \text{ は } \frac{n+1}{2} \text{ 個の元からなる．}$$

(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 の任意の元 $f(k)$ 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 9.2.3 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 15 (問題 15)

(1) k を整数とし $3x + 2y = k$ とおく．これを満たす 0 以上の整数解 $(x,\ y)$ の個数を $k = 0,\ 1,\ \cdots,\ 2008$ の k について加えればよい．

まず，$3x + 2y = k$ を満たすすべての整数の組を求める．

$$3k + 2(-k) = k$$

より任意の整数解 $(x,\ y)$ に対して

$$3(x - k) + 2(y + k) = 0$$

2 と 3 は互いに素なので，$x - k$ は 2 の，$y + k$ は 3 の倍数である．よって整数解 $(x,\ y)$ は整数 t を用いて

$$x = k - 2t,\ y = -k + 3t$$

と表せ，この形をしたものはすべて整数解である．

$x \geqq 0,\ y \geqq 0$ という条件は

$$\frac{k}{3} \leqq t \leqq \frac{k}{2}$$

と同値である．よって k に対しこの範囲にある整数 t の個数が，$3x+2y=k$ となる 0 以上の整数の組 $(x,\ y)$ の個数である．負でない整数 m を用いて k を場合に分け，個数を求める．

	t の範囲	t の個数
$k=6m$ のとき	$2m \leqq t \leqq 3m$	$m+1$ 個
$k=6m+1$ のとき	$2m+\frac{1}{3} \leqq t \leqq 3m+\frac{1}{2}$	m 個
$k=6m+2$ のとき	$2m+\frac{2}{3} \leqq t \leqq 3m+1$	$m+1$ 個
$k=6m+3$ のとき	$2m+1 \leqq t \leqq 3m+\frac{3}{2}$	$m+1$ 個
$k=6m+4$ のとき	$2m+\frac{4}{3} \leqq t \leqq 3m+2$	$m+1$ 個
$k=6m+5$ のとき	$2m+\frac{5}{3} \leqq t \leqq 3m+\frac{5}{2}$	$m+1$ 個

一つの m に対し個数は $6m+5$ 個ある．$2008=6\cdot 334+4$ なので $m=0,\ 1,\ \cdots,\ 334$ について $6m+5$ を加え，2009 のときの個数 335 個を除けばよい．

$$\begin{aligned}\therefore\quad \sum_{m=0}^{334}(6m+5)-335 &= 6\cdot 167\cdot 335+5\cdot 335-335\\ &= (1002+4)\cdot 335=337010\ (\text{個})\end{aligned}$$

(2) 不等式は $3x+2y+z \leqq 60$ と同値である．$3x+2y=k$ となる一組の $(x,\ y)$ に対し，z は $0 \leqq z \leqq 60-k$ の範囲に $60-k+1$ 個とれる．組 $(x,\ y)$ の個数に z の個数を乗じたものが，$3x+2y=k$ かつ $3x+2y+z \leqq 60$ となる整数の組 (x,y,z) の個数である．

$k=6m$ のとき	$(m+1)(60-6m+1)$ 個
$k=6m+1$ のとき	$m(60-6m)$ 個
$k=6m+2$ のとき	$(m+1)(60-6m-1)$ 個
$k=6m+3$ のとき	$(m+1)(60-6m-2)$ 個
$k=6m+4$ のとき	$(m+1)(60-6m-3)$ 個
$k=6m+5$ のとき	$(m+1)(60-6m-4)$ 個

これを加える．

$$(m+1)(300-30m-9)+m(60-6m)=-36m^2+321m+291$$

$m=0,\ \cdots,\ 9$ についてこれを加え，$3x+2y=60$ とき (このとき z は 0 のみ) の 11 個を加える．

$$\begin{aligned}\therefore\quad \sum_{m=0}^{9}(-36m^2+321m+291)+11 &= -6\cdot 9\cdot 10\cdot 19+321\cdot 45+2910+11\\ &= -10260+14445+2921=7106\ (\text{個})\end{aligned}$$

解答 16 (問題 16)

(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 17 (問題 17)

(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 18 (問題 18)

(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 19 (問題 19)

(1)

$$b(p^2+q^2)=apq\quad\cdots①$$

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

$$b({p'}^2+{q'}^2)=ap'q'\quad\cdots②$$

(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

$$\begin{aligned}
&{p'}^2+{q'}^2\text{と}p'q'\text{が互いに素でない}\\
\iff\quad&{p'}^2+{q'}^2+2p'q'\text{と}p'q'\text{が互いに素でない}\\
\iff\quad&(p'+q')^2\text{と}p'q'\text{が互いに素でない}\\
\iff\quad&p'+q'\text{と}p'q'\text{が互いに素でない}\\
\iff\quad&p'\text{か}q'\text{の少なくともいずれかと}p'+q'\text{が互いに素でない}\\
\iff\quad&p'\text{と}q'\text{が互いに素でない}
\end{aligned}$$

ゆえに $k=1$ となり， $b=p'q'$ ， $a={p'}^2+{q'}^2$ ．つまり

$$\sqrt{a+2b}=p'+q'.$$

これは自然数である.

解答 20 (問題 20)

(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 21 (問題 21)

(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

$$r = 2^{n+1}-1, \quad s = 2^{m+1}-1$$

解答 22 (問題 22)

$$\begin{aligned} 3^{n+1} + 4^{2n-1} &= 9 \cdot 3^{n-1} + 4 \cdot 16^{n-1} \\ &= 9 \cdot 3^{n-1} + 4 \cdot (13+3)^{n-1} \\ &\equiv 9 \cdot 3^{n-1} + 4 \cdot 3^{n-1} \,(\text{mod. } 13) \\ &= 13 \cdot 3^{n-1} \equiv 0 \,(\text{mod. } 13) \end{aligned}$$

解答 23 (問題 23)

$$\begin{aligned} 19^n + (-1)^{n-1}2^{4n-3} &= 19^n + 2 \cdot (-16)^{n-1} \\ &= (14+5)^n + 2 \cdot (5-21)^{n-1} \\ &\equiv 5 \cdot 5^{n-1} + 2 \cdot 5^{n-1} \equiv 0 \,(\text{mod. } 7) \end{aligned}$$

解答 24 (問題 24)

(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 25 (問題 25)

解 1　$n^9 - n^3 = n^2(n^7 - n)$ 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 2

$$\begin{aligned}
n^9 - n^3 &= n^3(n^3 - 1)(n^3 + 1) \\
&= (n-1)n(n+1)n^2(n^2 + n + 1)(n^2 - n + 1) \\
&= (n-1)\{(n-1)^2 + 3n\} \cdot n^3 \cdot (n+1)\{(n+1)^2 - 3n\}
\end{aligned}$$

n が 3 の倍数なら n^3 が 9 の倍数，n が 3 で割って 1 余る数なら $(n-1)\{(n-1)^2 + 3n\}$ が 9 の倍数，
n が 3 で割って 2 余る数なら $(n+1)\{(n+1)^2 + 3n\}$ が 9 の倍数となり，つねに 3 の倍数である．

解答 26 (問題 26)

(1) (i) $gcd(N,\ n) \neq 1$ となるものは，p または q の倍数である．したがって N より小さい自然数 n では

$$p,\ 2p,\ 3p,\ \cdots,\ (q-1)p$$
$$q,\ 2q,\ 3q,\ \cdots,\ (p-1)q$$

である．

(ii) $1 \leqq n < N$ の範囲で $gcd(N,\ n) \neq 1$ となるものが (i) より

$$(q-1)+(p-1) \text{ 個}$$

ある．同じ範囲で $gcd(N,\ n) = 1$ となるものはそれらを除いたものである．

$$\therefore \quad \phi(N) = pq - 1 - (q-1) - (p-1) = (p-1)(q-1)$$

(2) $N = pq$ なので (ii) から

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

つまり，

$$p+q = N+1-\phi(N),\ pq = N$$

よって，p と q を解としてもつ二次方程式は未知数を x とすれば次のようになる．

$$x^2 - \{N+1-\phi(N)\}x + N = 0$$

(3)

$$N+1-\phi(N) = 18426 = 2 \cdot 9213$$

である．よって

$$p,\ q = 9213 \pm \sqrt{9213^2 - 84754668} = 9213 \pm \sqrt{106276} = 9539,\ 8887$$

解答 27 (問題 27)

(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 28 (問題 28)

(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．

(i) $x_{n+1} + x_{n+2}$ 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

$$(p-1)a_n$$

(ii) $x_{n+1} + x_{n+2}$ 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 29 (問題 29)

(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．この元はすべて異なり 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 つの元 $\alpha^i,\ \alpha^j$ $(0 \leqq i,\ j \leqq n-1)$ に対して α^{i+j} も明らかに $x^n - 1 = 0$ の解なので，再び G の元である．

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 の元 z に対し，そのべき $z,\ z^2,\ z^3,\ \cdots$ もすべて G の元である．$z \in G$ 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 の元はすべて 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 の元 z の偏角 $\arg z$ は $0 \leqq \arg z < 2\pi$ でとるとする．

G の元で偏角が正で最小であるものを α とする．G の任意の元 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 $\arg \alpha$ の偏角より小さい元 $z\alpha^{-m}$ が存在し，G の元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 の元はすべて 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．

解答 30 (問題 30)

(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 の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 31 (問題 31)

(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 9.2.4　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.

他の演習問題にあるように，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.

(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

$$\begin{aligned}
g(1) &= 3f(1+2+3+4+5+6+0) = 3f(21) = 0 \\
g(2) &= 3f(1+4+2+2+4+1+0) = 3f(14) = 0 \\
g(3) &= 3f(1+1+6+1+6+6+0) = 3f(21) = 0 \\
g(4) &= 3f(1+2+4+4+2+1+0) = 3f(14) = 0 \\
g(5) &= 3f(1+4+5+2+3+6+0) = 3f(21) = 0 \\
g(6) &= 3f(1+1+1+1+1+1+0) = 3f(6) = 18
\end{aligned}$$

となるから, $n=6$ をとれば

$$g(6) = 18$$

解答 32 (問題 32)

(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 までては出来ない. 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．

注意 9.2.5 本問の (2) は正整数 n が 3 個の平方数の和とならないための十分条件を与えている．しかし (1) の 28 が示すように，これは必要条件ではない．

では正整数 n が 3 個の平方数の和とならないための必要十分条件は何か．実はそれもガウスが解決している．

$$n \text{ が正整数 } a \text{ と } b \text{ で } 4^a(8b-1) \text{ と表されること}$$

これが $n=x^2+y^2+z^2$ となる正整数 $x,\ y,\ z$ が存在しないための必要十分条件である．

『数論講義』(J.P,Serre) に載っている．

解答 33 (問題 33)

(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，

$$Q_1(x)=a_nx^{n-1},\ F_1(x)=F(x)-G(x)Q_1(x)$$

とおく．

$$G(x)Q_1(x)=(x-a)\cdot a_nx^{n-1}=a_nx^n-aa_nx^{n-1}$$

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．
$1\sim n-1$ 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．

解答 34 (問題 34)

(1) $p(x) = 1$ とすれば $f(x) = f(x)p(x)$ となるので，整式 $f(x)$ は $f(x)$ の約数である．

(2) 0 と異なる整式 $f(x)$ が整式 $g(x)$ なので，(1) から $f(x)$ は $f(x)$，$g(x)$ の公約数である．$f(x)$ の約数の次数は $f(x)$ の次数以下であるから，$f(x)$ は $f(x)$ と $g(x)$ の公約数のなかで次数最大である．つまり $f(x)$ は $f(x)$，$g(x)$ の最大公約数である．

(3) 整式 $g(x)$ を $f(x)$ で割った商を $q(x)$ とすると，

$$g(x) = f(x)q(x) + r(x)$$

である．整式 $d(x)$ が $r(x)$，$f(x)$ の公約数なので，$d(x)$ は $g(x)$ の約数ともなり，$d(x)$ は $f(x)$，$g(x)$ の公約数でもある．

ここで $f(x)$，$g(x)$ の最大公約数を $D(x)$ とすると，

$$d(x) \text{ の次数} \leqq D(x) \text{ の次数}$$

つぎに

$$r(x) = g(x) - f(x)q(x)$$

より $D(x)$ は $r(x)$ の約数にもなり，$D(x)$ は $r(x)$，$f(x)$ の公約数となる．この結果

$$D(x) \text{ の次数} \leqq d(x) \text{ の次数}$$

あわせて

$$D(x) \text{ の次数} = d(x) \text{ の次数}$$

となり，$d(x)$ が $f(x)$，$g(x)$ の最大公約数でもあることが示された．

解答 35 (問題 35)

解 1　$(x+1)^3$ を $x-1$ で割って

$$(x+1)^3 = (x-1)(x^2+4x+7)+8$$

これから

$$-\left(\frac{1}{8}x^2+\frac{1}{2}x+\frac{7}{8}\right)(x-1)+\frac{1}{8}(x+1)^2=1$$

となる．$p(x)f(x)+q(x)g(x)=1$ と辺々引いて

$$(x-1)\left\{p(x)+\frac{1}{8}x^2+\frac{1}{2}x+\frac{7}{8}\right\}+(x+1)^3\left\{q(x)-\frac{1}{8}\right\}=0$$

$x-1$ と $(x+1)^3$ は互いに素なので，ある整式 $T(x)$ を用いて

$$\begin{aligned} p(x)+\frac{1}{8}x^2+\frac{1}{2}x+\frac{7}{8} &= (x+1)^3T(x)\\ q(x)-\frac{1}{8} &= -(x-1)T(x) \end{aligned}$$

と表され，またこの形のものは与式を満たす．ゆえに任意の解は

$$\begin{aligned} p(x) &= -\frac{1}{8}x^2-\frac{1}{2}x-\frac{7}{8}+(x+1)^3T(x)\\ q(x) &= \frac{1}{8}-(x-1)T(x) \end{aligned}$$ ，($T(x)$ は任意の整式)

と表される．

次数最小のものは $T(x)=0$ のときである．

$$\begin{aligned} p(x) &= -\frac{1}{8}x^2-\frac{1}{2}x-\frac{7}{8}\\ q(x) &= \frac{1}{8} \end{aligned}$$

である．最高次数の係数が 1 で次数最小のものは $T(x)=1$ のときだから

$$\begin{aligned} p(x) &= x^3+\frac{23}{8}x^2+\frac{5}{2}x+\frac{1}{8}\\ q(x) &= -x+\frac{7}{8} \end{aligned}$$

である．

解 2　与式に $x=1,\ x=-1$ を代入して

$$q(1)(1+1)^3=1,\ p(-1)(-1-1)=1$$

これから $p(x),\ q(x)$ は，ある整式 $P(x),\ Q(x)$ を用いて

$$p(x)=(x+1)P(x)-\frac{1}{2},\ q(x)=(x-1)Q(x)+\frac{1}{8}$$

と表される．これを与式に代入して

$$(x-1)\left\{(x+1)P(x)-\frac{1}{2}\right\}+(x+1)^3\left\{(x-1)Q(x)+\frac{1}{8}\right\}=1$$

これから

$$\begin{aligned}(x^2-1)P(x)+(x^2-1)(x+1)^2Q(x) &= 1-\frac{(x+1)^3}{8}+\frac{x-1}{2}\\ &= \frac{(x^2-1)(-x-3)}{8}\end{aligned}$$

$$\therefore\quad P(x)=-(x+1)^2Q(x)-\frac{x+3}{8}$$

次数を小さくとるために，$Q(x)=0$ とおく．$P(x)=-\dfrac{x+3}{8}$.

このとき

$$\begin{aligned}p(x) &= (x+1)\left(-\frac{x+3}{8}\right)-\frac{1}{2}\\ &= -\frac{1}{8}x^2-\frac{1}{2}x-\frac{7}{8}\\ q(x) &= \frac{1}{8}\end{aligned}$$

逆にこれは与式を満たす.

次に与式を満たす任意の $p(x)$, $q(x)$ と，先に求めた一組の解を与式に代入し

$$\begin{aligned}&(x-1)p(x)+(x+1)^3q(x)=1\\ &(x-1)\left(-\frac{1}{8}x^2-\frac{1}{2}x-\frac{7}{8}\right)+(x+1)^3\left(\frac{1}{8}\right)=1\end{aligned}$$

の辺々を引く (以下は同じ).

解答 36 問題 36

解 1　(整式の除法を用いる方法)

$Q(x)$ は 2 次式なので，整式 $P(x)$ を $Q(x)$ で割った余りは 1 次以下の整式である．商を $A(x)$，余りを $ax+b$ とする．

$$P(x)=Q(x)A(x)+ax+b$$

このとき

$$\begin{aligned}\{P(x)\}^2 &= \{Q(x)A(x)\}^2\\ &\quad +2(ax+b)Q(x)A(x)+(ax+b)^2\end{aligned}$$

ところが $\{P(x)\}^2$ は $Q(x)$ で割り切れるので $\{P(x)\}^2=Q(x)B(x)$ とおける．これから

$$\begin{aligned}&Q(x)\left[B(x)-Q(x)\{A(x)\}^2\right.\\ &\quad\left.-2(ax+b)A(x)\right]=(ax+b)^2\end{aligned}$$

$Q(x)$ は 2 次式で，右辺は 2 次以下であるから，$B(x)-Q(x)\{A(x)\}^2-2(ax+b)A(x)$ は定数である．これを c とする．

$P(x)$ は $Q(x)$ で割り切れないので右辺は定数 0 ではない．つまり $c\neq 0$ である．よって $Q(x)$ は

$$Q(x)=\frac{1}{c}(ax+b)^2$$

と表される．$Q(x)$ は 2 次式だから $a \neq 0$ である．このとき方程式 $Q(x) = 0$ は重解 $x = -\dfrac{b}{a}$ を持つ．

解 2　(整式の整数論を用いる方法)

$Q(x) = 0$ の解を α と β とし，

$$Q(x) = a(x - \alpha)(x - \beta)$$

とおく．$\alpha \neq \beta$ と仮定する．このとき $x - \alpha$ と $x - \beta$ は互いに素である．よって任意の整式 $f(x)$ について $f(x)$ が $Q(x)$ で割りきれることと，$f(x)$ が $x - \alpha$ で割り切れかつ $x - \beta$ で割り切れることが同値である．もし $P(x)$ が因数 $x - \alpha$ をもたなければ，整式における素因数分解の一意性によって，$\{P(x)\}^2$ も因数 $x - \alpha$ をもたない．よってもし $\{P(x)\}^2$ が因数 $x - \alpha$ をもてば，$P(x)$ が因数 $x - \alpha$ をもつ．

$\{P(x)\}^2$ は $Q(x)$ で割り切れるので，$\{P(x)\}^2$ が因数 $x - \alpha$ と $x - \beta$ をもち，その結果 $P(x)$ が因数 $x - \alpha$ と $x - \beta$ をもつ．

ところがこれは $P(x)$ が $Q(x)$ で割りきれることを意味し，仮定と矛盾する．よって $\alpha = \beta$ であり，2 次方程式 $Q(x) = 0$ は $x = \alpha$ を重解にもつ．

解答 37　問題 37

解 1　(整式の除法を用いる方法)

$A(x)$ と $B(x)$ を $C(x)$ で割った商と余りをそれぞれ a, p と b, q とし，

$$\begin{aligned} A(x) &= aC(x) + p \\ B(x) &= bC(x) + q \end{aligned}$$

とおく．それぞれ 1 次式であるので，$ab \neq 0$ である．$\{A(x)\}^2 + \{B(x)\}^2 = \{C(x)\}^2$ より

$$a^2\{C(x)\}^2 + 2apC(x) + p^2 + b^2\{C(x)\}^2 + 2bqC(x) + q^2 = \{C(x)\}^2 \quad \cdots ①$$

$C(x)$ を $cx + d$ とすると，$c \neq 0$ で，両辺の x^2 の係数の比較より

$$a^2c^2 + b^2c^2 = c^2$$

これから

$$a^2 + b^2 = 1$$

である．このとき ① は

$$2apC(x) + p^2 + 2bqC(x) + q^2 = 0$$

となる．両辺の x の係数比較から

$$2apc + 2bqc = 0$$

その結果，$ap + bq = 0 \quad \cdots ②$ となり，さらに

$$p^2 + q^2 = 0 \quad \cdots ③$$

である．ここで $a \neq 0$ なので ② から

$$p = -\frac{bq}{a}$$

これを ③ に代入して

$$\frac{b^2q^2}{a^2} + q^2 = \frac{b^2 + a^2}{a^2}q^2 = \frac{1}{a^2}q^2 = 0$$

よって $q=0$ となり，③ から $p=0$.

$A(x)$ と $B(x)$ はともに $C(x)$ の定数倍であることが示された.

解 2　(整式の整数論を用いる方法)

$\{A(x)\}^2+\{B(x)\}^2=\{C(x)\}^2$ より

$$\{B(x)\}^2=\{C(x)+A(x)\}\{C(x)-A(x)\}$$

である．$C(x)+A(x)$ も $C(x)-A(x)$ も 1 次以下の整式であるから $\{B(x)\}^2$ の定数倍になることはない．したがって定数 k $(k\neq 0)$ が存在して

$$C(x)+A(x)=kB(x)$$
$$C(x)-A(x)=\frac{1}{k}B(x)$$

と表される．これから

$$A(x)=\frac{k^2-1}{2k}B(x),\ C(x)=\frac{k^2+1}{2k}B(x)$$

である．$A(x)$ も $C(x)$ も 1 次式なので $k^2\pm 1\neq 0$ である．

$$A(x)=\frac{k^2-1}{k^2+1}C(x),\ B(x)=\frac{2k}{k^2+1}C(x)$$

となり，$A(x)$ と $B(x)$ はともに $C(x)$ の定数倍であることが示された.

解答 38 問題 38　**解 1**

$f(x)$ を n $(n\geqq 0)$ 次，　$g(y)$ $(m\geqq 0)$ を m 次とし

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$$
$$g(y)=b_my^m+b_{m-1}x^{m-1}+\cdots+b_0$$

とおく．条件は $f(x)$ と $g(y)$ で対称なので $n\geqq m$ とする．

$y=\dfrac{1}{x}$ のとき条件は

$$\begin{aligned} f(x)g(y) &= f(x)g\left(\frac{1}{x}\right) \\ &= (a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0)\left(b_m\left(\frac{1}{x}\right)^m+b_{m-1}\left(\frac{1}{x}\right)^{m-1}+\cdots+b_0\right)=1 \\ \iff\quad & (a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0)(b_m+b_{m-1}x+\cdots+b_0x^m)=x^m \quad \cdots① \end{aligned}$$

となる.

$$b_0,\ b_1,\ \cdots,\ b_m$$

のなかでこの順に見て最初に 0 でない係数を b_{m-j} とする．上の条件は

$$\begin{aligned} & (a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0)(b_m+b_{m-1}x+\cdots+b_{m-j}x^j)=x^m \\ \iff\quad & a_nb_{m-j}x^{n+j}+\cdots=x^m \end{aligned}$$

これから $n+j=m$ であるが $n\geqq m$ より $j\neq 0$ なら $n+j>m$ で不可.

$$\therefore\quad j=0,\ n=m,\ a_nb_{m-j}=1$$

つまり $a_nb_n=1$ ．整数係数なので $a_n=b_n=\pm1$ で $g(y)=b_ny^n$ ．このとき ① より

$$x^n+b_n(a_{n-1}x^{n-1}+\cdots+a_0)=x^n$$

$b_n\neq0$ なので $a_{n-1}=\cdots=a_0=0$．ゆえに

$$f(x)=\pm x^n,\ g(y)=\pm y^n\quad(\text{複号同順})\quad n\text{ 非負整数}$$

解 2

$f(x)$ を n $(n\geqq0)$ 次，$g(y)$ $(m\geqq0)$ を m 次とし

$$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$$
$$g(y)=b_my^m+b_{m-1}x^{m-1}+\cdots+b_0$$

とおく．条件は $f(x)$ と $g(y)$ で対称なので $n\geqq m$ とする．

$y=\dfrac{1}{x}$ のとき条件は

$$\begin{aligned}f(x)g(y)&=f(x)g\left(\frac{1}{x}\right)\\&=(a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0)\left(b_m\left(\frac{1}{x}\right)^m+b_{m-1}\left(\frac{1}{x}\right)^{m-1}+\cdots+b_0\right)=1\\\iff&\quad(a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0)(b_m+b_{m-1}x+\cdots+b_0x^m)=x^m\quad\cdots①\end{aligned}$$

となる．

$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$ も $b_m+b_{m-1}x+\cdots+b_0x^m$ も x^m の約数となるが，x は既約なので，ともに x^l の定数倍という形をしている．次数を考えると $n=m$ で

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0=a_nx^n,\ b_m+b_{m-1}x+\cdots+b_0x^m=b_m$$

である．さらに $a_nb_m=1$ となり係数が整数なのでともに ±1 である．ゆえに

$$f(x)=\pm x^n,\ g(y)=\pm y^n\quad(\text{複号同順})\quad n\text{ 非負整数}$$

解答 39 (問題 39)　$p=2$ 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．

$p\geqq3$ とする．二項定理より

$$\begin{aligned}(a+bi)^p&=\sum_{k=0}^{p}{}_p\mathrm{C}_ka^{p-k}(ib)^k\\&=\sum_{m=0}^{\frac{p-1}{2}}(-1)^m{}_p\mathrm{C}_{2m}a^{p-2m}b^{2m}+i\left(\sum_{m=0}^{\frac{p-1}{2}}(-1)^m{}_p\mathrm{C}_{2m+1}a^{p-2m-1}b^{2m+1}\right)\end{aligned}$$

$(a+bi)^p$ 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

$$\begin{aligned}
&\sum_{m=0}^{\frac{p-1}{2}}(-1)^m{}_p\mathrm{C}_{2m+1}a^{p-2m-1}b^{2m+1}\\
=\ & pa^{p-1}b+\sum_{m=1}^{\frac{p-3}{2}}(-1)^m{}_p\mathrm{C}_{2m+1}a^{p-2m-1}b^{2m+1}+(-1)^{\frac{p-1}{2}}b^p\\
=\ & pa^{p-1}b+ab^2\left(\sum_{m=1}^{\frac{p-3}{2}}(-1)^m{}_p\mathrm{C}_{2m+1}a^{p-2m-2}b^{2m-1}\right)+(-1)^{\frac{p-1}{2}}b^p
\end{aligned}$$

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 40 (問題 40)

(1) 係数は実数なので，$a+bi$ が解ならその共役 $a-bi$ も解である．他の実数解を α とする．解と係数の関係から

$$\begin{cases}
(a+bi)+(a-bi)+\alpha=2a+\alpha=-8\\
(a+bi)(a-bi)+(a+bi)\alpha+(a-bi)\alpha=a^2+b^2+2a\alpha=m\\
(a+bi)(a-bi)\alpha=(a^2+b^2)\alpha=-60
\end{cases}$$

である．$\alpha=-8-2a$ より $(a^2+b^2)(-8-2a)=-60$ となるので

$$(a^2+b^2)(a+4)=30\quad\cdots①$$

である．30 の約数で a^2+b^2 の形の数，および ① となるようにそのとき $a+4$ のとるべき値を書くと

a^2+b^2	$0^2+1^2=1$	$1^2+1^2=2$	$1^2+2^2=5$	$1^2+3^2=10$
$a+4$	30	15	6	3

である．各 a^2+b^2 に対し，a と b の入れ替えと正負で 4 通り a がとれるが，そのうち $a+4$ がとるべき値になるものを選ぶと

$$(a,\ b) = (-1,\ \pm 3),\ (2,\ \pm 1)$$

のみである．それぞれ $\alpha=-6,\ m=22$ および $\alpha=-12,\ m=-43$ である．

よって条件を満たす m は $-6,\ -43$ である．

(2) (1) から $f(x)=0$ の解は

$$\begin{array}{ll} m=22 \text{ のとき} & -6,\ -1\pm 3i \\ m=-43 & -12,\ 2\pm i \end{array}$$

解答 41 (問題 41)

(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．

したがって組の各元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 9.2.6 この問題は定理 47 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

解答 42 (問題 42)

(1) (i) $(x,\ y)$ を任意の整数解とする．

$$\alpha x = \beta y$$

で α, β 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

$$q = a_1, \ \frac{r_1}{\beta} = \frac{1}{a_2 + \dfrac{1}{a_3 + \dfrac{1}{a_4}}}$$

次に

$$\frac{\beta}{r_1} = a_2 + \frac{1}{a_3 + \dfrac{1}{a_4}}$$

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 $r_3 = 1$

注意 9.2.7 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

$$\begin{aligned} & (1 + a_2 a_3)\alpha - (a_1 a_2 a_3 + a_1 + a_3)\beta = 1 \\ \therefore \quad & \alpha q - \beta p = 1 \end{aligned}$$

(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 43 (問題 43)

(1)

$$\begin{aligned} a_n + b_n\sqrt{2} &= (3+2\sqrt{2})^n \\ &= (3+2\sqrt{2})(3+2\sqrt{2})^{n-1} \\ &= (3+2\sqrt{2})(a_{n-1}+b_{n-1}\sqrt{2}) \\ &= (3a_{n-1}+4b_{n-1})+(2a_{n-1}+3b_{n-1})\sqrt{2} \end{aligned}$$

もし $b_n \neq 2a_{n-1}+3b_{n-1}$ なら

$$\sqrt{2} = -\frac{a_n - 3a_{n-1} - 4b_{n-1}}{b_n - 2a_{n-1} - 3b_{n-1}}$$

となる．$\sqrt{2}$ は無理数で右辺は有理数となり．矛盾.

$$\therefore \quad \begin{cases} a_n = 3a_{n-1}+4b_{n-1} \\ b_n = 2a_{n-1}+3b_{n-1} \end{cases}$$

(2) $n \geqq 2$ のとき

$$\begin{aligned} {a_n}^2 - 2{b_n}^2 &= (3a_{n-1}+4b_{n-1})^2 - 2(2a_{n-1}+3b_{n-1})^2 \\ &= {a_{n-1}}^2 - 2{b_{n-1}}^2 \end{aligned}$$

$$\therefore \quad {a_n}^2 - 2{b_n}^2 = {a_1}^2 - 2{b_1}^2 = 9 - 2\cdot 4 = 1$$

(3) (2) から

$$\frac{{a_n}^2}{{b_n}^2} - 2 = \frac{1}{{b_n}^2}$$

である．つまり

$$\frac{a_n}{b_n} - \sqrt{2} = \frac{1}{{b_n}^2} \cdot \frac{1}{\dfrac{a_n}{b_n} + \sqrt{2}}$$

ここで (1) から

$$\begin{pmatrix} a_n \\ b_n \end{pmatrix} = \begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} a_{n-1} \\ b_{n-1} \end{pmatrix}$$

なので，これを用いて $a_1 = 3,\ b_1 = 2$ から $a_n,\ b_n$ を順次求めると，

$$\begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} 17 \\ 12 \end{pmatrix},\ \begin{pmatrix} a_3 \\ b_3 \end{pmatrix} = \begin{pmatrix} 99 \\ 70 \end{pmatrix},\ \begin{pmatrix} a_4 \\ b_4 \end{pmatrix} = \begin{pmatrix} 577 \\ 408 \end{pmatrix}$$

である．したがって

$$\frac{a_4}{b_4} - \sqrt{2} = \frac{1}{408^2} \cdot \frac{1}{\dfrac{577}{408} + \sqrt{2}} < \frac{1}{10000}$$

求める有理数は $\dfrac{a_4}{b_4} = \dfrac{577}{408}$

解答 44 (問題 44)

(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)

$$\begin{aligned} a - \frac{P_n}{Q_n} &= \frac{P_{n-1} + P_na_n}{Q_{n-1} + Q_na_n} - \frac{P_n}{Q_n} = \frac{(P_{n-1} + P_na_n)Q_n - P_n(Q_{n-1} + Q_na_n)}{(Q_{n-1} + Q_na_n)Q_n} \\ &= \frac{(P_{n-1}Q_n - P_nQ_{n-1}}{(Q_{n-1} + Q_na_n)Q_n} = \frac{-(-1)^n}{(Q_{n-1} + Q_na_n)Q_n} \end{aligned}$$

$$\therefore \quad \left|a - \frac{P_n}{Q_n}\right| = \frac{1}{|(Q_{n-1} + Q_na_n)Q_n|}$$

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

$$\begin{aligned} |(Q_{n-1} + Q_na_n)Q_n| &= (Q_{n-1} + Q_na_n)Q_n \\ &\geqq a_nQ_n^2 > Q_n^2 \end{aligned}$$

$$\therefore \quad \left|a - \frac{P_n}{Q_n}\right| < \frac{1}{Q_n^2}$$

解答 45 (問題 45)

(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 46 (問題 46)

(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 47 (問題 47)

(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 48 (問題 48)

(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．

(1) 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．

解答 49 (問題 49)

(1) $\sqrt{3} = \dfrac{p}{q}$ となる整数 $p,\ q$ が存在したとして矛盾を示す．以下特に断らなければ文字は整数を表す．

証明法 1

$\sqrt{3}$ が無理数でない，つまり有理数とする． $\sqrt{3} = \dfrac{q}{p}$ とおく．ここで p と q は互いに素であるとできる．

$$\therefore \quad 3p^2 = q^2$$

数 q が 3 の倍数でなければ $q = 3k \pm 1$ とおける．$q^2 = (3k \pm 1)^2 = k^2 \pm 6k + 1$ より 3 の倍数でない数 q の平方 q^2 は 3 の倍数でない．ところが左辺が 3 の倍数なので q は 3 の倍数でなければならない．$q = 3q'$ とおける．すると

$$3p^2 = (3q')^2 \quad \Rightarrow \quad p^2 = 3q'^2$$

これから p も 3 の倍数となり， p と q が互いに素であることと矛盾した．

ゆえに $\sqrt{3}$ は無理数である．

証明法 2

$\sqrt{3}$ が無理数でない，つまり有理数とする． $\sqrt{3} = \dfrac{q}{p}$ とおく (既約である必要はない).

$$\therefore \quad 3p^2 = q^2$$

左辺の因数分解における因数 3 の個数は奇数である．右辺の因数分解における因数 3 の個数は偶数である

これは矛盾である．ゆえに $\sqrt{3}$ は無理数である．

証明法 3

$\sqrt{3}$ が無理数でない，つまり有理数とする．$\sqrt{3} = \dfrac{q}{p}$ とおく (既約である必要はない)..

$$\therefore \quad 3p^2 = q^2$$

証明法 1 と同様に 3 の倍数でない数の平方は 3 の倍数でない．ところが左辺が 3 の倍数なので q は 3 の倍数でなければならない．$q = 3q'$ とおける．すると

$$2p^2 = (2q')^2 \quad \Rightarrow \quad p^2 = 2q'^2$$

これから p も 3 の倍数となり $p = 3p'$ とおける．

再び

$$3p'^2 = q'^2$$

となる．同様にして p', q' とも 3 の倍数である．これは何回でも繰り返される．

つまり p も q も 3 で無限回割れる．これは $p = q = 0$ 以外では不可能である．

ゆえに $\sqrt{3}$ は無理数である．

(2) $a\omega + b$ が有理数 q であるとする．$a\omega + b = q$ において $a \neq 0$ なので

$$\omega = \frac{q - b}{a}$$

有理数の和，差，積，商は再び有理数なので，これは ω が無理数であることに矛盾した．

よって $a\omega + b$ は無理数である．

(3) $p,\ q,\ r,\ s$ がすべて有理数と仮定する．

△OAB の面積を二通りの方法で求める．

$$\triangle \mathrm{OAB} = \frac{1}{2}\mathrm{OA}^2 \sin 60^\circ = \frac{\sqrt{3}}{4}(p^2+q^2)$$

一方

$$\triangle \mathrm{OAB} = \frac{1}{2}|ps-qr|$$

である．ゆえに

$$\frac{\sqrt{3}}{4}(p^2+q^2) = \frac{1}{2}|ps-qr|$$

が成り立たねばならない．つまり

$$\frac{\sqrt{3}}{4}(p^2+q^2) - \frac{1}{2}|ps-qr| = 0$$

である．ここで (2) から左辺は無理数である．一方，右辺 0 は有理数で矛盾である．

よって $p,\ q,\ r,\ s$ のうち少なくとも 1 つは有理数とならないことが示された．

解答 50 (問題 50)

(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 の元である．ところがこの元の値 x_0+2y_0 は明らかに値 x_0 より大きい．

$(x_0,\ y_0)$ が A の元で値 x が最大のものであることに矛盾した．

ゆえに A は無限個の元をもつ．

$n=2$ で (1) を用いることにより A の二つの元 $(x,\ y)$ と $(z,\ t)$ に対して $(xz+2yt,\ xt+yz)$ も A の元である．

$(1,\ 1) \in A$ 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 51 (問題 51)

(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

$$\begin{aligned} (2y)^2-x^2 &= 4y^2-(2y^2\pm 1) \\ &= 2y^2\mp 1>0 \\ \therefore &\quad u=-x+2y>0 \\ x^2-y^2 &= (2y^2\pm 1)-y^2 \\ &= y^2\pm 1>0 \\ \therefore &\quad v=x-y>0 \\ &\quad \text{(複号同順)} \end{aligned}$$

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 の元の 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 の元で 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 の元ではない. 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 の元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.

$$\therefore \quad \lim_{n\to\infty} \frac{y_{n+1} - y_n}{x_{n+1} - x_n} = \frac{\sqrt{2}}{2}$$

9.3 出典と文献

9.3.1 入試問題出典

1 章

［98 お茶の水大］【1】／ユークリッドの互除法の原理
［91 阪大理系後期］【2】／ユークリッドの互除法の長さの評価
［80 京大文系］【3】／差で閉じた有限集合
［80 京大理系］【4】／差で閉じた有限集合
［85 お茶の水女子大］【5】／和と差で閉じた集合
［08 奈良県立医大］【6】／剰余系と解の存在
［00 大阪女子大］【7】／一次不定方程式の解の存在
［立命館大改題］【8】／一次不定方程式の一般解
［02 金沢大理系後期］【9】／領域内格子点の対応
［00 阪大理系前期］【10】／一次式で数を表す
［00 京大理系後期］【11】／一次不定方程式の一般解，格子点
［89 京大理系後期］【12】／格子点と三角形の面積
［91 東大理系前期］【13】／直線と格子点の距離
［90 京大理系後期］【14】／三角関数の値の集合
［08 名大理系 4 番 (a)］【15】／格子点の個数
［88 群馬大］【16】／$n!$ における素因数 2 の個数
［97 京大文系前期］【17】／約数の論証
［98 上智大］【18】／約数の個数とその和
［98 京大文系後期］【19】／約数の論証
［99 京大文系後期］【20】／ピタゴラス数の論証
［02 九大理系前期］【21】／約数の和に関する論証

2 章

［82 名古屋市大］【22】／倍数の証明
［東工大］【23】／倍数の証明
［82 九大］【24】／n 次方程式と整数
［01 京大文系前期］【25】／倍数の証明
［70 東大理系］【27】／1 の n 乗根，原始 n 乗根
［01 京大理系］【28】／1 の n 乗根
［01 京都府立医大］【29】／1 の n 乗根からなる集合
［98 奈良女子大改題］【30】／フェルマの小定理の数学的帰納法による証明
［95 京大文系後期］【31】／フェルマの小定理と応用
［98 横国大文系後期］【32】／3 個の平方数の和にならないための条件
［96 大阪教育大］【33】／式の除法

［90 京都教育大］【34】／式の互除法
［02 中央大］【??】／式の不定方程式
［06 京大文理系前期］【36】／式の整除問題
［06 京大文理系後期］【37】／式の整除問題
［00 お茶の水女子大］【38】／恒等式の決定
［00 京大文理系前期］【39】／ガウス整数の素数べき
［07 一橋前期］【40】／ガウス整数
［02 慶応医］【41】／素数の平方数の和への分解の初等的証明

3 章〜

［95 大阪府大］【6.1.1】／ある数列はペル方程式を満たす
［95 明治大］【6.1.2】／ペル方程式の解はある数列で得られる
［85 東工大］【6.1.2】／ペル方程式の解の構造
［93 早稲田］【42】／連分数による一次不定方程式の解
［04 名古屋大理系後期］【43】／ $\sqrt{2}$ の近似有理数
［00 上智大後期理工］【44】／無理数の近似有理数
［66 京大］【45】／格子点と正方形領域
［新潟大過去問］【46】／格子点と平行四辺形領域
［92 東大］【47】／線分上の格子点
［お茶の水女子大改題］【48】／格子点を頂点とする正多角形
［03 お茶の水女子大理系後期］【49】／格子点を頂点とする正三角形
［98 お茶の水女子大］【50】／ブラーマグプタの恒等式
［01 滋賀医大］【51】／双曲線上の格子点

9.3.2 参考文献

出版物：

- 初等整数論講義　第 2 版，高木貞治，共立出版，1971
- 代数的整数論 第 2 版，高木貞治，岩波書店，1971
- 数の概念，高木貞治，岩波書店，1970
- 解析的整数論，末綱恕一，岩波書店，1950
- 数論序説，小野孝，裳華房，1987
- 数論 I，加藤和也・黒川信重・斎藤毅，岩波書店，2005
- 数－体系と歴史，足立恒雄，朝倉書店，2002
- 数論講義，J.-P. セール (弥永健一訳)，岩波書店，1950
- 数論への出発，藤崎源二郎＋森田康夫＋山本芳彦，日本評論社，1980
- 素数，E. ボレル (芹沢正三訳)，文庫クセジュ，白水社，1959

- 整数論，J. イタール (村田全訳)，文庫クセジュ，白水社，1965

青空学園『数学対話』:

- 円周率を表す
- 素数の分布