

整数問題の攻略

～ 京都大学入試問題から学ぶ実戦的整数論入門～

2007 年版

奈良県立奈良高等学校 赤阪 正純

1 はじめに

史上最大の数学者ガウス (Gauss, Carl Friedrich 1777 ~ 1855 ドイツ) は

数学は科学の女王であり、
整数論は数学の女王である

という言葉を残した。つまり、「整数論は科学の中で最高位に位置する学問分野である」というわけだ。ともすれば、我々は「数学は科学の基礎であり、整数論は数学の基本である」と単純に捉えがちだが、それを「女王」という言葉で表現したガウスのセンスは素晴らしい。それは、科学の中で数学、とりわけ整数論が、最も美しく神秘的な魅力をもっていることを意味している。

そして、ガウスの言葉にはもう一つの意味が込められている。それは、数学の支柱となるような重要な考え方のほとんどがこの整数論に含まれていること、である。つまり、整数論は科学にとって最も大切な思考方法を学ぶことができる学問分野であるということだ。日本が生んだ最初の世界的数学者、高木貞治 (1875 ~ 1960) も「整数論の方法は繊細である、小心である、その理想は玲瓏にして些の陰翳をも留めざる所にある。代数学でも、函数論でも、又は幾何学でも、整数論的の試練を経て初めて精妙の境地に入るのである。」と述べている (初等整数論講義第 2 版序言)。代数的整数論の世界的権威で、類体論の創始者である氏のまことに奥の深い言葉である。

整数論の問題 (以下、整数問題) を解決する場合の基本的な考え方とは、すなわち、

- (1) 特殊な場合についての実験
- (2) 一般法則の推測
- (3) 法則の証明
- (4) 証明された法則の適用

である。確かに、これらの考え方は、数学に限らず科学の各分野に応用される考え方である。整数問題を考えることは、最高の思考訓練になる。

したがって、整数問題が難関大学を中心に頻出の分野である理由も理解できよう (特に、京都大学、一橋大学ではほぼ毎年出題されている)。変な受験テクニックや解法パターンの暗記に頼ることなく、本質をじっくり考えてもらおう、というのが大学側の意図するところであろう。

しかしながら、整数問題を解くには、整数特有の性質に着目することが多く、その性質を知っているかどうか正解へのカギを握っている。また、一部に他分野 (方程式、図形、関数など) との融合問題も見られ、見た目には整数問題かどうか分からない問題もあるが、示すべき内容、方法は共通している。いずれにしても、整数特有の性質、解決の手法を知らないと、どうにもならない。確かに、この整数特有の性質は「予備知識がなくても考えればわかること」ではあるが、極度の緊張状態の入試本番において思いつくのはなかなか厳しいものがあるため、十分な事前の対策が必要であろう。

整数問題を苦手とする受験生は多く、入試でも「ほとんど解けなかった」という感想をよく聞く。

また，できたと思っても，記述内容に論理的飛躍があることも多く，正答率は極めて低いと思われる．
ということは，逆に，整数問題が解ければ，他の受験生に差をつけ合格にグッと近づくことになるわけで，整数問題の出来，不出来が合否に大きな影響を及ぼすといっても過言ではない．

にも係わらず，現行の教育課程の下では，整数に関して，小学校で倍数や約数の性質について，中学校で素数や素因数分解について簡単に触れるだけであり，高等学校でも，整数に関して十分に時間をかけて学習することは，ない．このような状況であるから，整数問題を扱う適切な参考書や問題集も少なく，対策が立てにくいのが現状である．また，おそらく整数問題の唯一の本格的な参考書である『大学への数学 マスター・オブ・整数』（東京出版）は，内容があまりにも広範囲に渡っていて，少し難しすぎる（理学部数学科に進学して，将来，整数論を研究する気がある人は別だが）．確かにこの本を勉強すれば整数問題に関しては完璧になるが，他教科の学習のことも考えると，マスターするにはあまりにも時間がかかりすぎ，適切な参考書とはいえない．

そこで短期間で効率よく，整数問題の重要事項を理解するために，この冊子を作成した．これだけでほとんどの整数問題には対応できると思う．

本文の構成

- 整数問題の攻略（原則編）
- 整数問題の攻略（基礎編）
 - － 余りで分類する
 - － 素数 p の性質
 - － 偶奇性・周期性に注目する
 - － 互いに素
 - － ${}_pC_k$ は p の倍数
 - － 続・互いに素
- 整数問題の攻略（応用編）
 - － 格子点
 - － ガウス記号 $[x]$
 - － 有理数解をもつ方程式

- － Fermat の小定理
- － 数論的関数
- － 整数値多項式

- 京都大学で出題されたその他の整数問題
- 資料編

問題の構成

- 例
- 練習
- 演習問題
- 参考問題
- 総合演習問題

まずは，整数問題の攻略（原則編）を熟読して，基本的な考え方を確認すること．

それから整数問題の攻略（基礎編）を（この順に）学習してほしい．ここでは，整数問題を解くにあたっての基本的な技法を紹介してある．通常の入試問題ならこの基礎編の内容だけで十分である．

次の整数問題の攻略（応用編）は，より深く整数問題を理解したい人のために，興味深い内容をトピック的に並べてある．この応用編はかなり難易度が高いので，初めから完璧に理解しようとせず，大雑把に内容を掴む程度で良いだろう．整数問題では一般的な証明よりも，具体例による考察が重要であるため，証明の細部にこだわらず，具体例で意味を掴むことのほうが大切である．

したがって，扱う問題も例をなるべく多く紹介するようにした．

練習はポイントを確認，理解するための基本問題である．

演習問題は全て京都大学の入試問題から選んである．

また参考問題は京大以外の難関大学の入試問題を中心に精選してあるが，かなり難問なのでとばしても構わないだろう（あくまでも参考ということで）．

最後の総合演習問題は京大の整数問題の中から良問 11 問をセレクトした．これらの問題は，発想が

巧妙で、かなり難しく、おそらく合格者の中でも完答者は少なかったと思われるので、できなくても悲観する必要はない。しかし、こういう問題が解けると合格にグッと近づけるので、頑張って取り組んで欲しい。

なお、整数問題の攻略(応用編)には演習問題はない。すなわち京都大学の入試問題は整数問題の攻略(基本編)だけにある。したがって、京都大学志望者は、整数問題の攻略(基本編)をマスターした後、総合演習問題に取り組むと良いだろう。

また最後に京都大学で出題されたその他の整数問題として、本編では取り上げることができなかった整数問題をまとめておいた(1987年~2007年)。すべて解く必要はないが、図形との融合問題や、漸化式との融合問題など興味深い問題も多いので、各セクションの最初の問題は解いて欲しい。

また、資料編として、一橋大学の過去問題の中から、整数問題を集めておいたので参考にしてほしい。特に、京大文系志望の人は一橋大の問題を解くことを薦める。整数問題に限らず、一橋大の過去問に類似した問題が京大や阪大で実際に出題されている。例えば、京大2006年前期理系4番は一橋2005年後期1番に、阪大2006年後期理系2番は一橋2004年前期2番と本質的に同じ問題である。

本書の利用方法

京都大学志望者

整数問題の4原則 + α

↓

整数問題の攻略(基礎編)

↓

総合演習問題

↓

京都大学で出題されたその他の整数問題の各セクションの第1問

時間の余裕が十分にあり整数問題を極めたい人

順番に全部やってください。

それでは、整数問題の深遠な世界に入ろう。

2 整数問題の攻略(原則編)

まずはじめに、整数問題攻略の4原則 + α を述べる。これらは、ほとんど当たり前のことだが、意外と頭に入っていない(意識していない)人もいると思うので、確認しておこう。この4原則は常識として、これから使っていくので、しっかりと頭に入れておいてほしい。

整数問題の原則

整数は幅1でトビトビに存在する。

実数がベタ~ツと存在するのに対し、整数はトビトビに存在する。これを 実数の連続性、整数の離散性 という。

例 1

m, n を整数とするととき、次のことがいえる。

$$m < n < m + 1 \implies \text{矛盾}$$

$$m < n < m + 2 \implies n = m + 1$$

$$m \leq n < m + 1 \implies n = m$$

$$m < n \implies m + 1 \leq n$$

例 2

n の倍数は幅 n ごとにトビトビに存在する。つまり、適当に連続する n 個の整数をとれば、その中には必ず n の倍数が1個存在する。また余りの均等性より、連続する n 個の整数の中には n で割ったときの余りが $1, 2, \dots, n-1$ になる整数が1つずつ存在する。

例 3

a が n の倍数のとき、

$$-n < a < n \implies a = 0$$

例 4

$n > 3$ とする。 n と $n+2$ が共に素数のとき、 $n+1$ は6の倍数である。

ヒントと略解

$n > 3$ で n と $n+2$ が共に素数だから, n と $n+2$ は共に奇数である. よって, $n+1$ は偶数. $n, n+1, n+2$ は連続 3 整数だから, このうち 1 つは必ず 3 の倍数. $n > 3$ で n と $n+2$ が共に素数だから, $n+1$ が 3 の倍数になる. したがって, $n+1$ は 6 の倍数である.

注 1

n と $n+2$ が共に素数のとき, この 2 つの素数を双子素数と呼ぶ. 双子素数は $(3, 5), (5, 7), (11, 13), \dots$ など無限に存在すると考えられているが, 未だ証明されていない. 上の例は, $(3, 5)$ 以外の双子素数の間の数は必ず 6 の倍数であることを主張している.

例 5

一般に, k を 2 以上の自然数とすると, 連続する k 個の整数の積は必ず $k!$ の倍数になる (03 滋賀大 (前) に $k = 2, 4$ の場合の証明が出題されている). とくに, 連続 2 整数の積は偶数, 連続 3 整数の積は 6 の倍数であることは基本である.

ヒントと略解

連続する k 個の整数の中には, 必ず, k の倍数, $k-1$ の倍数, \dots 2 の倍数が存在することより明らか.

注 2

連続する k 個の整数の積は必ず $k!$ の倍数になることの証明はいろいろ考えられるが, 次の二項係数の式を見れば, 一目瞭然であろう (分子が連続する k 個の整数で, 二項係数 ${}_nC_k$ は整数だから).

$$\begin{aligned} {}_nC_k &= \frac{n!}{(n-k)!k!} \\ &= \frac{n(n-1)(n-2)\cdots(n-k+1)}{k!} \end{aligned}$$

整数問題の原則

整数問題では『積の形』をつくる!

例えば, x, y が実数のとき, $xy = 5$ を満たす (x, y) の組は無数に存在するが, x, y が整数のと

き, $xy = 5$ を満たす (x, y) の組は 4 組しか存在しない (原則 の実数の連続性, 整数の離散性を用いた). このように, 積の形を作れば, 解の範囲を絞り込むことができる. 積の形をつくる最大の目的は解の範囲を絞り込むことにある.

例 6

$xy + 3x + 2y + 5 = 0$ を満たす整数の組 (x, y) を全て求めよ. [06 東京薬大]

ヒントと略解

与式を $(x+2)(y+3) = 1$ の形に変形する (この変形方法は極めて重要である. 類題多数). したがって, $(x+2, y+3) = (1, 1), (-1, -1)$ となり, 整数の組 (x, y) が定まる.

次の問題は, 積の形に持ち込む典型例である. 左辺を因数分解, 右辺を素因数分解して因数を比較する. このような問題が京都大の大問として出題されていることに驚くが, さすがに京都大だけあって, その後の計算処理がやや面倒である. なお, 99 年に同志社大 (商) で「 $x^3 - y^3 = 98$ をみたす整数の組 (x, y) を全て求めよ」という問題が出題されていた!

演習問題 1

(1) $a^3 - b^3 = 65$ を満たす整数の組 (a, b) をすべて求めよ. [05 京都大 (前) 文]

(2) $a^3 - b^3 = 217$ を満たす整数の組 (a, b) をすべて求めよ. [05 京都大 (前) 理]

ヒントと略解

(1) $(a, b) = (4, -1), (1, -4)$

(2) $(a, b) = (9, 8), (-8, -9), (6, -1), (1, -6)$

さて, 積の形に持ち込む最大の目的は解の範囲を絞り込むことであつた. しかし積の形にできない場合もある. そんなときは不等式を利用して解の範囲を絞りこむ方法が用いられる. 特に, 与えられた方程式が対称式の場合, 文字の大小関係に着目して, 整数解の存在範囲を絞り込む方法もよく用いられる.

自然数には最小値が存在するが、最大値は存在しない(このことを「下に有界」という)。よって、自然数 n がある値 M 以下であることが示せれば、 n の候補は絞られる ($1 \leq n \leq M$)。したがって、文字の大小関係に注目して解の範囲を絞り込むには、大きい文字から順に消去していった、最初に 1 番小さい文字の範囲を決定する方法が用いられる。

次の問題が、最近、東京大で出題された。

例 7

$x + y + z = xyz$ を満たす正の整数の組 (x, y, z) で $x \leq y \leq z$ となるものを全て求めよ。

[06 東京大 (前) 文]

ヒントと略解

$x \leq y \leq z$ に注目して、 z を消去することを考える。つまり、 $x + y + z \leq z + z + z$ だから、 $xyz \leq 3z$ となり、 $xy \leq 3$ 。すなわち、 $xy = 1, 2, 3$ と定まる。このとき、 $(x, y) = (1, 1), (1, 2), (1, 3)$ と確定し、それぞれに対して z を調べる。

参考問題 1

n, a, b, c, d は 0 または正の整数であって、

$$n^2 - 6 = a^2 + b^2 + c^2 + d^2$$

$$n \geq a + b + c + d$$

$$a \geq b \geq c \geq d$$

をみたす。このような数の組 (n, a, b, c, d) をすべて求めよ。

[80 東京大 (文)]

ヒントと略解

大きい文字 a から順々に消去していった、最初に 1 番小さい文字 d の範囲を求める。

前問もそうだが、この大小関係の比較は、試行錯誤のうえに成せるものなので、実際にいろいろ試し、工夫する必要がある。

$$(n, a, b, c, d) = (4, 3, 1, 0, 0), (3, 1, 1, 1, 0).$$

注 3

もし対称式であるにも係わらず、文字に大小関係が与えられていない場合には、自分で大小関係を設

定し、最後にその設定を解除して整数解を求めること。

練習 1

$\frac{1}{l} + \frac{1}{m} + \frac{1}{n} = 1$ を満たす自然数の組 (l, m, n) は全部で何組あるか。

ヒントと略解

与式は対称式なので、 $l \leq m \leq n$ と設定しても一般性を失わない。このとき、 $\frac{1}{l} \geq \frac{1}{m} \geq \frac{1}{n}$ である。以下、前出の東大の問題と同様にして、 $l \leq m \leq n$ のとき、 $(l, m, n) = (2, 3, 6), (2, 4, 4), (3, 3, 3)$ と求まる。ここで、 (l, m, n) の大小関係をなくすと 10 組の解が存在することがわかる。

注 4

積の形に変形することができず、かつ文字に大小関係も設定できない場合には、1 つの文字について整理し、判別式を考えるという方法もある (当然ながら 2 次式の場合に限られる)。

例 8

$x^2 - 3xy + 3y^2 = 9$ を満たす $x > 0, y > 0$ の整数解を求めよ。

[06 昭和薬大]

ヒントと略解

x について整理し、 $x^2 - 3yx + (3y^2 - 9) = 0$ 。 x は実数 (整数) なので、判別式を D とすると、 $D = 9y^2 - 4(3y^2 - 9) \geq 0$ 。これより $y^2 \leq 12$ となり、 y は自然数なので、 $y = 1, 2, 3$ と定まる。このとき、それぞれに対して x を調べる。

次の京都大の問題は後期の理系の大問なので、一瞬身構えてしまうかもしれない。しかも「積の形をつくる」という原則に従おうとすると、なかなか積の形にならなくてますます焦ってくる! (ちなみに翌 02 年に愛媛大 (前) で「 $3x^2 + y^2 + 5z^2 - 2yz - 12 = 0$ をみたす整数の組 (x, y, z) をすべて求めよ。」という問題が出題された)

積の形も無理，大小比較も無理，となれば，次数が2次であることに注目して平方完成に持ち込む方法しか残らない．

演習問題 2

方程式

$$x^2 + 2y^2 + 2z^2 - 2xy - 2xz + 2yz - 5 = 0$$

をみたす正の整数の組 (x, y, z) をすべて求めよ．

[01 京都大 (後) 理]

x についての2次式とみて平方完成し， $\{x - (y + z)\}^2 + y^2 + z^2 = 5$ と変形する． $(x, y, z) = (3, 1, 2), (3, 2, 1)$ ．

さて，積の形にこだわるもう一つの理由は，次にあげる基本性質が成り立つからである．

整数問題の大原則

自然数 a, b, c, d について， a, b が互いに素であり， $ad = bc$ が成り立つとき，
 a は c の約数（つまり c は a で割り切れる）．
 b は d の約数（つまり d は b で割り切れる）．

感覚的に明らかであろう．簡単に説明すると， $d = \frac{bc}{a}$ と変形したとき，左辺は整数であるから，右辺は約分することによって整数にならざるをえないが， a と b が互いに素なので約分できないから， c が a で割り切れなければならない．

この性質は非常に重要で，整数問題ではほとんど全ての問題でこの事実を使うといっても過言ではない．なお互いに素とは最大公約数が1または共通の素因数を持たないという意味である（互いに素については後ほど詳しく解説する）．

例 9

正の整数 m, n, l が等式 $\frac{mn}{m+18} = l + \frac{1}{3}$ を満たしているとき， m は3の倍数であることを示せ．

ヒントと略解

m が主役なので，まずは m について整理する．分母を払うと m についての1次式になる．

$$\begin{aligned} \text{与式} \quad & \iff 3mn = (m+18)(3l+1) \\ & \iff (3n-3l-1)m = 2 \cdot 9(3l+1) \end{aligned}$$

このとき， $3n-3l-1$ は3で割ると2余る数なので，素因数分解したときに素因数3をもたないので，右辺の因数9と $3n-3l-1$ は互いに素なので，9は m の約数．よって m は9の倍数であり，3の倍数でもある．

ここで，最小公倍数，最大公約数の性質について確認しておこう．最小公倍数，最大公約数はその意味を簡単に小学校で学習しただけでそれ以降，本格的に扱うことはないが，以下の性質は常識として知っておいて欲しい．なお，証明は意外と難しい．

最小公倍数・最大公約数の性質

a, b の最小公倍数を L ，最大公約数を G とおくとき，次が成立する．

性質 a, b の公倍数は L の倍数である．

性質 a, b の公約数は G の約数である．

性質 $a = Ga', b = Gb'$ とおくとき，

a' と b' は互いに素である．

性質 $L = Ga'b'$ が成立する．

性質 $ab = GL$ が成立する．

練習 2

2つの正の整数 m と n の最大公約数を G ，最小公倍数を L とする．

$$\begin{cases} \log_3 L - \log_3 G = 2 + 3\log_3 2 \\ \log_2 L + \log_2 G = 7 + 4\log_2 3 \end{cases}$$

が成り立つとき， $G < m < n < L$ として， m, n を求めよ． [01 慶応大 (商)]

ヒントと略解

まずは，対数を消去する（この対数は単なる見掛け倒し）．

$\frac{L}{G} = 2^3 3^2$, $GL = 2^7 3^4$. よって $G = 12$.
 $m = pG$, $n = qG$ (p, q 互いに素) とすると,
 $L = pqG$ だから, $pq = 2^3 3^2$. $G < m < n < L$ から
 $1 < p < q < pq$ となるので, $p = 8, q = 9$. よって,
 $m = 96, n = 108$

参考問題 2

自然数 m に対して, m の相異なる素因数をすべてかけあわせたものを $f(m)$ で表すことにする. たとえば $f(72) = 6$ である. ただし $f(1) = 1$ とする. m, n を自然数, d を m, n の最大公約数とすると $f(d)f(mn) = f(m)f(n)$ となることを示せ.

[03 大阪大 (前) 文]

ヒントと略解

素因数に注目する (指数は考慮しない). m, n に現れる素因数で, 両方に共通に表れるものの積を p , m にだけ表れ n に表れない素因数の積を q , m にだけ表れ n に表れない素因数の積を r とすると,
 $f(d) = p, f(mn) = pqr, f(m) = pq, f(n) = pr$.

整数問題の大原則

1 以外の全ての自然数は, 素数の積に分解できる. そのような分解の方法は, 並べ方の順序を除いて, ただ一通りである.

… 素因数分解の一意性

素因数分解の一意性とは, 簡単にいうと, 自然数はただ一通りに素因数分解できるということである. よって, 両辺の素因数の指数の比較が可能となり, 実数の場合には解くことのできない方程式を解くことができる. なお, 素因数分解の指数は 0 以上で, この指数に注目することが重要である.

例 10

$7056 = 2^a 3^b 5^c 7^d$ をみたす整数 a, b, c, d を求めよ.

[02 群馬大 (前)]

ヒントと略解

左辺を素因数分解すると, $7056 = 2^4 3^2 7^2$ となるので, 両辺の指数を比較して, $a = 4, b = 2, c = 0, d = 2$.

例 11

p を自然数の定数とする. $2^m - 2^n = 2^p$ をみたす 0 以上の整数 m, n を求めよ.

ヒントと略解

左辺を 2^n でくくりだすと $2^n(2^{m-n} - 1) = 2^p$ となる (積の形にする!). $2^{m-n} - 1$ は奇数であることから, $2^{m-n} - 1 = 1$ になるしかなく,
 $n = p, m = p + 1$ と定まる.

練習 3

$2^m n - 2^{m-1} = 1000$ が成り立つとき, 正の整数 m, n を求めよ.

[04 甲南大 (理工)]

ヒントと略解

$2^{m-1}(2n - 1) = 2^3 5^3$ だから, $m = 4, n = 63$.

練習 4

2 つ以上の連続する整数の和は 2^k の形にはならないことを証明せよ.

[04 滋賀大 (前) 理]

a から連続する $n (\geq 2)$ 個の整数の和は,
 $\frac{n(2a + n - 1)}{2}$ である. これが 2^k になったとして矛盾を導く.

例 12

$\sqrt{2}$ が無理数であることを, 素因数分解の一意性を利用して証明せよ.

ヒントと略解

$\sqrt{2}$ が有理数だと仮定し $\sqrt{2} = \frac{n}{m}$ (m, n は互いに素) とおけば, $2m^2 = n^2$ となる. 両辺の素因数 2 の個数に着目すると, 左辺が奇数個, 右辺が偶数個なので矛盾.

素因数分解の一意性についての入試問題は次の東工大の問題が良いだろう. なお, 東工大の後期試験は毎年大問 2 問のみの出題であり, 次の問題がそのうちの 1 問であった.

参考問題 3

自然数 a, b, c が $3a = b^3, 5a = c^2$ を満たし, d^6 が a を割り切るような自然数 d は $d = 1$ に限るとする.

- (1) a は 3 と 5 で割り切れることを示せ
- (2) a の素因数は 3 と 5 以外にないことを示せ.
- (3) a を求めよ. [06 東工大 (後)]

ヒントと略解

「 d^6 が a を割り切るような自然数 d は $d = 1$ に限る」とは何を意味しているのか正しく解釈できるだろうか. (3) の答えは $a = 1125$.

最後に $+\alpha$ として, 整数問題で最も基本かつ重要な原則を述べておく.

整数問題の原則 $+\alpha$

整数問題では, まずは具体例を考えること. とにかく, 具体的にいろんな数を当てはめて実験する. そうすれば必ず, 規則性や法則が見えてくるはず. 式変形だけでは無理である.

整数問題に限らず, 見たこともないような問題に出会ったらどう対応すればよいのか. それは, まず具体例を考えることである. 特に整数問題では, この作業がとても大切である. とにかく数字を当てはめて実験 (計算) し, 規則性や法則を予想することである. しかし, 単に予想しただけでは数学にならないので, 最後に証明が必要である. 証明がわからなかったら, まずは具体例を証明してみよう. その証明方法を一般的な場合に拡張すればよいのだ.

「具体例で実験」
⇒「法則を予想」
⇒「証明」

という流れをつねに意識しておこう.

例 13

2 以上の自然数 n に対し, n と $n^2 + 2$ がともに素数になるのは $n = 3$ の場合に限ることを示せ.

[06 京大 (前) 理]

ヒントと略解

$n = 2, 3, 4, 5, \dots$ と 10 くらいまで実験すれば規則性が見えてくる. というか, そういう手段をとらないと, この問題は解けない. (この問題は後ほど取り上げる).

例 14

$\frac{2^n}{n} > n$ をみたす自然数 n の範囲を求めよ.

[79 京大 文]

ヒントと略解

この不等式を解こうとしても無理である. やはり, $n = 1, 2, 3, 4, 5, \dots$ と実験して, 適する n の範囲を予測し, その後, 証明するという方法をとる.

3 整数問題の攻略 (基礎編)

3.1 余りで分類する

すべての整数は n で割ったときの余りによって n 通りに分類される.

たとえば, 5 で割った余りが 0, 1, 2, 3, 4 のいずれであるかによって, 全整数は 5 通りに分類され, その各グループに含まれる数を k を整数として,

$$5k, 5k+1, 5k+2, 5k+3, 5k+4$$

と表す (場合によっては, $5k, 5k \pm 1, 5k \pm 2$ とすることもある. この方が計算が楽になることが多い). 全ての整数は, この 5 つのグループのいずれか 1 つに必ず属する. この考え方は, 無限個ある整数をグループ分けし, そのグループに属する数をまとめて扱う, という点において非常に重要な考え方である.

「すべての整数について ~であることを証明せよ」という問題では, 整数をある整数で割った余りで分類して考えることが多い. どの整数で割った余りで分類するかは, 問題に応じて考えるしかない. また「素数を求めよ」という問題でも, 余りによる分類は威力を発揮する (このことは次章で詳しく説明する).

ここで、合同式という新しい考え方を紹介しよう。高等学校では学習しないが、知っているとは大変便利な考え方である（この新しい考え方に馴染めない人は、ここからしばらくを読み飛ばしても構わない。ここから例 18 にスキップせよ）。

上の例で、5 で割った分類について、たとえば、6 と 11 は異なる整数であるが、共に 5 で割った余りは 1 に等しいので、同じグループに属する。このことを

$$6 \equiv 11 \pmod{5}$$

と表記し、6 と 11 は 5 を法として合同であるという。

一般に、ある 2 つの整数 a, b を自然数 m で割った余りが等しいとき、 a, b は m を法として合同であるといい、

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

と表す。この式のことを合同式という。

例 15

$$10 \equiv 3 \pmod{7}, \quad 4 \equiv -1 \pmod{5}$$

2 つの整数 a, b を自然数 m で割った余りが等しいとき、 $a - b$ は m で割り切れるから（ $\because a = mq_1 + r, b = mq_2 + r$ と表すと、 $a - b = m(q_1 - q_2)$ となるから）、合同式は次のように定義できる。

合同式の定義

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

$$\iff a, b \text{ を } m \text{ で割った余りが等しい}$$

$$\iff a - b \text{ が } m \text{ で割り切れる}$$

$a - b$ が m で割り切れるとき、 $a - b$ を m で割った余りが 0 だから、合同式で書き表すと

$$a - b \equiv 0 \pmod{m}$$

となる。この式は、始めの合同式の右辺を左辺に移項したに過ぎない。このように、合同式では普通の等式に似た式変形が可能である。

合同式の重要性質

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

$$\implies a + c \equiv b + d \pmod{m}$$

$$a - c \equiv b - d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

証明は「 $a \equiv b \pmod{m} \iff a - b$ が m の倍数である」により簡単に証明できる。3 番目の性質だけ証明しておく。

証明

$a \equiv b \pmod{m}$ より、 $a - b$ は m で割り切れるので、 $a - b = m\alpha$ とおける。同様に、 $c \equiv d \pmod{m}$ より $c - d = m\beta$ となる。このとき、 $ac = (b + m\alpha)(d + m\beta) = bd + m(d\alpha + b\beta + m\alpha\beta)$ 。つまり $ac - bd$ は m で割り切れる。よって $ac \equiv bd \pmod{m}$ が成立する。

終

また次の公式も成り立つ。

合同式の重要性質

$$a \equiv b \pmod{m} \implies a^n \equiv b^n \pmod{m}$$

つまり、合同式の記号 (\equiv) は割り算以外は通常の等号 ($=$) と全く同じである。

合同式の性質 (まとめ)

加法、減法、乗法については、合同式は等式と同様に扱ってよい。除法だけは合同式では使えない。

例 16

2007²⁰⁰⁷ を 17 で割った余りを求めよ。

ヒントと略解

$2007 = 17 \times 118 + 1$ だから $2007 \equiv 1 \pmod{17}$.
したがって、 $2007^{2007} \equiv 1^{2007} \equiv 1 \pmod{17}$.

なお、合同式を用いないなら、 $2007^{2007} = (17 \times 118 + 1)^{2007}$ の二項展開を考える．二項展開については後ほど説明する．

例 17

n を自然数とすると、 $3^{n+2} + 4^{2n+1}$ は 13 で割り切れるを示せ．

ヒントと略解

$$\begin{aligned} 3^{n+2} + 4^{2n+1} &\equiv 3^n \cdot 3^2 + 4^{2n} \cdot 4^1 \pmod{13} \\ &\equiv 9 \cdot 3^n + 4 \cdot 16^n \pmod{13} \\ &\equiv 9 \cdot 3^n + 4 \cdot 3^n \pmod{13} \\ &\equiv 13 \cdot 3^n \pmod{13} \\ &\equiv 0 \pmod{13} \end{aligned}$$

なお、 n が自然数だから、合同式を用いないなら、数学的帰納法による証明を行う．

次のような面白い問題が実際に出題されている．

練習 5

今日は金曜日です．以下の問いに答えなさい．

- (1) 10^6 日後は何曜日ですか．
- (2) 10^{100} 日後は何曜日ですか．
- (3) 3^{100} 日後は何曜日ですか．[00 熊本県立大 (前)]

ヒントと略解

曜日は 7 日周期であるから、7 で割った余りに注目すればよい． $10^6 \equiv 3^6 \equiv 9^3 \equiv 2^3 \equiv 1 \pmod{7}$.
などと計算する．

合同式の扱いに慣れたらどうか．それでは、この章のタイトルでもあった余りで分類する問題を考えよう．

まずは、次の問題を考えてみよう．

例 18

n^2 が 5 の倍数ならば、 n は 5 の倍数であることを証明せよ．

ヒントと略解

まずは、対偶をとる．すなわち、「 n が 5 の倍数でないならば、 n^2 は 5 の倍数でない」ことを証明する．整数 n を 5 で割った余りで分類して考える．

合同式を利用しない解答

$n = 5k \pm 1, 5k \pm 2$ とおく ($n = 5k + 1, 5k + 2, 5k + 3, 5k + 4$ においても同じであるが、計算が少なくてすむ) .

$n = 5k \pm 1$ のとき、

$$n^2 = (5k \pm 1)^2 = 5(5k^2 \pm 2k) + 1$$

$n = 5k \pm 2$ のとき、

$$n^2 = (5k \pm 2)^2 = 5(5k^2 \pm 4k) + 4$$

したがって、いずれの場合も 5 の倍数にならない．

合同式を利用した解答

合同式を用いる場合も、 $n \equiv 1, 2, 3, 4 \pmod{5}$ と設定するよりも、 $n \equiv \pm 1, \pm 2 \pmod{5}$ と設定したほうが、計算は少ない．

$n \equiv \pm 1 \pmod{5}$ のとき、

$$n^2 \equiv (\pm 1)^2 \equiv 1 \pmod{5}$$

$n \equiv \pm 2 \pmod{5}$ のとき、

$$n^2 \equiv (\pm 2)^2 \equiv 4 \pmod{5}$$

したがって、いずれの場合の $n \not\equiv 0 \pmod{5}$ である．

注 5

$n = 5k \pm 1, 5k \pm 2$ とおいた最初の方法では、展開したときに $5k$ が関係している項は明らかに 5 で割り切れるので余りには影響しないこと、つまり、余りに関与するのは、定数部分 $(\pm 1)^2, (\pm 2)^2$ であることに気付くだろう．この定数部分にだけ着目した解答が 2 番目の合同式を用いた解答である．

上の例からもわかるように、合同式は、余りで分類する問題において、計算の簡略化、答案のスリム化に有効であるが、言い換えれば、ただそれだけの

ことであり，合同式など使わずに，従来の分類方法でも全く問題はない．

しかし，やはり使えたほうが便利だと思うし，時間も大幅に短縮できると思うので（特に指数型の問題で威力を発揮する．本章最後に紹介する），以下の問題では，合同式を用いない解答と合同式を用いた解答の２種類を並列することにする．合同式の扱いに慣れない人は，合同式を用いた解答は無視しても構わない．

例 19

任意の整数 n に対し， $n^3 + 2n$ は 3 の倍数であることを示せ．

ヒントと略解

全ての整数を順番に調べるわけにはいけないので，整数を分類して調べる．どの整数で割った余りで分類するかというと，問題文に「3 の倍数であることを示せ」とあるので，3 で割った余りで分類するのがよい．

m を整数として， $n = 3m$ ， $3m \pm 1$ として与式に代入して 3 の倍数であることを確認する．

$n = 3m$ のとき，

$$n^3 + 2n = (3m)^3 + 2(3m) = 3(9m^2 + 2m)$$

$n = 3m \pm 1$ のとき，

$$\begin{aligned} n^3 + 2n &= (3m \pm 1)^3 + 2(3m \pm 1) \\ &= 3(9m^3 \pm 9m^2 + 5m \pm 1) \end{aligned}$$

合同式を利用した解答

$n \equiv 0 \pmod{3}$ のとき，

$$n^3 + 2n \equiv 0^3 + 2 \cdot 0 \equiv 0 \pmod{3}$$

$n \equiv \pm 1 \pmod{3}$ のとき，

$$\begin{aligned} n^3 + 2n &\equiv (\pm 1)^3 + 2(\pm 1) \\ &\equiv \pm 3 \equiv 0 \pmod{3} \end{aligned}$$

なお，この問題は，次のように式変形でも解くことができる．

$$\begin{aligned} n^3 + 2n &= n^3 - n + 3n \\ &= n(n^2 - 1) + 3n \\ &= n(n+1)(n-1) + 3n \end{aligned}$$

$n(n+1)(n-1)$ は連続 3 整数の積なので 6 の倍数（つまり 3 の倍数）．よって， $n^3 + 2n$ は 3 の倍数．

ここで，非常に重要な倍数約数に関する性質を紹介しよう．

倍数の重要性質

p, q を互いに素な自然数とするととき，
 n が pq の倍数

$$\iff n \text{ が } p \text{ の倍数かつ } q \text{ の倍数}$$

感覚的に明らかであろう．例えば，12 の倍数は 3 の倍数かつ 4 の倍数であり，15 の倍数は 3 の倍数かつ 5 の倍数である．これは，大きな数の倍数であるかどうかを判定するときに利用される．

合同式で表現すれば，次のようになる．

倍数の重要性質

p, q を互いに素な自然数とするととき，
 $n \equiv 0 \pmod{pq}$

$$\iff n \equiv 0 \pmod{p} \text{ かつ } n \equiv 0 \pmod{q}$$

注 6

p, q を互いに素な自然数とするととき，

$$n \equiv a \pmod{pq}$$

$$\iff n \equiv a \pmod{p} \text{ かつ } n \equiv a \pmod{q}$$

も成立する．余りが全て同じであることに注意せよ．

練習 6

n を整数とするととき， $2n^3 - 3n^2 + n$ は 6 の倍数であることを示せ．

ヒントと略解

6 の倍数であることの証明だからといって，6 で分類する必要はない（分類してもできるが）．「6 の倍数 = 2 の倍数かつ 3 の倍数」に着目すれば，与式が 2 の倍数になること，3 の倍数にもなることの両方が（別々に）示せれば OK． $2n^3 - 3n^2 + n = n(n-1)(2n-1)$ になるので，連続 2 整数の積を含むから，2 の倍数になるのは明らか．

注 7

上の問題で因数分解した形 $n(n-1)(2n-1)$ を見て、なにか感じないだろうか。じつは、

$$\sum_{k=1}^{n-1} k^2 = \frac{(n-1)n(2n-1)}{6}$$

であるので、左辺は整数の和だから明らかに整数。よって $n(n-1)(2n-1)$ が 6 の倍数になるのも当然。

しかし、もとの問題は「 n が整数のとき」であり、この方法は「 n が自然数のとき」に考えられることだから、そのまま適用はできないが、興味深いことではある。

練習 7

すべての自然数 n に対して、

$$\frac{n^5}{15} + \frac{n^4}{6} + \frac{n^3}{3} + \frac{n^2}{3} + \frac{n}{10}$$

が自然数になることを示せ。[01 宮城大]

ヒントと略解

まずは、通分して分子を因数分解せよ。

驚くべきことに、京都大で次の問題が大問で出題された。9 で割り切れることの証明だからといって 9 で割った余りで分類するだろうか？

演習問題 3

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。[01 京都大(前)文]

ヒントと略解

因数分解して積の形をつくる。

特に、次に紹介する平方数 n^2 を 4 または 3 で割った余りの分類は非常に重要で、このことをテーマにした入試問題は数多い。滋賀大(00 前)、千葉大(01 前)、富山県立大(03 前)、関西学院大(02)

平方数の分類(その 1)

平方数 n^2 を 4 で割った余りは 0 または 1 である。つまり、

n が偶数のとき、 n^2 を 4 で割ると余り 0

n が奇数のとき、 n^2 を 4 で割ると余り 1

である。また、

n が奇数のとき、 n^2 を 8 で割ると余り 1

である。

合同式を用いて表現すれば、

平方数の分類(その 2)

n が偶数のとき、 $n^2 \equiv 0 \pmod{4}$

n が奇数のとき、 $n^2 \equiv 1 \pmod{4}$

n が奇数のとき、 $n^2 \equiv 1 \pmod{8}$

証明

n が偶数のとき、 $n = 2m$ とおくと、 $n^2 = (2m)^2 = 4m^2$ となり、4 で割り切れる。

n が奇数のとき、 $n = 2m + 1$ とおくと、 $n^2 = (2m + 1)^2 = 4m^2 + 4m + 1$ となり、4 で割ると 1 余る。またこのとき、 $m(m+1)$ は連続 2 整数の積なので偶数であるから、 $4m(m+1)$ は 8 の倍数である。よって、 $4m(m+1) + 1$ は 8 で割ると 1 余る。

終

平方数の分類(その 3)

平方数 n^2 を 3 で割った余りは、0 または 1 である。つまり、

n が 3 の倍数のとき、

n^2 を 3 で割ると余り 0

n が 3 の倍数でないとき、

n^2 を 3 で割ると余り 1

である。

合同式を用いて表現すれば、

平方数の分類 (その)

$$n \equiv 0 \pmod{3} \text{ のとき } , n^2 \equiv 0 \pmod{3}$$

$$n \equiv 1 \pmod{3} \text{ のとき } , n^2 \equiv 1 \pmod{3}$$

$$n \equiv 2 \pmod{3} \text{ のとき } , n^2 \equiv 1 \pmod{3}$$

練習 8

平方数の分類 (その) を証明せよ .

例 20

m, n を整数とするととき ,

$$m^2 = 4n + 2 \implies \text{矛盾}$$

$$m^2 = 3n + 2 \implies \text{矛盾}$$

例 21

n が 3 の倍数でない奇数のとき , n^2 を 12 で割った余りを求めよ .

ヒントと略解

12 で割った余りを考えるからといって , 12 で分類する必要はない (何の数で分類するかを本能的にかぎわける能力も必要) . この場合は , n が 3 の倍数でない奇数であることから , 6 でわった余りで分類する . つまり $n = 6m + 1, 6m + 5$ とおく . このとき n^2 に代入して計算すれば 12 で割った余りはすぐに確認できる .

しかし , 平方数の分類に注目し , 次のようにも考えることができる .

合同式を利用した解答

n が 3 の倍数でないので , 平方数の分類 より $n^2 \equiv 1 \pmod{3}$. さらに n が奇数だから , 同じく平方数の分類 より $n^2 \equiv 1 \pmod{4}$. したがって , $n^2 \equiv 1 \pmod{3}$ かつ $n^2 \equiv 1 \pmod{4}$ だから $n^2 \equiv 1 \pmod{12}$. つまり , n^2 を 12 で割った余りは 1 である .

練習 9

n は正の整数で , 2 でも 3 でも割り切れないとする . このとき , $n^2 - 1$ は 24 で割り切れることを示せ . [02 東京女大 (文理)]

ヒントと略解

前問と同様 , 24 で分類するはずもなく , 「2 でも 3 でも割り切れない」とあるので 6 による分類を行う . つまり , n が 2 でも 3 でも割り切れない $\iff n = 6m + 1, 6m + 5$ とおける . しかし , 前問のように , $n^2 - 1$ に代入してすぐに 24 の倍数であるかどうかはわからない . 前問でうまくいったのは単なる偶然である . これが数学の面白いところでもある . この問題では偶奇性を考える必要がある . 次章偶奇性で再び取り上げることにしよう .

しかし , この問題も平方数の分類に注目し , 合同式で考えると次のように極めて単純に結果がでる .

合同式を利用した解答

n が 3 の倍数でないので , 平方数の分類 より $n^2 \equiv 1 \pmod{3}$. さらに n が奇数だから , 同じく平方数の分類 より $n^2 \equiv 1 \pmod{8}$. したがって , $n^2 \equiv 1 \pmod{3}$ かつ $n^2 \equiv 1 \pmod{8}$ だから $n^2 \equiv 1 \pmod{24}$. よって $n^2 - 1$ は 24 で割り切れる .

それでは , 平方数の分類に関する重要な問題を紹介しよう .

練習 10

a, b, c はどの 2 つも 1 以外の共通な約数をもたない正の整数とする . a, b, c が , $a^2 + b^2 = c^2$ をみたしているとき , 次の問いに答えよ .

- (1) c は奇数であることを証明せよ .
- (2) a, b のうち , 1 つは 3 の倍数であることを証明せよ .
- (3) a, b のうち , 1 つは 4 の倍数であることを証明せよ . [04 旭川医大 (後)]

ヒントと略解

- (1) a, b, c はどの 2 つも 1 以外の共通な約数をもたない正の整数だから a, b が共に偶数にな

ることではない。

(2) a, b のうち「2 つとも 3 の倍数」「2 つとも 3 の倍数でない」、それぞれの場合に矛盾が生じることを示せば良い。

(3) a, b のうち「2 つとも 4 の倍数」「2 つとも 4 の倍数でない」、それぞれの場合に矛盾が生じることを示せば良い。

いずれも、合同式を利用すればスマートな解答になる。

演習問題 4

n, a, b を 0 以上の整数とする。 a, b を未知数とする方程式

$$(*) \quad a^2 + b^2 = 2^n$$

を考える。

(1) $n \geq 2$ とする。 a, b が方程式 (*) を満たすならば、 a, b はともに偶数であることを証明せよ (ただし 0 は偶数に含める)。

(2) 0 以上の整数 n に対して、方程式 (*) を満たす 0 以上の整数の組 (a, b) をすべて求めよ。

[04 京都大 (前) 文]

ヒントと略解

(1) a, b が「共に奇数」「1 つが奇数で他方が偶数」の場合に矛盾生じることを示す。合同式を利用すればスマートな解答になる。

(2) a, b が共に偶数だから、 $a^2 + b^2 = 2^n$ の両辺は 2 で何回か割れるはず。

一橋大学から類題を一つ出しておく。文字が 4 つに増えてはいるが全く同じである。ちなみにこの問題と全く同じ問題が横浜国大 (00 前) で出題されている。

参考問題 4

整数 a, b, c, d が等式 $a^2 + b^2 + c^2 = d^2$ をみたすとする。

(1) d が 3 の倍数でないならば、 a, b, c の中に 3 の倍数がちょうど 2 つあることを示せ。

(2) d が 2 の倍数でも 3 の倍数でもないならば、 a, b, c のうち少なくとも 1 つは 6 の倍数であることを示せ。 [94 一橋大 (後)]

ヒントと略解

(1) d が 3 の倍数でないことから、 $d = 3k \pm 1$ とおいて、直接 2 個であることを証明するか、背理法的に a, b, c の中に 3 の倍数が 0 個、1 個、3 個ある場合に矛盾が生じることを示すか。

(2) (1) 同様、 d が 2 の倍数でも 3 の倍数でもないから、 $d = 6k \pm 1$ とおいて、直接証明するか、「少なくとも」とあるので背理法を用いるか。

本問も合同式を利用すれば、スマートな解答になるう。

これまで、 n^2 や n^3 などの形ばかり扱ってきた。

では 2^n や 3^n などのように、 n が指数の場合には、どのようにすればよいのだろうか。

一般に、 n^2 や n^3 の場合は n として全ての整数をとることが多いのに対し、 2^n や 3^n などの指数型の場合には、 n として自然数をとることが多い (n が負の整数になると整数問題でなくなる!) したがって、数学的帰納法による証明も考えれるが、ここでは整数問題としての手法を紹介する。

それには、次の因数分解の公式が重要な役割を果たす。

重要公式

公式 n を自然数とするとき、

$$\begin{aligned} & a^n - b^n \\ &= (a - b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + a^2b^{n-3} + ab^{n-2} + b^{n-1}) \end{aligned}$$

公式 n が奇数のとき、

$$\begin{aligned} & a^n + b^n \\ &= (a + b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 + \cdots + a^2b^{n-3} - ab^{n-2} + b^{n-1}) \end{aligned}$$

この因数分解は指数の形の式を「積の形に変形する」ことができるという点で大変重要である。 $a^n - b^n$ は全ての自然数 n で $a - b$ を因数にもち、 $a^n + b^n$ は n が奇数のときだけ $a + b$ を因数にもつことに注意しよう。

次の問題は、 m, n に適当に数を代入して規則性を見つける解答もあるが（できなくはないがかなり面倒）、上の因数分解が頭にあると簡単にわかるだろう。

演習問題 5

m, n は自然数で、 $m < n$ をみたすものとする。 $m^n + 1, n^m + 1$ がともに 10 の倍数となる m, n を 1 組与えよ。 [96 京都大 (後) 理]

例 22

全ての自然数 n に対して、 $10^n - (-1)^n$ は 11 で割り切れることを示せ。 [01 津田塾大 (英文)]

ヒントと略解

上の因数分解の公式 で $a = 10, b = -1$ とすれば、

$$\begin{aligned} 10^n - (-1)^n &= (10 + (-1))(10^{n-1} + \cdots + (-1)^{n-1}) \\ &= 11(10^{n-1} + \cdots + (-1)^{n-1}) \end{aligned}$$

となり、11 の倍数になることがわかる。

実は、合同式がその威力を発揮するのは、このような問題である。

合同式を利用した解答

$-1 \equiv 10 \pmod{11}$ だから、 $10^n - (-1)^n \equiv 10^n - 10^n \equiv 0 \pmod{11}$ 。

練習 11

2^n を 7 で割ったときの余りが 1 であることの必要十分条件は、 n が 3 の倍数であることを示せ。

[01 岡山県立大 (中期)]

ヒントと略解

「 n が 3 の倍数 $\implies 2^n$ を 7 で割ったときの余りが 1」の証明。

$n = 3k$ とおくと、 $2^n = 2^{3k} = 8^k$ となる。 $8^k = (7 + 1)^k$ とみて二項展開すれば、7 で割った余りが 1 になることがわかる。

「 2^n を 7 で割ったときの余りが 1 $\implies n$ が 3 の倍数」の証明。

対偶を証明する。 $n = 3k \pm 1$ のとき、 2^n を 7 で割ったときの余りが 1 でないことを示す。

練習 12

(1) すべての自然数 n に対して $4^n - 1$ が 3 で割り切れることを示せ。

(2) $2^n + 1$ が 3 で割り切れるような自然数 n の満たすべき条件を求めよ。 [05 同志社大 (法・工)]

ヒントと略解

(1) $4^n - 1 = 4^n - 1^n$ となるので、前問と同様に、公式 で $a = 4, b = 1$ とすれば、

$$\begin{aligned} 4^n - 1^n &= (4 - 1)(4^{n-1} + \cdots + 1^{n-1}) \\ &= 3(4^{n-1} + \cdots + 1^{n-1}) \end{aligned}$$

となり、3 の倍数になることがわかる。

(2) とりあえず実験してみれば、 n が奇数のときに 3 で割り切れることが予測できよう。あとは $n = 2m$ のとき 3 の倍数にならないこと、 $n = 2m + 1$ のとき、3 の倍数になることを示せばよい。(1) の結果を利用する。

この問題でも合同式がその威力を発揮する。

合同式を利用した解答

(1) $4 \equiv 1 \pmod{3}$ だから、 $4^n - 1 \equiv 1^n - 1 \equiv 0 \pmod{3}$ 。よって 3 の倍数になる。

(1) $2 \equiv -1 \pmod{3}$ だから、 $2^n + 1 \equiv (-1)^n + 1 \pmod{3}$ 。したがって $(-1)^n + 1 \equiv 0 \pmod{3}$ になるための条件は、 n が奇数であること。

例 23

2^n を 3 で割った余りを求めよ。

ヒントと略解

$n = 1, 2, 3, \dots$ と調べていけば, 3 で割った余りがどうなるか予想は立つと思う. この予想を実際に証明するには二項定理を用いて展開する.

二項定理

$$(a+b)^n = \sum_{k=0}^n {}_nC_k a^{n-k} b^k$$

$$\begin{aligned} 2^n &= (3-1)^n \\ &= \sum_{k=0}^n {}_nC_k 3^{n-k} (-1)^k \\ &= 3^n + 3^{n-1}(-1) + \dots + 3(-1)^n + (-1)^n \\ &= (3 \text{ の倍数}) + (-1)^n \end{aligned}$$

したがって, n が偶数のとき余り 1, n が奇数のとき余り -1 , つまり余り 2 であることがわかる.

この問題でも合同式は便利である.

合同式を利用した解答

$2 \equiv -1 \pmod{3}$ だから, $2^n \equiv (-1)^n \pmod{3}$.
したがって, 2^n を 3 で割った余りは $(-1)^n$ を 3 で割った余りに等しい. 以下同様.

練習 13

- (1) 正の整数 n で $n^3 + 1$ が 3 で割り切れるものを全て求めよ.
- (2) 正の整数 n で $n^n + 1$ が 3 で割り切れるものを全て求めよ. [03 一橋大 (前)]

ヒントと略解

(1) は n を 3 で分類すればよい. 合同式を用いると早い.

(2) はとりあえず n を 3 で分類して考えるが, 3 の倍数は何乗しても 3 の倍数であり, 3 で割って 1 余る数は何乗しても 3 で割って 1 余るのに対し (このことは二項展開で確認する必要あり), 3 で割って 2 余る数を 3 で割ったときの余りは一定ではない. 3 で割って 2 余る数をさらに分類する必要がある. 先程の例がヒントになっている.

本問は, 合同式を用いない場合は, 二項定理による展開が必要であるが, 合同式を用いると, そのわずらわしさが無い.

上の一橋大の問題で, **ヒントと略解** に述べたことがそのまま出題された.

参考問題 5

n を自然数とする. 以下の問いに答えよ.

- (1) n を 3 で割った余りが 1 ならば, すべての自然数 m に対して n^m を 3 で割った余りは 1 であることを示せ.
- (2) n を 3 で割った余りが 2 ならば, すべての奇数 m に対して n^m を 3 で割った余りは 2 であることを示せ.
- (3) n^m を 3 で割った余りが 2 となる自然数 m があれば, n を 3 で割った余りも 2 であることを示せ. [07 お茶の水女大 (前) 理]

参考問題 6

自然数 n に対し, $S_n = 1^n + 2^n + 3^n + 4^n$ とおく. このとき,

- (1) S_n が 6 の倍数であるための条件を求めよ.
- (2) S_n が 12 の倍数にならないことを示せ.

[00 奈良県立医大 (前)]

本章のまとめ

n^2 や n^3 などの整式型の問題では, あえて合同式を用いなくても, 余りでの分類や, 連続整数の積の倍数性を用いれば解けるが, 2^n や 3^n などの指数型の問題では, 合同式は効果的な役割を果たす. 合同式を用いないならば, 二項展開や複雑な因数分解などを用いなければならない. なお, 指数型の場合, n は自然数であるので, 数学的帰納法による証明もできる.

本章で扱った手法はとても大切であり, この後の章でも必携であるので, しっかりと理解し, 使えるようになって欲しい.

3.2 素数 p の性質

素数をテーマにした入試問題も数多く見られるが、「素数の問題は難しい」と先入観を持っている人は少なくない。確かに、素数に関する本格的な問題は非常に難しく、世界中のプロの数学者の頭脳を結集しても歯が立たない状況にある。だから、高校生を対象にした大学入試で扱う程度の素数の問題は、そんなに高級な手段を用いなくても解けるようになっているわけで、恐れる必要は全くない。

大学入試における素数の問題では、次にあげる性質を知っているだけで十分であろう。素数の性質をまとめておく。

素数 p の性質

p を素数とすると、次の性質が成り立つ。

性質 ab が p で割り切れる

\Rightarrow 「 a が p で割り切れる」

or 「 b が p で割り切れる」

性質 $p = ab$

$\Rightarrow (a, b) = (1, p) \text{ or } (p, 1)$

性質 p は a ($1 \leq a \leq p-1$) と互いに素

性質 p は $(p-1)!$ と互いに素

例 24

n を 2 以上の自然数とすると、 $n^4 + 4$ は素数にはならないことを示せ。 [04 宮崎大 (前)]

ヒントと略解

「素数にならない = 合成数である」ことから積の形に変形できれば完了。実際、

$$\begin{aligned} n^4 + 4 &= (n^2 + 2)^2 - 4n^2 \\ &= (n^2 - 2n + 2)(n^2 + 2n + 2) \end{aligned}$$

と因数分解できる。

練習 14

$n^4 + n^2 + 1$ が素数になるような自然数 n を全て求めよ。 [06 玉川大 (工)]

ヒントと略解

複 2 次式の因数分解を思い出そう。

千葉大 (後) で素数に関する問題が続けて出題された。いずれも問題も「積の形をつくる」がポイントである。

練習 15

自然数 x, y を用いて、 $p^2 = x^3 + y^3$ と表されるような素数 p を全て求めよ。また、このときの x, y をすべて求めよ。 [01 千葉大 (後) 理]

ヒントと略解

$x^3 + y^3 = (x + y)(x^2 - xy + y^2) = p^2$ であるので、様々な素因数の組合せが考えられる。一つ一つ検証していくしかない。 x, y に関して対称式だから、始めに $x \leq y$ と設定しても一般性を失うことはない。

練習 16

a, b は 2 以上の整数とする。

(1) $a^b - 1$ が素数ならば、 $a = 2$ であり、 b は素数であることを証明せよ。

(2) $a^b + 1$ が素数ならば、 $b = 2^c$ (c は整数) と表せることを証明せよ。 [07 千葉大 (後) 理]

ヒントと略解

$x^n - y^n, x^n + y^n$ の因数分解の公式を利用せよ。

例 25

p を素数とすると、 $n = p! + 1$ は p 以下の素数では割り切れないことを示せ。 [00 成城大 (経)]

ヒントと略解

有名問題。 p 以下の素数で実際に割ってみれば良い。

注 8

上の例は $p! + 1$ が「 p 以下の素数では割り切れない、 p より大きい数」であることを主張するもので、

このことを用いて、ユークリッドは『原論』の中で、素数が無限に存在することの証明を述べている。興味のある人はユークリッドの証明を考えてみよう。

また「～をみたす素数 p を求めよ」という問題もある。先程も述べたように素数を見つけることはプロの数学者でも困難なことである。だから、高校生が入試問題で素数を求めることができるのは、かなり特別な場合であり、まずは

「実験して規則性を予想」 \Rightarrow 「証明」

という流れが基本である。

「証明」の方法は、その規則性によるが、整数の余りによる分類(または合同式)、数学的帰納法を利用する場合が多い。

例 26

n を自然数とする。 $n, n+2, n+4$ がいずれも素数であるのは $n=3$ の場合だけであることを示せ。

[04 早大(政経)]

ヒントと略解

とりあえず、 n を 3 で割った余りで分類すれば。

注 9

例 4 で紹介したように、差が 2 であるような素数の組を双子素数とよぶ。これに対して、上記の早稲田大の問題は、さしあたって『三つ子素数』とでも言うならば、 $n > 3$ の範囲には三つ子素数は存在しないことを主張している。例 2 の結果を用いれば、 $n > 3$ の範囲の双子素数の間の数は 6 の倍数であるので、 $n > 3$ の範囲に『三つ子素数』が存在しないことは明らかである($n \sim n+4$ の中に 6 の倍数が 2 個存在することになる！)。

この早稲田大の問題の類題が京大で出題された。

演習問題 6

2 以上の自然数 n に対し、 n と $n^2 + 2$ がともに素数になるのは $n=3$ の場合に限ることを示せ。

[06 京都大(前) 理]

ヒントと略解

いろいろな n で試せば、規則性がわかると思う。 n^2 があるので、平方数の 3 で割った余りの分類が頭にあれば、方針はすぐに立つと思う。

また、前年には、一橋大でも同様の問題が出題されている。

参考問題 7

- (1) $p, 2p+1, 4p+1$ がいずれも素数であるような p をすべて求めよ。
- (2) $q, 2q+1, 4q-1, 6q-1, 8q+1$ がいずれも素数であるような q をすべて求めよ。

[05 一橋大(後)]

ヒントと略解

前問の京都大の問題同様に、まずは実験してみて規則性を発見せねばならない。何の数で割った余りで分類すればよいのか。

また、次のような問題も過去には出題されたが、見た目の複雑さに動じてはいけない。ここでもやはり、「実験して規則性を予想」 \Rightarrow 「証明」証明方法としては、数学的帰納法か合同式を利用する。

参考問題 8

整数 $19^n + (-1)^{n-1}2^{4n-3}$ ($n=1, 2, 3, \dots$) のすべてを割り切る素数を求めよ。 [86 東工大]

ヒントと略解

全てを割り切る素数は実験すれば見当がつく。あとは証明だが、数学的帰納法または合同式を利用すればよい。

3.3 偶奇性・周期性

この章では、整数問題を解くときに重要な考え方である「偶奇性」と「周期性」について説明する。

3.3.1 偶奇性

整数の問題を考えると、その数の偶奇性（その数が偶数なのか奇数なのか）があらかじめわかっていると、かなり手間が省けて都合が良い。いきなり問題を解き始める前に、その数の偶奇性がどうなっているのか、まず考えること。

偶奇性が判定できるのは、次のように和、差、積の偶奇がわかる場合がほとんどである。

整数の偶奇性

2つの整数 m, n について次の偶奇性が成り立つ。

$m + n$ が偶数 $\iff m, n$ の偶奇は一致する
 $m - n$ が偶数 $\iff m, n$ の偶奇は一致する
 $m + n$ が奇数 $\iff m, n$ の偶奇は一致しない
 $m - n$ が奇数 $\iff m, n$ の偶奇は一致しない
 mn が奇数 $\iff m, n$ は共に奇数

例 27

各辺の長さが整数となる直角三角形がある。この直角三角形の内接円の半径は整数であることを示せ。 [02 お茶の水女大 (後) 理数]

ヒントと略解

$A=90^\circ$ とすると、 $a^2 = b^2 + c^2$ となり、このとき内接円の半径 r は

$$r = \frac{b + c - a}{2}$$

となる。 $a^2 = b^2 + c^2$ より、 $(b+c)^2 - a^2 = 2bc =$ 偶数であるから、 $b+c$ と a の偶奇性は一致する（つまり、 $b+c$ と a は共に偶数か共に奇数）。よって、 $b+c-a$ は必ず偶数になるので、 r は整数である。

練習 17

a, b を整数とし、2次方程式 $x^2 + ax + b = 0$ を考える。この方程式の判別式 D が平方数ならであるならば、解は全て整数であることを示せ。

[06 津田塾大 (数)]

ヒントと略解

$D = a^2 - 4b = m^2$ とおけば、解は $x = \frac{-a \pm \sqrt{D}}{2} = \frac{-a \pm m}{2}$ 。これが整数になるには、 a, m の偶奇性はどうなればよいのかを考えよ。積の形に変形して $(a+m)(a-m) = 4b$ から方針はたつ。

次の問題は前章で取り上げた問題である。偶奇性を利用した解答を紹介する。

練習 18

n は正の整数で、2でも3でも割り切れないとする。このとき、 $n^2 - 1$ は24で割り切れることを示せ。 [02 東京女大 (文理)]

ヒントと略解

「2でも3でも割り切れない」とあるので6による分類を行う。つまり、 n が2でも3でも割り切れない $\iff n = 6m + 1, 6m + 5$ とおける。

$n = 6m + 1$ のとき、

$$\begin{aligned}
 n^2 - 1 &= (n+1)(n-1) \\
 &= (6m+2)6m \\
 &= 12m(3m+1)
 \end{aligned}$$

$(3m+1) - m = 2m+1$ (奇数) だから、 m と $3m+1$ の偶奇性は一致しない。したがって、どちらか一方が偶数になるので、積 $m(3m+1)$ は偶数。

$n = 6m + 5$ のとき、

$$\begin{aligned}
 n^2 - 1 &= (n+1)(n-1) \\
 &= (6m+6)(6m+4) \\
 &= 12(m+1)(3m+2)
 \end{aligned}$$

$(3m+2) - (m+1) = 2m+1$ (奇数) だから、 $m+1$ と $3m+2$ の偶奇性は一致しない。したがって、どちらか一方が偶数になるので、積 $(m+1)(3m+2)$ は偶数。

偶奇性に注目すれば、それぞれの最後の式が24の倍数であることがわかる。

演習問題 7

p は 3 以上の素数であり, x, y は $0 \leq x \leq p, 0 \leq y \leq p$ を満たす整数であるとする. このとき, x^2 を $2p$ で割った余りと, y^2 を $2p$ で割った余りが等しければ, $x = y$ であることを示せ.

[03 京都大 (前) 文]

ヒントと略解

x^2 を $2p$ で割った余りと, y^2 を $2p$ で割った余りが等しいことから, $x^2 - y^2$ が $2p$ の倍数になる. 積の形に変形して, $(x + y)(x - y) = 2pk$ とおき, 偶奇性を考えよ.

演習問題 8

2 つの奇数, a, b にたいして, $m = 11a + b, n = 3a + b$ とおく. つぎの (1), (2) を証明せよ.

- (1) m, n の最大公約数は, a, b の最大公約数を d として, $2d, 4d, 8d$ のいずれかである.
- (2) m, n はともに平方数であることはない (整数の 2 乗である数を平方数であるという).

[89 京都大 (後) 理]

ヒントと略解

(1) m, n の最大公約数を g とおき, $m = gm', n = gn'$ とする (m', n' は互いに素). このとき, $g(m' - n') = 8a, g(11n' - 3m') = 8b$ となる. ここから g が $8a$ と $8b$ の約数であることがわかる.

(2) m, n はともに平方数であると仮定して矛盾をいう. m, n はともに偶数であることに注意せよ.

注 10

この問題の (1) はユークリッドの互除法が背景にある.

演習問題 9

k は 0 または正の整数とする. 方程式 $x^2 - y^2 = k$ の解 (a, b) で, a, b がともに奇数であるものを奇数解とよぶ.

(1) 方程式 $x^2 - y^2 = k$ が奇数解をもてば, k は 8 の倍数であることを示せ.

(2) 方程式 $x^2 - y^2 = k$ が奇数解をもつための必要十分条件を求めよ. [92 京都大 (後) 文]

ヒントと略解

(1) 奇数解を $x = 2m + 1, y = 2n + 1$ として代入, 積の形に変形して偶奇性を確認.

(2) k が 8 の倍数であることの必要性は (1) で言えているが, 十分性は? 任意の 8 の倍数 k に対する奇数 x, y の実例が見つければよい, という発想がないと厳しいだろう.

3.3.2 周期性

「ある状態が繰り返しおこっている」とき「周期性をもつ」という. 整数問題だけに限らず, 数学においては周期性を考えることは重要である. 周期性を見つける方法はただ一つ, ひたすら実験することである.

例 28

3^{1000} の 1 の位の数字を求めよ.

ヒントと略解

$3^1, 3^2, 3^3, 3^4, 3^5, \dots$ の 1 の位を順に調べると, 3, 9, 7, 1, 3, 9, 7, 1, \dots と周期 4 で繰り返す. したがって, 3^{1000} の 1 の位は 1 である ($\because 1000$ は 4 で割り切れる).

練習 19

7^{2007} の 1 の位の数字を求めよ. また, 47^{2007} の 1 の位の数字も求めよ

練習 20

2000^n を 7 で割った余りを a_n とし, $S_n = a_1 + a_2 + \dots + a_n$ とおく. このとき, S_n が 7 で割り切れる最小の n を求めよ. [00 同志社大 (商)]

ヒントと略解

とりあえず, 実験して a_n を予測しよう.

参考問題 9

[79 東京大 (共)]

$11^{12^{13}}$ の 10 の位を求めよ．ただし， $11^{12^{13}}$ とは， 11 の 12^{13} 乗のことであり， 11^{12} の 13 乗のことではない．[第 17 回日本数学オリンピック予選 (2007)]

演習問題 10

整数 n に対し， $f(n) = \frac{n(n-1)}{2}$ とおき， $a_n = i^{f(n)}$ と定める．ただし， i は虚数単位を表す．このとき， $a_{n+k} = a_n$ が任意の整数 n に対して成り立つような正の整数 k をすべて求めよ．

[01 京都大 (前) 理]

ヒントと略解

これもとりあえず，実験して a_n を予測しよう．求めるものは a_n の周期にあたるものである．答えは k は 8 の倍数．

演習問題 11

n は 0 または正の整数とする． a_n を， $a_0 = 1$ ， $a_1 = 2$ ， $a_{n+2} = a_{n+1} + a_n$ によって定める． a_n を 3 で割った余りを b_n とし， $c_n = b_0 + \dots + b_n$ とおく．

- (1) b_0, \dots, b_9 を求めよ．
- (2) $c_{n+8} = c_n + c_7$ であることを示せ．
- (3) $n+1 \leq c_n \leq \frac{3}{2}(n+1)$ が成り立つことを示せ．

[94 京都大 (前) 理]

最後に東大の問題を 2 問あげておく．この問題も，実験して規則性を発見するしか方法はない (合同式を用いれば，解答はかなりスムーズになる)．

参考問題 10

a を正の整数とし，数列 $\{u_n\}$ を次のように定める．

$$u_1 = 2, \quad u_2 = a^2 + 2, \\ u_n = au_{n-2} - u_{n-1} \quad (n = 3, 4, 5, \dots)$$

このとき，数列 $\{u_n\}$ の項に 4 の倍数が現れないために， a のみたすべき必要十分条件を求めよ．

実は，驚くべきことに，14 年後に同じく東京大学で次の問題が出題された．このことから，過去問対策は 10 年～15 年前の問題を中心に対策すべきであろう．

参考問題 11

整数からなる数列 $\{a_n\}$ を漸化式

$$a_1 = 1, \quad a_2 = 3, \\ a_{n+2} = 3a_{n+1} - 7a_n \quad (n = 1, 2, 3, \dots)$$

のよって定める．

- (1) a_n が偶数になることと， n が 3 の倍数になることは同値であることを示せ．
- (2) a_n が 10 の倍数になるための条件を (1) と同様の形式で求めよ． [93 東京大 (前) 理]

3.4 互いに素

「互いに素であることを証明せよ」という問題は整数問題では頻出であるので，この証明方法は絶対にマスターせねばならない．

まずは「互いに素」の意味を確認しよう．

「 a, b が互いに素であるとはどういうことか」と聴くと，概ね次のように答える人が多い．

a, b が互いに素であるとは，...

定義 a, b が 1 以外の公約数をもたない (否定的定義)

定義 a, b の最大公約数が 1 である (肯定的定義)

互いに素の定義として，これらは数学的に完全に正しい．

では，上のように定義した場合，互いに素であることの証明はどのようなになるだろうか．

おそらく，次のような論法になると思われる．

定義 を用いた証明方法

a, b が 1 以外の公約数 d をもつと仮定して
矛盾を示す (背理法) .

定義 を用いた証明方法

a, b の最大公約数を G とおいて $G = 1$ である
ことを示す .

これら 2 通りの証明の筋道は間違いではない . この証明方法で上手くいく場合もある . しかし , 実際にいろんな問題にあたっていると , 上手くいかない場合のほうが多いことに気付くであろう .

次の例で考えてみよう .

例 29

a, b が互いに素であるとき , $a + b, ab$ は互いに素であることを示せ .

解

$a + b, ab$ が 1 以外の公約数 d をもつと仮定すると ,

$$\begin{aligned} a + b &= d \times m \\ ab &= d \times m \end{aligned}$$

となる (m, n は整数) . このとき , ……

解

$a + b, ab$ の最大公約数を G とすると ,

$$\begin{aligned} a + b &= G \times m \\ ab &= G \times m \end{aligned}$$

となる (m, n は互いに素) . このとき , ……

実は , これらの証明だと , なかなか先に進まない .
その理由は , 公約数や最大公約数をただ漠然と設定したことに原因がある .

ではどうすべきだったのか .

ポイント

公約数を素数と設定する .

つまり , 互いに素の定義として次のように定める .

「互いに素」の定義

a, b が互いに素であるとは , a, b が共通の素数 p をもたないことである .

この定義を用いると , 互いに素であることの証明方法は次のようになる .

「互いに素」であることの証明方法

a, b が互いに素であることを証明するには ,
 a, b が共通の素数 p で割り切れると仮定して矛盾を示す .

互いに素であることを証明するには , この証明方法を用いるとうまくいく場合が多い .

もちろん例外もある . この証明方法を優先的に利用する , と考えよう . 上手くいかないときに先程の定義 による証明や別証明を考えるのだ .

練習 21

- (1) a, b が互いに素であるとき , $a + b, ab$ は互いに素であることを示せ .
- (2) a, b が互いに素であるとき , $(a + b)^2, ab$ は互いに素であることを示せ .
- (3) a, b が互いに素であるとき , $a^2 + b^2, ab$ は互いに素であることを示せ .

注 11

上の練習問題は逆も成立する . つまり ,

$$\begin{aligned} a + b, ab \text{ が互いに素} &\implies a, b \text{ は互いに素} \\ (a + b)^2, ab \text{ が互いに素} &\implies a, b \text{ は互いに素} \\ a^2 + b^2, ab \text{ が互いに素} &\implies a, b \text{ は互いに素} \end{aligned}$$

証明は対偶をとることで簡単に示せる .

例 30

任意の自然数 k に対して , 連続する 2 つの自然数 $k, k + 1$ は互いに素であることを示せ .

[06 大教大 (前)]

ヒントと略解

$k, k + 1$ が共通の素因数 p をもつと仮定し ,
 $k = p\alpha, k + 1 = p\beta$ とおく . このとき $p(\beta - \alpha) = 1$ となるので矛盾が示せる .

練習 22

連続する 2 つの奇数は互いに素であることを示せ。

練習 23

a を 2 以上の自然数とすると、 $a, a^2 + 1$ は互いに素であることを示せ。

このように「互いに素」は整数問題では頻出の重要なテーマである。すでに、整数問題の大原則で互いに素であるときに成立する重要性質を紹介した。ここで、もう一度紹介しておこう。

整数問題の大原則

自然数 a, b, c, d について、 a, b が互いに素であり、 $ad = bc$ が成り立つとき、
 a は c の約数 (つまり c は a で割り切れる)。
 b は d の約数 (つまり d は b で割り切れる)。

「互いに素」であるときに成立する重要性質として、もう一つ紹介しておく。

「互いに素」の性質

自然数 a, b, c について、 a, b が互いに素であり、 $ab = c^2$ が成り立つとき、 a も b も平方数 (整数の 2 乗の形で表される数) である。

これも感覚的に明らかであろう。簡単に説明すると、まず、 a または b が 1 のときは明らか。それ以外の場合を考えると、 a が平方数でなければ、 a を素因数分解したとき、ある素数 p で「 p の奇数乗」という因数が現れるはずである。ところが、 a, b が互いに素だから、 b は p を因数にもつことはなく、結局、 ab を素因数分解したときも、やはり p の指数は奇数のはず。これは右辺が平方数 (全ての指数が偶数) であることに矛盾。よって a は平方数。同様に b も平方数。

例 31

a, b, c はどの 2 つも互いに素な自然数で、 $a^2 + b^2 = c^2$ をみたすものとする。このとき次の問いに答えよ。

- (1) a, b が共に奇数であるということはないことを証明せよ。
- (2) a, b のうち偶数である方を d とする。このとき、 $c + d, c - d$ は共に平方数であることを示せ。

ヒントと略解

(1) については、平方数の分類で既に紹介しているので説明省略。(2) については、 a, b が互いに素だから、共に偶数ということはないので、一方が偶数、もう一方が奇数ということになる。 a, b のうち偶数を d 、奇数を e とおくと、

$$d^2 + e^2 = c^2 \iff e^2 = (c + d)(c - d)$$

となり、 $c + d, c - d$ が互いに素であることが証明できれば、 $c + d, c - d$ は共に平方数であるといえる。したがって、 $c + d, c - d$ が共通の素因数 p をもつと仮定し矛盾を示す。なお、 $c + d, c - d$ は共に奇数であることに注意する (偶奇性!)。

演習問題 12

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。

[98 京都大 (後) 文]

演習問題 13

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。

[99 京都大 (後) 文]

これまで、互いに素であることの証明を「互いに素でないとは仮定して矛盾」という方法で証明してきたが、直接証明することもできる。それにはユークリッドの互除法を用いる。

ユークリッドの互除法とは、2つの数の最大公約数を求めるアルゴリズム(計算過程)のことである。最大公約数を実際に計算して、1になれば互いに素、1にならないければ互いに素ではない、というわけである。

ユークリッドの互除法

a, b を自然数とし、 a を b で割ったときの商を q 、余りを r とする。つまり、 $a = bq + r$ であるとき、 a, b の最大公約数と b, r の最大公約数は一致する。

証明

a, b の最大公約数を G とするとき、 $a = Ga'$ 、 $b = Gb'$ (a' と b' は互いに素) とおける。いま、 a を b で割って $a = bq + r$ (商を q 、 r は余りで $0 \leq r < b$) となったとすれば、

$$\begin{aligned} r &= a - bq \\ &= Ga' - Gb'q \\ &= G(a' - b'q) \end{aligned}$$

となり、 r も G の倍数である。

次に、 $b = Gb'$ 、 $r = G(a' - b'q)$ を考えると、 a' と b' が互いに素ならば、 b' と $a' - b'q$ も互いに素なので、 a, b の最大公約数と b, r の最大公約数は一致する。

終

具体例で検証する方がわかりやすいだろう。

例 32

703 と 209 の最大公約数をユークリッドの互除法によって求めると、

$$\begin{aligned} 703 &= 209 \times 3 + 76 \\ 209 &= 76 \times 2 + 57 \\ 76 &= 57 \times 1 + 19 \\ 57 &= 19 \times 3 + 0 \end{aligned}$$

つまり、 a, b の最大公約数を (a, b) で表すと、

$$\begin{aligned} &(703, 209) \\ &= (209, 76) \\ &= (76, 57) \\ &= (57, 19) \\ &= 19 \end{aligned}$$

最大公約数は 19 である。

703 と 208 の最大公約数をユークリッドの互除法によって求めると、

$$\begin{aligned} 703 &= 208 \times 3 + 79 \\ 208 &= 79 \times 2 + 50 \\ 79 &= 50 \times 1 + 29 \\ 50 &= 29 \times 1 + 21 \\ 29 &= 21 \times 1 + 8 \\ 21 &= 8 \times 2 + 5 \\ 8 &= 5 \times 1 + 3 \\ 5 &= 3 \times 1 + 2 \\ 3 &= 2 \times 1 + 1 \\ 2 &= 1 \times 2 + 0 \end{aligned}$$

つまり、 a, b の最大公約数を (a, b) で表すと、

$$\begin{aligned} &(703, 208) \\ &= (208, 79) \\ &= (79, 50) \\ &= (50, 29) \\ &= (29, 21) \\ &= (21, 8) \\ &= (8, 5) \\ &= (5, 3) \\ &= (3, 2) \\ &= (2, 1) \\ &= 1 \end{aligned}$$

最大公約数は 1 である。つまり 703 と 208 は互いに素。

上の例からもわかるように、次の定理が成立する。

ユークリッドの互除法の定理

互除法における、0 でない最後の余りが、最大公約数である。

練習 24

20853 と 3843 の最大公約数を,

- (1) 素因数分解を利用する方法
 - (2) ユークリッドの互除法を利用する方法
- の 2 通りで求めよ. [02 同志社大 (商)]

このように, ユークリッドの互除法は具体的な数値の場合には有効であるが, この章の始めに紹介した文字式の場合は残念ながら, 効果的ではない. しかし, 次に紹介する問題の設問 (2) は, ユークリッドの互除法でないと解けない問題であるが, 設問 (1) がそのヒントになっているので, ユークリッドの互除法を知らなくても大丈夫である. でも, 知っていたほうが見通しは立ちやすいだろう.

練習 25

- (1) 自然数 a, b, c, d に, $\frac{b}{a} = \frac{c}{a} + d$ の関係があるとき, a と c が互いに素ならば, a と b も互いに素であることを証明せよ.
- (2) 任意の自然数 n に対し, $28n + 5$ と $21n + 4$ は互いに素であることを証明せよ.

[00 大阪市大 (前) 理]

練習 26

x, y を互いに素な自然数とすると, $\frac{4x + 9y}{3x + 7y}$ は既約分数であることを証明せよ.

3.5 ${}_pC_k$ は p の倍数

二項係数 ${}_nC_r$ は整数であるので, 二項係数をテーマにした整数問題も頻繁に出題される. 特に, 京都大学の入試問題では, 素数 p について「 ${}_pC_k$ は p の倍数」ということは常識として出題されているようだ.

この章で二項係数 (二項定理) に関する整数問題をまとめておこう.

まず始めに二項係数の基本性質を確認しよう.

二項係数の性質

基本性質	${}_k{}_nC_k = {}_{n-1}C_{k-1}$
------	---------------------------------

基本性質	${}_nC_k = {}_{n-1}C_k + {}_{n-1}C_{k-1}$
------	---

証明

いずれも, ${}_nC_k = \frac{n!}{k!(n-k)!}$ を用いて証明できる. また, 組合せの意味からも説明できるが, ここでは省略する.

終

注 12

整数問題では主に

基本性質

 が利用される.

基本性質

 は確率の期待値の計算でも利用される重要な性質である.

二項係数の性質

素数 p について, ${}_pC_k$ ($k = 1, 2, \dots, p-1$) は p の倍数

証明

基本性質	より,
------	-----

$${}_k{}_pC_k = {}_{p-1}C_{k-1}$$

が成立するので, ${}_k{}_pC_k$ は p の倍数である. k ($k = 1, 2, \dots, p-1$) は p の倍数ではないので, ${}_pC_k$ は p の倍数になる.

終

例 33

p を素数とする. このとき, 任意の正の整数 n に対し, $(n+1)^p - n^p - 1$ は p で割り切れることを示せ. [06 早大 (政経)]

ヒントと略解

二項定理より

$$\begin{aligned}
 (n+1)^p &= \sum_{k=0}^p {}_pC_k n^k \\
 &= n^p + \sum_{k=1}^{p-1} {}_pC_k n^k + 1
 \end{aligned}$$

だから,

$$(n+1)^p - n^p - 1 = \sum_{k=1}^{p-1} {}_p C_k n^k$$

となる. $k {}_p C_k$ は p の倍数であるから, 右辺は p の倍数.

練習 27

p を素数とする. このとき, 3^p を p で割ったときの余りを求めよ. また, 3^{p-1} を p で割ったときの余りを求めよ. [01 明大 (商)]

注 13

上の例, 練習では『フェルマーの小定理』が背景にある.

演習問題 14

a, b は $a > b$ をみたす自然数とし, p, d は素数で $p > 2$ とする. このとき, $a^p - b^p = d$ であるならば, d を $2p$ で割った余りが 1 であることを示せ. [95 京都大 (前) 理]

ヒントと略解

$a^p - b^p$ を因数分解せよ.

二項係数の性質

素数 p と整数 m について, ${}_m C_p$ が p で割り切れるための必要十分条件は m が p の倍数であることである.

証明

基本性質 より,

$${}_m C_p = m {}_{m-1} C_{p-1}$$

が成立する.

$${}_{pm-1} C_{p-1} = \frac{(pm-1)(pm-2)\cdots(pm-p+1)}{(p-1)!}$$

となるので, ${}_{pm-1} C_{p-1}$ の分子の各項はいずれも p で割り切れないので, ${}_{pm-1} C_{p-1}$ は p で割り切れない. よって, ${}_{pm-1} C_{p-1}$ は p と互いに素となり,

${}_m C_p$ が p で割り切れる $\iff m$ が p で割り切れる
が成立する.

終

演習問題 15

n が相異なる素数 p, q の積, $n = pq$, であるとき, $(n-1)$ 個の数 ${}_n C_k$ ($1 \leq k \leq n-1$) の最大公約数は 1 であることを示せ. [97 京都大 (前) 理]

ヒントと略解

「 $(n-1)$ 個の数の最大公約数が 1」と言われても, $(n-1)$ 個全てに注目するのは無理である. $(n-1)$ 個の中から適当に 2 つ選んで互いに素になっていれば $(n-1)$ 個全ての最大公約数が 1 といえる.

注 14

一般に, 「 ${}_n C_k$ ($k = 1, 2, \dots, n-1$) は p の倍数」であることが知られている (つまり $n = 1$ の場合が今回のテーマであった). 証明は難しい. なお, 次に紹介するように, $p = 2$ の場合が 99 年に東京大で出題された.

参考問題 12

- (1) k を自然数とする. m を $m = 2^k$ とするとき, $0 < n < m$ をみたすすべての整数 n について, 二項係数 ${}_m C_n$ は偶数であることを示せ.
- (2) 以下の条件をみたす自然数 m をすべて求めよ.
条件: $0 \leq n \leq m$ をみたすすべての整数 n について二項係数 ${}_m C_n$ は奇数である.

[99 東京大 (前) 理]

なんと, 同じ 99 年 (しかも同じ日!) に同じ問題が広島市大で出題されている. 驚くべきことに, 東大の (2) の問題の答えが, そのまま広島市大で出題されている. しかも, 05 年には, その逆が岐阜大 (後) で出題された.

参考問題 13

- (1) $2^n C_k$ ($k = 1, 2, \dots, 2^n - 1$) は偶数であることを示せ.

- (2) ${}_{2^n-1}C_k$ ($k = 1, 2, \dots, 2^n - 1$) は奇数であることを示せ． [99 広島市立大 (前)]

参考問題 14

n を 2 以上の自然数とする．二項係数 ${}_nC_k$ ($k = 1, 2, \dots, n - 1$) がすべて偶数ならば，適当な自然数 k を用いて $n = 2^k$ と表されることを示せ． [05 岐阜大 (後)]

参考問題 15

- (1) n が偶数， r が奇数のとき， ${}_nC_r$ は偶数であることを示せ．
 (2) n を 4 で割った余りが 1 であり，かつ r を 4 で割った余りが 0 でも 1 でもなければ， ${}_nC_r$ が偶数となることを示せ．
 (3) m を 2 以上の自然数とする． n を 2^m で割った余りが 1 であり，かつ r を 2^m で割った余りが 0 でも 1 でもなければ， ${}_nC_r$ が偶数となることを示せ． [02 お茶の水女大 (後) 理数]

3.6 続・互いに素

前章で「互いに素」を定義した．この章では「互いに素」であるときに成立する性質を紹介する．内容はかなり難しいが，大学入試での整数問題の最終地点のつもりで頑張ってください．

次に紹介する性質は，非常に重要で，これをテーマにした問題は数多くある．

あまりにも重要な性質なので「整数問題の基本定理」とよぶことにしよう．

この基本定理は内容も当然のことながら，実はその証明方法が極めて重要である．証明方法をしっかりと理解してほしい．

整数問題の基本定理

a, b が互いに素であるとする．このとき， $b - 1$ 個の相異なる整数

$$1a, 2a, 3a, \dots, (b-1)a$$

を b で割った余り全体は，1 から $b - 1$ までの全ての整数である

つまり， b で割った余りには，1 から $b - 1$ までの整数が 1 回ずつすべて (順不同で) 現れる．

おそらく，一読しただけでは，意味はよくわからないと思うので，まずは具体的な数字で確認してみよう．

例 34

互いに素な a, b で， $a = 3, b = 8$ として「整数問題の基本定理」を確認する．

$1 \times 3, 2 \times 3, 3 \times 3, 4 \times 3, 5 \times 3, 6 \times 3, 7 \times 3$ を 8 で割った余りを求めると，

$$\begin{aligned} 1 \times 3 &= 3 \longrightarrow \text{余り } 3 \\ 2 \times 3 &= 6 \longrightarrow \text{余り } 6 \\ 3 \times 3 &= 9 \longrightarrow \text{余り } 1 \\ 4 \times 3 &= 12 \longrightarrow \text{余り } 4 \\ 5 \times 3 &= 15 \longrightarrow \text{余り } 7 \\ 6 \times 3 &= 18 \longrightarrow \text{余り } 2 \\ 7 \times 3 &= 21 \longrightarrow \text{余り } 5 \end{aligned}$$

確かに，余りは 1, 2, 3, 4, 5, 6, 7 が 1 回ずつ現れている．

次に，互いに素でない a, b で， $a = 6, b = 8$ として「整数問題の基本定理」を確認する．

$1 \times 6, 2 \times 6, 3 \times 6, 4 \times 6, 5 \times 6, 6 \times 6, 7 \times 6$ を 8 で割った余りを求めると，

$$\begin{aligned} 1 \times 6 &= 6 \longrightarrow \text{余り } 6 \\ 2 \times 6 &= 12 \longrightarrow \text{余り } 4 \\ 3 \times 6 &= 18 \longrightarrow \text{余り } 2 \\ 4 \times 6 &= 24 \longrightarrow \text{余り } 0 \\ 5 \times 6 &= 30 \longrightarrow \text{余り } 6 \\ 6 \times 6 &= 36 \longrightarrow \text{余り } 4 \\ 7 \times 6 &= 42 \longrightarrow \text{余り } 2 \end{aligned}$$

となり、余りは 1, 2, 3, 4, 5, 6, 7 が 1 回ずつ現れることはない。

それでは「整数問題の基本定理」を証明しよう。繰り返し言うが、この証明方法が重要なので、しっかりと理解してほしい。

証明

$b-1$ 個の数 $ka (k=1, 2, \dots, b-1)$ を b で割った余りを r とおくと、 a, b は互いに素だから、 r は $1, 2, \dots, b-1$ のいずれかの数である。よって、 $b-1$ 個の余りが全て異なることを示せばよい。

$k_1, k_2 (1 \leq k_1 < k_2 \leq b-1)$ として、 ak_1, ak_2 を b で割った余りが同じであると仮定すると、

$$ak_1 = bq_1 + r_k$$

$$ak_2 = bq_2 + r_k$$

$$\therefore a(k_2 - k_1) = b(q_2 - q_1)$$

a, b 互いに素より、 $k_2 - k_1$ は b の倍数である。ところが、 $1 \leq k_1 < k_2 \leq b-1$ より、 $1 \leq k_2 - k_1 \leq b-2$ だから、 $k_2 - k_1$ は b の倍数にはならない。よって、矛盾。

したがって、 $b-1$ 個の数 $ka (k=1, 2, \dots, b-1)$ を b で割った余りは全て異なるので、題意は証明された。

終

注 15

上の基本定理では、 $b-1$ 個の整数について述べているが、 ba を b で割った余りは 0 であるので、 ba も追加して、次のように表現する場合もある。

a, b が互いに素であるとする。このとき、 b 個の相異なる整数

$$1a, 2a, 3a, \dots, (b-1)a, ba$$

を b で割った余り全体は、0 から $b-1$ までの全ての整数である。

しかし、本論では、最初に紹介した方を基本定理とよぶ。

「整数問題の基本定理」から、次の 2 つの重要なことが導かれる。

整数問題の基本定理からわかること

a, b が互いに素 $\iff am + bn = 1$ となる整数 m, n が存在する。

証明

(\implies) の証明

a, b が互いに素のとき、「整数問題の基本定理」より、 $ka (k=1, 2, \dots, b-1)$ の中に、 b で割ると余りが 1 になるものが必ず存在するので、そのときの商を q とおくと、

$$ka = bq + 1$$

$$\therefore ak + b(-q) = 1$$

となる整数 k, q が存在し、 $k = m, -q = n$ において題意は成立する。

(\impliedby) の証明

a, b が互いに素でないと仮定すると、共通の素因数 p が存在し、 $a = pa', b = pb'$ となる。このとき、

$$am + bn = 1$$

$$pa'm + pb'n = 1$$

$$p(a'm + b'n) = 1$$

この式は矛盾である。

終

注 16

上にあげた「整数問題の基本定理からわかること」を「互いに素」の定義とする場合もある。この場合、前章の練習問題も全く別の証明になる。

例 35

a を 2 以上の自然数とすると、 $a, a^2 + 1$ は互いに素であることを「整数問題の基本定理からわかること」を利用して示せ。

ヒントと略解

$a \times (-a) + (a^2 + 1) \times 1 = 1$ より、 $ax + (a^2 + 1)y = 1$ をみたす整数が存在するので、 $a, a^2 + 1$ は互いに素である。

注 17

この問題にはユークリッドの互除法が関係している． $a^2 + 1$ を a で割ると商が a ，余りが 1，つまり，

$$a^2 + 1 = a \times a + 1$$

だから， a と $a^2 + 1$ の最大公約数は， a と 1 の最大公約数に等しい．

なお，明治大（商）で，ここまでの部分の証明が，そのまま出題された．証明の復習も兼ねて，取り組んでみよう．

練習 28

自然数 a, b について， $am + bn = 1$ を満たす整数 m, n が存在するための必要十分条件は， m と n の最大公約数が 1 であること証明せよ．[02 明治大（商）]

a, b が互いに素であるとき， $am + bn = 1$ となる整数 m, n を実際に求めてみよう．

例 36

$3x + 5y = 1$ を満たす整数を求めよ．

ヒントと略解

まずは，とにかく 1 組の解を見つける．上の例では， $x = 2, y = -1$ としよう．このとき，

$$\begin{aligned} 3x + 5y &= 1 \\ 3(2) + 5(-1) &= 1 \end{aligned}$$

の辺々を引くと，

$$\begin{aligned} 3(x - 2) + 5(y + 1) &= 0 \\ 3(x - 2) &= 5(-y + 1) \end{aligned}$$

となる．3 と 5 は互いに素だから， $x - 2 = 5k$ とおけ，このとき， $-y + 1 = 3k$ となる．したがって， $x = 5k + 2, y = -3k + 1$ と定まる．

上の例では，1 組の解が簡単に見つかったが，いつも簡単に見つかるとは限らない．簡単には見つか

らない場合にはユークリッドの互除法を利用すればよいのだが，入試でユークリッドの互除法を用いなければ解けない問題など，まず出題されないのでここでは説明は省略させていただく（ユークリッドの互除法については整数問題の大原則の章を参照せよ）．

次の問題は，その 1 組の求め方が容易ではない問題であるが，ユークリッドの互除法を用いるまでもない．

参考問題 16

3 以上 9999 以下の奇数 a で， $a^2 - a$ が 10000 で割り切れるものをすべて求めよ．

[05 東京大（前）共]

ヒントと略解

$a^2 - a = a(a - 1)$ ．連続する 2 整数は互いに素であることを思い出そう．答えは $a = 625$ ．

またさらに，次のことが言える．

整数問題の基本定理からわかること

a, b が互いに素であるとき， $am + bn$ (m, n は整数) は任意の整数値をとることができる．つまり， $am + bn$ の形ですべての整数を表現することができる．

証明

a, b が互いに素であるとき，「整数問題の基本定理からわかること」より，

$$am + bn = 1$$

となる整数 m, n が存在する．このとき，任意の整数 c に対して，両辺を c 倍すると，

$$a(cm) + b(cn) = c$$

が得られる．

終

このことをテーマにした入試問題として次の問題をあげておく．

参考問題 17

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) を格子点とよぶ. 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 $\frac{2}{5}$ 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.

[91 東京大 (前) 理]

ヒントと略解

$$r = \frac{1}{2\sqrt{29}}$$

なお, a, b が互いに素であるとき, $am + bn$ の形の式のとり得る値については非常に奥が深く, 次に一応紹介するが, かなり難しいので, 無視しても構わない.

$am + bn$ のとり得る値 (難!)

a, b が互いに素であるとき, $am + bn$ は

m, n は整数

\Rightarrow すべての整数値をとることができる.

m, n は自然数

$\Rightarrow ab+1$ 以上の整数はすべて表現できる.

つまり, 表現できない最大の整数 ab .

$m \geq 0, n \geq 0$

$\Rightarrow (a-1)(b-1)$ 以上の整数はすべて

表現できる. つまり, 表現できない最

大の整数は $(a-1)(b-1) - 1$.

実は, 上の結果が阪大と津田塾大でそのまま出題された.

参考問題 18

どのような負でない 2 つの整数 m と n を用いても, $x = 3m + 5n$ とは表すことができない正の整数 x をすべて求めよ.

[00 大阪大 (前) 理]

ヒントと略解

$(3-1)(5-1) = 8$ 以上の整数はすべて表現できるので, 7 以下の自然数をチェックするだけの問題 (7 以下自然数が全て表現できない, というわけではない).

参考問題 19

自然数 x と y を用いて $3x + 59y$ の形で表せる自然数を $< 3, 59 >$ -数ということにする.

(1) 178 以上の自然数はすべて $< 3, 59 >$ -数であることを示せ.

(2) 177 は $< 3, 59 >$ -数でないことを示せ.

[05 津田塾大 (数)]

ヒントと略解

どうして 177 や 178 という数字がいきなり出てきたのかわかるであろう.

4 整数問題の攻略 (応用編)

4.1 格子点

xy 平面上の点で x 座標と y 座標が共に整数である点を格子点という. 格子点に関する問題で最も多いのは「与えられた領域内に存在する格子点の個数を求めよ」という問題で, このタイプの問題は, 適当な直線 (または平面) で切断し, その直線上 (または平面上) の格子点の個数を数え, Σ 計算に持ち込むという方法で解決するため, 数列分野の問題として扱われる. しかし, この章では, あくまでも整数問題であることを意識して, いくつかの問題を取り上げてみたい.

まず始めに, 線分上の格子点については, 次のことが重要である.

線分上の格子点

a, b が互いに素であるとき, 格子点 $P(a, b)$ と原点 O に対して, 線分 OP 上には両端を除いて格子点は存在しない.

証明

線分 OP の方程式は, $y = \frac{b}{a}x$ ($0 < x < a$) である. a, b が互いに素であり, $0 < x < a$ に a の倍数は存在しないので, $\frac{b}{a}x$ ($0 < x < a$) が整数になることはない. つまり, 線分 OP 上に格子点は存在しない.

終

線分上の格子点

格子点 $P(a, b)$ と原点 O に対して、線分 OP 上の両端を除く格子点の個数は $G - 1$ 個である。ここで、 G は m と n の最大公約数である。

証明

m と n の最大公約数を G とする。このとき $m = Gm'$, $n = Gn'$ であり、 m' と n' は互いに素である。 $P'(m', n')$ とおくと、「線分上の格子点」より線分 OP' 上には両端を除いて格子点は存在しない。

よって、線分 OP 上の格子点の全ては、
 $(m', n'), (2m', 2n'), \dots, ((G-1)m', (G-1)n')$
 の $G - 1$ 個である。

終

参考問題 20

3 点 $P(a, b)$, $Q(c, d)$, $R(a + c, b + d)$ は格子点であるとする。また、線分 OP , OQ 上には端点以外に格子点はなく、平行四辺形 $OPRQ$ の面積は 2 とする。このとき、線分 PQ の中点 M は格子点であることを示せ。ただし、格子点とは x 座標、 y 座標がともに整数となる点のことである。

[99 津田塾大 (情数)]

ヒントと略解

まずは、平行四辺形の面積を a, b, c, d で表す。中点が格子点であるとはどういうことなのだろうか。文字の偶奇性に注目する必要があるだろう。

次に、直線上の格子点について「整数問題の基本定理」から導かれる重要な事実を紹介する。

直線上の格子点

a, b が互いに素であるとき、任意の自然数 c に対して、 xy 平面の直線 $ax + by = c$ 上に格子点が無数個あり、それらは等間隔で並ぶ。

証明

「整数問題の基本定理からわかること」より、
 $ax_0 + by_0 = c$ となる整数 x_0, y_0 が存在する。

$$ax + by = c$$

$$ax_0 + by_0 = c$$

$$\therefore a(x - x_0) = b(y_0 - y)$$

a, b が互いに素より、 $x - x_0 = bk$ となり、このとき、 $y_0 - y = ak$ となる。

したがって、

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

これが、直線 $ax + by = c$ 上の格子点全部で、これはベクトル $(b, -a)$ を間隔として等間隔に並ぶ。

終

4.2 ガウス記号 $[x]$

ガウス記号 $[x]$ もまた難関大学では頻出であるが、数学で、不連続関数の例として $y = [x]$ のグラフの紹介があるだけで、ガウス記号の整数論的意味は置き去りになってしまっている。そのためか、なじみが薄く、苦手とする受験生も多いと思われる。この章では、「記号の意味はわかるが問題が解けない」という人のために、代表的な入試問題を紹介し、ガウス記号についての苦手意識を解消させたい。

ガウス記号 $[x]$ の定義

実数 x に対して、 $n \leq x$ をみたす最大の整数 n を記号 $[x]$ で表す。

すなわち、 x を超えない最大の整数が $[x]$ である。

例 37

$$[9.18] = 9, \quad [7] = 7, \quad [-2.7] = -3, \quad [-4] = -4$$

ガウス記号 $[x]$ の定義より、次の重要な関係が成り立つ。

ガウス記号 $[x]$ の基本性質

$$\begin{aligned} [x] = n &\iff n \text{ は整数} \\ &\iff n \leq x < n + 1 \\ &\iff [x] \leq x < [x] + 1 \\ &\iff x - 1 < [x] \leq x \end{aligned}$$

上記の基本性質より, $[x]$ の問題は不等式と整数の問題に言い換えられることに注目しよう.

また, 次の関係もよく用いられる.

$$n \text{ が整数のとき, } [n + x] = n + [x]$$

証明

$[n + x] = a$ とおくと, a は整数で,

$$\begin{aligned} a = [n + x] &\iff a \leq n + x < a + 1 \\ &\iff a - n \leq x < (a - n) + 1 \\ &\iff [x] = a - n \end{aligned}$$

これに, $a = [n + x]$ を用いて, $[n + x] = n + [x]$ が成立する.

終

練習 29

$a_n = \left[\frac{n^2 + 2}{3} \right]$ とするとき, $\sum_{k=1}^n a_k$ を n の式で表せ.

ヒントと略解

まずは $n = 1, 2, 3, \dots$ と実験してみて規則性を把握する必要がある. 平方数の 3 で割ったときの分類を利用することに気付くだろう.

$$m, n \text{ を自然数とする. } m \div n \text{ の商は } \left[\frac{m}{n} \right] \text{ に一致する.}$$

証明

$m \div n$ の商を q , 余りを r とおくと,

$$\begin{aligned} m &= nq + r \quad (0 \leq r < n) \\ \frac{m}{n} &= q + \frac{r}{n} \quad \left(0 \leq \frac{r}{n} < 1 \right) \\ \therefore \left[\frac{m}{n} \right] &= \left[q + \frac{r}{n} \right] = q + \left[\frac{r}{n} \right] = q + 0 = q \end{aligned}$$

終

以上のこと (だけ) をテーマにした問題を紹介しておく. 見た目の複雑さに戸惑ってはいけない (この問題は見掛け倒しである). 落ち着いて $[x]$ の意味を考えればできる.

練習 30

n を 2 以上の自然数とし, 自然数 a に対して, $(a)_n$ は a を n で割ったときの余りとする. このとき, 以下の問いに答えよ.

- (1) 自然数 a に対して, $a = \left[\frac{a}{n} \right] n + (a)_n$ を示せ.
- (2) 自然数 a, b, c に対して,

$$\begin{aligned} &\left[\frac{a(bc)_n}{n} \right] + a \left[\frac{bc}{n} \right] \\ &= \left[\frac{b(ca)_n}{n} \right] + b \left[\frac{ca}{n} \right] \\ &= \left[\frac{c(ab)_n}{n} \right] + c \left[\frac{ab}{n} \right] \end{aligned}$$

を示せ.

[05 横浜市大 (前) 医]

例 38

p, N を自然数とするとき, $1, 2, 3, \dots, N$ の内の p の倍数は $\left[\frac{N}{p} \right]$ 個.

例 39

p :素数, N :自然数に対して, $1, 2, 3, \dots, N$ の内, 素因数分解したときの素因数 p の指数が k となるものは, $\left[\frac{N}{p^k} \right] - \left[\frac{N}{p^{k+1}} \right]$ 個である.

ヒントと略解

$\{p^k \text{の倍数}\} \supset \{p^{k+1} \text{の倍数}\}$ (集合としての包含関係) であることに注目する. このことは, 後ほど紹介する数論的関数の項でも扱う.

最初に述べたように, ガウス記号 $[x]$ の問題は, 不等式と整数の問題に言い換えることができるが, 加えて, 数直線は座標平面上の格子点の問題と見て幾何学的に扱うことが少なくない.

練習 31

p, q を互いに素な自然数とすると,

$$\sum_{k=1}^{p-1} \left[\frac{kq}{p} \right]$$

を p, q で表せ.

ヒントと略解

直線 $y = \frac{q}{p}x$ を考え, 座標平面上の格子点をイメージする. 問題の和は, 何を意味しているのだろうか?

参考問題 21

実数 x に対して, x を越えない最大の整数を $[x]$ で表す. $a_m = [\sqrt{m}]$ ($m = 1, 2, 3, \dots$) に対して, 数列 b_1, b_2, \dots を $b_1 = 0, k \geq 2$ のとき $a_m < k \leq a_{m+1}$ となる m に対して $b_k = m$ と定める.

次の問いに答えよ.

- (1) 数列 $\{b_k\}$ の一般項を求めよ.
- (2) すべての自然数 n に対して,

$$\sum_{m=1}^{n^2} a_m + \sum_{k=1}^n b_k = n^3$$

が成り立つことを示せ.

- (3) $\sum_{m=1}^{n^2} [\sqrt{m}]$ を求めよ. [99 大阪大 (後)]

ヒントと略解

座標平面上の格子点をイメージせよ.

練習 32

n の正の約数すべての個数を $f(n)$ で表すとき,

$$\sum_{k=1}^n f(k) = \sum_{k=1}^n \left[\frac{n}{k} \right]$$

であることを示せ.

[04 千葉大 (後) 理]

ヒントと略解

正の約数の個数は, 後の「数論的関数」の章で紹介するが, ここでは, そんなことを知らなくても, 座標平面上の格子点に対応させて考えればよい.

参考問題 22

n を 2 以上の自然数とすると,

$$[x] + \left[x + \frac{1}{n} \right] + \dots + \left[x + \frac{n-1}{n} \right] = [nx]$$

を示せ.

ヒントと略解

数直線上の格子点をイメージせよ. いきなり一般的な証明が無理なら, $n = 2, 3$ あたりでまず証明してみよう.

参考問題 23

実数 x に対し, x を越えない最大の整数を $[x]$ で表す.

- (1) 正の実数 a と自然数 m に対し, 不等式 $\frac{[ma]}{a} \leq m < \frac{[ma] + 1}{a}$ を示せ.
- (2) 正の実数 a と b が $\frac{1}{a} + \frac{1}{b} = 1$ を満たし, さらにある自然数 m と n に対し $[m\alpha] = [n\beta]$ が成り立つならば a と b はともに有理数であることを証明せよ. [92 慶応大 (理工)]

上の慶応大の問題に非常に似た問題として, 次の問題がある.

参考問題 24

正の無理数 α, β が $\frac{1}{\alpha} + \frac{1}{\beta} = 1$ を満たすとき, どんな正の整数 m, n をとっても, $[m\alpha] = [n\beta]$ が成り立たないことを示せ. [99 中央大 (情)]

注 18

ここに紹介した慶応大，中央大の問題は『レーリー (Lord Rayleigh) の定理』とよばれるものが背景にある．レーリーは，振動する弦の倍音と，もとの弦を 2 つの部分に分割して得られる 2 本の弦の同様な振動数の重ね合わせに関する研究から，次の結果を得た．

レーリーの定理

α, β は方程式

$$\frac{1}{\alpha} + \frac{1}{\beta} = 1$$

を満たす正の無理数とし，2 つの整数列を

$$A = \{[n\alpha] \mid n = 1, 2, 3, \dots\}$$

$$B = \{[m\beta] \mid m = 1, 2, 3, \dots\}$$

により定義する．このとき，

$$A \cap B = \phi$$

$$A \cup B = \{\text{自然数全体}\}$$

が成立する．

この定理は，逆も成立する．つまり $[n\alpha], [m\beta]$ を合わせると，自然数全体が重複なしに表されるための条件は，

$$\alpha, \beta \text{ が無理数で } \frac{1}{\alpha} + \frac{1}{\beta} = 1$$

が成立することである．重複があるとする α, β は有理数である．

有理数，無理数の話が出たので，最後に北大の問題を紹介して，ガウス記号の学習を終えることにしよう．

参考問題 25

実数 x に対して， x 以下の整数のうちで最大のものを $[x]$ と書くことにする． $c > 1$ として， $a_n = \frac{[nc]}{c} (n = 1, 2, \dots)$ とおくとき，以下の (1), (2), (3) を証明せよ．

(1) すべての n に対して， $[a_n]$ は n または $n-1$ に等しい．

(2) c が有理数のときは， $[a_n] = n$ となる n が存在する．

(3) c が無理数のときは，すべての n に対して $[a_n] = n-1$ となる． [97 北大 (前) 理]

4.3 有理数解をもつ方程式

この章では，整数係数の n 次方程式 $f(x) = 0$ が有理数解をもつための条件に関する問題を紹介する．

まず始めに，整数係数の方程式には次の重要な事実がある．

整数係数の整方程式の有理数解 整数係数の整方程式

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = 0 \quad (a_n \neq 0)$$

が有理数の解を持つならば，その有理数の解は

$$\frac{a_0 \text{ の約数}}{a_n \text{ の約数}}$$

の形である．とくに， $a_n = 1$ ならば，有理数解は整数であって， a_0 の約数である．

このことをテーマにした問題は極めて多い．特に，2 次方程式，3 次方程式の場合は頻出である．

例 40

a, b, c を整数とする． x に関する 3 次方程式 $x^3 + ax^2 + bx + c = 0$ が有理数の解をもつとき，その解は整数であることを示せ． [02 神戸大 (前) 理]

ヒントと略解

有理数解を $x = \frac{q}{p} (p, q \text{ 互いに素})$ とおいて代入する．積の形をつくり， $p = 1$ を示す．

練習 33

整数 a, b, c, d を係数とする 3 次方程式 $ax^3 + bx^2 + cx + d = 0$ が有理数の解 $\frac{q}{p} (p, q \text{ は互いに素な整数})$ をもつとき， a は p で割り切れることを示せ． [98 岡山県立大 (C) 情工]

これら 2 つの問題は本質的に同じである．なお，京都大では 96 年に文系で n 次式の場合の問題が出題されている．総合問題演習[3]を参照せよ．

練習 34

p, q を整数とし， $f(x) = x^2 + px + q$ とおく．

- (1) 有理数 a が方程式 $f(x) = 0$ の一つの解ならば， a は整数であることを示せ．
- (2) $f(1)$ も $f(2)$ も 2 で割り切れないとき，方程式 $f(x) = 0$ は整数の解をもたないことを示せ．

[00 愛媛大 (前) 理]

また，特に 2 次方程式，3 次方程式が整数解を持つときに関する問題では，解と係数の関係を利用する場合が多い．東京理科大薬 (99)，産業医大 (02)，上智 (01 経済) など多数出題されている．

例 41

2 次方程式 $x^2 - 3ax + 2a - 3 = 0$ が 2 つの整数解を持つように a を定めよ． [04 自治医大]

ヒントと略解

2 つの整数解を $\alpha, \beta (\alpha \leq \beta)$ とする．解と係数の関係より， $\alpha + \beta = 3a$ ， $\alpha\beta = 2a - 3$ ．これらの式から， a を消去して，

$$\begin{aligned}\alpha\beta &= 2\frac{\alpha + \beta}{3} - 3 \\ \left(\alpha - \frac{2}{3}\right)\left(\beta - \frac{2}{3}\right) &= -\frac{23}{9} \\ \therefore (3\alpha - 2)(3\beta - 2) &= -23\end{aligned}$$

$\alpha \leq \beta$ を考慮して， $\alpha = -7$ ， $\beta = 1$ を得る．よって， $a = -2$ ．

注 19

上の例題では， a を求めるにも係わらず， a を消去して考えていることに注意しよう．いきなり目的のモノに飛びつかずに，周りから攻めていっている解答の流れを感じて欲しい．大切な考え方である．

練習 35

p を素数とする． x に関する 2 次方程式 $px^2 + (5 - p^2)x - 3p = 0$ が整数の解を持つのは $p = 2$ のときに限ることを示せ． [03 千葉大 (前) 理]

ヒントと略解

先程の例題を真似て，解と係数の関係を用いよう．とすると上手くいかない．なぜか？先の例題は「2 つの整数解」であったが，この問題では単に「整数解」としか書いてないので，「整数解を $\alpha, \beta (\alpha \leq \beta)$ とする」とはおけないのである！（整数解と分数解かもしれない）．とりあえず，整数解を m とおこう．あとは整数問題の大原則に従う．

練習 36

定数 p, q, r は， $p > q > r$ を満たしている．3 次方程式 $x^3 + px^2 + qx + r = 0$ の解は，連続する 3 つの整数 $n - 1, n, n + 1$ であるとする．このとき， n の値と p, q, r を求めよ． [03 大阪大 (後) 理]

ヒントと略解

3 次方程式の解に関する問題をみると，いきなり微分してグラフ考察を始める人が多い．「とりあえず微分…」という発想は余りにも単純すぎる．3 次方程式の解に関する問題では，因数分解できないか考える，無理ならグラフ考察，だが本問の場合，3 つの整数解が具体的にわかっているので解と係数の関係を利用することを考えて欲しい．あとは $p > q > r$ の大小関係から n の範囲を絞り込めばよい．

以前にも，大阪大では整数解に関する問題が出題されていた．

練習 37

次の条件 (イ)，(ロ) を同時に満たす整数 a, b の組 (a, b) をすべて求めよ．

(イ) 2 次方程式 $X^2 + aX + b = 0$ の 2 つの解が共に 2 以上の整数である．

(ロ) 不等式 $3a + 2b \leq 0$ が成り立つ

[96 大阪大 (前) 理]

ヒントと略解

2つの整数解を α, β とおいて、解と係数の関係を利用し、 $3\alpha + 2\beta \leq$ の大小関係から α, β の範囲を絞り込めばよい。前問と全く同じ発想である。

4.4 フェルマーの小定理

フェルマー (Fermat, Pierre de 1601~1655 フランス) の名前は、1994年にプリンストン大学の A. ワイルズが 350 年以上未解決だった世紀の難問『フェルマーの最終定理』を証明したことによって一躍有名になった。『フェルマーの最終定理』とは、

$n \geq 3$ のとき、 $x^n + y^n = z^n$ を満たす自然数の組 (x, y, z) は存在しない

というものである。フェルマーは 1630 年ごろ、自分が勉強中の本の片隅に「そのことについて真に驚嘆すべき証明を発見したが、余白が狭すぎて書けない」というメモを残し、この世を去ってしまった。

以来、フェルマーの幻の証明を完成させようと数多くの数学者が挑戦したが、誰も証明数することができず、350 年後の A. ワイルズの登場を待たねばならなかった。

『フェルマーの最終定理』は、その結果を使って何か新しいことができる、という定理ではない。過去の数学者の証明しようという 350 年間の努力の中から、新しい数学的アイデアや発見がたくさん生まれ、数学が大きく発展したことが『フェルマーの最終定理』が我々にもたらした最大の収穫であった。結果的に 350 年以上も要したものの、決して無駄な 350 年間ではなかった。なお、証明の核心部分には、谷山豊、志村五郎という 2 人の日本人数学者のアイデアが用いられていることは、我々日本人が誇りに思っていきたいことだと思う。核心部分に用いられた『谷山 = 志村予想』とよばれるアイデアは、若くして自ら命を絶った谷山と、その谷山の意味を受け継ぎ、谷山の業績を世界に紹介した志村との友情の証である。

注 20

『フェルマーの最終定理』に関する参考文献を紹介しておく。興味のある人はぜひ読んでほしい。

・「フェルマーの最終定理」(サイモン・シン著 青木薫 訳 新潮文庫)

・「天才数学者たちが挑んだ最大の難問」(アミール・D・アグゼル著 吉永良正 訳 早川書房)

さて、ここで紹介する『フェルマーの小定理』とは『最終定理』と区別する意味で『小定理』と呼ばれているが、決して「小さい」定理ではなく、応用範囲の広い立派な定理である。ごく稀に、これをテーマにした入試問題が出題されるが、別に知らなくても、これまでに学習した整数問題の攻略を利用すれば解ける問題ばかりなので、整数論に特別興味がある人以外は無視して構わないだろう(ちなみに、最近の出題としては 2006 年に慶応大(総合政策)で『小定理』の証明問題が出題されたが、わかりにくい問題設定で、かえって混乱を生じた)。

『フェルマーの小定理』とは次のようなものである。

フェルマーの小定理

p を素数とすると、 p と互いに素な任意の整数 a に対して、

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

が成立する。

一応、これまでに学習したことだけを使って『フェルマー (Fermat) の小定理』を 2 通りの方法で証明しておく(別に理解できなくても構わない)。

証明

その

p は a と互いに素だから「整数問題の基本定理」より、相異なる $p-1$ 個の整数

$$1a, 2a, 3a, \dots, (p-1)a$$

を p で割った余り全体は、 1 から $p-1$ までの全ての整数である。つまり、 2 つの集合

$$S = \{1a, 2a, 3a, \dots, (p-1)a\}$$

$$T = \{1, 2, 3, \dots, p-1\}$$

は $\text{mod } p$ で集合として完全に一致する。したがって、それぞれの要素の積を考えると、

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

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

$(p-1)!$ は p の倍数でないので、

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

その

二項定理より、

$$(x+y)^p = {}_p C_0 x^p y^0 + {}_p C_1 x^{p-1} y^1 + {}_p C_2 x^{p-2} y^2 + \dots + {}_p C_{p-1} x^1 y^{p-1} + {}_p C_p x^0 y^p$$

$$= x^p + {}_p C_1 x^{p-1} y^1 + {}_p C_2 x^{p-2} y^2 + \dots + {}_p C_{p-1} x^1 y^{p-1} + y^p$$

ここで、 ${}_p C_k$ ($k = 1, 2, \dots, p-1$) は p の倍数だから、

$$(x+y)^p \equiv x^p + y^p \pmod{p}$$

また、これを利用すれば、

$$(x+y+z)^p = ((x+y)+z)^p$$

$$\equiv (x+y)^p + z^p \pmod{p}$$

$$\equiv x^p + y^p + z^p \pmod{p}$$

も成立する。したがって、同様にして、任意の a 個の整数についても成立する。

$$(x_1 + x_2 + \dots + x_a)^p \equiv x_1^p + x_2^p + \dots + x_a^p \pmod{p}$$

ここで、 $x_1 = x_2 = \dots = x_a = 1$ とすれば、

$$\underbrace{(1+1+\dots+1)^p}_{a \text{ 個}} \equiv \underbrace{1+1+\dots+1}_{a \text{ 個}} \pmod{p}$$

$$\therefore a^p \equiv a \pmod{p}$$

a と p は互いに素であるので、

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

注 21

証明 その の最後の式を『フェルマーの小定理』とする場合もあり、むしろ、この形のほうが実戦的である。すなわち、

p を素数とすると、任意の自然数 a に対して、

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

が成立する。

なお、この場合、 a は素数 p と互いに素である必要はないことに注意しよう。

それでは『フェルマーの小定理』に関する入試問題を紹介しよう。

例 42

$n^5 - n$ は 30 の倍数であることを示せ。

[04 京教大 (後)]

ヒントと略解

まず、フェルマーの小定理より、 $n^5 - n$ は 5 の倍数。また、 $n^5 - n = n(n^2 - 1)(n^2 + 1) = n(n+1)(n-1)(n^2 + 1)$ と変形でき、 $n(n+1)(n-1)$ は連続 3 整数の積だから 6 の倍数。よって $n^5 - n$ は 30 の倍数である。

もし、フェルマーの小定理を用いずに、 $n^5 - n$ は 5 の倍数を証明するには、やはり 5 で割った余りによる分類で考えるしかない。つまり、 $n^5 - n = n(n+1)(n-1)(n^2 + 1)$ だから、

$n = 5k$ のとき n が 5 の倍数

$n = 5k + 1$ のとき $n - 1$ が 5 の倍数

$n = 5k + 2$ のとき $n^2 + 1$ が 5 の倍数

$n = 5k + 3$ のとき $n^2 + 1$ が 5 の倍数

$n = 5k + 4$ のとき $n + 1$ が 5 の倍数

となることを確認する。もちろん合同式を利用してよい。

終

練習 38

どんな自然数 n についても $n^7 - n$ は 42 で割り切れることを示せ。

次の例は、違う大学で全く同じ問題が出題された例。

練習 39

- (1) p を素数とするとき、 2^p を p で割った余りを求めよ。 [98 奈女大 (後) 理]
 (2) p を素数とするとき、 $2^{p-1} - 1$ は p で割り切れることを示せ。 [00 図書館情報大 (前)]

ヒントと略解

実際の出題では、それぞれ「 ${}_pC_k$ は p の倍数であることを証明せよ」という問題が最初におかれていた。

次の問題は、フェルマーの小定理の証明がそのまま出題された有名な例。さすがに京大受験者といえども直接の証明は無理と大学側が判断したのか、珍しく「数学的帰納法で」という親切な注意があるものの、結局は ${}_pC_k$ は p の倍数を知らないといけない。

演習問題 16

p を素数とするとき、どんな自然数 n についても $n^p - n$ は p で割り切れることを数学的帰納法で証明せよ。 [77 京都大 文]

4.5 数論的関数

数論的関数とは、整数を定義域にもつ関数のことで、この章では入試でも扱われる代表的な数論的関数を 4 つ紹介する。

まずはじめに紹介する数論的関数は、約数に関する関数であり、これは教科書等でも扱われているように基本的である (証明は省略する)。

約数の個数を表す関数

自然数 N が、 $N = p^\alpha q^\beta r^\gamma \cdots$ と素因数分解されるとき、 N の正の約数の個数は、

$$(\alpha + 1)(\beta + 1)(\gamma + 1) \cdots$$

で表される。

約数の総和を表す関数

自然数 N が、 $N = p^\alpha q^\beta r^\gamma \cdots$ と素因数分解されるとき、 N の正の約数の総和は、

$$(1 + p + p^2 + \cdots + p^\alpha) \times (1 + q + q^2 + \cdots + q^\beta) \times (1 + r + r^2 + \cdots + r^\gamma) \cdots$$

で表される。

例 43

648 の正の約数の個数と、その約数の総和を求めよ。

ヒントと略解

$648 = 2^3 3^4$ であるから、正の約数の個数は $(3 + 1)(4 + 1) = 20$ 個。

約数の総和は $(1 + 2 + 2^2 + 2^3)(1 + 3 + 3^2 + 3^3 + 3^4) = 1815$ 。

例 44

正の整数 n の正の約数の個数を $d(n)$ で表すとき、 $d(n)$ が奇数であることと、 n が平方数であることは同値であることを示せ。 [03 慶応大 (理工)]

ヒントと略解

n の素因数分解を $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ とすれば、 $d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$ となる。

$d(n)$ が奇数

$$\iff (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) \text{ が奇数}$$

$$\iff \alpha_1 + 1, \alpha_2 + 1, \dots, \alpha_k + 1 \text{ が奇数}$$

$$\iff \alpha_1, \alpha_2, \dots, \alpha_k \text{ が偶数}$$

$$\iff n \text{ は平方数}$$

練習 40

a を自然数とし、 a の正の約数すべての和を $S(a)$ で表す。

- (1) p を素数とし, n を自然数とするとき, $S(p^n)$ を求めよ.
- (2) 自然数 a, b が互いに素のとき, $S(ab) = S(a)S(b)$ を示せ. [05 京教大 (後)]

参考問題 26

整数 $n > 1$ が $n = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ と素因数分解されるとき, もし n の正の約数のすべての積が n^2 に等しいならば, n の正の約数の個数は $\boxed{\text{(ア)}}$ 個であり, このときの m は $\boxed{\text{(イ)}}$ または $\boxed{\text{(ウ)}}$ である. [99 東海大 (医)]

これら以外にも

約数の個数に関する問題:

産業医大 (00), 久留米医大 (06), 群馬大 (05 前期)

約数の総和に関する問題:

九州大 (02 前期), 中央大 (04 理工)

などで, 出題されている.

ここから, 残りの 2 つの数論的関数を紹介する.

なお, 京都大学では過去にこれらの関数が出題されたことはないし, 今後も出題の可能性は低いと思われる. なぜなら, この数論的関数は,

一般的な理論は高校の範囲を逸脱するので出題できないから, どうしても具体的な問題になってしまいうこと

証明を理解せず, 単に公式を暗記しているだけの生徒が「~の公式より」と一気に解いてしまうと, その生徒の数学力を正しく判断することができず, 試験としての意味がないこと

などの理由が考えられ, 京都大学の出題精神に反するからである.

したがって, 以下の問題では, あまり細部にはこだわらずに, 読みすすめて欲しい.

$N!$ に含まれる素因数 p を表す関数

N を自然数とし $N! = N(N-1)(N-2) \cdots 3 \cdot 2 \cdot 1$ に含まれる素因数 p の個数は,

$$\left[\frac{N}{p} \right] + \left[\frac{N}{p^2} \right] + \left[\frac{N}{p^3} \right] + \cdots$$

となる.

注 22

上の表記では, 無限和のような形になっているが, 実際には有限和である. つまり, $p^l \leq N < p^{l+1}$ とすると, $\left[\frac{N}{p^{l+1}} \right] = 0$ だから,

$$\left[\frac{N}{p} \right] + \left[\frac{N}{p^2} \right] + \cdots + \left[\frac{N}{p^l} \right]$$

となる.

証明

1 から N までの p の倍数の個数は $\left[\frac{N}{p} \right]$ であり, p^2 の倍数の個数は $\left[\frac{N}{p^2} \right]$ である. したがって, 1 から N までの p の倍数の中で, p^2 の倍数でないものの個数は,

$$\left[\frac{N}{p} \right] - \left[\frac{N}{p^2} \right]$$

である.

同じく, p^2 の倍数の中で, p^3 の倍数でないものの個数は,

$$\left[\frac{N}{p^2} \right] - \left[\frac{N}{p^3} \right]$$

である.

同様に, p^k の倍数の中で, p^{k+1} の倍数でないものの個数は,

$$\left[\frac{N}{p^k} \right] - \left[\frac{N}{p^{k+1}} \right]$$

である.

p, N に対して, $p^l \leq N < p^{l+1}$ となる整数 l が定まり, このとき,

$$\left[\frac{N}{p^{l+1}} \right] = 0$$

だから, $N!$ に含まれる p の指数は,

$$\begin{aligned} & 1 \left(\left[\frac{N}{p} \right] - \left[\frac{N}{p^2} \right] \right) + 2 \left(\left[\frac{N}{p^2} \right] - \left[\frac{N}{p^3} \right] \right) + \\ & \quad \cdots + l \left(\left[\frac{N}{p^l} \right] - \left[\frac{N}{p^{l+1}} \right] \right) \\ &= \left[\frac{N}{p} \right] + \left[\frac{N}{p^2} \right] + \cdots + \left[\frac{N}{p^l} \right] \end{aligned}$$

終

さて、この関数を最も利用するのは次のような問題である。

例 45

30! は 1 桁目から何桁目まで 0 が続く整数であるか。 [06 金沢工大 (工)]

ヒントと略解

10 = 2 × 5 であるから、30! の中に含まれる 2 と 5 の素因数の個数を調べればよいが、明らかに素因数 2 の個数の方が多いので、素因数 5 の個数を調べる。

$\left\lfloor \frac{30}{5} \right\rfloor + \left\lfloor \frac{30}{5^2} \right\rfloor = 6 + 1 = 7$ だから、素因数 5 の個数は 7 個。よって、30! = 10⁷N (N は素因数 5 を含まない整数) となるので、7 桁目まで 0 が続く。

練習 41

1000! を計算したとき、末尾に現れる 0 の個数を求めよ。 [02 岡山理科大 (理工)]

参考問題 27

N を正の整数とする。10 進数で表した n! について、1 の位から 10^{m-1} 位までの数字が全部 0 で、10^m の位が 0 でないとき、関数 f(m) の値を m とする。このとき、次の値を求めよ。

- (1) f(10), f(100)
- (2) $\lim_{n \rightarrow \infty} \frac{f(10^n)}{10^n}$ 。 [91 東工大 (前)]

参考問題 28

n を自然数とする。

- (1) k を n 以下の自然数とする。2ⁿ 以下の自然数のうち 2^k の倍数であるが 2^{k+1} の倍数でないものは全部で何個あるか。
- (2) (2ⁿ)! は 2^{2ⁿ-1} の倍数であるが、2^{2ⁿ} の倍数ではないことを示せ。 [91 東京女子大 (数理)]

オイラー関数 φ(N)

m > 1 のとき、m よりも小さくて m と互いに素な自然数の個数を φ(m) で表す。m = 1 に対しては、φ(1) = 1 と定める。これをオイラー関数という。

オイラー関数には次の性質が成り立つ。

オイラー関数の性質

性質 p を素数とするととき、

$$\varphi(p^k) = p^k - p^{k-1}.$$

特に、φ(p) = p - 1

性質 a, b が互いに素なら、

$$\varphi(ab) = \varphi(a)\varphi(b).$$

上の **性質** については、1 から p^k までの中に、p で割り切れる数が p^{k-1} 個あることから、明らかである。

性質 については、厳密な証明は難しいので具体例で確認することにしよう。「どうしても証明を」という人は初等整数論の本を参考にすること。

最後に、一般的な φ(N) の計算式を導いてみよう。

自然数 N が次のように素因数分解されているとする。

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$$

このとき、p₁^{α₁}, p₂^{α₂}, …, p_n^{α_n} のどの 2 つも互いに素だから、**性質** より、

$$\varphi(N) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \cdots \varphi(p_n^{\alpha_n})$$

次に、**性質** を用いて、

$$\begin{aligned} \varphi(N) &= (p_1^{\alpha_1} - p_1^{\alpha_1-1})(p_2^{\alpha_2} - p_2^{\alpha_2-1}) \cdots \\ &\quad \cdots (p_n^{\alpha_n} - p_n^{\alpha_n-1}) \\ &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \\ &\quad \cdots \left(1 - \frac{1}{p_n}\right) \\ &= N \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_n}\right) \end{aligned}$$

これが、φ(N) の一般的な計算式である。

例 46

60 以下の自然数で 60 と互いに素なものの個数は,
 $60 = 2^2 \times 3 \times 5$ だから,

$$\begin{aligned}\varphi(60) &= 60 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \\ &= 60 \times \frac{1}{2} \times \frac{2}{3} \times \frac{4}{5} \\ &= 16 \text{ 個}\end{aligned}$$

である.

ちなみに, 実際に確認すると, 60 以下で 60 と互いに素な自然数は,

$$1, 7, 11, 13, 17, 19, 23, 29, \\ 31, 37, 41, 43, 47, 49, 53, 59$$

の 16 個である.

注 23

入試で, 一般的なオイラー関数の証明が出題されることはないが, 具体例での証明や, 性質 性質 から導かれる

異なる素数 p, q に対して,

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

の証明が入試で出題されることが多い.

参考問題 29

n を自然数とし, $m \leq n$ で m と n の最大公約数が 1 となる自然数 m の個数を $f(m)$ とする.

- (1) $f(15)$ を求めよ.
- (2) p, q を互いに異なる素数とする. このとき $f(pq)$ を求めよ. [03 名古屋大 (前) 文]

この他にも, オイラー関数の問題は, 横浜市大医 (06 前), 佐賀大 (05 前), 早大 (05 社会科学) 等が出題されている.

注 24

オイラー関数 $\varphi(n)$ に対して, 次のオイラーの定理が成立する. オイラーの定理は RSA 暗号理論などにも応用される重要な定理である.

オイラーの定理

n と互いに素な任意の整数 a に対して,

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

が成立する.

p を素数とすると, $\varphi(p) = p-1$ だから, オイラーの定理で $n = p$ とした場合が, フェルマーの小定理である. オイラーの定理の証明はフェルマーの小定理の証明とほとんど同じであるが, いちおう紹介しておこう.

証明

1 から n までの整数で n と互いに素な数を

$$r_1, r_2, \dots, r_{\varphi(n)}$$

と表す. さらにこれらの数に a をかけたもの

$$ar_1, ar_2, \dots, ar_{\varphi(n)}$$

を考える. a と r_i が n と互いに素だから, ar_i と n は互いに素である. また, $ar_1, ar_2, \dots, ar_{\varphi(n)}$ はそれぞれ n を法として合同ではありえない. 実際,

$$ar_i \equiv ar_j \pmod{n}$$

ならば,

$$a(r_i - r_j) \equiv 0 \pmod{n}$$

ここで, n と a が互いに素なので,

$$r_i - r_j \equiv 0 \pmod{n}$$

$$r_i \equiv r_j \pmod{n}$$

すなわち, $i = j$ となるからである.

n と互いに素な数は, $r_1, r_2, \dots, r_{\varphi(n)}$ のどれか 1 つと合同になるので, $ar_1, ar_2, \dots, ar_{\varphi(n)}$ の順序を適当に入れ替えたものが, $r_1, r_2, \dots, r_{\varphi(n)}$ とそれぞれ合同になる. したがって, それらを掛け合わせたものも合同になる. 即ち,

$$ar_1 \cdot ar_2 \cdots ar_{\varphi(n)} \equiv r_1 \cdot r_2 \cdots r_{\varphi(n)} \pmod{n}$$

$$(a^{\varphi(n)} - 1)r_1 \cdot r_2 \cdots r_{\varphi(n)} \equiv 0 \pmod{n}$$

ここで, $r_1, r_2, \dots, r_{\varphi(n)}$ が n と互いに素であることから,

$$a^{\varphi(n)} - 1 \equiv 0 \pmod{n}$$

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

が成立する．

終

4.6 整数値多項式

全ての整数 n に対して $f(n)$ が整数になる多項式 $f(x)$ を整数値多項式と呼ぶことにする．

整数値多項式に関する問題は入試では頻出であるが、ほとんどが、2 次式、3 次式での具体的な場合である（京都大でも、過去に 3 次式の場合が 1 度だけ出題されただけ）．一般の n 次式の場合は、最後に参考問題として紹介する東京大の問題があるが、極めて難しいので、理解できなくても構わない．この章では、2 次式、3 次式の具体例を中心に話を進めるが、一般の n 次式の整数値多項式についても触れている．そこは無理せず、読み飛ばしても構わない．なお、整数値多項式では係数は一般に整数とは限らないことを最初に確認しておく（係数が整数だったら意味がない．係数が整数でないにも係わらず、全ての整数で整数値をとることが重要でなのである）．

まずは、整数値多項式の簡単な入試問題から始めよう．

例 47

$$f(x) = x^2 + ax + b \text{ とする．}$$

- (1) すべての整数 n に対して $f(n)$ が整数であるとする．このとき、 a, b は整数であることを示せ．
- (2) すべての整数 n に対して、 $f(n)$ が偶数となるための a, b の条件を求めよ．

[99 津田塾大 (国際)]

ヒントと略解

「すべての整数で成立する」ことから、まずは特定の整数でチェックし a, b を f を用いて表すことを考える．

整数値多項式で最も重要な性質は次のことである．

整数値多項式の重要性質

n を自然数、 $f(x)$ を n 次の多項式とする． $f(0), f(1), \dots, f(n)$ がすべて整数ならばすべての整数 m に対して、 $f(m)$ は整数になる．つまり、 $f(x)$ は整数値多項式である．

なお、この重要性質が、先日行われた東京工大の AO 入試 (2007 年 11 月 24 日実施) でそのまま出題された．東工大では 1993 年にも全く同じ問題が出題されている．この証明は重要なので後ほど紹介する．

この重要性質 から、次の重要性質 がわかる．

整数値多項式の重要性質

n を自然数、 $f(x)$ を n 次の多項式とする．連続する $n+1$ 個の整数 $l, l+1, \dots, l+n$ について $f(l), f(l+1), \dots, f(l+n)$ がすべて整数ならばすべての整数 m に対して、 $f(m)$ は整数になる．つまり、 $f(x)$ は整数値多項式である．

証明

$h(x) = f(x+l)$ とおくと、 $h(x)$ は n 次多項式で、 $h(0), h(1), \dots, h(n)$ はすべて整数になるので、すべての整数 m に対して、 $h(m)$ は整数になる．つまり、すべての整数 m に対して、 $f(m)$ も整数になるので、 $f(x)$ は整数値多項式である．

終

注 25

当然ながら、整数値多項式の重要性質 は逆も成り立つ．

さて、重要性質 は、例えば $f(x)$ が 2 次式なら、連続 3 整数で $f(x)$ の値が整数になれば、全ての整数で $f(x)$ の値は整数になることを意味している．

これも入試では主に 2 次式、3 次式の場合の出題が多く、宮崎大学では上の性質の 2 次式の場合がそのまま出題された．

例 48

実数 a, b, c について, $f(x) = ax^2 + bx + c$ とおく. $f(0), f(1), f(2)$ がいずれも整数であるとき, 次の各問いに答えよ.

- (1) $2a, 2b$ はいずれも整数であることを示せ.
- (2) すべての整数 n について, $f(n)$ は整数であることを示せ. [03 宮崎大 (前)]

ヒントと略解

整数多項式の証明のポイントを, この問題を使って解説する.

まず, $f(0) = k, f(1) = l, f(2) = m$ とおく. このとき,

$$\begin{cases} f(0) = c & = k \\ f(1) = a + b + c & = l \\ f(2) = 4a + 2b + c & = m \end{cases}$$

この実数 a, b, c についての連立方程式をとき, 実数 a, b, c を, 整数 k, l, m を用いて表すと,

$$a = \frac{m + k - 2l}{2}, \quad b = \frac{4l - 3k - m}{2}, \quad c = k$$

となる. 与式に代入して, k, l, m で整理する.

$$\begin{aligned} f(n) &= \frac{m + k - 2l}{2}n^2 + \frac{4l - 3k - m}{2}n + k \\ &= m\frac{n(n-1)}{2} + k\frac{(n-1)(n-2)}{2} - ln(n-2) \end{aligned}$$

$n(n-1), (n-1)(n-2)$ は連続 2 整数の積なので偶数. よって, $\frac{n(n-1)}{2}, \frac{(n-1)(n-2)}{2}$ は整数だから, すべての整数 n に対して, $f(n)$ は整数になる.

注 26

上の例では, 整数問題として扱うために, 実数 a, b, c から整数 k, l, m へ, 主体を移していることを意識しよう.

練習 42

$f(x) = ax^3 + bx^2 + cx$ は, $x = 1, -1, -2$ で整数値 $f(1) = r, f(-1) = s, f(-2) = t$ をとるとする.

- (1) a, b, c を r, s, t の式で表せ.
- (2) すべての整数 n について, $f(n)$ は整数になることを示せ. [03 岡山大 (前)]

ヒントと略解

先の例題の 3 次式版. まったく同様である. ちなみに, 3 次式だから連続 4 整数値を設定せねばならないのに, 3 つしかない... と思うかもしれないが, $x = 0$ のときに整数値になることは自明なので, 始めから省略しているのである.

このように, 2 次式や 3 次式の場合は, 多少計算が煩雑になるが, 上記の方法で解決できる. しかし, より高い次数や一般の n 次の整数値多項式を扱うときは, この方法では限界がある.

そこで, 次の重要性質 が利用される.

整数値多項式の重要性質

$f(x)$ が整数値多項式

\iff ある整数 k について $f(k)$ が整数で, $f(x+1) - f(x)$ は整数値多項式である.

証明

(\implies) は明らか.

(\impliedby) について. ある整数 k で $f(k)$ が整数で, $f(x+1) - f(x)$ は整数値多項式であることから, $f(k+1) - f(k)$ も整数となり, $f(k), f(k+1)$ はともに整数. よって, これを繰り返すことで, すべての整数 m に対して $f(m)$ は整数となる. したがって, $f(x)$ は整数値多項式である.

終

注 27

$f(x)$ は n 次式だと, $f(x+1) - f(x)$ は $n-1$ 次で, 次数が 1 つ下がることに注意しよう.

この重要性質が 2 次式の場合にそのまま出題された例が次の問題である.

練習 43

多項式 $f(x) = ax^2 + bx + c$ について考える． $f(x)$ が整数値であるとは， x が整数のとき $f(x)$ が常に整数になることである．

- (1) $a = 0$ とする． $f(x) = bx + c$ が整数値であるための必要十分条件は， b, c が共に整数であることを証明せよ．
- (2) 2 つの条件
 $() f(0)$ が整数である．
 $()$ 多項式 $f(x+1) - f(x)$ が整数値である．
 が成り立てば， $f(x)$ が整数値になることを示せ．必要なら数学的帰納法を利用せよ．逆に $f(x)$ が整数値であるとき， $()$ ， $()$ が成り立つことを示せ．
- (3) $f(x) = ax^2 + bx + c$ が整数値であるための a, b, c が満たすべき条件を求めよ．

[00 広島大 (前) 理]

この問題の証明方法は，そのまま一般の n 次式の場合にも適用される．

それでは，この証明方法を参考にして，いよいよ最初に紹介した東工大の AO 入試問題 (2007 年) の証明に入ろう．整数問題の証明というよりは数学的帰納法の証明であるが，これまで学習した，整数値多項式の重要性質を用いているので，そなお，1993 年前期に出題されたときは，「 n 次の多項式」となっていた以外は，問題文は全く同じであった．

整数値多項式の重要性質 の証明

n を自然数， $P(x)$ を n 次多項式とする． $P(0), P(1), \dots, P(n)$ が整数ならばすべての整数 k に対して， $P(k)$ は整数であることを証明せよ．

[07 東工大 AO]

証明

n 次多項式 $P(x)$ に対して， $P(0), P(1), \dots, P(n)$ が整数ならばすべての整数 k に対し， $P(k)$ は整数 \dots であることを次数 n に関する数学的帰納法で証明する．

$n = 1$ のとき

$P(x) = ax + b$ とおける．いま， $P(0) = b, P(1) = a + b$ はともに整数であるので，

$$a = P(1) - P(0), \quad b = P(0)$$

も整数である．よって，すべての整数 k に対し， $P(k) = ak + b$ は整数であるから， \quad が示された．

$n = m(m \geq 1)$ のとき， \quad が成立すると仮定する．いま， $Q(x)$ を $m+1$ 次多項式で

$$Q(0), Q(1), \dots, Q(m+1) \text{ は整数} \dots$$

を満たすものとする．

$$\begin{aligned} & Q(x+1) - Q(x) \\ &= \{a(x+1)^{m+1} + \dots\} - (ax^{m+1} + \dots) \\ &= (m \text{ 次式}) \end{aligned}$$

であるから， m 次多項式 $P(x)$ を用いて，

$$Q(x+1) - Q(x) = P(x) \dots$$

と表せる．すると より，

$$P(0), P(1), \dots, P(m) \text{ は整数}$$

であるから，帰納法の仮定 より，すべての整数 k に対し， $P(k)$ は整数である．

よって， より， $Q(l)$ が整数ならば，

$$Q(l+1) = P(l) + Q(l), \quad Q(l-1) = Q(l) - P(l-1)$$

はともに整数である．これと， $Q(0)$ が整数であることより，帰納的に，すべての整数 k に対し， $Q(k)$ は整数である．したがって， $n = m+1$ のときもが成り立つ．

以上より， \quad が成り立つことが示された．

終

参考問題 30

整式 $h(x)$ が「すべての整数 n に対して $h(n)$ は整数である」という条件をみたすとき， $h(x)$ は整数値多項式であるという．

- (1) $f(x)$ が整数値多項式であるとき，整式 $g(x) = f(x+1) - f(x)$ も整数値多項式であることを示せ．

- (2) $f(x)$ が 2 次の整数値多項式であるとき, $f(x)$ の x^2 の係数の 2 倍は整数であることを示せ .
- (3) $f(x)$ が 3 次の整数値多項式であるとき, $f(x)$ の x^3 の係数の 6 倍は整数であることを示せ .
- (4) m が自然数で, $f(x)$ が m 次の整数値多項式であるとき, $f(x)$ の x^m の係数の $m!$ 倍は整数であることを示せ . [05 京教大 (後)]

上の問題の最後の問 (4) の内容, 「 $f(x)$ が m 次の整数値多項式であるとき, $f(x)$ の x^m の係数の $m!$ 倍は整数である」ということは, 整数値多項式の重要な性質であり, このことは次の重要な事実に基づく .

多項式の重要性質

$g_k(x)$ を

$$g_0(x) = 1$$

$$g_1(x) = x$$

$$g_k(x) = \frac{1}{k!} x(x+1) \cdots (x+k-1) \quad (k = 2, 3, \dots)$$

とおくと, $g_k(x)$ は整数値多項式で, 任意の n 次多項式 $f(x)$ は適当な定数 $a_0, a_1, a_2, \dots, a_n$ を用いて,

$$f(x) = \sum_{k=0}^n a_k g_k(x)$$

の形で書き表すことができる .

証明

$x(x+1) \cdots (x+k-1)$ は x が整数のとき, 連続する k 整数の積となるので $k!$ の倍数である . したがって, $g_k(x)$ は k 次の整数値多項式である .

任意の n 次多項式 $f(x)$ を n 次多項式 $g_n(x)$ で割ると,

$$f(x) = a_n g_n(x) + h_{n-1}(x)$$

$h_{n-1}(x)$ は $n-1$ 次以下の多項式である . さらに, $h_{n-1}(x)$ を $g_{n-1}(x)$ で割ると,

$$h_{n-1}(x) = a_{n-1} g_{n-1}(x) + h_{n-2}(x)$$

$h_{n-2}(x)$ は $n-2$ 次式以下の多項式である . よって,

$$f(x) = a_n g_n(x) + a_{n-1} g_{n-1}(x) + h_{n-2}(x)$$

これを順次繰り返すことにより,

$$f(x) = \sum_{k=0}^n a_k g_k(x)$$

の形で書き表すことができる .

終

このことは, つまり, どんな多項式も, $g_k(x)$ という整数値多項式 (の線形結合の形) で書き表せるということを主張する . $g_k(x)$ という整数値多項式は, 整数値多項式問題の根幹部分をなす重要な多項式である .

ここから次の重要性質 が導かれる .

整数値多項式の重要性質

$f(x)$ が n 次の整数値多項式ならば, 適当な整数 $a_0, a_1, a_2, \dots, a_n$ を用いて,

$$f(x) = \sum_{k=0}^n a_k g_k(x)$$

の形で書き表すことができる .

証明

次数 n に関する帰納法で証明する .

$n = 1$ のとき

$f(x) = ax + b$ とおける . いま, $f(0) = b, f(1) = a + b$ はともに整数であるので,

$$a = f(1) - f(0), \quad b = f(0)$$

も整数である . よって, $f(x) = (f(1) - f(0))x + f(0)$ とかけるので, $n = 1$ のときは成立する .

$n = k - 1$ のとき, 成立すると仮定する (つまり任意の $k - 1$ 次の多項式は題意の形に書き表せると仮定する) .

このとき, $n = k$ のときを考える .

k 次の整数値多項式 $f(x)$ の最高次の係数が A のとき, $a_k = Ak!$ と a_k を定めると, $f(x) - a_k g_k(x)$ は最高次の係数が消去され, $(k - 1)$ 次以下の多項式になる .

$f(x) - a_k g_k(x)$ は, x に連続する k 個の整数

$$-(k-1), -(k-2), \dots, 0$$

を代入すると, 整数値をとるので ($\because x(x)$ はもともと整数値多項式だし, $a_k g_k(x)$ の部分は 0 になる), $f(x) - a_k g_k(x)$ は $k-1$ 次の整数値多項式になる (\because 重要性質). よって, $n = k-1$ の仮定より, 適当な整数 $a_0, a_1, a_2, \dots, a_{k-1}$ を用いて,

$$f(x) - a_k g_k(x) = \sum_{j=0}^{k-1} a_j g_j(x) \quad \dots$$

の形で書き表すことができる. ここで, $x = 1$ を代入すると, $g_k(1) = 1$ より,

$$f(1) - a_k = \sum_{j=0}^{k-1} a_j g_j(1)$$

両辺は整数だから, a_k も整数である. よって, を移項して

$$f(x) = \sum_{j=0}^k a_j g_j(x)$$

したがって, $n = k$ のときも成立する.

以上より, 全ての自然数 n で題意は成立する.

終

注 28

当然ながら, 整数値多項式の重要性質 は逆も成り立つ.

この重要性質 より, n 次の整数値多項式の x^n の係数は, a_n を整数として, $\frac{a_n}{n!}$ である. 先程の、

05 京教大 (後) 問 (4) の問題はこのことであった. また, 京都大でも, この重要性質 が出題されている. 総合問題演習 2 を参照せよ.

ここで, かなり煩雑になってきたので, これまでの結果をまとめておこう.

整数値多項式の重要性質 (まとめ)

$f(x)$ を n 次以下の (複素係数の) 整式とするとき, 次の各条件はすべて同値である.

- (1) $f(k)$ が整数値多項式
- (2) $f(0), f(1), \dots, f(n)$ がすべて整数
- (3) $f(l), f(l+1), \dots, f(l+n)$ がすべて整数となるような整数 l が存在する.
- (4) ある整数 k について $f(k)$ が整数で, $f(x+1) - f(x)$ は整数値多項式である.
- (5) 次の式をみたす整数 $a_0, a_1, a_2, \dots, a_n$ が存在する.

$$f(x) = \sum_{k=0}^n a_k g_k(x)$$

参考問題 31

実数 a, c に対し, $f(x) = ax^2 + 4x + c$ とおく. このとき, $k = 1, 2$ に対して次の命題を考える.

$P(k)$: 『すべての整数 n に対して, $f(n)$ は整数の k 乗となる』

- (1) $P(1)$ が成り立つための必要十分条件は, a, c がともに整数であることを示せ.
- (2) a が正の整数であることは, $P(2)$ が成り立つための必要条件であることを示せ.
- (3) $P(2)$ が成り立つための必要十分条件は, $a = 4, c = 1$ または $a = 1, c = 4$ であることを示せ. [02 札幌医科大学 (前)]

参考問題 32

k を正整数とし, x を変数とする k 次多項式 $P_k(x)$ について, 次の条件

$$(C) \quad \begin{cases} P_k(x) - P_k(x-1) = x^{k-1} \\ P_k(0) = 0 \end{cases}$$

を考える. ただし, $x^0 = 1$ と定める. このとき, 次の問いに答えよ.

- (1) $k = 1, 2$ に対し, $P_k(x)$ を求めよ.

- (2) すべての $k \geq 3$ に対し, 条件 (C) をみたす $P_k(x)$ が存在し, しかもただ一つであることを示せ.
- (3) 正整数 k に対し, k 次の多項式 $Q_k(x)$ を次の条件が成立するように定める.

$$\begin{cases} Q_k(x) = Q_k(1) = \cdots = Q_k(k-1) = 0 \\ Q_k(k) = 1 \end{cases}$$

このとき, k 個の整数 c_1, c_2, \dots, c_k がそれぞれただ一つ存在して, $P_k(x) = \sum_{j=1}^k c_j Q_j(x)$ で表されることを示せ.

[00 東京大 (後) 理]

ヒントと略解

$P_k(x) = a_k x^k + a_{k-1} x^{k-1} + \cdots + a_0$ において, (C) の条件式に代入して両辺の係数比較をすると, a_k, a_{k-1}, \dots, a_1 の順に係数が一意的に定まる.

$P_k(0) = 0$ なので, $a_0 = 0$ である. また, x が整数で,

$$x \geq 0 P_k(x) = P_k(0) + \sum_{j=1}^x \{P_k(j) - P_k(j-1)\}$$

$$x < 0 P_k(x) = P_k(0) - \sum_{j=x+1}^0 \{P_k(j) - P_k(j-1)\}$$

とかけるので, $P_k(x)$ は任意の整数 x について整数値をとる関数である.

$$Q_m(x) = \frac{x(x-1) \cdots (x \bmod + 1)}{m!} \quad (m \text{ は自然数})$$

となるが, これは, 先程の重要性質 の $f(x)$ を $P_k(x)$ に, $g_k(x)$ を $Q_m(x)$ に読み替えればそのまま証明になっている.

4.7 総合演習問題

～ 京大整数問題ベスト 11 ～

1

2007 年文理共通

p を 3 以上の素数とする. 4 個の整数 a, b, c, d が次の 3 条件

$$a + b + c + d = 0,$$

$$ad - bc + p = 0,$$

$$a \geq b \geq c \geq d$$

を満たすとき, a, b, c, d を p を用いて表せ.

Comment & Hint

まだ記憶に新しい昨年度の問題. ようするに a, b, c, d についての連立方程式を解け, ということ. しかし, 連立方程式は文字の数と式の数的一致していれば完璧に解けるが, この場合は一致していない. しかし a, b, c, d は整数であることと, a, b, c, d の大小関係を利用することで, 解の範囲を絞り込むことができる. p が 3 以上の素数であることも関係している. 「整数問題の大原則」に書かれていることだけを用いれば正解できるだろう.

2

1990 年前期文理共通

三角形 ABC において, $\angle B = 60^\circ$, B の対辺の長さ b は整数, 他の 2 辺の長さ a, c はいずれも素数である. このとき三角形 ABC は正三角形であることを示せ.

Comment & Hint

図形と整数との融合問題. まずは, 三角形に関する知っている公式を手当たり次第に (といっても正弦, 余弦定理くらいしかないと思うが) つくることだろう. そして「整数問題の大原則」を利用する. 三角形の成立条件を忘れないように.

3 1999 年前期文系

0 以上の整数 x に対して, $C(x)$ で x の下 2 桁を表すことにする. たとえば, $C(12578) = 78$, $C(6) = 6$ である. n を 2 でも 5 でも割り切れない正の整数とする.

- (1) x, y が 0 以上の整数のとき, $C(nx) = C(ny)$ ならば, $C(x) = C(y)$ であることを示せ.
- (2) $C(nx) = 1$ となる 0 以上の整数 x が存在することを示せ.

Comment & Hint

「整数問題の基本定理」の証明方法を真似ればよいのだが, 文系の問題としては少しキビシイだろう. (1) は背理法を用いるのが良いだろう. (2) は (1) がヒントになってはいるが, (1) をどのように利用するのなかなか思いつかない.

4 2000 年前期理系

p を素数, a, b を互いに素な正の整数とすると, $(a + bi)^p$ は実数でないことを示せ. ただし i は虚数単位を表す.

Comment & Hint

Symple だが、なかなか難問. とりあえず, 二項定理で展開して, 実部と虚部に分解することから始めよう. やはり京大の場合, 「 ${}_pC_k$ は p の倍数」は常識としているようだ.

5 京都大学 1995 年後期文系

自然数 n の関数 $f(n), g(n)$ を

$f(n) = n$ を 7 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.

Comment & Hint

京大のセンスが光る, 実にユニークな問題である. 単なる型破りなパズル的な問題ではない良問. 「周期性」に気付くかどうか. とにかくひたすら実験しよう.

6 1996 年後期文系

n は 2 以上の自然数, p は素数, a_0, a_1, \dots, a_{n-1} は整数とし, n 次式

$$f(x) = x^n + pa_{n-1}x^{n-1} + \dots + pa_ix^i + \dots + pa_0$$

を考える.

- (1) 方程式 $f(x) = 0$ が整数解 α を持てば, α は p で割り切れることを示せ.
- (2) a_0 が p で割り切れなければ, 方程式 $f(x) = 0$ は整数解を持たないことを示せ.

Comment & Hint

(2) は対偶をとる. (1) を利用して証明できる.

なお, 整数問題の攻略 (応用編) の, 有理数解をもつ方程式の章を参考にすること.

7 1988 年 B 日程文系

$f(x) = ax^3 + bx^2 + cx$ を x の 3 次式とする．すべての整数 n に対して $f(n)$ が整数になるための必要十分条件は適当な整数 p, q, r をとると，

$$f(x) = \frac{p}{6}x(x+1)(x+2) + \frac{q}{2}x(x+1) + rx$$

と表されることであることを示せ．

Comment & Hint

十分性はほとんど明らかであるから，必要性をどう示すかがポイント．特定の整数に注目するのが良いだろう．

なお，整数問題の攻略（応用編）の，整数値多項式の章を参考にする．

8 2000 年後期理系

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 $a \geq 2$ 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 1 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．

Comment & Hint

まず， a と $a^2 + 1$ が互いに素であることを証明せねばならない．

次からの 3 問は，1990 年前後にだけ出題された幻の難問「後期理学部専用問題」である．

9 1991 年後期理系（理学部専用問題）

整数を係数とする 3 次多項式 $f(x)$ が次の条件 (*) をみたしている．

(*) 任意の自然数 n に対し， $f(n)$ は $n(n+1)(n+2)$ で割り切れる．

このとき，ある整数 a があって， $f(x) = ax(x+1)(x+2)$ となることを示せ．

Comment & Hint

$f(n)$ が $n(n+1)(n+2)$ で割り切れるから， $f(x)$ が $x(x+1)(x+2)$ で割り切れる，つまり $f(x) = ax(x+1)(x+2)$ となるのは当たり前じゃないのか，と思うかもしれないが，そうではない．整数の割り算と整式の割り算を混同してはいけない（例えば， $f(x) = x(x+1)(x+2) + 12x$ のとき， $f(x)$ は $x(x+1)(x+2)$ で割り切れないが $f(1) = 18$ は $1(1+1)(1+2) = 6$ で割り切れるし， $f(2) = 48$ は $2(2+1)(2+2) = 24$ で割り切れる！）．最初に $f(x)$ をどのように設定するのがポイントである．

なお，整数問題の攻略（応用編）の，整数値多項式の章を参考にする．

10 1989 年後期理系（理学部専用問題）

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 $O(0, 0)$ ， $A(a, b)$ ， $B(a, b+1)$ ， $C(0, 1)$ 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) の格子点全体を P_1, P_2, \dots, P_t とするとき， $\triangle OP_i A$ ($i = 1, 2, \dots, t$) の面積のうちの最小値を求めよ．ただし $a > 1$ とする．

Comment & Hint

格子点に関する問題であるが、結局は「整数問題の基本定理」に帰着する。特に (2) は、その証明そのものである。

なお、整数問題の攻略 (応用編) の、格子点の章を参考にする。

11 1990 年後期理系 (理学部専用問題)

- n を奇数とし $f(x) = \left| \sin \frac{2\pi x}{n} \right|$ とする。
- (1) 集合 $\{f(k) \mid k \text{ は整数} \}$ は何個の要素を持つか。
- (2) m を n と素な整数とすると、集合 $\{f(mk) \mid k \text{ は } 0 \leq k \leq \frac{n-1}{2} \text{ なる整数} \}$ は m によらず一定であることを示せ。

Comment & Hint

当時、高校生だった私は、この問題の意味がサッパリ分からず手も足も出なかった！「整数問題の基本定理」の証明方法を真似ればよいが、とにかく難しい。「集合」についての確かな知識と経験が要求されるという点において印象深い問題である。京大の全過去問の中でベスト 5 に入る難問ではないだろうか。

5 京都大学で出題されたその他の整数問題

京都大学では整数問題が頻繁に出題されている。とくに 1988 年以降に多く見られ、1988 年～2007 年の 20 年間で 48 題出題されている。文系理系の内訳は、文系 16 問、理系 29 問、文理共通 3 問で、やや理系の方が多い。

ここでは、これまでに扱うことができなかった、その他の整数問題をまとめて紹介する。

なお、有理数や無理数に関する問題も整数問題として位置づけてることにする。なぜなら有理数を $\frac{q}{p}$ (p, q は互いに素) と設定すれば、整数問題として扱うことができるからである。また、本質的に整

数問題ではない問題でも、整数 (自然数) を扱う問題に関する限り全て収録した。

5.1 図形との融合問題

まず、図形との融合問題を紹介する。「整数問題」と「図形問題」は相反する気がするが、図形的性質を数式化することで、代数的な問題と解釈できる。

1 2000 年前期文系

三角形 ABC において、辺 BC, CA, AB の長さをそれぞれ a, b, c とする。三角形 ABC は次の条件 (イ), (ロ), (ハ) を満たすとする。

(イ) とともに 2 以上である自然数 p と q が存在して、 $a = p + q, b = pq + p, c = pq + 1$ となる。

(ロ) 自然数 n が存在して a, b, c のいずれかは 2^n である。

(ハ) $\angle A, \angle B, \angle C$ のいずれかは 60° である。

(1) $\angle A, \angle B, \angle C$ を大きさの順に並べよ。

(2) a, b, c を求めよ。

2 2000 年後期文系

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。

(1) 格子点を頂点とする三角形の面積は $\frac{1}{2}$ 以上であることを示せ。

(2) 格子点を頂点とする凸四角形の面積が 1 であるとき、この四角形は平行四辺形であることを示せ。

5.2 数列・漸化式の問題

漸化式の問題は本質的に数列分野に属するが、数列の各項が整数の場合は整数問題として扱うことにした。

1 1997 年前期理系

自然数 n と n 項数列 $a_k (1 \leq k \leq n)$ が与えられていて、次の条件 (イ), (ロ) を満たしている。

(イ) $a_k (1 \leq k \leq n)$ はすべて正整数で、すべて 1 と $2n$ の間にある。 $1 \leq a_k \leq 2n$ 。

(ロ) $s_j = \sum_{k=1}^j a_k$ とおくと、 $s_j (1 \leq j \leq n)$ はすべて平方数である。(整数の 2 乗である数を平方数という。)

このとき、

(1) $s_n = n^2$ であることを示せ。

(2) $a_k (1 \leq k \leq n)$ を求めよ。

2 1996 年前期理系

与えられた自然数 k に対し、数列 $\{a_n\}$ を、 $a_1 = 0, a_n = \left\lceil \frac{a_{n-1} + k}{3} \right\rceil (n \geq 2)$ によって定める。ただし、実数 t に対し $[t]$ は t を越えない最大の整数を表す。

(1) $k = 8$ および $k = 9$ のとき、数列 $\{a_n\}$ を求めよ。

(2) すべての自然数 n に対し、次の 2 つの不等式 $a_n \leq \frac{k-1}{2}, a_n \leq a_{n+1}$ が成り立つことを示せ。

(3) $a_n = a_{n+1}$ ならば、 n 以上のすべての整数 m に対し $a_n = a_m$ であることを示し、このときの a_n の値を求めよ。

3 1995 年前期文系

数列 $\{a_n\}$ を、 $a_n = -an^2 + bn + c$ ($n = 1, 2, 3, \dots$) によって定める。このとき、次の 2 つの条件 (イ), (ロ) をみたす自然数 a, b, c を求めよ。

(イ) $4, x_1, x_2$ はこの順で等差数列である。

(ロ) すべての自然数 n に対して $\left(\frac{x_n + x_{n+1}}{2}\right)^2 \geq x_n x_{n+1} + 1$ が成り立つ。

4 1992 年前期理系

a_1, b_1, c_1 は正の整数で、 $a_1^2 + b_1^2 = c_1^2$ を満たしている。 $n = 1, 2, \dots$ について、 $a_{n+1}, b_{n+1}, c_{n+1}$ を次式で決める。

$$a_{n+1} = |2c_n - a_n - 2b_n|$$

$$b_{n+1} = |2c_n - 2a_n - b_n|$$

$$c_{n+1} = 3c_n - 2a_n - 2b_n$$

(1) $a_n^2 + b_n^2 = c_n^2$ を数学的帰納法により証明せよ。

(2) $c_n > 0$ および $c_n \geq c_{n+1}$ を示せ。

(3) $c_m > c_{m+1} = c_{m+2}$ となったときの m について、 $a_m : b_m : c_m$ を求めよ。

5.3 格子点の問題 (数列分野)

格子点の問題の中でも、数列分野に属する問題を 2 問あげておく。以下の 2 問は放物線か円かの違いを除けば本質的に全く同じ問題である。

1 1998 年後期理系

a, m は自然数で a は定数とする。 xy 平面内の点 (a, m) を頂点とし、原点と点 $(2a, 0)$ を通る放物線を考える。この放物線と x 軸とで囲まれる領域の面積を S_m 、この領域の内部および境界線上にある格子点の数を L_m とする。このとき、極限值 $\lim_{m \rightarrow \infty} \frac{L_m}{S_m}$ を求めよ。 xy 平面上の格子点とはその点の x 座標と y 座標がともに整数となる点のことである。

2 2004 年後期理系

n を自然数とする。 xy 平面内の、原点を中心とする半径 n の円の、内部と周をあわせたものを C_n であらわす。次の条件 (*) を満たす 1 辺の長さが 1 の正方形の数を $N(n)$ とする。

(*) 正方形の 4 頂点はすべて C_n に含まれ、4 頂点の x および y 座標はすべて整数である。

このとき、 $\lim_{n \rightarrow \infty} \frac{N(n)}{n^2} = \pi$ を証明せよ。

5.4 約数・倍数の問題

ここで取り上げる 2 問は、本編に入れるかどうか迷った問題で、できれば 2 問とも解いて欲しい。

1 1998 年前期理系

$f(x) = x^2 + 7$ とおく。

- (1) n は 3 以上の自然数で、ある自然数 a にたいして $f(a)$ は 2^n の倍数になっているとする。このとき (a) と $f(a + 2^{n-1})$ のうち少なくとも一方は 2^{n+1} の倍数であることを示せ。
- (2) 任意の自然数 n にたいして $f(a_n)$ が 2^n の倍数となるような自然数 a_n が存在することを示せ。

2 1997 年前期文系

自然数 n の約数の個数を d とする。 n の約数すべてを小さい順に並べて得られる数列を a_k ($1 \leq k \leq d$) とする。したがって、 $a_1 = 1, a_d = n, a_k < a_{k+1}$ ($1 \leq k < d$) である。このとき、 n に対する次の 2 つの条件 (イ)、(ロ) は互いに同値 ((イ) \iff (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、 $\frac{1}{a_3} + \frac{1}{a_6} = \frac{1}{a_2}$ となる。

5.5 整式との融合問題

実は、整式との融合問題は難易度最高レベルの問題に属する。どの問題もかなり難しく、文系での問題は見られない。特に後期理系の問題は厳しい。

1 2002 年後期理系

$f(x)$ は x^n の係数がすべて 1 である x の n 次式である。相異なる n 個の有理数 q_1, q_2, \dots, q_n に対して $f(q_1), f(q_2), \dots, f(q_n)$ がすべて有理数であれば、 $f(x)$ の係数はすべて

有理数であることを、数学的帰納法を用いて示せ。

2 1999 年前期理系

以下の問いに答えよ。 $\sqrt{2}, \sqrt{3}, \sqrt{6}$ が無理数であることは使ってよい。

- (1) 有理数 p, q, r について、 $p + q\sqrt{2} + r\sqrt{3} = 0$ ならば、 $p = q = r = 0$ であることを示せ。
- (2) 実数係数の 2 次式 $f(x) = x^2 + ax + b$ について、 $f(1), f(1 + \sqrt{2}), f(\sqrt{3})$ のいずれかは無理数であることを示せ。

3 1999 年後期理系

a, b を整数、 u, v を有理数とする。 $u + v\sqrt{3}$ が $x^2 + ax + b = 0$ の解であるならば、 u と v は共に整数であることを示せ。ただし $\sqrt{3}$ が無理数であることは使ってよい。

4 1996 年後期理系

n は自然数とする。

- (1) すべての実数 θ に対し

$$\cos n\theta = f_n(\cos \theta)$$

$$\sin n\theta = g_n(\cos \theta) \sin \theta$$

をみたし、係数がともにすべて整数である n 次式 $f_n(x)$ と $n - 1$ 次式 g_n が存在することを示せ。

- (2) $f'_n(x) = ng_n(x)$ であることを示せ。

- (3) p を 3 以上の素数とすると、 $f_p(x)$ の $p - 1$ 次以下の係数はすべて p で割り切れることを示せ。

5.6 行列・1 次変換との融合問題

行列・1 次変換との融合問題は、見た目がそれらしく見えるだけで、式変形すれば単なる普通の整数問題であることが多い。以下の問題はいずれも 1 次変換全盛期の前々教育課程の問題であり、1 次変換が復活を遂げた今、一つの指針となるかもしれない。

1 1994 年後期理系

a, b, c, d を整数とし, 行列 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

を考える. $\begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ とし, 自

然数 n に対して, $A^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$ とする.

このとき,

(1) $n \geq 0$ について, $c_{n+2} - (a+d)c_{n+1} + (ad-bc)c_n = 0$ を示せ.

(2) p を素数とし, $a+d$ は p で割り切れないものとする. ある自然数 k について, c_k と c_{k+1} が p で割り切れるならば, すべての n について c_n は p で割り切れることを示せ.

2 1994 年後期文系

a, b, c, d を整数とし, 行列 $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

を考え, 自然数 n に対して, $A^n = \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix}$

とする. このとき,

(1) $c_{n+2} - (a+d)c_{n+1} + (ad-bc)c_n = 0$ を示せ.

(2) p を素数とし, $ad-bc$ は p で割り切れないものとする. ある自然数 k について, c_k と c_{k+1} が p で割り切れるならば, すべての n について c_n は p で割り切れることを示せ.

3 1991 年後期理系

平面上で次の方程式を満たす点全体の集合を C_1 , $10x^2 + 14xy + 5y^2 = 1$ を満たす点全体の集合を C_2 とする.

$$x^2 + y^2 - 1 = 0$$

$$10x^2 + 14xy + 5y^2 = 1$$

(1) a, b, c, d は負でない整数で $ad-bc > 0$

を満たしている. さらに $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

の定める 1 次変換 f が C_2 を C_1 に写している, すなわち $f(C_2) = C_1$ である. このとき, a, b, c, d を求めよ.

(2) C_2 上の点で x 座標, y 座標とも整数であるものは何個あるか.

4 1988 年 A 日程理系

$A = \begin{pmatrix} 2 & -3 \\ -1 & 2 \end{pmatrix}$ とする.

(1) $\begin{pmatrix} x' \\ y' \end{pmatrix} = A \begin{pmatrix} x \\ y \end{pmatrix}$ で, $x^2 - 3y^2 = 1$,

$x > 0, y \geq 1$ ならば, $x'^2 - 3y'^2 = 1$, $0 \leq y' < y$ が成立することを示せ.

(2) x, y が $x^2 - 3y^2 = 1$ をみたす自然数ならば, ある自然数をとると $\begin{pmatrix} 1 \\ 0 \end{pmatrix} =$

$A^n \begin{pmatrix} x \\ y \end{pmatrix}$ となることを示せ.

5.7 その他

最後に, どの枠に入れてよいかわからない問題をまとめておく. 整数特有の性質を前面に出した問題ではないが, 解いてみても良いだろう.

1 1989 年後期理系

2 次方程式 $ax^2 - bx + 3c = 0$ において, a, b, c は一桁の自然数であり, 二つの解 α, β は $1 < \alpha < 2, 5 < \beta < 6$ をみたす. このとき, a, b, c を求めよ.

2 1992 年前期文理共通

θ は $0 < \theta < \frac{\pi}{2}$ の範囲の角とする.

(1) $\sin 3\theta = \sin 2\theta$ を満たす θ を求めよ.

(2) m, n を 0 以上の整数とする. θ についての方程式 $\sin 3\theta = m \sin 2\theta + n \sin \theta$ が解をもつときの (m, n) と, そのときの θ を求めよ.

3 2002 年前期文理共通

$f(x) = x^4 + ax^3 + bx^2 + cx + 1$ は整数を係数とする x の 4 次方程式とする．4 次方程式 $f(x) = 0$ の重複も込めた 4 つの解のうち，2 つは整数で残りの 2 つは虚数であるという．このとき， a, b, c の値を求めよ．

4 2007 年文系

n を 1 以上の整数とするととき，次の 2 つの命題はそれぞれ正しいか．正しいときは証明し，正しくないときはその理由を述べよ．

命題 p : ある n に対して， \sqrt{n} と $\sqrt{n+1}$ は共に有理数である．

命題 q : すべての n に対して， $\sqrt{n+1} - \sqrt{n}$ は共に無理数である．

5 2004 年後期理系

n を自然数とする．次の 3 つの条件 (1), (2), (3) をすべて満たす自然数の組 (a, b, c, d) はいくつあるか． n を用いて表せ．

- (1) $1 \leq a < d \leq n$
- (2) $a \leq b < d$
- (3) $a < c \leq d$

6 2002 年前期文系

4 個の整数 $1, a, b, c$ は $1 < a < b < c$ を満たしている．これらの中から相異なる 2 個を取り出して和を作ると， $1+a$ から $b+c$ までのすべての整数が得られるという． a, b, c を求めよ．

6 資料編～一橋大学の整数問題～

京都大学と並んで，整数問題が頻繁に出題されるのが一橋大学である．以下に最近 20 年の整数問題をすべて列挙した．京都大学と比べると「～であることを示せ」という問題よりも「～を求めよ」とい

うタイプの問題の方が多い．いきなり京大の問題はキツイ，という人は，一橋大学の問題からはじめると良いだろう．はじめに述べたように，京大，阪大で類題が出題されている．

1 2007 年前期

m を整数とし， $f(x) = x^3 + 8x^2 + mx + 60$ とする．

- (1) 整数 a と，0 でない整数 b で， $f(a+bi) = 0$ をみ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．

2 2007 年後期

直角をはさむ二辺の長さが a, b の直角三角形がある．内接円の半径を r とする．

- (1) r を a, b で表せ．
- (2) a, b は整数とし， $r = 5$ とする．このような a, b の組をすべて求めよ．

3 2006 年前期

次の条件 (a), (b) をともにみたす直角三角形を考える．ただし，斜辺の長さを p ，その他の 2 辺の長さを q, r とする．

- (a) p, q, r は自然数で，そのうち少なくとも 2 つは素数である．
- (b) $p + q + r = 132$

- (1) q, r のどちらかは偶数であることを示せ．
- (2) p, q, r の組をすべて求めよ．

4 2006 年後期

正の整数 n に対して， $n = k + 2l$ をみたすような 0 以上の整数の組 (k, l) の個数を a_n とする．また， $n = p + 2q + 3r$ をみたすような 0 以上の整数の組 (p, q, r) の個数を b_n とする．

- (1) a_n を n で表せ．
- (2) n が 6 の倍数のとき， b_n を n で表せ．

5 2005 年前期

k は整数であり、3 次方程式 $x^3 - 13x + k = 0$ は 3 つの異なる整数解をもつ。 k とこれらの整数解をすべて求めよ。

6 2005 年後期

- (1) $p, 2p + 1, 4p + 1$ がいずれも素数であるような p をすべて求めよ。
- (2) $q, 2q + 1, 4q - 1, 6q - 1, 8q + 1$ がいずれも素数であるような q をすべて求めよ。

7 2004 年前期

a, b, c は整数で、 $a < b < c$ をみたす。放物線 $y = x^2$ 上に 3 点 $A(a, a^2), B(b, b^2), C(c, c^2)$ をとる。

- (1) $\angle BAC = 60^\circ$ とはならないことを示せ。ただし、 $\sqrt{3}$ が無理数であることを証明なしに用いてよい。
- (2) $a = -3$ のとき、 $\angle BAC = 45^\circ$ となる組 (b, c) をすべて求めよ。

8 2004 年後期

- (1) すべての正の奇数 k は、 $m > n \geq 0$ をみたす整数 m, n によって $k = m^2 - n^2$ と表されることを示せ。
- (2) すべての正の偶数 k で、 $m > n \geq 0$ をみたす整数 m, n によって $k = m^2 - n^2$ と表されるものをすべて求めよ。

9 2003 年前期

- (1) 正の整数 n で $n^3 + 1$ が 3 で割り切れるものをすべて求めよ。
- (2) 正の整数 n で $n^n + 1$ が 3 で割り切れるものをすべて求めよ。

10 2003 年後期

n を正の整数とする。

- (1) $x^2 + y < n^2$ をみたす正の整数 x, y の組 (x, y) の個数 a_n を求めよ。
- (2) $\sqrt{x^2 + y}$ を越えない最大の整数が n であるような正の整数 x, y の組 (x, y) の個数 b_n を求めよ。

11 2002 年前期

k, x, y は正の整数とする。三角形の 3 辺の長さが $\frac{k}{x}, \frac{k}{y}, \frac{1}{xy}$ で、周の長さが $\frac{25}{16}$ である。 k, x, y を求めよ。

12 2001 年後期

m を正の整数とする。 $m^3 + 3m^2 + 2m + 6$ はある正の整数の 3 乗である。 m を求めよ。

13 2000 年前期

a, b, c を正の整数とする。複素数 $w = a + bi, z = c + di$ が $w^2 z = 1 + 18i$ をみたす。 a, b, c, d を求めよ。

14 2000 年後期

- (1) $2 \leq a < b \leq M$ をみたすすべての整数 a, b について不等式 $3(a^2 + b^2) < 2(a + b)^2$ が成立するような正の整数 M のうち最大のものを求めよ。
- (2) $2 \leq a < b < c \leq N$ をみたすすべての整数 a, b, c について不等式 $3(a^2 + b^2 + c^2) < (a + b + c)^2$ が成立するような正の整数 N のうち最大のものを求めよ。

15 1999 年前期

p, q は素数で、 $p < q$ とする。

- (1) $\frac{1}{p} + \frac{1}{q} = \frac{1}{r}$ をみたす整数 r は存在しないことを示せ。
- (2) $\frac{1}{p} - \frac{1}{q} = \frac{1}{r}$ をみたす整数 r が存在するのは、 $p = 2, q = 3$ のときに限ることを示せ。

16 1999 年後期

正の整数 n に対し、 $f(z) = z^{2n} + z^n + 1$ とする。

- (1) $f(z)$ を $z^2 + z + 1$ で割ったときの余りを求めよ。
- (2) $f(z)$ を $z^2 - z + 1$ で割ったときの余りを求めよ。

17 1998 年前期

正の整数 n を 8 で割った余りを $r(n)$ と

おく．正の整数の組 (a, b) は，条件 $0 < a - r(a) < \frac{4}{3}r(b)$, $0 < b - r(b) < \frac{4}{3}r(ab)$ をみたすとする．

- (1) $a - r(a)$ と $r(b)$ を求めよ．
- (2) a と b を求めよ．

18

1998 年後期

- (1) $\log_5 3$ は無理数であることを示せ．
- (2) $\log_{10} r$ が有理数となる有理数 r は $r = 10^q (q = 0, \pm 1, \pm 2)$ に限ることを示せ．
- (3) 任意の正の整数 n に対して， $\log_{10}(1 + 3 + 3^2 + \cdots + 3^n)$ は無理数であることを示せ．

19

1997 年前期

すべての正の整数 n に対して $5^n + an + b$ が 16 の倍数となるような 16 以下の正の整数 a, b を求めよ．

20

1996 年前期

- (1) 2 つの自然数の組 (a, b) は，条件

$$a < b \quad \text{かつ} \quad \frac{1}{a} + \frac{1}{b} < \frac{1}{4}$$

をみたす．このような組 (a, b) のうち， b の最も小さいものをすべて求めよ．

- (2) 3 つの自然数の組 (a, b, c) は，条件

$$a < b < c \quad \text{かつ} \quad \frac{1}{a} + \frac{1}{b} + \frac{1}{c} < \frac{1}{3}$$

をみたす．このような組 (a, b, c) のうち， c の最も小さいものをすべて求めよ．

21

1995 年前期

正の整数の組 (m, n) で条件 $0 < \left| \frac{n}{m} - 0.4 \right| \leq \frac{1}{100}$ をみたすもののうち， m が最も小さい (m, n) を求めよ．

22

1995 年後期

座標平面の x 軸上に点 $A(15, 0)$ があり， y 軸上の $y > 0$ の部分に点 B がある．原点 O と直線 AB との距離，および OB の長さは，ともに整数である．点 B の座標を求めよ．

23

1994 年前期

- (1) 実数 x, y が等式 $x^2 - 2xy + y^2 - x - y = 0$ \cdots をみたし， $x - y$ が整数ならば， x も y は整数であることを示せ．

- (2) 等式 をみたす格子点 (x, y) のうちで，点 $(100, 100)$ に最も近いものを求めよ．ただし格子点とは， x 座標， y 座標がともに整数であるような座標平面上の点のことである．ことを示せ．

24

1994 年後期

整数 a, b, c, d が等式 $a^2 + b^2 + c^2 = d^2$ をみたすとする．

- (1) d が 3 の倍数でないならば， a, b, c の中に 3 の倍数がちょうど 2 つあることを示せ．
- (2) d が 2 の倍数でも 3 の倍数でもないならば， a, b, c のうち少なくとも 1 つは 6 の倍数であることを示せ．

25

1993 年後期

m, n を正の整数とする． x についての 2 次方程式 $12x^2 - mx + n = 0$ の 2 つの実数解を小数第 2 位で四捨五入して 0.3 および 0.7 を得た． m, n を求めよ．

26

1992 年前期

n を正の整数とする．

- (1) n^2 と $2n + 1$ は互いに素であることを示せ．
- (2) $n^2 + 2$ が $2n + 1$ の倍数になる n を求めよ．

27

1991 年後期

x は 0 でない実数とする．

- (1) $x + \frac{1}{x}$ が整数ならばすべての正の整数に対して $x^n + \frac{1}{x^n}$ も整数であることを示せ．
- (2) $x - \frac{1}{x}$ が 0 以外の整数ならば $x^n - \frac{1}{x^n}$ も整数でないことを示せ．

28

1990 年前期

直角三角形の 3 辺の長さがすべて整数のとき，面積は 2 の整数倍であることを示せ．