# 整 数 問 題 の 攻 略 (基礎編)

直前講習特別講座
奈良県立奈良高等学校
赤阪 正純

## 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 $n$ 個のグループに分類される．

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 個のグループに分類され，その各グループに含まれる数を $k$ を整数として，

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

と表す (場合によっては，$5k$, $5k\pm1$, $5k\pm2$ ととることもある．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 個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 5** 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 1**

$$10\equiv 3 \pmod 7,\qquad 4\equiv -1 \pmod 5$$

---

***Remark* 1**

上の例の 2 つ目の式は，$-1$ を 5 で割ると余りが 4 であることを意味している．負の整数を正の整数で割った余りはなじみがないかもしれない．一般に，整数 $a$(正でも負でもよい) を正の整数 $b(>0)$ で割ったときの，商を $q$, 余りを $r$ と書くことにすると，

$$a=bq+r \quad (0\leqq r\leqq b-1)$$

と表記される．ここで，余り $r$ は $0\leqq r\leqq b-1$ という条件が付くが，商 $q$ には何の条件もないことに注意しよう．つまり，**商は負の整数でも構わない**．したがって，$-1$ を 5 で割ると

$$-1=5\times(-1)+4$$

と表記され，商が $-1$，余り 4 となる．

□

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 $m$ 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☆**

$$a\equiv b \pmod m$$
$$\Longleftrightarrow a,\ b \text{ を } m \text{ で割った余りが等しい}$$
$$\Longleftrightarrow a-b \text{ が } m \text{ で割り切れる}$$

$a-b$ 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．

**☆合同式の加法・減法・乗法☆**

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

のとき，次の等式が成立する．

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

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

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

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．

証明終

また次の公式も成り立つ．

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

つまり，合同式の記号 ($\equiv$) は加法，減法，乗法については通常の等号 ($=$) と全く同じである．

では，除法はどうであろうか．まずは，具体例で確認してみよう．

---

**例 2**

例えば，合同式

$$35 \equiv 5 \pmod{6}$$

の両辺を 5 で割って，

$$7 \equiv 1 \pmod{6}$$

は成立する．しかし，合同式

$$14 \equiv 8 \pmod{6}$$

は両辺を 2 で割って，

$$7 \equiv 4 \pmod{6}$$

とはならない．

---

このように，両辺を割っても合同関係が成立する場合と，しない場合がある．通常の等号の場合のようにはいかない．

では，どのような場合に除法が可能なのだろうか．

合同式の除法には，次の性質がある．

**☆合同式の除法☆**

$ac \equiv bc \pmod{m}$ のとき，

$c$ と $m$ が互いに素のとき，

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

$c$ と $m$ が互いに素でないとき，$c$ と $m$ の最大公約数を $d(>1)$ とすると，

$$a \equiv b \left(\mathrm{mod}\ \frac{m}{d}\right)$$

が成立する．

証明

$ac \equiv bc \pmod{m}$ のとき，

$$(a - b)c \equiv 0 \pmod{m}$$

より，$(a - b)c$ は $m$ で割り切れる．よって，$c$ と $m$ が互いに素のとき，$a - b$ が $m$ で割り切れるので，

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

となり，$a \equiv b \pmod{m}$ が成立する．

$c$ と $m$ が互いに素でないとき，最大公約数を $d$ とすれば，

$$c = dc',\quad m = dm' \quad (c' \text{と } m' \text{は互いに素})$$

このとき，$(a-b)dc'$ は $dm'$ で割り切れるので，$(a-b)c'$ は $m'$ で割り切れる

$$(a - b)c' \equiv 0 \pmod{m'}$$

$c'$ と $m'$ は互いに素なので，

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

となり，$a\equiv b \pmod{\dfrac{m}{d}}$ が成立する．

証明終

このように，合同式の両辺を共通の因数で割るときは，適当に法を変更しなければならない．

共通の因数が法 $m$ と互いに素のときだけ，法が変化せずにそのまま割り算でき (このことは等式 $ac=bc$ から $a=b$ を導くには $c\neq 0$ という条件が必要であることに類似している)．互いに素でない時は，法が $m$ ではなく，$\dfrac{m}{d}$ に変化して，割り算ができるのである．

したがって，先程の例では，合同式

$$35\equiv 5 \pmod 6$$

は 6 と 5 が互いに素だから，そのまま両辺を 5 で割ることができ，

$$7\equiv 1 \pmod 6$$

が成立する．また，合同式

$$14\equiv 8 \pmod 6$$

は 2 と 6 が互いに素でないから，そのまま割り算はできず，法が $\dfrac{6}{2}=3$ に変化して，

$$7\equiv 4 \pmod 3$$

となる．

☆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．ただし，除法については少し条件が必要．

---

**例 3**

$2007^{2007}$ を 17 で割った余りを求めよ．

---

【考え方】

$2007^{2007}$ を実際に計算することは不可能である．そこで，とりあえず 2007 を 17 で割った余りを考えると $\cdots$

【解説】

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

$$2007^{2007}\equiv 1^{2007}\equiv 1 \pmod{17}$$

となるので，余りは 1 である．

■

***Remark* 2**

なお，合同式を用いないなら，

$$2007^{2007}=(17\times 118+1)^{2007}$$

の二項展開を考えねばならない．二項展開については後ほど説明する．

□

---

**例 4**

$n$ を自然数とするとき，$3^{n+2}+4^{2n+1}$ は 13 で割り切れることを示せ．

---

【解説】

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

よって，$3^{n+2}+4^{2n+1}$ は 13 で割り切れる．

■

***Remark* 3**

なお合同式を用いないなら，$n$ が自然数だから数学的帰納法による証明を行うことになる．

$n=1$ のときは成立する．

$n=k$ のとき 13 で割り切れると仮定すると，$3^{k+2}+4^{2k+1}=13m$ とおけ，

$$\begin{aligned} &3^{(k+1)+2}+4^{2(k+1)+1}\\ =&3\times 3^{k+2}+4^2\times 4^{2k+1}\\ =&3\cdot 3^{k+2}+(3+13)4^{2k+1}\\ =&3(3^{k+2}+4^{2k+1})+13\cdot 4^{2k+1}\\ =&3\cdot 13m+13\cdot 4^{2k+1}\\ =&13(3m+4^{2k+1})\end{aligned}$$

となるので，$n=k+1$ のときも 13 で割り切れる．

よって，数学的帰納法により，$3^{n+2}+4^{2n+1}$ は 13 で割り切れる

□

次のような面白い問題が実際に出題されている．

---

## 練習問題 1

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．

[2000 年熊本県立大前期]

---

**【考え方】**

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．

**【解説】**

(1) 土曜日　(2) 火曜日　(3) 火曜日

■

合同式の扱いに慣れただろうか．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 5**

$n^2$ が 5 の倍数ならば，$n$ は 5 の倍数であることを証明せよ．

---

**【考え方】**

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．

**【解説】**

合同式を利用しない解答

$n$ は 5 の倍数ではないので，$n = 5k \pm 1,\ 5k \pm 2$ とおく ($n = 5k+1,\ 5k+2,\ 5k+3,\ 5k+4$ とおいても同じであるが，計算が少なくてすむ．特に 2 乗する計算では効果的)．

$n = 5k \pm 1$ 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 $n^2$ は 5 の倍数にならない．よって，対偶が証明されたので，もとの命題も証明された．

合同式を利用した解答

$n \not\equiv 0 \pmod 5$ であるので，$n \equiv \pm 1,\ \pm 2 \pmod 5$ とおく (合同式を用いる場合でも，$n \equiv 1,\ 2,\ 3,\ 4 \pmod 5$ とおくよりも，計算が少なくてすむ)．

$n \equiv \pm 1 \pmod 5$ 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 $n^2 \not\equiv 0 \pmod 5$ である．よって，対偶が証明されたので，もとの命題も証明された．

■

***Remark* 4**

$n = 5k \pm 1,\ 5k \pm 2$ 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 6**

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．

---

**【考え方】**

全ての整数を順番に調べるわけにはいかないので，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．

合同式を利用しない解答では $m$ を整数として，$n=3m,\ 3m+1,\ 3m+2$ として与式に代入して 3 の倍数であることを確認してみた．もちろん $3m,\ 3m\pm1$ と設定しても構わないが，計算途中の数字が大きくなることを実感してもらうために，あえて設定しなかった．合同式を利用した解答でも，$n\equiv 0,\ 1,\ 2\pmod 3$ と設定したが，それほど計算は大変ではないことがわかる．

**【解説】**

合同式を利用しない解答

$n=3m$ のとき，

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

$n=3m+1$ のとき，

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

$n=3m+2$ のとき，

$$\begin{aligned}n^3+2n&=(3m+2)^3+2(3m+2)\\&=3(9m^3+18m^2+12m+4)\end{aligned}$$

よって，いずれの場合においても 3 の倍数になるので，任意の整数 $n$ で $n^3+2n$ は 3 の倍数である．

合同式を利用した解答

$n\equiv 0\pmod 3$ のとき，

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

$n\equiv 1\pmod 3$ のとき，

$$n^3+2n\equiv 1^3+2\cdot 1\equiv 3\equiv 0\pmod 3$$

$n\equiv 2\pmod 3$ のとき，

$$n^3+2n\equiv 2^3+2\times 2\equiv 12\equiv 0\pmod 3$$

よって，いずれの場合においても，$n^3+2n\equiv 0\pmod 3$ となるので任意の整数 $n$ で $n^3+2n\equiv 0\pmod 3$ である．

■

***Remark* 5**

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．

□

***Remark* 6**

後ほど紹介する**平方数の分類 (その①)** を用いれば，この問題は，ほとんど自明であることに気付くであろう．

□

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き，

$n$ が $pq$ の倍数 $\iff$ $n$ が $p$ の倍数かつ $q$ 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き，

$$n\equiv 0\pmod{pq}\iff\begin{cases}n\equiv 0\pmod p\\ n\equiv 0\pmod q\end{cases}$$

***Remark* 7**

一般に，$a$ を整数，$p,\ q$ を互いに素な自然数とするとき，

$$n\equiv a\pmod{pq}\iff\begin{cases}n\equiv a\pmod p\\ n\equiv a\pmod q\end{cases}$$

も成立する．余りが全て同じであることに注意せよ．

□

---

## 練習問題 2

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

---

【考え方】

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．まず，積の形に変形するために因数分解を行う．

【解説】

合同式を利用しない解答

$2n^3-3n^2+n=n(n-1)(2n-1)$ になるので，連続 2 整数の積 $n(n-1)$ を含むから，2 の倍数になるのは明らか．あとは，これが 3 の倍数でもあることを示せばよい．

$n=3k$ のとき，$n$ が 3 の倍数，

$n=3k+1$ のとき，$n-1=3k$ が 3 の倍数，

$n=3k+2$ のとき，$2n-1=6k+3$ が 3 の倍数，

になるので，$n(n-1)(2n-1)$ は常に 3 の倍数になる．

よって，$n(n-1)(2n-1)$ は 6 の倍数になる．

合同式を利用した解答

$n\equiv 0 \pmod 3$ のとき，

$$2n^3-3n^2+n\equiv 0 \pmod 3$$

$n\equiv 1 \pmod 3$ のとき，

$$2n^3-3n^2+n\equiv 2-3+1\equiv 0 \pmod 3$$

$n\equiv 2 \pmod 3$ のとき，

$$2n^3-3n^2+n\equiv 16-12+2\equiv 6\equiv 0 \pmod 3$$

よって，$2n^3-3n^2+n$ は 3 の倍数である．

■

### ***Remark*** 8

またこの問題も，式変形でも 6 の倍数であることがわかる．

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

$n(n-1)(n+1)$ は連続 3 整数の積なので 6 の倍数．また，$3n(n-1)$ も 6 の倍数．

よって，$n(n-1)(2n-1)$ は 6 の倍数．

□

### ***Remark*** 9

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．

□

---

## 練習問題 3

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．

[2001 年宮崎大]

---

【考え方】

まずは，通分して分子を因数分解せよ．なお，はじめに $n(n+1)(2n+1)$ は常に 6 の倍数になることを示す必要があるが，前問と同様なので省略する．3 で割った分類，式変形，$\Sigma k^2$ の公式などで証明ができる．

【解説】

$$\begin{aligned}\text{与式}&=\frac{2n^5+5n^4+10n^3+10n^2+3n}{30}\\ &=\frac{n(n+1)(2n+1)(n^2+n+3)}{30}\end{aligned}$$

となるので，与式が自然数になるには，分子が 30 の倍数であることを示せばよい．$n(n+1)(2n+1)$ は常に 6 の倍数であるので，$n(n+1)(2n+1)(n^2+n+3)$ が 5 の倍数になることを示せばよい．

合同式を利用しない解答

$n=5k$ のときは $n$ 自体が 5 の倍数であり，

$n=5k+1$ のときは $n^2+n+3=5(5k^2+3k+1)$，

$n=5k+2$ のときは $2n+1=5(2k+1)$，

$n=5k+3$ のときは $n^2+n+3=5(5k^2+7k+3)$，

$n=5k+4$ のときは $n+1=5(k+1)$

となるので全ての場合で 5 の倍数になる．

よって，すべての自然数に対して

$$n(n+1)(2n+1)(n^2+n+3)$$

は 30 の倍数になるので，与式は自然数である．

合同式を利用した解答

合同式を用いると，最後の計算が少し楽になる．
$n \equiv 0 \pmod 5$ のときは $n \equiv 0 \pmod 5$，
$n \equiv 1 \pmod 5$ のときは

$$n^2+n+3 \equiv 1^2+1+3 \equiv 0 \pmod 5$$

$n \equiv 2 \pmod 5$ のときは

$$2n+1 \equiv 4+1 \equiv 0 \pmod 5$$

$n \equiv 3 \pmod 5$ のときは

$$n^2+n+3 \equiv 3^2+3+3 \equiv 0 \pmod 5$$

$n \equiv 4 \pmod 5$ のときは

$$n+1 \equiv 4+1 \equiv 0 \pmod 5$$

よって，すべての自然数に対して

$$n(n+1)(2n+1)(n^2+n+3) \equiv 0 \pmod{30}$$

になるので，与式は自然数である．

■

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？この場合は 3 で割った余りで分類する．

---

## 京大入試問題 1

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．

[2001 年前期文系]

---

**【考え方】**

因数分解して積の形をつくる．この問題では，合同式を利用しても利用しなくても，ほとんど差はない．むしろ，合同式を利用した方がややこしい．合同式を利用した答案の方が因数分解をさらに細かくやっていることに注意しよう．なお，途中の細かい計算過程は省略させていただく．

**【解説】**

合同式を利用しない解答

$$\begin{aligned} n^9-n^3 &= n^3(n^6-1) \\ &= n^3(n^3+1)(n^3-1) \end{aligned}$$

より，
$n=3k$ のときは $n^2$ が 9 の倍数になる．
$n=3k+1$ のときは $n^3-1$ が 9 の倍数になる．
$n=3k+2$ のときは $n^3+1$ が 9 の倍数になる．
以上より，任意の整数 $n$ に対し $n^9-n^3$ は 9 で割り切れる．

合同式を利用した解答

$$\begin{aligned} n^9-n^3 &= n^3(n^6-1) \\ &= n^3(n^3+1)(n^3-1) \\ &= n^3(n+1)(n^2-n+1)(n-1)(n^2+n+1) \end{aligned}$$

より，
$n \equiv 0 \pmod 3$ のときは，$n^2 \equiv 0 \pmod 9$，
$n \equiv 1 \pmod 3$ のときは

$$n-1 \equiv 0 \pmod 3$$
$$n^2+n+1 \equiv 0 \pmod 3$$

だから，$(n-1)(n^2+n+1) \equiv 0 \pmod 9$．
$n \equiv 2 \pmod 3$ のときは

$$n+1 \equiv 0 \pmod 3$$
$$n^2-n+1 \equiv 0 \pmod 3$$

だから，$(n+1)(n^2-n+1) \equiv 0 \pmod 9$．
以上より，任意の整数 $n$ に対し $n^9-n^3 \equiv 0 \pmod 9$ である．

■

さて，次に，整数の分類に関して最も重要な「平方数の分類」についてまとめておこう．

特に，平方数 $n^2$ を 3，4，5，8 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)）．

まずは，平方数を 3，4，5，8 で割った余りについて下の表にまとめてみよう (紙面の都合で $n=7$ の場合しか書いてないが，各自で $n=10$ の場合までは確かめて欲しい)．

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|---|
| $n^2$ | 1 | 4 | 9 | 16 | 25 | 36 | 49 |
| $n^2$ を 3 で割った余り | 1 | 1 | 0 | 1 | 1 | 0 | 1 |
| $n^2$ を 4 で割った余り | 1 | 0 | 1 | 0 | 1 | 0 | 1 |
| $n^2$ を 5 で割った余り | 1 | 4 | 4 | 1 | 0 | 1 | 4 |
| $n^2$ を 8 で割った余り | 1 | 4 | 1 | 0 | 1 | 4 | 1 |

## 練習問題 4

上の平方数の分類の表からわかることを述べよ．

---

【解説】

平方数を 3 で割った余りは，0 か 1．
平方数を 4 で割った余りは，0 か 1．
平方数を 5 で割った余りは，0 か 1 か 4．
平方数を 8 で割った余りは，0 か 1 か 4．
に限られる．

■

平方数を 3，4，5 で割った余りについて，もう少し詳しくまとめておこう．

☆平方数の分類 (その①) ☆

平方数 $n^2$ を 3 で割った余りは，0 または 1 に限られる．

$n$ 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①) ☆

$$n \equiv 0 \pmod 3 \Longleftrightarrow n^2 \equiv 0 \pmod 3$$
$$n \not\equiv 0 \pmod 3 \Longleftrightarrow n^2 \equiv 1 \pmod 3$$

---

## 練習問題 5

平方数の分類 (その①) を証明せよ．

---

【解説】

($\Longrightarrow$ の証明)
$n = 3k$ のとき，

$$n^2 = (3k)^2 = 9k^2$$

となり，$n^2$ は 3 で割り切れる．
$n = 3k \pm 1$ のとき，

$$n^2 = (3k \pm 1)^2 = 9k^2 \pm 6k + 1$$

となり，$n^2$ は 3 で割ると 1 余る．
($\Longleftarrow$ の証明)
待遇を考えれば，簡単に証明できる．

■

☆平方数の分類 (その②) ☆

平方数 $n^2$ を 4 で割った余りは，0 または 1 に限られる．

$n$ 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．

合同式を用いて表現すれば，

☆平方数の分類 (その②) ☆

$$n \equiv 0 \pmod 2 \Longleftrightarrow n^2 \equiv 0 \pmod 4$$
$$n \equiv 1 \pmod 2 \Longleftrightarrow n^2 \equiv 1 \pmod 4$$

---

## 練習問題 6

平方数の分類 (その②) を証明せよ．

---

【解説】

($\Longrightarrow$ の証明)
$n$ 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，

$$n^2 = (2m+1)^2 = 4m(m+1) + 1$$

となり，4 で割ると 1 余る．
($\Longleftarrow$ の証明)
待遇を考えれば，簡単に証明できる．

■

☆平方数の分類 (その③) ☆

平方数 $n^2$ を 5 で割った余りは，0 または 1 または 4 である．つまり，
$n$ が 5 で割り切れるとき，
$n^2$ を 5 で割ると余り 0
$n$ を 5 で割って余りが 1 または 4 のとき，
$n^2$ を 5 で割ると余り 1
$n$ を 5 で割って余りが 2 または 3 のとき，
$n^2$ を 5 で割ると余り 4
である．

合同式を用いて表現すれば，

☆平方数の分類 (その③) ☆

$$\begin{aligned} n &\equiv \ \ 0 \pmod 5 \Longleftrightarrow n^2 \equiv 0 \pmod 5 \\ n &\equiv \pm 1 \pmod 5 \Longleftrightarrow n^2 \equiv 1 \pmod 5 \\ n &\equiv \pm 2 \pmod 5 \Longleftrightarrow n^2 \equiv 4 \pmod 5 \end{aligned}$$

## 練習問題 7

平方数の分類 (その③) を証明せよ．

【解説】

($\Longrightarrow$ の証明)

$n = 5k$ のとき，

$$n^2 = (5k)^2 = 25k^2$$

となり，5 で割り切れる．

$n = 5k+1$ のとき，

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

$n = 5k+4$ のとき，

$$n^2 = (5k+4)^2 = 5(5k^2+8k+3)+1$$

となり，5 で割ると 1 余る．

また，$n = 5k+2$ のとき，

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

$n = 5k+3$ のとき，

$$n^2 = (5k+3)^2 = 5(5k^2+6k+1)+4$$

となり，5 で割ると 4 余る．

($\Longleftarrow$ の証明)

待遇を考えれば，簡単に証明できる．

■

☆平方数の分類 (その④) ☆

平方数 $n^2$ を 8 で割った余りは，0 または 1 または 4 に限られる．

$n$ が 4 で割り切れるとき，

$n^2$ を 8 で割ると余り 0

$n$ を 4 で割ると 2 余るとき，

$n^2$ を 8 で割ると余り 4

$n$ を 4 で割ると余り 1, 3(つまり $n$ 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④) ☆

$$\begin{aligned} n &\equiv 0 \pmod 4 \text{ のとき，} n^2 \equiv 0 \pmod 8 \\ n &\equiv 2 \pmod 4 \text{ のとき，} n^2 \equiv 4 \pmod 8 \\ n &\equiv 1 \pmod 2 \text{ のとき，} n^2 \equiv 1 \pmod 8 \end{aligned}$$

## 練習問題 8

平方数の分類 (その④) を証明せよ．

【解説】

($\Longrightarrow$ の証明)

$n = 4k$ のとき，

$$n^2 = (4k)^2 = 16k^2$$

となり，8 で割り切れる．

$n = 4k+2$ のとき，

$$n^2 = (4k+2)^2 = 16k^2+16k+4 = 8(2k^2+2k)+4$$

となり，8 で割ると 4 余る．

$n = 2k+1$ のとき，

$$n^2 = (2k+1)^2 = 4k^2+4k+1 = 4k(k+1)+1$$

となり，$k(k+1)$ は連続する 2 整数の積だから偶数．よって，$4k(k+1)$ は 8 の倍数になるので，このとき，8 で割ると 1 余る．

($\Longleftarrow$ の証明)

待遇を考えれば，簡単に証明できる．

**例 7**

$m$, $n$ を整数とするとき，

$$\begin{aligned} m^2 &= 3n+2 \ \Longrightarrow \text{矛盾} \\ m^2 &= 4n+2 \ \Longrightarrow \text{矛盾} \\ m^2 &= 5n+3 \ \Longrightarrow \text{矛盾} \\ m^2 &= 8n+5 \ \Longrightarrow \text{矛盾} \end{aligned}$$

次の例は，駿台の東大実戦模試で出題された問題である．こういう問題は見た瞬間に「当り前じゃないか！」と思えるようになってほしい．

**例 8**

$$x^2 = 5y + 2$$

を満たす整数 $x$, $y$ は存在しないことを証明せよ．

---

【解説】

$x^2 = 5y + 2$ は $x^2$ を 5 で割ると 2 余ることを意味しているが，平方数を 5 で割った余りは，0 か 1 か 4 に限られるから，この式は矛盾である．

■

***Remark* 10**

以下，本文では平方数の分類は公式として用いることにする．つまり「平方数の分類①より ···」などという表現を使っていく．しかし，これはあくまでも本文内だけでの決めごとであって，一般的ではない．平方数の分類の公式など一般にあるわけもなく，**記述入試問題の答案では，先の練習問題で書いた解答をもう一度そのまま再現せねばならない**ので注意すること．

□

**発展 1**

これまでの平方数の分類から，$p$ を素数とするとき，

$$n^2 \equiv 0 \pmod{p} \Longrightarrow n \equiv 0 \pmod{p}$$

が成立することは明らかである (待遇を考える)．

しかし，例えば，平方数の分類①より

$$n^2 \equiv 1 \pmod{3} \Longrightarrow n \equiv 1,\ 2 \pmod{3}$$

であるが，

$$n^2 \equiv 2 \pmod{3} \Longrightarrow \text{矛盾}$$

である．これは，$n^2 \equiv 1 \pmod{3}$ **には解が存在するが，** $n^2 \equiv 2 \pmod{3}$ **には解が存在しない**ことを意味している．

このように，2 次の合同方程式

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

に解が存在するのか，存在しないのか，は重要な問題である．

冒頭で紹介したガウスは，この問題を完全に解決し，**平方剰余の相互法則**として一つの理論を完成させた．**平方剰余の相互法則**は初等整数論の基盤とも言えるもので，その後の整数論の発展には欠かせない重要な理論となった．ガウス自身，この理論には特別の感情を持っていたようで，8 種類のまったく異なる証明を残している．興味ある人は調べてみよう．

□

---

**例 9**

$n$ 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．

---

【考え方】

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．

【解説】

合同式を利用しない解答

$n$ が 3 の倍数でない奇数であることから，$n = 6m+1,\ 6m+5$ とおける．このとき $n^2$ に代入して計算すれば 12 で割った余りが 1 になることが簡単に確認できる．なお，$n = 6m \pm 1$ と設定すれば，さらに計算が簡単になる．

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．

■

---

**練習問題 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．

[2002 年東京女子大 (文理)]

【考え方】

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，

$$n \text{ が } 2 \text{ でも } 3 \text{ でも割り切れない}$$
$$\Longleftrightarrow n = 6m+1,\ \ 6m+5 \ \ (\text{または，} n = 6m \pm 1)$$

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．前問のように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，ここでは合同式による解答のみを紹介しよう．

【解説】

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．

## 練習問題 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．

[2004 年旭川医大後期]

【考え方】

(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．また，奇数の 2 乗は 8 で割ると 1 余ることにも注目する．

(1)(2) では，合同式を利用すれば少しスマートな解答になる．

【解説】

合同式を利用しない解答

(1)

$c$ が偶数だと仮定すると，$a$, $b$, $c$ 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 $a$, $b$ は共に奇数でなければならない．$a$, $b$ を共に奇数とすると，平方数の分類☒より $a^2$, $b^2$ はそれぞれ 4 で割ると 1 余るので，$a^2+b^2$ は 4 で割ると 2 余る．平方数の分類☒より，平方数を 4 で割った余りは 0 か 1 しかないので，これが平方数 $c^2$ になることはない．よって，$c$ は奇数である．

(2)

$a$, $b$ が共に 3 の倍数であるとすると，平方数の分類☒より $a^2$, $b^2$ はそれぞれ 3 で割り切れるので，$a^2+b^2$ も 3 で割り切れる．平方数の分類☒より，平方数 $c^2$ が 3 で割り切れるならば，$c$ も 3 の倍数になるので，$a$, $b$, $c$ は全て 3 の倍数になり，$a$, $b$, $c$ 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であることに矛盾する．

$a$, $b$ が共に 3 の倍数でないとすると，平方数の分類☒より $a^2$, $b^2$ はそれぞれ 3 で割ると 1 余るので，$a^2+b^2$ は 3 で割ると 2 余る．平方数の分類☒より平方数 $c^2$ は 3 で割ると余りが 0 か 1 しかないので矛盾する．

以上より，$a$, $b$ のうち 1 つは 3 の倍数である．

(3)

(1) より，$a$, $b$ のうち，どちらか一方は偶数で，他方は奇数であるから，$a$ を偶数，$b$ を奇数として一般性を失わない．いま $a$ が 4 の倍数でないとすると，$a=4k+2$ とおけ，$a^2=(4k+2)^2=16k^2+16k+4$ となるので，$a^2$ は 8 で割ると 4 余る．

また，平方数の分類☒より，奇数の平方数は 8 で割ると 1 余るから，$b$, $c$ は共に奇数なので，$c^2-b^2$ は 8 で割り切れる．

よって，$a^2=c^2-b^2$ は成立しない．したがって，$a$ は 4 の倍数である．

合同式を利用した解答

(1)

$c \equiv 0 \pmod 2$ だと仮定すると，$a$, $b$, $c$ 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 $a \equiv 1 \pmod 2$, $b \equiv 1 \pmod 2$ でなければならない．このとき，平方数の分類☒より，$a^2 \equiv 1 \pmod 4$, $b^2 \equiv 1 \pmod 4$ なので，$a^2+b^2 \equiv 2 \pmod 4$．しかし，平方数の分類☒より $c^2 \equiv 0 \ or \ 1 \pmod 4$ なので矛盾．よって，$c$ は奇数である．

(2)

$a \equiv 0 \pmod 3$, $b \equiv 0 \pmod 3$ とすると，平方数の分類☒より，$a^2 \equiv 0 \pmod 3$, $b^2 \equiv 0 \pmod 3$ なので，$a^2+b^2 \equiv 0$

(mod 3)．平方数の分類☒より，$c^2 \equiv 0 \pmod 3$ ならば，$c \equiv 0 \pmod 3$ なので，$a$, $b$, $c$ は全て 3 の倍数になり，$a$, $b$, $c$ 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であることに矛盾する．

$a$, $b$ が共に 3 の倍数でないとすると，平方数の分類☒より，$a^2 \equiv 1 \pmod 3$, $b^2 \equiv 1 \pmod 3$ なので，$a^2 + b^2 \equiv 2 \pmod 3$．平方数の分類☒より，$c^2 \equiv 0 \ or \ 1 \pmod 3$ なので矛盾する．

以上より，$a$, $b$ のうち 1 つは 3 の倍数である．

■

## 応用問題 1

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．

[1990 年一橋大前期]

【考え方】

三平方の定理 $a^2 + b^2 = c^2$ より，$a$, $b$, $c$ の偶奇性は決まる．先ほどの問題同様，平方数の分類を考えて，平方数を 4 または 8 で割った余りを考えよう．

【解説】

直角三角形の 3 辺を $a$, $b$, $c$ とし，$c$ を斜辺とする．このとき，三角形の面積 $S$ は

$$S = \frac{1}{2}ab$$

となる．$a^2 + b^2 = c^2$ より，$a$, $b$ が共に奇数になることはない．なぜならば，共に奇数だと，$a$ も $b$ も 4 で割ると 1 余るので，$a^2 + b^2$ は 4 で割ると 2 余ることになり，平方数を 4 で割った余りは 0 か 1 なので矛盾するからである．よって，ともに偶数か，一方が偶数で他方が奇数．

$a$, $b$ が共に偶数のとき，$ab$ は 4 の倍数になるので $S = \frac{1}{2}ab$ は 2 の整数倍である．

$a$, $b$ のうち一方が偶数で他方が奇数のとき，$a$ を偶数，$b$ を奇数とする．このとき $c$ は奇数である．このとき，$a$ が 4 の倍数であることを示すために，$a$ が 4 の倍数でないと仮定し $a = 4k + 2$ とおくと，

$$a^2 = (4k + 2)^2 = 16k^2 + 16k + 4 = 16k(k + 1) + 4$$

より，$a^2$ を 8 で割った余りは 4 である．$b$, $c$ は奇数なので，8 で割った余りが 1 だから，$a^2 + b^2 = c^2$ は成立しない．よって，$a$ は 4 の倍数である．したがって，$S = \frac{1}{2}ab$ は 2 の整数倍である．

以上より，$S = \frac{1}{2}ab$ は 2 の整数倍である．

■

一橋大学からもう 1 問類題を出しておく．文字が 4 つに増えてはいるが，先ほどの問題と全く同じである．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．

## 応用問題 2

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．

[1994 年一橋大後期]

【考え方】

(1) 背理法を利用する．$a$, $b$, $c$ の中に 3 の倍数が 3 個，1 個，0 個ある場合に矛盾が生じることを示す．

(2) $d$ 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，背理法による証明を行う．先ほどの練習問題では 8 で割った余りに注目したが，この問題では何で割った余りに注目すればよいのだろうか．ここが最大のポイントになる．

本問も (1) では，合同式を利用できるが，ほとんど大差ないので合同式による解答は省略する．

【解説】

(1)

$d$ は 3 の倍数ではないので，平方数の分類☒より，$d^2$ は 3 で割ると 1 余る．

(i)$a$, $b$, $c$ がすべて 3 の倍数であるとき，平方数の分類☒より，$a^2$, $b^2$, $c^2$ はすべて 3 で割り切れるので，$a^2 + b^2 + c^2$ も 3 で割り切れる．$d^2$ は 3 で割ると 1 余るから矛盾．

(ii)$a$, $b$, $c$ の中に 3 の倍数が 1 個あるとき，平方数の分類☒より，$a^2$, $b^2$, $c^2$ はそのうち 1 つが 3 で割り切れ，残りの 2 つは 3 で割ると 1 余るので，$a^2 + b^2 + c^2$ は 3 で割ると 2 余る．$d^2$ は 3 で割ると 1 余るから矛盾．

(iii)$a$, $b$, $c$ がすべて 3 の倍数でないとき，平方数の分類☒より，$a^2$, $b^2$, $c^2$ はすべて 3 で割ると 1 余るので，$a^2 + b^2 + c^2$ は 3 で割ると 3 余る，つまり 3 で割り切れる．$d^2$ は 3 で割ると 1 余るから矛盾．

以上より，$a$, $b$, $c$ の中に 3 の倍数がちょうど 2 つある．

(2)

(1) より，$a$, $b$, $c$ の中に 3 の倍数がちょうど 2 つあるので，$a = 3l$, $b = 3m$, $c = 3n \pm 1$ と表しても一般性を失わない．このとき，6 の倍数になる可能性があるのは $a$ または $b$ であ

る．よって，$a$, $b$ ともに 6 の倍数でないと仮定すると，$l$, $m$ はともに奇数になるので $l=2p+1$, $m=2q+1$ とおけ，$a=6p+3$, $b=6q+3$ となる．また，$d$ が 2 の倍数でも 3 の倍数でもないから $d=6k\pm1$ とおける．

このとき，

$$\begin{aligned}c^2&=d^2-a^2-b^2\\&=(6k\pm1)^2-(6p+3)^2-(6q+3)^2\\&=36k^2\pm12k+1-36p^2-36p-9-36q^2-36q-9\\&=12(6k^2\pm1-3p^2-3p-3q^2-3q-2)+7\end{aligned}$$

なので，$c^2$ は 12 で割ると 7 余る．一方，

$$\begin{aligned}c^2&=(3n+1)^2\\&=9n^2+6n+1\\&=6n(n+1)+3n^2+1\end{aligned}$$

$n(n+1)$ は偶数なので $6n(n+1)$ は 12 で割り切れるので，$c^2$ を 12 で割った余りは $3n^2+1$ を 12 で割った余りに一致する．しかし平方数の分類☒により，$n^2$ を 4 で割った余りは 0 か 1 にしかならないから $3n^2+1$ を 12 で割った余りは 1 か 4 に限られる．よって，矛盾である．

■

---

## 京大入試問題 2

$n$, $a$, $b$ を 0 以上の整数とする．$a$, $b$ を未知数とする方程式

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

を考える．

(1) $n\geqq 2$ 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．

[2004 年前期文系]

---

**【考え方】**

(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．なお，この問題でも (1) で合同式も利用できるが，それほど大差ないので省略する．

(2) (1) より，$n\geqq 2$ ならば $a$, $b$ 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．

**【解説】**

合同式を利用しない解答

(1)

$a$, $b$ のうち 1 つが奇数で他方が偶数の場合，$a^2+b^2$ は奇数になるので矛盾．また，どちらも奇数の時，$a^2$ と $b^2$ はともに 4 で割ると 1 余るので，$a^2+b^2$ は 4 で割ると 2 余る．いま $n\geqq 2$ だから，$2^n$ は 4 の倍数になるので矛盾．よって，$a$, $b$ はともに偶数である．

(2)

$n\geqq 2$ のとき，(1) より $a$, $b$ が共に偶数だから，$a=2a_1$, $b=2b_1$ とおけ，$(*)$ に代入して，${a_1}^2+{b_1}^2=2^{n-2}$ となる．さらに，$n-2\geqq 2$ ならば，$a_1=2a_2$, $b_1=2b_2$ とおけて，${a_2}^2+{b_2}^2=2^{n-4}$ となる．この操作を繰り返すと，右辺が $2^0$ か $2^1$ になる．

$n$ が偶数のとき，$n=2k$ とおいて，上の操作を $k$ 回繰り返すと

$${a_k}^2+{b_k}^2=2^0=1$$

これをみたす $(a_k,\ b_k)$ は，$(a_k,\ b_k)=(1,\ 0),\ (0,\ 1)$．よって，$(a,\ b)=2^k(a_k,\ b_k)=(2^{\frac{n}{2}},\ 0),\ (0,\ 2^{\frac{n}{2}})$．

$n$ が奇数のとき，$n=2k+1$ とおいて，上の操作を $k$ 回繰り返すと

$${a_k}^2+{b_k}^2=2^1=2$$

これをみたす $(a_k,\ b_k)$ は，$(a_k,\ b_k)=(1,\ 1)$．よって，$(a,\ b)=2^k(a_k,\ b_k)=(2^{\frac{n-1}{2}},\ 2^{\frac{n-1}{2}})$．

■

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．

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．

☆因数分解の重要公式☆

公式① $n$ 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② $n$ 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．

---

**例 10**

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．

[2001 年津田塾大 (英文)]

---

【考え方】

この問題は，因数分解の公式そのものなので難しくない．しかし，合同式がその威力を発揮するのは，まさにこのような問題である．合同式を利用した解法をぜひ学んでほしい．

【解説】

合同式を利用しない解答

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．

合同式を利用した解答

$-1\equiv 10 \pmod{11}$ だから，

$$10^n-(-1)^n\equiv 10^n-10^n\equiv 0 \pmod{11}$$

となるので，11 の倍数である．

■

---

## 練習問題 11

(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．

[2005 年同志社大]

---

【考え方】

(1) は因数分解の公式そのものである．

(2) は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，合同式はその威力を発揮する．

【解説】

合同式を利用しない解答

(1)

$4^n-1=4^n-1^n$ となるので，前問と同様に，公式①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)

$n=2m$ のとき，

$$2^n+1=2^{2m}+1=4^m+1=4^m-1+2$$

となり，(1) より，$4^m-1$ は 3 の倍数だから，$2^n+1$ は 3 で割ると 2 余る．

$n=2m+1$ のとき，

$$2^n+1=2^{2m+1}+1=4^m\times 2+1=2(4^m-1)+3$$

となり，(1) より，$4^m-1$ は 3 の倍数だから，$2^n+1$ は 3 で割り切れる．

よって，$2^n+1$ が 3 で割り切れるような自然数 $n$ は $n$ が奇数であることである．

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．

(2)

$2\equiv -1 \pmod{3}$ 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．

■

---

## 練習問題 12

$k$ と $m$ は正の整数とする．

(1) $m$ が奇数のとき，$k^m+2^m$ は $k+2$ で割り切れることを示せ．

(2) $m$ が偶数のとき，$k^m+2^m$ は $k+2$ で割り切れれば，$k+2$ は $2^{m+1}$ の約数になることを示せ．

---

**【考え方】**

(1) は $m$ が奇数なので因数分解の公式をそのまま適用すればよい．

(2) は $m$ が偶数なので，$k^m+2^m$ は式としては因数分解できない (つまり数値として $k+2$ で割り切れているということ)．しかし，$k^m-2^m$ ならば式として因数分解でき $k+2$ で割り切れることになる．

**【解説】**

(1)

$m$ が奇数だから，

$$\begin{aligned}&k^m+2^m\\=&(k+2)(k^{m-1}-k^{m-2}2+\cdots-k2^{m-2}+2^{m-1})\end{aligned}$$

と因数分解できるので，$k^m+2^m$ は $k+2$ で割り切れる．

(2)

$m$ が偶数のとき，$k^m+2^m$ が $k+2$ で割り切れることより，

$$k^m+2^m=(k+2)A$$

とおける．また，

$$\begin{aligned}&k^m-2^m\\=&k^m-(-2)^m\\=&\{k-(-2)\}B\\=&(k+2)B\end{aligned}$$

と因数分解できる．よって，

$$\begin{cases}k^m+2^m=(k+2)A & \cdots①\\ k^m-2^m=(k+2)B & \cdots②\end{cases}$$

よって，① − ② より，

$$2^{m+1}=(k+2)(A-B)$$

よって，$k+2$ は $2^{m+1}$ の約数になる．

■

次の問題は，$m$, $n$ に適当に数を代入して規則性をみつける方法もある (できなくはないがかなり面倒．一度各自で規則性を調べてみよ)．しかし，これも因数分解を考えれば方針は簡単にわかるだろう．

---

## 京大入試問題 3

$m$, $n$ 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．

[1996 年後期理系]

---

**【考え方】**

「$m^n+1$, $n^m+1$ がともに 10 の倍数となる $m$, $n$ を 1 組与えよ．」ということなので，とにかく条件に合う $m$, $n$ を見つけさえすればよい．つまり自分に都合の良いように勝手に設定する．

因数分解の公式から,$m$, $n$ が共に奇数であれば，$m^n+1$, $n^m+1$ は共に因数分解できることになる．

**【解説】**

$m$, $n$ が共に奇数であれば，$m^n+1$, $n^m+1$ は次のように因数分解できる．

$$m^n+1=(m+1)(m^{n-1}-m^{n-2}+m^{n-3}-\cdots+m^2-m+1)$$
$$n^m+1=(n+1)(n^{m-1}-n^{m-2}+n^{m-3}-\cdots+n^2-n+1)$$

よって，$m^n+1$, $n^m+1$ がともに 10 の倍数となるには，$m+1$ と $n+1$ をともに 10 の倍数にすればよいので，$m<n$ となる $m$, $n$ として，$m=9$, $n=19$ とおけばよい．

■

### ***Remark*** 11

上の問題で「自分に都合の良いように勝手に設定してよいので，$m$, $n$ が共に奇数とする」と述べたが，$m$, $n$ は必然的に共に奇数にならざるをえない．なぜなら，$m$, $n$ のうち少なくとも一方が偶数のときは，$m^n+1$, $n^m+1$ の少なくとも一方が奇数となり，$m^n+1$, $n^m+1$ がともに 10 の倍数となることはないからである．

□

さて，先ほどより指数型の問題では 2 つの因数分解の公式が重要であると述べてきたが，もうひとつ，忘れてはならない公式がある．

それは，次にあげる二項定理である．

☆二項定理☆

$$(a+b)^n=\sum_{k=0}^{n}{}_n\mathrm{C}_k a^{n-k}b^k$$

二項定理より，

$$\begin{aligned}(a+b)^n &={}_n\mathrm{C}_0a^nb^0+{}_n\mathrm{C}_1a^{n-1}b^1+\cdots\\ &\quad\cdots+{}_n\mathrm{C}_{n-1}a^1b^{n-1}+{}_n\mathrm{C}_na^0b^n\\ &=(a\text{ の倍数})+b^n\end{aligned}$$

となるので，$(a+b)^n$ を $a$ で割った余りは，$b^n$ を $a$ で割った余りに等しいことがわかる．このことは合同式からも明らかである．つまり，

$$a+b\equiv b \pmod a$$

だから，

$$(a+b)^n\equiv b^n \pmod a$$

また，$m$ を整数とするとき，

$$am+b\equiv b \pmod a$$

だから，

$$(am+b)^n\equiv b^n \pmod a$$

であることもわかる．この，合同式の性質から明らかなことを二項定理を用いて証明したわけである．

これらは公式として使いたいところだが，やはり入試本番の記述答案では，二項定理できちんと書いて示した方が良いであろう．

整数問題で二項定理を利用するのは意外かもしれないが，とても重要で役に立つ公式である．先ほどの同志社大学の練習問題は因数分解を用いて解答したが，二項定理でも解くことができるので，もう一度紹介する．

## 練習問題 13

(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．

[2005 年同志社大]

【解説】

(1)
二項定理より，

$$\begin{aligned}4^n&=(3+1)^n\\ &=\sum_{k=0}^{n}{}_n\mathrm{C}_k3^{n-k}1^k\\ &={}_n\mathrm{C}_03^n1^0+{}_n\mathrm{C}_13^{n-1}1^1+\cdots\\ &\quad\cdots+{}_n\mathrm{C}_{n-1}3^11^{n-1}+{}_n\mathrm{C}_n3^01^n\\ &=(3\text{ の倍数})+1\end{aligned}$$

なので，$4^n-1$ は 3 の倍数である．

(2)
二項定理より，

$$\begin{aligned}2^n+1&=(3-1)^n+1\\ &=\sum_{k=0}^{n}{}_n\mathrm{C}_k3^{n-k}(-1)^k\\ &={}_n\mathrm{C}_03^n(-1)^0+{}_n\mathrm{C}_13^{n-1}(-1)^1+\cdots\\ &\quad\cdots+{}_n\mathrm{C}_{n-1}3^1(-1)^{n-1}+{}_n\mathrm{C}_n3^0(-1)^n+1\\ &=(3\text{ の倍数})+(-1)^n+1\end{aligned}$$

なので，これが 3 の倍数になるためには，$(-1)^n+1=0$ でなければならないので，$n$ は奇数である．

■

## 練習問題 14

$4^n-1$ が 15 の倍数となるような $n$ をすべて求めよ．

[2008 年大阪大後期理系より]

【考え方】

先ほどの同志社の問題の結果を知っていれば，$4^n-1$ が 3 の倍数になることがわかるので，あとは $4^n-1$ が 5 の倍数にもなることを示せばよい．$4^n-1=(5-1)^n-1$ と変形すれば $n$ の条件はわかるだろう．

なお，同志社の問題の結果を知らない場合，直接に 15 の倍数であることを示すこともできる．別解で紹介しよう．この場合，$n=1,\ 2,\ 3,\ \cdots$ と実際に計算して結果を予測せねばならないことに注意しよう．

【解説】

(同志社大の結果を利用して)$4^n-1$ は 3 の倍数になる．

また，

$$\begin{aligned}4^n-1&=(5-1)^n-1\\ &=(5\text{ の倍数})+(-1)^n-1\end{aligned}$$

であるので，これが 5 の倍数になるための条件は $n$ が偶数であることである．

よって，$4^n-1$ が 15 の倍数となるような $n$ は

$$n=2k\quad(k\text{ は 0 以上の整数})$$

である．

【別解 1】

(実際に計算し，$n$ が偶数の時が 15 の倍数になると予想をした上で)

$n=2k$ のとき，

$$\begin{aligned}4^n-1&=4^{2k}-1\\&=16^k-1\\&=(16-1)(16^{k-1}+16^{k-2}+\cdots 1)\\&=15(16^{k-1}+16^{k-2}+\cdots 1)\end{aligned}$$

であるので，15 の倍数になる．

$n=2k+1$ のとき，

$$\begin{aligned}4^n-1&=4^{2k+1}-1\\&=4\times 16^k-1\\&=4(16^k-1)+3\end{aligned}$$

$(16^k-1)$ は 15 の倍数であるので，$4(16^k-1)+3$ は 15 の倍数にならない．

よって，$4^n-1$ が 15 の倍数となるような $n$ は

$$n=2k\quad (k \text{ は } 0 \text{ 以上の整数})$$

である．

■

---

**例 11**

$2^n$ を 3 で割った余りを求めよ．

---

【考え方】

$n=1,\ 2,\ 3,\cdots$ 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．この問題でも合同式を利用すると計算が速く簡単である．

【解説】

合同式を利用しない解答

二項定理より，

$$\begin{aligned}2^n&=(3-1)^n\\&=\sum_{k=0}^{n}{}_n\mathrm{C}_k 3^{n-k}(-1)^k\\&={}_n\mathrm{C}_0 3^n(-1)^0+{}_n\mathrm{C}_1 3^{n-1}(-1)^1+\cdots\\&\qquad\cdots+{}_n\mathrm{C}_{n-1}3^1(-1)^{n-1}+{}_n\mathrm{C}_n 3^0(-1)^n\\&=(3\text{ の倍数})+(-1)^n\end{aligned}$$

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．

合同式を利用した解答

$2\equiv -1 \pmod 3$ だから，$2^n\equiv(-1)^n \pmod 3$．よって，$2^n$ を 3 で割った余りは $(-1)^n$ を 3 で割った余りに等しい．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．

■

---

## 練習問題 15

$2^n$ 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．

---

【考え方】

必要十分条件を求めるのだから，双方向の証明をせねばならない．直接証明が困難な場合は，対偶命題を証明すると良い．なお，ここでも合同式は，素晴らしい働きをする．

【解説】

合同式を利用しない解答

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

$n=3m$ とおくと，$2^n=2^{3m}=8^m$ となる．二項定理より，

$$\begin{aligned}2^n&=8^m\\&=(7+1)^m\\&=\sum_{k=0}^{m}{}_m\mathrm{C}_k 7^{m-k}1^k\\&={}_m\mathrm{C}_0 7^m+{}_n\mathrm{C}_1 7^{m-1}+\cdots+{}_m\mathrm{C}_{m-1}7^1+{}_m\mathrm{C}_m 7^0\\&=(7\text{ の倍数})+1\end{aligned}$$

よって，7 で割った余りが 1 である．

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

対偶を証明する．

$n=3m+1$ のとき，$2^n=2^{3m+1}=2\times 8^m$ となる．二項定理より，

$$\begin{aligned}2^n&=2\times 8^m\\&=2(7+1)^m\\&=2\sum_{k=0}^{m}{}_m\mathrm{C}_k 7^{m-k}1^k\\&=2({}_m\mathrm{C}_0 7^m+{}_m\mathrm{C}_1 7^{m-1}+\cdots+{}_m\mathrm{C}_{m-1}7^1+{}_m\mathrm{C}_m 7^0)\\&=2((7\text{ の倍数})+1)\\&=(7\text{ の倍数})+2\end{aligned}$$

よって，7 で割った余りが 2 である．

$n=3m+2$ のとき, $2^n=2^{3m+2}=4\times 8^m$ となる．二項定理より，

$$\begin{aligned}2^n&=4\times 8^m\\&=4(7+1)^m\\&=4\sum_{k=0}^{m}{}_m\mathrm{C}_k 7^{m-k}1^k\\&=4({}_m\mathrm{C}_0 7^m+{}_m\mathrm{C}_1 7^{m-1}+\cdots+{}_m\mathrm{C}_{m-1}7^1+{}_m\mathrm{C}_m 7^0)\\&=4((7\text{ の倍数})+1)\\&=(7\text{ の倍数})+4\end{aligned}$$

よって，7 で割った余りが 4 である．

したがって，$n$ が 3 の倍数でないとき，$2^n$ を 7 で割ったときの余りが 1 ではない．

以上より，対偶が証明された．

合同式を利用した解答

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

$n=3m$ とおくと，$2^n=2^{3m}=8^m$ となる．

$$8^m\equiv 1^m\equiv 1 \pmod 7$$

より，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 $\Longrightarrow$ $n$ が 3 の倍数」の証明．

対偶を証明する．

$n=3m+1$ のとき，$2^n=2^{3m+1}=2\times 8^m$ となるので，

$$2\times 8^m\equiv 2\times 1^m\equiv 2 \pmod 7$$

より，7 で割った余りが 2 になることがわかる．

$n=3m+2$ のとき，$2^n=2^{3m+2}=4\times 8^m$ となるので，

$$4\times 8^m\equiv 4\times 1^m\equiv 4 \pmod 7$$

より，7 で割った余りが 4 になることがわかる．

したがって，$n$ が 3 の倍数でないとき，$2^n$ を 7 で割ったときの余りが 1 ではない．

以上より，対偶が証明された．

■

## 練習問題 16

(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．

[2003 年一橋大前期]

【考え方】

(1) は, $n=1,\ 2,\ 3,\ 4,\ \cdots$ と実験してみると，規則性が見えてくると思う．すると，$n$ を 3 で分類すればよいことに気付くだろう．合同式を用いると早い．

(2) も，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，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ろう．先程の例がヒントになっている．

(1)(2) ともに，$n=3m,\ 3m+1,\ 3m+2$ と設定してもよいが，$n=3m,\ 3m\pm 1$ と設定した方が，特に (2) において，効力を発する．

本問でも，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ない．なお，二項定理の計算では，途中の展開式を省略した．各自で補って考えてほしい．

【解説】

合同式を利用しない解答

(1)

$n=3m$ のとき，

$$\begin{aligned}n^3+1&=(3m)^3+1\\&=27m^3+1\end{aligned}$$

$n=3m+1$ のとき，

$$\begin{aligned}n^3+1&=(3m+1)^3+1\\&=27m^3+27m^2+9m+1+1\\&=3(9m^3+9m^2+3m)+2\end{aligned}$$

$n=3m-1$ のとき，

$$\begin{aligned}n^3+1&=(3m-1)^3+1\\&=27m^3-27m^2+9m-1+1\\&=3(9m^3-9m^2+3m)\end{aligned}$$

したがって，$n^3+1$ が 3 で割り切れる $n$ は，3 で割って 2 余る自然数．

(2)

$n=3m$ のとき，

$$\begin{aligned}n^n+1&=(3m)^{3m}+1\\&=(3\text{ の倍数})+1\end{aligned}$$

$n=3m+1$ のとき，

$$\begin{aligned}n^n+1&=(3m+1)^{3m+1}+1\\&=\sum_{k=0}^{3m+1}{}_{3m+1}\mathrm{C}_k(3m)^{3m+1-k}1^k+1\\&=(3\text{ の倍数})+1^{3m+1}+1\\&=(3\text{ の倍数})+2\end{aligned}$$

$n=3m-1$ のとき，

$$\begin{aligned} n^n+1 &= (3m-1)^{3m-1}+1 \\ &= \sum_{k=0}^{3m-1} {}_{3m-1}\mathrm{C}_k (3m)^{3m-1-k}(-1)^k+1 \\ &= (3\text{ の倍数})+(-1)^{3m-1}+1 \end{aligned}$$

よって，$n^n+1$ を 3 で割った余りは，$(-1)^{3m-1}+1$ である．

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

よって，$m$ が偶数の時 $-(-1)^m+1=-1+1=0$ で，奇数の時 $-(-1)^m+1=1+1=2$ となるので，$m$ が偶数の時に，3 で割り切れる．このとき，$m=2l$ とすると，$n=3(2l)-1=6l-1$．すなわち，$n$ は 6 で割ると 5 余る自然数．

したがって，$n^n+1$ が 3 で割り切れる $n$ は，6 で割って 5 余る自然数である．

合同式を利用した解答

(1)

$n\equiv 0 \pmod 3$ のとき，$n^3+1\equiv 1 \pmod 3$．

$n\equiv 1 \pmod 3$ のとき，$n^3+1\equiv 2 \pmod 3$．

$n\equiv 2 \pmod 3$ のとき，$n^3+1\equiv 9\equiv 0 \pmod 3$

だから，$n\equiv 2 \pmod 3$

(2)

$n\equiv 0 \pmod 3$ のとき，

$$n^n+1\equiv 0^n\equiv 1 \pmod 3$$

$n\equiv 1 \pmod 3$ のとき，

$$n^n+1\equiv 1^n+1\equiv n+1\equiv 2 \pmod 3$$

$n\equiv 2 \pmod 3$ のとき，

$$n^n+1\equiv 2^n+1\equiv (-1)^n+1 \pmod 3$$

だから，

$$(-1)^n+1\equiv 0 \pmod 3$$

となるのは，$n\equiv 2 \pmod 3$ かつ $n\equiv 1 \pmod 2$ のときである．

よって，$n\equiv 5 \pmod 6$

■

***Remark* 12**

$n\equiv 2 \pmod 3$ のとき，$n$ をすべて 2 に変えて，

$$n^n+1\equiv 2^2+1 \pmod 3$$

としてはいけない．

□

**発展 2**

最後の結論部分は，連立合同方程式

$$\begin{cases} n\equiv 2 \pmod 3 \cdots ☒ \\ n\equiv 1 \pmod 2 \cdots ☒ \end{cases}$$

の解が，$n\equiv 5 \pmod 6$ であることを意味している．この連立合同方程式は，『中国剰余定理 (Chinese reminder theorem)』により，解が一意に存在することが分かっているが，具体的に解くには，次のようにする．

まず，☒より，$n=2t+1$ となるので，

$$n=2t+1\equiv 2 \pmod 3$$

$$\therefore 2t\equiv 1 \pmod 3$$

両辺を 2 倍して，

$$\therefore t\equiv 2 \pmod 3$$

よって，

$$n\equiv 2\cdot 2+1\equiv 5 \pmod 6$$

となる．

合同式を利用しない解答の最後の部分と比べてほしい．全く同じ内容を，合同式を利用してわざわざ難しそうに表現しているだけのような気がしないだろうか．

□

---

## 応用問題 3

$n$ 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．

[2007 年お茶女大前期理系]

---

【考え方】

(1) は，そのまま $n=3l+1$ とおいて計算すればわかる．

(2) も同様に，$n=3l+2$ とおいても構わないが，計算がかな

り面倒になる．$m$ が奇数であることも考慮して，$n=3l-1$ とおくのが良いだろう．

【解説】

合同式を利用しない解答

(1)

$n=3l+1$ のとき，二項定理より，

$$\begin{aligned}(3l+1)^m &= \sum_{k=0}^{m} {}_m\mathrm{C}_k (3l)^{m-k} 1^k \\ &= (3\text{ の倍数})+1\end{aligned}$$

となるので，$n^m$ を 3 で割った余りは 1 である．

(2)

$n=3l-1$ とおくと，

$$\begin{aligned}(3l-1)^m &= \sum_{k=0}^{m} {}_m\mathrm{C}_k (3l)^{m-k} (-1)^k \\ &= (3\text{ の倍数})+(-1)^m\end{aligned}$$

となる．$m$ は奇数だから，$(-1)^m=-1$.

よって，$n^m$ を 3 で割った余りは 2 である．

(3)

$n$ が 3 の倍数ならば，全ての自然数 $m$ に対して $n^m$ も 3 の倍数であり，$n$ が 3 で割って 1 余るならば，全ての自然数 $m$ に対して $n^m$ も 3 で割って 1 余る．

したがって，ある自然数 $m$ に対して，$n^m$ を 3 で割って余りが 2 であるならば，$n$ を 3 で割った余りは 0 でも 1 でもない．すなわち 2 である．

合同式を利用した解答

(1)

$n\equiv 1 \pmod 3$ のとき，

$$n^m \equiv 1 \pmod 3$$

だから，$n^m$ を 3 で割った余りは 1 である．

(2)

$n\equiv 2 \pmod 3$ のとき，

$$n^m \equiv 2^m \equiv (-1)^m \pmod 3$$

である．このとき，$m$ が奇数ならば，

$$n^m \equiv -1 \equiv 2 \pmod 3$$

となるので，$n^m$ を 3 で割った余りは 2 である．

■

## 応用問題 4

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．

[2003 年奈良県立医大前期]

【考え方】

「6 の倍数＝ 2 の倍数かつ 3 の倍数」に注目．$S_n$ は明らかに 2 の倍数になるので，$S_n$ が 3 の倍数になるための条件を考えればよい．なお，合同式を利用しない解答では当然，二項定理を利用せねばならないが，記述の煩わしさから，最大限簡略化して表現してみた．やはり合同式を利用した方が，解答はスリムになる．

【解説】

合同式を利用しない解答

(1)

$S_n=1^n+2^n+3^n+4^n$ において，$1^n+3^n$ は常に偶数になるので，$S_n$ は偶数である．よって，$S_n$ が 3 の倍数になる条件を考える．そのためには，$3^n$ は 3 の倍数だから，$1^n+2^n+4^n$ が 3 の倍数になればよい．$1^n+2^n+4^n=1+(3-1)^n+(3+1)^n$ だから，$1^n+2^n+4^n$ を 3 で割った余りは $1+(-1)^n+1$ だから，これが 3 で割り切れるためには，$(-1)^n=1$, すなわち $n$ が偶数であれば良い．よって，$S_n$ が 6 の倍数になる条件は，$n$ が偶数であること．

(2)

$S_n$ が 3 の倍数でない場合は明らかに $S_n$ は 12 の倍数にならない．$S_n$ が 3 の倍数のとき，$S_n$ が 4 の倍数にならないことを示せばよい．(1) より $S_n$ が 3 の倍数のとき $n$ は偶数である．$n\geqq 2$ だから $2^n$ は 4 の倍数になり，$4^n$ は 4 の倍数だから，$1^n+3^n$ が 4 の倍数になるかどうか考える．$1^n+3^n=1+(4-1)^n$ だから，$1^n+3^n$ を 4 で割った余りは $1+(-1)^n$. ここで $n$ は偶数だから，余りは 2 となる．つまり 4 の倍数ではない．したがって，$S_n$ は 4 の倍数にはならない．

以上より，$S_n$ は 12 の倍数にならない．

合同式を利用した解答

(1)

$S_n=1^n+2^n+3^n+4^n$ において，

$$S_n \equiv 1^n+0^n+1^n+0^n \equiv 2 \equiv 0 \pmod 2$$

だから，$S_n$ は偶数である．よって，$S_n$ が 3 の倍数になる条件を考える．

$$S_n \equiv 1^n+(-1)^n+0^n+1^n \equiv (-1)^n+2 \pmod 3$$

だから，$n$ が偶数であれば, 3 で割り切れる．よって，$S_n$ が 6 の倍数になる条件は，$n$ が偶数であること．

(2)

$S_n$ が 3 の倍数でない場合は明らかに $S_n$ は 12 の倍数にならない．$S_n$ が 3 の倍数のとき，$S_n$ が 4 の倍数にならないこ

とを示せばよい．(1) より $S_n$ が 3 の倍数のとき $n$ は偶数である．よって，$n=2m$ とおくと，

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

したがって，$S_n$ は 4 の倍数にはならない．

以上より，$S_n$ は 12 の倍数にならない．

■

***Remark* 13**

上の 合同式を利用しない解答 の本質部分は，次の二項定理による計算である．時間的に余裕があれば，きちんと答案に書いた方が望ましい．

$$\begin{aligned} 2^n &= (3-1)^n \\ &= \sum_{k=0}^{n} {}_nC_k 3^{n-k}(-1)^k \\ &= {}_n\mathrm{C}_0 3^n(-1)^0 + {}_n\mathrm{C}_1 3^{n-1}(-1)^1 + \cdots \\ &\qquad \cdots + {}_n\mathrm{C}_{n-1} 3^1(-1)^{n-1} + {}_n\mathrm{C}_n 3^0(-1)^n \\ &= (3\text{ の倍数}) + (-1)^n \end{aligned}$$

$$\begin{aligned} 4^n &= (3+1)^n \\ &= \sum_{k=0}^{n} {}_nC_k 3^{n-k}1^k \\ &= {}_n\mathrm{C}_0 3^n 1^0 + {}_n\mathrm{C}_1 3^{n-1}1^1 + \cdots \\ &\qquad \cdots + {}_n\mathrm{C}_{n-1} 3^1 1^{n-1} + {}_n\mathrm{C}_n 3^0 1^n \\ &= (3\text{ の倍数}) + 1 \end{aligned}$$

$$\begin{aligned} 3^n &= (4-1)^n \\ &= \sum_{k=0}^{n} {}_nC_k 4^{n-k}(-1)^k \\ &= {}_n\mathrm{C}_0 4^n(-1)^0 + {}_n\mathrm{C}_1 4^{n-1}(-1)^1 + \cdots \\ &\qquad \cdots + {}_n\mathrm{C}_{n-1} 4^1(-1)^{n-1} + {}_n\mathrm{C}_n 4^0(-1)^n \\ &= (4\text{ の倍数}) + (-1)^n \end{aligned}$$

□

**☆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，$n$ を余りで分類したり，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整数問題の基本的，かつ最重要な手法である．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．

## 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☆**

$p$ を素数とするとき，次の性質が成り立つ．

性質① $ab$ が $p$ で割り切れる
$\Longrightarrow$ $a$ または $b$ が $p$ で割り切れる

性質② $p=ab \Longrightarrow (a,\ b)=(1,\ p)$ or $(p,\ 1)$

性質③ $p$ は $a$ $(1 \leqq a \leqq p-1)$ と互いに素

性質④ $p$ は $(p-1)!$ と互いに素

特に，素数に関する問題を解くには，

①積の形をつくること
②実験して規則性を予想すること

が重要である．

まずは，これらを意識した問題から始めよう．

---

**例 12**

$n$ を 2 以上の自然数とするとき，$n^4+4$ は素数にはならないことを示せ．

---

**【考え方】**

「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よい．

**【解説】**

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

と因数分解できる．$n \geqq 2$ だから，

$$\begin{aligned} n^2-2n+2 &= (n-1)^2+1 \geqq 2 \\ n^2+2n+2 &= (n+1)^2+1 \geqq 10 \end{aligned}$$

となるので，$n^4+4$ は素数にはならない．

■

---

## 練習問題 17

$n^4+n^2+1$ が素数になるような自然数 $n$ を全て求めよ．

---

**【考え方】**

複 2 次式の因数分解を思い出そう．

**【解説】**

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

だから，$n^4+n^2+1$ が素数 $p$ になるとき，

$$(n^2+n+1,\ n^2-n+1) = (p,\ 1),\ (1,\ p)$$

の組み合わせが考えられるが，$n$ は自然数なので，$n^2+n+1 \geqq 3$ だから，$(n^2+n+1,\ n^2-n+1) = (p,\ 1)$ の場合しかない．このとき，$n^2-n+1=1$ より $n=1$ となり，$n^2+n+1=3$ は素数である．よって，求める自然数は $n=1$．

■

---

## 練習問題 18

$3p+1$ が平方数になるような素数 $p$ は $p=5$ のときに限ることを証明せよ．

---

**【考え方】**

問題文の言い回し注意しよう．「平方数になるような素数 $p$ は $p=5$ のときに限る」ことを示すには，

・$p=5$ 以外のすべての素数で平方数にならないことを示す．

・平方数になるのは $p=5$ だけであることを示す．

の二つの方法が考えられるが，どちらの方が証明しやすいだろうか．当然，後者の方である．したがって，まず，「$3p+1$ が平方数になる」ことを定式化するために，$3p+1=m^2$ とおくことから始まるだろう．

**【解説】**

$3p+1=m^2$ とすると，$3p=(m+1)(m-1)$ だから，

| $m+1$ | 1 | 3 | $p$ | $3p$ |
|---|---|---|---|---|
| $m-1$ | $3p$ | $p$ | 3 | 1 |

これらの各場合を検証し，$p=5$ を得る．

■

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．

---

## 練習問題 19

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．

[2001 年千葉大後期理系]

---

**【考え方】**

$x^3+y^3=(x+y)(x^2-xy+y^2)=p^2$ より，素因数の組合せを考え，一つ一つ検証していくしかない．

**【解説】**

$x^3+y^3=(x+y)(x^2-xy+y^2)=p^2$ より，

| $x+y$ | 1 | $p$ | $p^2$ |
|---|---|---|---|
| $x^2-xy+y^2$ | $p^2$ | $p$ | 1 |

の各場合が考えられる．

(i) $(x+y,\ x^2-xy+y^2) = (1,\ p)$ の場合
$x,\ y$ は自然数だから，$x+y \geqq 2$ となるので不適．

(ii) $(x+y,\ x^2-xy+y^2) = (p,\ p)$ の場合

$x^2-xy+y^2=(x+y)^2-3xy=p$ より，

$$x+y=p,\quad xy=\frac{p^2-p}{3}$$

よって，$x,\ y$ は

$$t^2-pt+\frac{p^2-p}{3}=0$$

の実数解だから，判別式 $\geqq 0$ より，

$$D=p^2-4\frac{p^2-p}{3}\geqq 0$$

これより，$p^2-4p\leqq 0$ だから $0\leqq p\leqq 4$. これを満たす素数は $p=2,\ 3$ となる.

$p=2$ のとき，$p^2=4=x^3+y^3$ を満たす自然数はない.

$p=3$ のとき，$p^2=9=x^3+y^3$ を満たす自然数は $(x,\ y)=(1,\ 2),\ (2,\ 1)$ と存在する.

(iii) $(x+y,\ x^2-xy+y^2)=(p^2,\ 1)$ の場合

$x^2-xy+y^2=1$ より $x^2-yx+y^2-1=0$ を $x$ の 2 次方程式とみて，$x$ は実数だから，判別式 $\geqq 0$ より，

$$D=y^2-4(y^2-1)\geqq 0$$

これより，$y^2\leqq\frac{4}{3}$ だから $y=1$. このとき $x^2-x=0$ となるので $x=1$ と定まる ($x,\ y$ は自然数だから). このとき，$x+y=2=p^2$ を満たす素数 $p$ は存在しない.

以上より，$p=3,\ (x,\ y)=(1,\ 2),\ (2,\ 1)$.

(ii) の場合の別解

$x+y=x^2-xy+y^2$ より，$x^2-(y+1)x+y^2-y=0$ として判別式 $\geqq 0$ より，

$$D=(y+1)^2-4(y^2-y)\geqq 0$$

これより，$3y^2-6y-1\leqq 0$ だから

$$\frac{3-2\sqrt{2}}{3}\leqq y\leqq\frac{3+2\sqrt{3}}{3}$$

これを満たす自然数 $y$ は $y=1,\ 2$ となる. それぞれの場合に $x$ を求めて $p$ を決定する.

■

## 練習問題 20

$a,\ b$ 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.

[2007 年千葉大後期理系]

【考え方】

$x^n-y^n,\ x^n+y^n$ の因数分解の公式を利用せよ.

【解説】

(1)

$$\begin{aligned}&a^b-1\\=&a^b-1^b\\=&(a-1)(a^{b-1}+a^{b-2}1+a^{b-3}1^2+\\&\qquad\cdots+a^2 1^{b-3}+a1^{b-2}+1^{b-1})\\=&(a-1)(a^{b-1}+a^{b-2}+a^{b-3}+\cdots+a^2+a+1)\end{aligned}$$

であり，$a^{b-1}+a^{b-2}+a^{b-3}+\cdots+a^2+a+1>1$ なので，$a^b-1$ が素数 $p$ に等しいとき，

$$\begin{aligned}&a-1=1\\&a^{b-1}+a^{b-2}+a^{b-3}+\cdots+a^2+a+1=p\end{aligned}$$

となる. つまり $a=2$ である.

次に「$2^b-1$ が素数のとき $b$ も素数である」ことを背理法を利用して証明する.

$b$ が素数でないと仮定すると，$b=mn(m,\ n$ は 2 以上の整数) とおけるので，

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

となり，$2^{mn}-1$ は素数ではない. よって矛盾.

以上より，$a=2$ で $b$ は素数である.

(2) $b$ が奇数の因数 $l$ をもつとき，$b=lm(l$ は奇数) とすると，

$$\begin{aligned}&2^{lm}+1\\=&(2^m)^l+1^l\\=&(2^m+1)((2^m)^{l-1}-(2^m)^{l-2}+(2^m)^{l-3}-\\&\qquad\cdots+(2^m)^2-2^m+1)\end{aligned}$$

となるので，これは素数にはならない.

■

**発展 3**

上の問題の (1) では，

$$2^n-1\text{ が素数}\quad\Longrightarrow\quad n\text{ は素数}$$

は真であることがわかったが，その逆，

$$n\text{ が素数}\quad\Longrightarrow\quad 2^n-1\text{ は素数}$$

は真ではない ($2^{11}-1=2047=23\times 89$).

一般に，$2^p-1$($p$ は素数) の形をした素数を Mersenne 素数という．指数 $p$ がどのような素数のときに $2^p-1$ が素数になるのかはまだ完全に解明されていない．

ちなみに，$p<10000$ の素数で $2^p-1$ が素数になる $p$ は

$$p=2,3,5,7,13,17,17,31,61,89,107,127,521,607,$$
$$1279,2203,2281,3217,4253,4423,9689,9941$$

で全てである．

「Mersenne 素数の研究」は，そのまま「大きな素数の研究」につながっている．素数は無限に存在することは分かっているが (後ほど証明する)，具体的に大きな素数を見つけることは，暗号理論などにも応用される重要な研究テーマである．

2008 年 8 月現在，知られている最も大きな素数は $2^{43112609}-1$ で，1297 万 8789 桁の素数である．これはわずか 46 番目の Mersenne 素数で，47 番目の Mersenne 素数を求めることが次の課題である．

□

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 $\Longrightarrow$ 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 13**

$p$ を 5 以上の素数とするとき，$p^2+2$ は必ず合成数になることを証明せよ．

---

**【考え方】**

まずは，$p$ にいろいろな素数を代入して実験してみよう．

| $p$ | 5 | 7 | 11 | 13 | 17 | 19 | 23 |
|---|---|---|---|---|---|---|---|
| $p^2+2$ | 27 | 51 | 123 | 172 | 251 | 363 | 531 |

「合成数になる」ということは「ある数の倍数になる」ということだから，表をじっくりと見て，ある数の倍数になっていないかどうかを考える．

**【解説】**

5 以上の素数は，3 で割って余りが 1 の素数と余りが 2 の素数に分かれる．

$p=3m+1$ のとき，

$$p^2+2=(3m+1)^2+2=3(3m^2+2m+1)$$

$p=3m+2$ のとき，

$$p^2+2=(3m+2)^2+2=3(3m^2+2m+2)$$

だから，いずれの場合も 3 の倍数になっているので，$p^2+2$ は合成数である．

■

***Remark* 14**

平方数の分類①を考えれば明らかな問題であろう．

□

---

**京大入試問題 4**

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．

[2004 年前期理系]

---

**【考え方】**

このような問題ではまず $n$ にいろいろな数を代入して，規則性を予測し，証明の糸口を見つけることが大切である．

| $n$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| $n^2+2$ | 6 | 11 | 18 | 27 | 37 | 51 | 66 | 83 |

確かに，共に素数になるのは $n=3$ だけであることがわかるが，逆に，両方とも素数になっていない組に共通する性質を考えよう．素数にならない＝合成数＝ある数の倍数であることに注意する．すると，素数でない数に共通する性質として，それらがすべて 3 **の倍数になっている**ことがわかると思う．つまり，$n$, $n^2+2$ のいずれか 1 つが必ず 3 の倍数になっていることに気づくことが重要である．そうすれば，$n$ を 3 で割った余りで分類すればとよいことがわかると思う．さらに，$n^2$ 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．

**【解説】**

$n=2$ のとき，$n^2+2=6$ は素数ではない．

$n\geqq 3$ のとき，$k$ を自然数として，$n=3k,\ 3k+1,\ 3k+2$ とおける．

$n=3k$ のとき，$n$ が素数になるのは $k=1$ のときに限られる．このとき，$n=3,\ n^2+2=11$ はともに素数である．

$n=3k+1$ のとき，

$$\begin{aligned} n^2+2 &= (3k+1)^2+2 \\ &= 9k^2+6k+3 \\ &= 3(3k^2+2k+1) \end{aligned}$$

$3k^2+2k+1 \geqq 6$ であるので，$n^2+2$ は素数ではない．

$n=3k+2$ のとき，

$$\begin{aligned} n^2+2 &= (3k+2)^2+2 \\ &= 9k^2+12k+6 \\ &= 3(3k^2+4k+2) \end{aligned}$$

$3k^2+2k+1 \geqq 9$ であるので，$n^2+2$ は素数ではない．

以上より，$n$ と $n^2+2$ がともに素数になるのは，2 以上の自然数 $n$ では，$n=3$ に限られる．

■

この京都大の問題と全く同じ問題が 2 年前に早稲田大で出題されていた．

---

## 練習問題 21

$n$ 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．

[2004 年早稲田大 (政経)]

---

**【考え方】**

先ほどの京都大の問題と同様に，まずはいろいろな $n$ で試して，規則性を発見することが必要である．

| $n$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|
| $n+2$ | 3 | 4 | 5 | 6 | 7 | 9 | 8 | 9 | 11 |
| $n+4$ | 5 | 6 | 7 | 8 | 9 | 10 | 9 | 10 | 13 |

京都大の問題と全く同じ状況であることに気づくと思う．

つまり，3 数とも素数になるのは $n=3$ だけであることがわかるが，逆に，3 数とも素数にならない組に共通する性質として，それらがすべて 3 **の倍数になっている**ことがわかると思う．つまり，$n,\ n+2,\ n+4$ のいずれか 1 つが必ず 3 の倍数になっていることに気づくことが重要である．そうすれば，$n$ を 3 で割った余りで分類すればとよいことがわかると思う．

**【解説】**

$n=1,\ 2$ のときは，$n,\ n+2,\ n+4$ がいずれも素数であることはない．

$n \geqq 3$ のとき，$k$ を自然数として，$n=3k,\ 3k+1,\ 3k+2$ とおける．

$n=3k$ のとき，$n$ が素数になるのは $k=1$ のときに限られる．このとき，$n=3,\ n+2=11,\ n+4=7$ はともに素数である．

$n=3k+1$ のとき，$n+2=3k+3=3(k+1)$．$k+1 \geqq 2$ であるので，$n+2$ は素数ではない．

$n=3k+2$ のとき，$n+4=3k+6=3(k+2)$．$k+2 \geqq 3$ であるので，$n+4$ は素数ではない．

以上より，$n,\ n+2,\ n+4$ がいずれも素数になる自然数 $n$ は，$n=3$ に限られる．

■

***Remark*** **15**

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 4 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 ($n$〜$n+4$ の中に 6 の倍数が 2 個存在することになる！)．

□

また，一橋大でも同様の問題が出題されている．

---

## 応用問題 5

(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．

[2005 年一橋大後期]

---

**【考え方】**

京都大，早稲田大の問題同様に，まずは実験してみて規則性を発見せねばならない．

| $p$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| $2p+1$ | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 |
| $4p+1$ | 9 | 13 | 17 | 21 | 25 | 29 | 33 | 37 |

| $q$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|
| $2q+1$ | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 |
| $4q-1$ | 7 | 11 | 15 | 19 | 23 | 27 | 31 | 35 |
| $6q-1$ | 11 | 17 | 23 | 29 | 35 | 41 | 47 | 53 |
| $8q+1$ | 17 | 25 | 33 | 41 | 49 | 57 | 65 | 73 |

何の数で割った余りで分類すればよいのだろうか．

**【解説】**

(1)

$p=2$ のとき，$4p+1=9$ は素数ではない．

$p=3$ のとき，$p,\ 2p+1,\ 4p+1$ がいずれも素数である．

$p>3$ のとき，$k$ を自然数として，$p=3k+1,\ 3k+2$ とおける．

$p=3k+1$ のとき，$2p+1=2(3k+1)+1=3(2k+1)$ となるので，$2p+1$ は素数ではない．

$p=3k+2$ のとき，$4p+1=4(3k+2)+1=3(4k+3)$ となるので，$4p+1$ は素数ではない．

以上より，$p,\ 2p+1,\ 4p+1$ がいずれも素数であるのは，$p=3$ に限られる．

(2)

$q=2$ のときは，全て素数となる．

$q=3$ のときは，$8q+1=25$ は素数ではない．

$q=5$ のときは，全て素数となる．

$q>5$ のとき，$k$ を自然数として，$q=5k+1,\ 5k+2,\ 5k+3,\ 5k+4$ とおける．

$q=5k+1$ のとき，$6q-1=6(5k+1)-1=5(6k+1)$ となるので，$6q-1$ は素数ではない．

$q=5k+2$ のとき，$2q+1=2(5k+2)+1=5(2k+1)$ となるので，$2q+1$ は素数ではない．

$q=5k+3$ のとき，$8q+1=8(5k+3)+1=5(8k+5)$ となるので，$8q+1$ は素数ではない．

$q=5k+4$ のとき，$4q-1=4(5k+4)-1=5(4k+3)$ となるので，$4q-1$ は素数ではない．

以上より，$q,\ 2q+1,\ 4q-1,\ 6q-1,\ 8q+1$ がいずれも素数であるのは，$q=2,\ 5$ に限られる．

■

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」 $\Longrightarrow$ 「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．

---

## 応用問題 6

整数 $19^n+(-1)^{n-1}2^{4n-3}$ $(n=1,\ 2,\ 3,\ \cdots)$ のすべてを割り切る素数を求めよ．

[1986 年東工大]

---

**【考え方】**

まずは，$n=1,\ 2,\ 3,\ \cdots$ と代入して，全てを割り切る素数を見つける必要がある．

**【解説】**

$a_1=19+2=21=7\times 3$

$a_2=19^2-2^5=329=7\times 47$

となるので，全てを割り切る素数は 7 であることが予想される．よって，「$a_n$ が 7 で割り切れること」を数学的帰納法で証明する．

(i) $n=1$ のときは，$a_1=21$ は 7 の倍数になるので，明らかに成立．

(ii) $n=k$ のとき成立すると仮定すると，

$$\begin{aligned}a_{k+1}&=19^{k+1}+(-1)^k2^{4(k+1)-3}\\&=19\cdot 19^k-(-1)^{k-1}\cdot 2^4\cdot 2^{4k-3}\\&=19\cdot 19^k-16\cdot(-1)^{k-1}\cdot 2^{4k-3}\\&=19\cdot 19^k-16(a_k-19^k)\\&=35\cdot 19^k-16a_k\\&=7\cdot 5\cdot 19^k-16a_k\end{aligned}$$

したがって，$n=k$ の仮定より $a_k$ は 7 の倍数だから，$a_{k+1}$ も 7 の倍数になる．よって，$n=k+1$ のときも成立する．

(i)(ii) より，全ての自然数 $n$ で成立する．

よって，求める素数は 7 である．

■

***Remark* 16**

帰納法を使わずに，合同式でも 7 の倍数になることを証明できるが，式変形にはかなりの工夫と経験が必要かもしれない．

$$\begin{aligned}&19^n+(-1)^{n-1}2^{4n-3}\\\equiv\ &19^n+(-1)^{n-1}2^{4n-4}2^1 &&\pmod 7\\\equiv\ &5^n+(-1)^{n-1}16^{n-1}2^1 &&\pmod 7\\\equiv\ &5^n+(-16)^{n-1}2^1 &&\pmod 7\\\equiv\ &5^n+2\cdot 5^{n-1} &&\pmod 7\\\equiv\ &5\cdot 5^{n-1}+2\cdot 5^{n-1} &&\pmod 7\\\equiv\ &7\cdot 5^{n-1} &&\pmod 7\\\equiv\ &0 &&\pmod 7\end{aligned}$$

□

それでは最後に，素数が無限にあることの証明を紹介しておこう．

---

## 応用問題 7

素数は無限に存在することを示せ．

---

**【考え方】**

背理法による．素数が有限個だったと仮定して矛盾を示す．

**【解説】**

素数が有限個であったと仮定すると，最大の素数が存在するので，その素数を $M$ とおく．すなわち，

$$2,\ 3,\ 5,\ \cdots M$$

が素数の全てである．

このとき，

$$a = 2 \cdot 3 \cdot 5 \cdot \cdots \cdot M + 1$$

とすると，$a$ は自然数なので，素数であるか合成数であるかのいずれかである．

$a$ が素数ならば，$a$ は $M$ よりも大きい素数になるので，$M$ の最大性に矛盾する．

$a$ が合成数ならば，全ての素数 2, 3, 5, $\cdots M$ で割り切れなければならないが $a$ を 2, 3, 5, $\cdots M$ のいずれの素数で割っても 1 余るので，$a$ を割り切る素数は 2, 3, 5, $\cdots M$ より大きな素数になる．これは $M$ の最大性に矛盾する．

よって，素数は無限に存在することが示せた．

■

**発展 4**

ユークリッドは『原論』の中で，素数が無限に存在することを示したが，背理法は用いられていない．興味のある人は，ユークリッドがどのように証明したのかを調べてみよう．

□

# 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．

### 3.0.1　偶奇性

整数の問題を考えるとき，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 $\Longleftrightarrow$ $m$, $n$ の偶奇は一致する
$m-n$ が偶数 $\Longleftrightarrow$ $m$, $n$ の偶奇は一致する
$m+n$ が奇数 $\Longleftrightarrow$ $m$, $n$ の偶奇は一致しない
$m-n$ が奇数 $\Longleftrightarrow$ $m$, $n$ の偶奇は一致しない
$mn$ が奇数 $\Longleftrightarrow$ $m$, $n$ は共に奇数

---

**例 14**

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．

[2002 年お茶女大後期 (理数)]

---

**【考え方】**

まずは，内接円の半径 $r$ を 3 辺 $a$, $b$, $c$ で表すことから始めよう

**【解説】**

$c$ を直角三角形の斜辺として一般性を失わない．このとき，内接円の半径 $r$ は

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

となる (各自で求めよ．整数問題の範疇でないので省略する)．$a^2+b^2=c^2$ より，$(a+b)^2-c^2 = 2ab =$ 偶数 であるから，$b+c$ と $a$ の偶奇性は一致する (つまり，$a+b$ と $c$ は共に偶数か共に奇数)．よって，$a+b-c$ は必ず偶数になるので，$r$ は整数である．

**【別解 1】**

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

$a^2+b^2=c^2$ より，$a$, $b$ が共に奇数になることはない (平方数の分類のところで詳しく述べたので理由は省略)．よって，$a$ も $b$ も偶数の時，$c$ も偶数になるから，$a+b-c$ は偶数．

$a$, $b$ のうち，どちらか一方が偶数で他方が奇数の時，$c$ は奇数になるので，$a+b-c$ は偶数．

したがって，いずれの場合も，$a+b-c$ は偶数になるので，$r$ は整数である．

■

---

**練習問題 22**

$a$, $b$ 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．

[2006 年津田塾大 (数)]

---

**【考え方】**

$D = a^2 - 4b = m^2$ とおけば，解は $x = \dfrac{-a \pm \sqrt{D}}{2} = \dfrac{-a \pm m}{2}$．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．

【解説】

$D=a^2-4b=m^2$ とおけば，解は

$$x=\frac{-a\pm\sqrt{D}}{2}=\frac{-a\pm m}{2}$$

となる．$D=a^2-4b=m^2$ より，$(a+m)(a-m)=4b=$ 偶数 となる．また，$(a+m)+(a-m)=2a=$ 偶数 ともなるので，$a+m$ と $a-m$ は共に偶数である．

したがって，解の分子部分 $-a+m$ と $-a-m$ が偶数だから，解は整数になる．

■

***Remark* 17**

上の問題は逆も成立する．つまり，

判別式が平方数　$\Longleftrightarrow$　解は整数

なお，このことは $x^2$ の係数が 1 で，他の係数も整数の 2 次方程式においてのみいえることであり，一般的には当然成り立ってはいない．

□

## 練習問題 23

$p$, $q$ を整数とし，$f(x)=x^2+px+q$ とおく．$f(1)$ 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．

【考え方】

$f(1)$ も $f(2)$ も 2 で割り切れないことから，$p$ と $q$ の偶奇性が決まる．

【解説】

$f(1)=1+p+q$ が 2 で割り切れないことから，$p+q$ は偶数．$f(2)=4+2p+q$ が 2 で割り切れないことから，$q$ は奇数．したがって，$p$ も $q$ も奇数となる．

方程式 $f(x)=0$ が整数の解 $x=m$ をもつと仮定すると，$f(m)=0$ より，

$$m^2+pm+q=0$$
$$m(m+p)+q=0$$

$(m+q)-m=q$(奇数) だから，$m+q$ と $m$ の偶奇性は一致しないので，積 $m(m+q)$ は偶数である．

したがって，$m(m+p)+q=$ (偶数) + (奇数) が 0 になることはない

つまり，方程式 $f(x)=0$ は整数の解をもたない．

■

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．

## 練習問題 24

$n$ 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．

[2002 年東京女大 (文理)]

【考え方】

「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 $\Longleftrightarrow$ $n=6m+1, 6m+5$ (または，$n=6m\pm1$) とおける．

【解説】

$n=6m+1$ 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．よって，$12m(3m+1)$ は 24 の倍数．

$n=6m+5$ 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．よって，$12(m+1)(3m+2)$ は 24 の倍数．

以上より，$n^2-1$ が 24 の倍数であることがわかる．

■

***Remark* 18**

もし，偶奇性に気付かなければ，上の各場合において，$m=2k$, $m=2k+1$ と $m$ を偶奇でさらに場合分けして調べるしかない．

□

## 練習問題 25

正の整数の組 $(a,\ b)$ で $a$ 以上 $b$ 以下の整数の総和が 500 となるものをすべて求めよ．ただし，$a<b$ とする．

[1999 年大阪大前期文系]

---

【考え方】

まずは，等差数列の和の公式から，$a$ と $b$ の関係式をつくろう．整数問題の大原則「積の形をつくる」「素因数分解の一意性」を利用するだけだが，因数の組合せが多く大変そうだが...

【解説】

$a$ 以上 $b$ 以下の整数の総和は，初項 $a$，公差 1，項数 $b-a+1$ の等差数列の和だから，$\dfrac{(a+b)(b-a+1)}{2}$ である．これが 500 に等しいので，

$$(a+b)(b-a+1)=2^3\times 5^3$$

ここで，$(a+b)-(b-a+1)=2a-1=$ 奇数 だから，$a+b$ と $b-a+1$ の偶奇性は一致しない．奇数である方は $5,\ 5^2,\ 5^3$ のいずれかであり，$2a-1>0$ より，$a+b>b-a+1$ なので，

| $a+b$ | 200 | 40 | 125 |
|---|---|---|---|
| $b-a+1$ | 5 | 25 | 8 |

と組合せが決まるので，

$$(a,\ b)=(98,\ 102),\ (8,\ 32),\ (59,\ 66)$$

と定まる．

■

---

## 練習問題 26

$p,\ q$ を素数とする．このとき，$p+q,\ p-q$ も共に素数になるような $p,\ q$ を求めよ．

---

【考え方】

前の章で扱った素数の問題である．そこでは「素数は実験に限る」と述べたが，この問題では実験しようにも手掛かりが全くなく困ってしまう．しかし，$p+q,\ p-q$ と，和，差の形になっていることに注目し，偶奇性を考えれば手掛かりがつかめる．なお，この問題は京大プレ (平成 13 年) の問題．

【解説】

$(p+q)+(p-q)=2p=$ 偶数 なので，$p+q$ と $p-q$ の偶奇性は一致する．$p,\ q,\ p+q,\ p-q$ はいずれも素数であり，偶数の素数は 2 のみであるから，$p+q$ と $p-q$ がともに偶数になることはない．よって，$p+q$ と $p-q$ はともに奇数である．そのためには，$p$ と $q$ の偶奇は一致してはならないので，$p>q$ より，$q=2$ と定まる．

したがって，$p+2$ と $p-2$ がともに素数になるような素数 $p$ を決定する．

まず，$p=3$ の場合は不適である．$p>3$ である素数は，1 以上の整数 $k$ を用いて，$p=3k+1,\ 3k+2$ と書くことができる．

$p=3k+1$ のとき，$p+2=3(k+1)$ となり，$k+1\geqq 2$ だから $p+2$ は素数ではない．

$p=3k+2$ のとき，$p-2=3k$ となり，$k\geqq 1$ だから $p+2$ が素数になるのは $k=1$ のときに限られる．すなわち，$p=5$ である．

よって，以上より，条件を満たす素数 $p,\ q$ は $p=5,\ q=2$.

■

***Remark* 19**

つまり，$p-2,\ p,\ p+2$ がともに素数になるような素数 $p$ を決定する問題であり，これは，先ほどの**練習問題 34** と同じである．

□

---

## 京大入試問題 5

$p$ は 3 以上の素数であり，$x,\ y$ は $0\leqq x\leqq p,\ 0\leqq y\leqq p$ 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．

[2003 年前期文系]

---

【考え方】

$x^2$ 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，$(x+y)(x-y)$ が $2p$ の倍数になることがわかる．ここで，素因数 2 と $p$ の分配を考えるのだが，$x+y$ と $x-y$ の偶奇性を考えることで，組合せが限定される．

【解説】

$$x^2=2pq_1+r$$
$$y^2=2pq_2+r$$

より，$x^2-y^2=2p(q_1-q_2)$ となる．つまり，$(x+y)(x-y)$ が $2p$ の倍数になる．

また，$(x+y)+(x-y)=2y=$ (偶数) だから $x+y$ と $x-y$ の積と和が共に偶数になるので，$x+y$ と $x-y$ は共に

偶数になる．いま，$p$ は 3 以上の素数だから奇数である．よって，$x+y$ と $x-y$ の少なくとも一方は $2p$ の倍数になる．

$0 \leqq x \leqq p,\ 0 \leqq y \leqq p$ より，

$$0 \leqq x+y \leqq 2p,\ -p \leqq x-y \leqq p$$

となるので，$x+y$ が $2p$ の倍数になるのは，$x+y=0,\ 2p$ のときで，$x-y$ が $2p$ の倍数になるのは $x-y=0$ のときである．いずれの場合も $x=y$ となるので，題意は証明された．

■

---

## 京大入試問題 6

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)．

[1989 年後期理系]

---

**【考え方】**

(1) まずは $m$ と $n$ の最大公約数を $g$ とおき，$m=gm'$，$n=gn'$ ($m'$，$n'$ は互いに素) としよう．この問題の場合，$a$ と $b$ の最大公約数を持ち出さないといけないので，$a$，$b$ 主体で話を進めるために，$a$，$b$ を $m$，$n$ で表すことを考える．つまり，$g(m'-n')=8a$，$g(11n'-3m')=8b$ となる．ここから $g$ が $8a$ と $8b$ の約数であることがわかる．問題は，ここからである．

(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．

**【解説】**

(1)

$m$ と $n$ の最大公約数を $g$ とし，

$$m=gm',\ n=gn'\quad (m',\ n'\text{は互いに素})$$

とおく．このとき，

$$m-n=g(m'-n')=8a$$
$$11n-3m=g(11n'-3m')=8b$$

となる．このことから $g$ が $8a$ と $8b$ の約数であり，$a$ と $b$ の最大公約数が $d$ だから

$$g \text{ は } 8d \text{ の約数} \quad \cdots ☒$$

になることがわかる．

また，$a$，$b$ は $d$ の倍数なので $m$，$n$ も $d$ の倍数である．$a$，$b$ が奇数であることより，$m$，$n$ は偶数．また $d$ は奇数だから，$m$，$n$ は $2d$ の倍数である．つまり，

$$g \text{ は } 2d \text{ の倍数} \quad \cdots ☒$$

したがって，☒☒より，$g$ は $8d$ の約数かつ $2d$ の倍数だから，$d$ は，$2d$，$4d$，$8d$ のいずれかである．

(2)

$m$，$n$ がともに平方数であると仮定すると，$m$，$n$ は偶数だから，$m=(2M)^2$，$n=(2N)^2$ とおける．$m-n=8a$ に代入すると，$4(M+N)(M-N)=8a$，すなわち，

$$(M+N)(M-N)=2a \quad \cdots ☒$$

である．いま，$(M+N)+(M-N)=2M=$ 偶数 だから，$M+N$ と $M-N$ は積和が偶数なので共に偶数になる．つまり $(M+N)(M-N)$ は 4 の倍数になるが，このとき☒より，$a$ は偶数になり，$a$ が奇数であることに矛盾する．

よって，$m$，$n$ がともに平方数であることはない．

■

### ***Remark*** 20

実は，この問題の (1) はユークリッドの互除法が背景にある．ユークリッドの互除法については後ほど説明する．

□

---

## 京大入試問題 7

$k$ 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．

[1992 年後期文系]

---

**【考え方】**

(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する．

(2) (1) の流れから考えて，求める必要十分条件は「$k$ が 8 の倍数であること」だと考えられるだろう．「奇数解をもつ $\Longrightarrow$ $k$ は 8 の倍数」は (1) で示せたが，その逆，「$k$ が 8 の倍

数 $\Longrightarrow$ 奇数解をもつ」ことの証明が問題である．奇数解をもつことを証明する最も手っ取り早い方法は，実際に奇数解をつくってみせることである．つまり，任意の 8 の倍数 $k$ に対して，奇数解 $x,\ y$ の実例が見つかればよい．

【解説】

(1)

奇数解を $x=2m+1,\ y=2n+1$ として代入すると，$(2m+1)^2-(2n+1)^2=k$ より，

$$4(m+n+1)(m-n)=k$$

ここで，$(m+n+1)+(m-n)=2m+1=$ 奇数 だから，$m+n+1$ と $m-n$ の偶奇性は一致しない．つまり，$m+n+1$ と $m-n$ のどちらか一方は偶数で，他方は奇数になるので積 $(m+n+1)(m-n)$ は必ず偶数．

よって，$4(m+n+1)(m-n)$ は 8 の倍数になるので，$k$ は 8 の倍数になる．

(2)

$k$ が 8 の倍数のとき，$k=8l$ とおくと，$x^2-y^2=8l\ \cdots$ ☒ となる．

ここで，$x=2l+1,\ y=2l-1$ を☒に代入すると成立しているため，$x=2l+1,\ y=2l-1$ は☒の奇数解である．よって，任意の 8 の倍数 $k$ に対して，$x^2-y^2=k$ を満たす奇数解が存在する．

(1) より，方程式 $x^2-y^2=k$ が奇数解をもてば，$k$ は 8 の倍数であることが示せているので，求める必要十分条件は，$k$ が 8 の倍数であること，である．

■

***Remark* 21**

(2) で，いきなり $x=2l+1,\ y=2l-1$ が表れていることに疑問を持つ人もいるだろう．実は，$x^2-y^2=(x+y)(x-y)=8l$ だから，$x+y=4l,\ x-y=2$ と勝手に設定して，$x,\ y$ を求めたのである．「どうして勝手に決めてよいのか」とか「他に組合せはないのか」とか思うかもしれない．しかし，【考え方】で述べたように，ここでは，とにかく何でもいいから奇数解を具体的に見つけさえすればよいわけだから，このような方法でも構わないのである．結果オーライということで．

□

### 3.0.2 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 15**

$3^{1000}$ の 1 の位の数字を求めよ．

---

【考え方】

まずは，$3^1,\ 3^2,\ 3^3,\ 3^4,\ 3^5,\cdots$ の 1 の位を順に調べて，規則性を予測する．

【解説】

$3^1,\ 3^2,\ 3^3,\ 3^4,\ 3^5,\cdots$ の 1 の位を順に調べると，$3,\ 9,\ 7,\ 1,\ 3,\ 9,\ 7,\ 1,\cdots$ 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)．

■

***Remark* 22**

一般に，任意の $x$ に対して，$f(x+a)=f(x)$ を満たす最小の正の数 $a$ を $f(x)$ の周期という．つまり，$a$ がこの関係を満たす最小の正の数かどうか確認しなければ $a$ が周期であるとは断言できない．したがって，上の例題の解答は単なる予想に過ぎず，厳密性に欠けると指摘されるかもしれないが，あまり気にしないでおこう．

気になる人は，1，2，3 は周期ではないことを確認し，$3^{n+4}$ と $3^n$ の 1 の位の数字が等しいこと，つまり，$3^{n+4}-3^n$ が 10 の倍数であることを示せばよい．

□

***Remark* 23**

1 の位の数字を調べるには合同式が有効である．つまり，

$$\begin{aligned}&a\text{ と }b\text{ の 1 の位の数字が等しい}\\ \Longleftrightarrow\ &a\equiv b\pmod{10}\end{aligned}$$

であるので，

$$3^{1000}\equiv 9^{500}\equiv(-1)^{500}\equiv 1\pmod{10}$$

だから，$3^{1000}$ の 1 の位は 1 とわかる．

また．$3^{n+4}$ と $3^n$ の 1 の位の数字が等しいことも，

$$3^{n+4}\equiv 3^4 3^n\equiv 81\cdot 3^n\equiv 3^n\pmod{10}$$

より，簡単にわかる．

□

---

## 練習問題 27

$7^{2007}$ 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

---

【考え方】

例 28 と同様に，$7^1,\ 7^2,\ 7^3,\ 7^4,\ 7^5,\cdots$ の 1 の位を順に調べて規則性を予測すること．

【解説】

$7^1,\ 7^2,\ 7^3,\ 7^4,\ 7^5,\cdots$ の 1 の位を順に調べると，$7,\ 9,\ 3,\ 1,\ 7,\ 9,\ 3,\ 1,\cdots$ と周期 4 で繰り返す．したがって，$7^{2007}$ の 1 の位は 3 である (2007 を 4 で割ると余り 3)．

また，$47^1,\ 47^2,\ 47^3,\ 47^4,\ 47^5,\cdots$ も 1 の位だけに注目して順に調べると，$7,\ 9,\ 3,\ 1,\ 7,\ 9,\ 3,\ 1,\cdots$ と周期 4 で繰り返す．したがって，$47^{2007}$ の 1 の位の数字は $7^{2007}$ の 1 の位の数字と同じで 3 である．

■

***Remark* 24**

$7^{2007}$ と $47^{2007}$ の 1 の位の数字が等しいことも合同式を用いれば簡単にわかる．つまり，$47 \equiv 7 \pmod{10}$ だから，

$$47^{2007} \equiv 7^{2007} \pmod{10}$$

である．

合同式を用いないなら，二項定理を利用して，

$$47^{2007} = (40+7)^{2007} = (10\text{ の倍数}) + 7^{2007}$$

とするしかない (途中の展開式は以前に詳しくやったので省略)．

□

---

## 練習問題 28

$2000^n$ を 7 で割った余りを $a_n$ とし，$S_n = a_1 + a_2 + \cdots + a_n$ 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．

[2000 年同志社大 (商)]

---

【考え方】

まずは実験して $a_n$ を予測するのだが，実際に，$2000^1,\ 2000^2,\ 2000^3,\ 2000^4,\ 2000^5,\cdots$ を計算してから 7 で割るだろうか？

2000 を 7 で割った余りは 5 であるので，$2000 = 7q + 5$ とおける．よって，二項定理より，

$$2000^2 = (7q+5)^2 = (7\text{ の倍数}) + 5^2$$
$$2000^3 = (7q+5)^3 = (7\text{ の倍数}) + 5^3$$
$$2000^4 = (7q+5)^4 = (7\text{ の倍数}) + 5^4$$

となるので，$a_n$ は $5^n$ を 7 で割った余りに等しいことがわかる．2000 に比べると計算は小さくなるが，これでもまともに計算するのは大変である．

この問題は，合同式を利用するに限る．

【解説】

$2000 \equiv 5 \pmod{7}$ であるので，

$$2000^2 \equiv 5^2 \equiv 4 \pmod{7}$$
$$2000^3 \equiv 5^3 \equiv 5\cdot 5^2 \equiv 5\cdot 4 \equiv 20 \equiv 6 \pmod{7}$$
$$2000^4 \equiv 5^4 \equiv (5^2)^2 \equiv 4^2 \equiv 2 \pmod{7}$$
$$2000^5 \equiv 5^5 \equiv 5^2\cdot 5^3 \equiv 4\cdot 6 \equiv 24 \equiv 3 \pmod{7}$$
$$2000^6 \equiv 5^6 \equiv (5^3)^2 \equiv 6^2 \equiv 36 \equiv 1 \pmod{7}$$
$$2000^7 \equiv 5^7 \equiv 5^1\cdot 5^6 \equiv 5^1 \equiv 5 \pmod{7}$$

以後，$5, 4, 6, 2, 3, 1$ を繰り返していく．

したがって，

$$5+4+6+2+3+1 = 21$$

ではじめて 7 で割り切れるから，最小の $n$ は $n = 6$.

■

---

## 応用問題 8

$11^{12^{13}}$ 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)]

---

【考え方】

まずは，$11^n$ の 10 の位に表れる数字の規則性を調べよう．

$$\begin{aligned}
11^1 &= 11\\
11^2 &= 121\\
11^3 &= 1331\\
11^4 &= 14641\\
11^5 &= 161051\\
11^6 &= 1771561\\
11^7 &= 19487171\\
11^8 &= 214358881\\
11^9 &= 2357947691\\
11^{10} &= 25937424601
\end{aligned}$$

よって，$11^n$ の 10 の位は $1, 2, 3, 4, 5, 6, 7, 8, 9, 0, \cdots$ を繰り返すことが予想される．まずは，この予想が正しいことを証明しよう．下 1 桁が 1 であることにも注意．

【解説】

$$\begin{aligned}11^n-1&=11^n-1^n\\&=(11-1)(11^{n-1}+11^{n-2}+\cdots+11^1+1)\\&=10(11^{n-1}+11^{n-2}+\cdots+11^1+1)\end{aligned}$$

である．

$11^{n-1}+11^{n-2}+\cdots+11^1+1$ の 1 の位を $a$ とすると，$11^n-1$ の 10 の位の数字は $a$，1 の位の数字は 0 だから，$11^n$ の 10 の位の数字は $a$ である．$n$ 個の数 $11^{n-1}, 11^{n-1}, \cdots, 11^1, 1$ は全て 1 の位が 1 であるので，$a$ は $n$ を　mod 10 で考えた数字に等しく，

$$n \equiv a \pmod{10}$$

したがって，$11^{12^{13}}$ の 10 の位の数字は，$12^{13}$ を　mod 10 で考えた数字に等しい．

$$12^{13} \equiv 2^{13} \equiv 1024 \times 8 \equiv 2 \pmod{10}$$

だから，$11^{12^{13}}$ の 10 の位の数字は 2 である．

■

---

## 京大入試問題 8

整数 $n$ に対し，$f(n)=\dfrac{n(n-1)}{2}$ 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．

[2001 年前期理系]

---

**【考え方】**

虚数単位 $i$ があるので，一瞬ひいてしまうが，具体的に実験して $a_n$ を計算すると，なんということはない．周期が 8 であることが簡単に予測される．あとは，このことを証明するだけである．

**【解説】**

$m$ を整数とする．$i^4=1$ に注意して，各場合を調べると，

$n=8m$ のとき，　$a_n=i^{4m(8m-1)}=1$
$n=8m+1$ のとき，　$a_n=i^{(8m+1)4m}=1$
$n=8m+2$ のとき，　$a_n=i^{(4m+1)(8m+1)}=i$
$n=8m+3$ のとき，　$a_n=i^{(8m+3)(4m+1)}=-i$
$n=8m+4$ のとき，　$a_n=i^{(4m+2)(8m+3)}=-1$
$n=8m+5$ のとき，　$a_n=i^{(8m+5)(4m+2)}=-1$
$n=8m+6$ のとき，　$a_n=i^{(4m+3)(8m+5)}=-i$
$n=8m+7$ のとき，　$a_n=i^{(8m+7)(4m+3)}=i$

となるので，$a_n$ は

$$1,\ 1,\ i,\ -i,\ -1,\ -1,\ -i,\ i$$

のくり返しであるから周期は 8 である．よって，$k$ は 8 の倍数．

■

---

## 京大入試問題 9

$n$ 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，$c_n=b_0+\cdots+b_n$ とおく．

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

[1994 年前期理系]

---

**【考え方】**

(1)(2) 前問同様に，まずは具体的に実験して規則性を予測することから始まるのだが，うまく規則性を見つけられるだろうか．

(3) 数学的帰納法で示すことになるのだが，(2) で求めた $\{c_n\}$ の漸化式が隣接 2 項間ではないことに注意しよう．通常の帰納法，つまり，$n=1$ のときを確認し，$n=k$ のときの成立を仮定して，$n=k+1$ のときの成立を示すという方法では，全ての $n$ について示すことにはならない．

**【解説】**

(1)

規則に従って，$\{a_n\}$，$\{b_n\}$，$\{c_n\}$ を計算すると，

| $n$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| $a_n$ | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | 55 | 89 |
| $b_n$ | 1 | 2 | 0 | 2 | 2 | 1 | 0 | 1 | 1 | 2 |
| $c_n$ | 1 | 3 | 3 | 5 | 7 | 8 | 8 | 9 | 10 | 12 |

となる．

$\{b_n\}$ は $1,2,0,2,2,1,0,1$ のくり返しである．

(2)

$$\begin{aligned}c_{n+8}&=b_0+\cdots+b_{n+8}\\&=c_n+(b_{n+1}+b_{n+2}+\cdots+b_{n+8})\end{aligned}$$

(1) より，$\{b_n\}$ は $1,2,0,2,2,1,0,1$ と周期 8 でくり返すので，$b_{n+1}$，$b_{n+2}$，$\cdots$，$b_{n+8}$ はちょうど 1 周期分に相当する．よって，

$$b_{n+1}+b_{n+2}+\cdots+b_{n+8}=b_0+b_1+\cdots+b_7=c_7$$

以上より，$c_{n+8}=c_n+c_7$ であることが示された．

(3)

$$n+1 \leqq c_n \leqq \frac{3}{2}(n+1) \quad \cdots ☒$$

$0 \leqq n \leqq 7$ のときは☒は成立している．

$n=k$ のとき，☒が成立すると仮定すると，$k+1 \leqq c_k \leqq \frac{3}{2}(k+1)$ であり，(2) より $c_{k+8}=c_k+c_7=ck+9$ だから，

$$k+1+9 \leqq c_{k+8} \leqq \frac{3}{2}(k+1)+9$$

このとき，

$$\frac{3}{2}(k+1)+9 \leqq \frac{3}{2}\{(k+8)+1\}$$

だから，

$$(k+8)+1 \leqq c_{k+8} \leqq \frac{3}{2}\{(k+8)+9\}$$

となる．これは $n=k+8$ のときの☒の成立を意味している．

よって，数学的帰納法により題意は証明された．

■

***Remark* 25**

$a_{n+2}=a_{n+1}+a_n$ より，$b_{n+2}$ は $b_{n+1}+b_n$ を 3 で割った余りになる．このことはつまり，$\bmod 3$ での足し算を意味している．解答中の表で $\{b_n\}$ の部分がまさに，$\bmod 3$ の足し算になっていることを確認せよ．

□

---

## 応用問題 9

整数からなる数列 $\{a_n\}$ を漸化式

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

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．

[1993 年東京大前期理系]

---

**【考え方】**

いまは，周期性や規則性をテーマに話を進めているので心配ないと思うが，このような問題では，まずは漸化式を解こうと思ってはいけない．解けなくはないが，解いたところで事態は悪くなる一方である．

とにかく $a_n$ を計算していき，規則性を考えていくのだが，この問題の場合，数字がだんだん大きくなってきて，かなり計算が大変になってくるので，少し工夫が必要である．

(1) は $a_n$ の偶奇性に関する性質を問う問題．3 の倍数番目だけ偶数になることを示せばよい．つまり，$a_n$ が，奇，奇，偶，奇，奇，偶，$\cdots$ と並んでいることを示せばよく，そのためには，$a_n$ の偶奇性の周期が 3 であることを示すことが目標となる．

(2) は 10 の倍数が「2 の倍数かつ 5 の倍数」であることに注目する．(1) より $a_n$ が 2 の倍数になるのは 3 の倍数番目であることが分かっているので，あとは 5 の倍数になるのは何番目なのかを調べることがポイント．実験して 5 の倍数になるところを見つけよう．

なお，合同式を用いると，もう少しすっきりした解答になるので，各自で試みてもらいたい．

**【解説】**

(1)

$$\begin{aligned} a_{n+3} &= 3a_{n+2}-7a_{n+1} \\ &= 3(3a_{n+1}-7a_n)-7a_{n+1} \\ &= 2a_{n+1}-21a_n \end{aligned}$$

なので，$a_{n+3}$ と $a_n$ の偶奇性は一致する．$a_1=1$(奇数)，$a_2=3$(奇数)，$a_3=2$(偶数) なので，以後，この周期で続いていくので，偶数である項は，$a_3$，$a_6$，$a_9$，$\cdots$ と 3 の倍数番目に現れる．

よって，$a_n$ が偶数になることと，$n$ が 3 の倍数になることとは同値である

(2)

(1) より，

$$\begin{aligned} a_{n+4} &= 2a_{n+2}-21a_{n+1} \\ &= 2(3a_{n+1}-7a_n)-21a_{n+1} \\ &= -15a_{n+1}-14a_n \\ &= -15(a_{n+1}+a_n)+a_n \end{aligned}$$

なので，$a_{n+4}$ を 5 で割った余りと $a_n$ を 5 で割った余りは等しい．$a_1=1$，$a_2=1$，$a_3=3$，$a_4=-15$ なので，5 の倍数は $a_4$ だけである．つまり，$a_n$ が 5 の倍数になるのは，$n$ が 4 の倍数になるときだけである．

よって，$a_n$ が 2 の倍数になるのは，$n$ が 3 の倍数になるときだけであり，$a_n$ が 5 の倍数になるのは，$n$ が 4 の倍数になるときだけであるので，$a_n$ が 10 の倍数になるための必要十分条件は，$n$ が 12 の倍数であることである．

■

実は，驚くべきことに，14 年前に同じく東京大学で次の問題が出題されていた．このことからも，過去問は 10 年〜15 年前の問題を中心に対策すべきであろう．

## 応用問題 10

$a$ を正の整数とし，数列 $\{u_n\}$ を次のように定める．

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

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．

[1979 年東京大文理共通]

**【考え方】**

$a$ を含むとはいえ，$u_1$，$u_2$，$u_3$，$\cdots$ を計算してみよう．

$$u_1 = 2$$
$$u_2 = a^2 + 2$$
$$u_3 = -a^2 + 2a - 2$$
$$u_4 = a^3 + a^2 + 2$$

$a$ がどういうときに，$\{u_n\}$ の項に 4 の倍数が現れるのか，現れないのかを考えるのだが，まず，$u_4$ をみれば明らかなように，$a$ が 4 で割ると 1 余る数のときに，$u_4$ は 4 の倍数になるので，この場合は不適．では，これ以外の場合はどうなのであろうか．

$a$ が 4 の倍数のとき，$u_1$，$u_2$，$u_3$，$u_4$ は全て 4 で割ると余りか 2.

$a$ が 4 で割ると 2 余る数のとき，$u_1$，$u_2$，$u_3$，$u_4$ は全て 4 で割ると余りは 2.

$a$ が 4 で割ると 3 余る数のとき，$u_1$，$u_2$，$u_3$，$u_4$ は全て 4 で割ると余りは 2 か 3.

ここで，大胆な仮説を立てる．「$a$ を 4 で割って余り 1 以外の場合が全部，条件に適するのかもしれない」と．

たった 4 つの項の情報だけから，このように予測するのはちょっと強引な持っていき方かもしれないが，東大数学の場合，これくらいの大胆さは必要である．何もせずに考え込むよりも，とりあえず何かやってみて駄目ならまた考え直そう，という強気な姿勢が大切である．

なお，この問題も合同式を用いると，すっきりした解答になるので，各自で試みてもらいたい．

**【解説】**

(i) $a = 4m + 1$ のとき，

$$\begin{aligned} u_4 &= a^3 + a^2 + 2 \\ &= (4m+1)^3 + (4m+1)^2 + 2 \\ &= (4m+1)^3 + (4m+1)^2 + 2 \\ &= 4(16m^3 + 16m^2 + 5m + 1) \end{aligned}$$

よって，$u_4$ が 4 の倍数になるので，不適．

(ii) $a = 4m + 2$ のとき，

$a$ も $u_1$ も $u_2$ も 4 で割ると 2 余る数である．3 以上の自然数 $n$ に対して，$u_{n-2} = 4k + 2$, $u_{n-1} = 4l + 2$ のとき，漸化式より，

$$\begin{aligned} u_n &= au_{n-2} - u_{n-1} \\ &= (4m+2)(4k+2) - (4l+2) \\ &= 4(4mk + 2m + 2k - l) + 2 \end{aligned}$$

だから，$u_n$ も 4 で割ると 2 余る数になる．よって，帰納的により，$\{u_n\}$ の項は全て 4 で割ると 2 余る数になるので，$\{u_n\}$ の項に 4 の倍数は現れない．

(iii) $a = 4m + 3$ のとき，

$a$ と $u_2$ は 4 で割ると 3 余る数で，$u_1$ は 4 で割ると 2 余る数である．3 以上の自然数 $n$ に対して，$u_{n-2} = 4k + 2$, $u_{n-1} = 4l + 3$ のとき，漸化式より，

$$\begin{aligned} u_n &= au_{n-2} - u_{n-1} \\ &= (4m+3)(4k+2) - (4l+3) \\ &= 4(4mk + 2m + 3k - l) + 3 \end{aligned}$$

だから，$u_n$ は 4 で割ると 3 余る数になる．

$u_{n-2} = 4k + 3$, $u_{n-1} = 4l + 3$ のとき，漸化式より，

$$\begin{aligned} u_n &= au_{n-2} - u_{n-1} \\ &= (4m+3)(4k+3) - (4l+3) \\ &= 4(4mk + 3m + 3k - l + 1) + 2 \end{aligned}$$

だから，$u_n$ は 4 で割ると 2 余る数になる．

$u_{n-2} = 4k + 3$, $u_{n-1} = 4l + 2$ のとき，漸化式より，

$$\begin{aligned} u_n &= au_{n-2} - u_{n-1} \\ &= (4m+3)(4k+3) - (4l+2) \\ &= 4(4mk + 3m + 3k - l + 1) + 3 \end{aligned}$$

だから，$u_n$ は 4 で割ると 3 余る数になる．よって，帰納的により，$\{u_n\}$ の項は全て 4 で割ると余りが，2,2,3 の繰り返しになるので，$\{u_n\}$ の項に 4 の倍数は現れない．

(iv) $a = 4m$ のとき，

$u_1$ も $u_2$ も 4 で割ると 2 余る数である．3 以上の自然数 $n$ に対して，$u_{n-2} = 4k + 2$, $u_{n-1} = 4l + 2$ のとき，漸化式より，

$$\begin{aligned} u_n &= au_{n-2} - u_{n-1} \\ &= 4m(4k+2) - (4l+2) \\ &= 4(4mk + 2m - l - 1) + 2 \end{aligned}$$

だから，$u_n$ も 4 で割ると 2 余る数になる．よって，帰納的により，$\{u_n\}$ の項は全て 4 で割ると 2 余る数になるので，$\{u_n\}$ の項に 4 の倍数は現れない．

以上，(i)〜(iv) より，求める条件は，$a$ を 4 で割ったときの余りが 1 ではないこと，である．

■

# 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，$\cdots$
>
> 定義①　$a$, $b$ が 1 以外の公約数をもたない
> (否定的定義)
>
> 定義②　$a$, $b$ の最大公約数が 1 である
> (肯定的定義)

***Remark*** **26**

「互いに素」を「互いに素数」と勘違いしている人が意外と多い．「$a$, $b$ が互いに素である」と「$a$, $b$ が素数である」は全く違う意味である．しかし「2 つの異なる素数は互いに素である」は正しいので注意しよう．

□

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①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②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 16**

$a$, $b$ 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①

$a+b$, $ab$ が 1 以外の公約数 $d$ をもつと仮定すると，

$$a+b = d \times m$$
$$ab = d \times m$$

となる ($m$, $n$ は整数)．このとき，$\cdots\cdots$

解②

$a+b$, $ab$ の最大公約数を $G$ とすると，

$$a+b = G \times m$$
$$ab = G \times m$$

となる ($m$, $n$ は互いに素)．このとき，$\cdots\cdots$

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，$a$, $b$ **が共通の素因数 $p$ 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最初の定義①，定義②による証明や別証明を考えるのだ)．

では具体的に，どのような証明方法になるのかを見ていくことにしよう．

そのためには，すでに紹介した☆整数問題の第三原則☆と☆素数 $p$ の性質①②☆を利用する．もう一度，紹介しておく．

**☆整数問題の第三原則☆**

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 $c$ の約数であり，$b$ は $d$ の約数である．つまり $c$ は $a$ で割り切れ，$d$ は $b$ で割り切れる．

**☆素数 $p$ の性質☆**

$p$ を素数とするとき，次の性質が成り立つ．

性質① $ab$ が $p$ で割り切れる
$\Longrightarrow a$ または $b$ が $p$ で割り切れる

性質② $p = ab \Longrightarrow (a,\ b) = (1,\ p)$ or $(p,\ 1)$

これらの性質をうまく利用して，互いに素であることの証明をする．

---

## 練習問題 29

(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，$a^2+b^2,\ ab$ は互いに素であることを示せ．

---

**【考え方】**

背理法による．つまり (1) では，$a+b,\ ab$ が共通の素数 $p$ で割り切れると仮定して矛盾を示す．

**【解説】**

(1)

$a+b,\ ab$ 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，

$$a+b = pm \cdots ①$$
$$ab = pn \cdots ②$$

となる．②より，$a$ または $b$ が素数 $p$ で割り切れる．$a$ が $p$ で割り切れるとき，①より $b = pm - a$ だから，$b$ も $p$ で割り切れることになり，$a,\ b$ が互いに素であることに矛盾する．$b$ が $p$ で割り切れる場合も同様である．

したがって，$a+b,\ ab$ は互いに素である．

(2)

$a^2+b^2,\ ab$ 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，

$$a^2+b^2 = pm \cdots ①$$
$$ab = pn \cdots ②$$

となる．②より，$a$ または $b$ が素数 $p$ で割り切れる．$a$ が $p$ で割り切れるとき，$a = p\alpha$ とおいて①に代入すると，$b^2 = pm - p^2\alpha^2 = p(m - p\alpha^2)$．よって $b$ も $p$ で割り切れることになり，$a,\ b$ が互いに素であることに矛盾する．$b$ が $p$ で割り切れる場合も同様である．

したがって，$a^2+b^2,\ ab$ は互いに素である．

■

***Remark* 27**

上の練習問題は逆も成立する．つまり，必要十分条件である．

$$a+b,\ ab \text{ が互いに素} \Longleftrightarrow a,\ b \text{ は互いに素}$$
$$a^2+b^2,\ ab \text{ が互いに素} \Longleftrightarrow a,\ b \text{ は互いに素}$$

証明は対偶をとることで簡単に示せる．

□

---

**例 17**

(1) 連続する 2 つの自然数は互いに素であることを示せ．

(2) 連続する 2 つの奇数は互いに素であることを示せ．

---

**【考え方】**

2 つの数が共通の素因数 $p$ をもつと仮定して矛盾を導く．

**【解説】**

(1)

連続する 2 つの自然数 $k,\ k+1$ 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 $p \geqq 2$ より矛盾．よって，連続する 2 つの自然数は互いに素である．

(2)

連続する 2 つの奇数 $2k-1,\ 2k+1$ が共通の素因数 $p$ をもつと仮定し，$2k-1 = p\alpha,\ 2k+1 = p\beta$ とおく ($p$ は奇数の素因数なので $p \geqq 3$)．このとき，$p(\beta - \alpha) = 2$ となるので $p \geqq 3$ より矛盾．よって，連続する 2 つの奇数は互いに素である．

■

---

## 練習問題 30

$n^3-m^2n+m^2=0$ をみたす整数 $m$, $n$ は $m=n=0$ に限ることを示せ．

---

【考え方】

いったい「互いに素」と何の関係があるのか，と思ってしまうだろう．原則に従って積の形に変形しようとするが無理なようである．ならば，次数に注目して整理すると・・・

【解説】

$m$ の方が次数が低いので $m$ で整理すると，

$$m^2=\frac{n^3}{n-1}$$

$\dfrac{n^3}{n-1}$ は整数にならねばならないが，$n-1$ と $n$ は互いに素なので，$n-1=\pm1$ すなわち，$n=0,\ 2$ になるしかない．$n=2$ のとき，$m=\pm\sqrt{8}$ となり整数にならないので，与式をみたす整数 $m$, $n$ は $m=n=0$ に限られる．

■

---

## 練習問題 31

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

---

【考え方】

$a$，$a^2+1$ が共通の素因数 $p$ をもつと仮定して，これまで同様に考えればよいが，具体的に共通の素因数がないことを実際に示す方法も考えられる．

【解説】

$a$，$a^2+1$ が共通の素因数 $p$ をもつと仮定すると，$a=p\alpha$, $a^2+1=p\beta$ とおける．このとき $p^2\alpha^2+1=p\beta$ より，$p(\beta-p\alpha^2)=1$ となるので矛盾．よって，$a$，$a^2+1$ は互いに素である．

【別解】

$a$ の素因数を小さいほうから順番に，$p_1,\ p_2,\ \cdots,\ p_n$ とすると，これら全ての素因数で $a^2+1$ を割ると，いずれの場合も割っても 1 余る．よって，$a$ と $a^2+1$ に共通の素因数は存在しない．

■

***Remark* 28**

$a$ と $a^2+1$ は互いに素であることの証明は，まだあと 2 通りある．後ほど紹介する．合計 4 種類の証明は極めて重要である．

□

---

## 応用問題 11

$n$ は正の整数とする．$x^{n+1}$ を $x^2-x-1$ で割った余りを $a_nx+b_n$ とおく．

(1) 数列 $a_n$, $b_n$ $(n=1,\ 2,\ 3,\ \cdots)$ は

$$\begin{cases} a_{n+1}=a_n+b_n \\ b_{n+1}=a_n \end{cases}$$

を満たすことを示せ．

(2) $n=1,\ 2,\ 3,\ \cdots$ に対して，$a_n$, $b_n$ は共に正の整数で，互いに素であることを証明せよ．

[2002 年東京大前期文理共通]

---

【考え方】

(1) は漸化式を立てる問題である．$x^{n+1}$ のときの式から，$x^{n+2}$ の式を作り出す必要がある．理想的な形を想定しつつ，うまく式変形すること．

(2) は数学的帰納法で証明するのがよいだろう．

【解説】

(1)

$x^{n+1}$ を $x^2-x-1$ で割った商を $Q_n(x)$ とおくと，

$$x^{n+1}=(x^2-x-1)Q_n(x)+a_nx+b_n$$

と書ける．この式の両辺に $x$ をかけて，

$$\begin{aligned} x^{n+2}&=x(x^2-x-1)Q_n(x)+a_nx^2+b_nx \\ &=x(x^2-x-1)Q_n(x)+a_n(x^2-x-1) \\ &\qquad +(a_n+b_n)x+a_n \\ &=(x^2-x-1)\{xQ_n(x)+a_n\}+(a_n+b_n)x+a_n \end{aligned}$$

これは，$x^{n+2}$ を $x^2-x-1$ で割った余りが，$(a_n+b_n)x+a_n$ であることを意味しているので，

$$\begin{cases} a_{n+1}=a_n+b_n \\ b_{n+1}=a_n \end{cases}$$

が成立する．

(2)

数学的帰納法で証明する．

(i) $n=1,\ 2,\ 3,\ \cdots$ に対して，$a_n,\ b_n$ は共に正の整数であること．

$$x^2=(x^2-x-1)+x+1$$

だから，$a_1=b_1=1$ である．

$a_k,\ b_k$ が共に正の整数であると仮定すると，(1) の結果より，$a_{k+1},\ b_{k+1}$ も正の整数になるので，全ての自然数 $n$ に対して，$a_n,\ b_n$ は共に正の整数である．

(ii) $n=1,\ 2,\ 3,\ \cdots$ に対して，$a_n,\ b_n$ は共に互いに素であること．

まず，$a_1=b_1=1$ であるので，$a_1$ と $b_1$ は互いに素である．次に

$$a_k,\ b_k\text{が互いに素} \implies a_{k+1},\ b_{k+1}\text{も互いに素} \quad \cdots①$$

を証明する．

$a_{k+1},\ b_{k+1}$ 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，

$$a_{k+1}=p\alpha,\ b_{k+1}=p\beta$$

とおける．(1) の結果より，

$$a_k=b_{k+1}=p\beta,\ b_k=a_{k+1}-b_{k+1}=p(\alpha-\beta)$$

となるので，$a_k,\ b_k$ も互いに素ではない．

よって，⊠の対偶が証明されたので，⊠は真である．全ての自然数 $n$ に対して，$a_n,\ b_n$ は互いに素である．

■

「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るが，証明しておこう．

証明

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．

証明終

---

**例 18**

(1) 連続する 2 つの自然数の積は平方数にはならないことを示せ．

(2) 連続する 3 つの自然数の積は平方数にはならないことを示せ．

---

【考え方】

連続する自然数の積，$n(n+1)$ や $n(n+1)(n+2)$ が平方数になったと仮定して矛盾を導く．連続する 2 つの自然数は互いに素であること，また，連続する 2 整数の中には 2 の倍数が 1 個しかないこと，連続する 3 整数の中には 3 以上の倍数が 1 個しかないことも，証明の重要なヒントである．

【解説】

(1)

連続する 2 つの自然数 $n,\ n+1$ は互いに素だから，それらの積 $n(n+1)$ が平方数になるとき，$n$ も $n+1$ 平方数になる．しかし，2 つの自然数の平方の差は $k^2-l^2=(k+l)(k-l)\geqq 2$ なので，平方数が連続する 2 整数になることはない．よって，$n$ と $n+1$ がともに平方数になることはない．

したがって，連続する 2 つの自然数の積は平方数にはならない．

(2)

連続する 3 つの自然数の積 $n(n+1)(n+2)$ において，$n(n+2)$ と $n+1$ が互いに素であることを証明する．

$n(n+2)$ と $n+1$ 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，

$$n(n+2)=p\alpha,\quad n+1=p\beta$$

とおける．ここで，$p\neq 2$ である．なぜならば，$p=2$ ならば，$n(n+2)$ と $n+1$ が共に偶数になるが，$n+1$ が偶数のとき $n$ と $n+2$ は共に奇数になるので，$n(n+2)$ は偶数にはならない．よって，$p\neq 2$ である．

$n(n+2)=p\alpha$ より，$n$ または $n+2$ が $p$ で割り切れる．すなわち，

$$n\text{ と }n+1\text{ が共に 3 以上の素数 }p\text{ で割り切れる}$$

または

$$n+1\text{ と }n+2\text{ が共に 3 以上の素数 }p\text{ で割り切れる}$$

ことになるが，連続する 2 整数が共に 3 以上の素数 $p$ で割り切れることはないから矛盾である．

よって，$n(n+2)$ と $n+1$ が互いに素である．

したがって，$n(n+2)$ と $n+1$ は共に平方数になる．

$n=2k$ のとき，

$$n(n+2)=2k(2k+2)=2^2k(k+1)$$

が平方数になるので，$k(k+1)$ が平方数になるが，(1) より矛盾．

$n=2k+1$ のとき，

$$n(n+2)=(2k+1)(2k+3)$$

が平方数になる．$2k+1$ と $2k+3$ は連続する奇数なので互いに素であるので，$2k+1$ と $2k+3$ は共に平方数になる．平方数の差は $(m+1)^2-m^2=2m+1>3$ なので，矛盾．

したがって，連続する 3 つの自然数の積は平方数にはならない．

■

## 練習問題 32

$a$, $b$, $c$ 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ありえ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．

【考え方】

(1) については，平方数の分類で既に紹介しているので問題ないだろう．

(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，

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

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！)．

【解説】

(1)

$a$, $b$ が共に奇数であるとき，$a^2$ も $b^2$ も 4 で割ると 1 余るので，$a^2+b^2$ は 4 で割ると 2 余る数である．平方数を 4 で割った余りは 0 か 1 なので，4 で割ると 2 余る数は平方数にはならない．よって，$a^2+b^2=c^2$ は成立しないので，$a$, $b$ が共に奇数であるということはありえない．

(2)

$a$, $b$ 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，

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

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．

$c+d$, $c-d$ が共通の素因数 $p$ をもつと仮定すると，$c+d=p\alpha$, $c-d=p\beta$ となるので，$2c=p(\alpha+\beta)$. $c+d$, $c-d$ は共に奇数なので，素因数 $p\neq 2$ なので，$c$ が $p$ で割り切れる．このとき，$d$ も $p$ で割り切れることになり，$c$ と $d$ が互いに素であることに矛盾する．

■

## 京大入試問題 10

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．

[1999 年後期文系]

【考え方】

(1) は，これまた平方数の分類を利用する．問題ないだろう．

(2) は，$\dfrac{a+c}{2}$ が平方数になることを示せばよい．$a^2+b^2=c^2$ より，$\left(\dfrac{c+a}{2}\right)\left(\dfrac{c-a}{2}\right)=\left(\dfrac{b}{2}\right)^2$ と変形できることに注目する．$a$, $c$ が奇数，$b$ は偶数なので，$\dfrac{c+a}{2}$, $\dfrac{c-a}{2}$, $\dfrac{b}{2}$ はいずれも自然数であるから，先ほど紹介した「互いに素」の性質を利用すればよい．つまり，$\dfrac{c+a}{2}$ と $\dfrac{c-a}{2}$ が互いに素であることが証明できれば，$\dfrac{c+a}{2}$ と $\dfrac{c-a}{2}$ が共に平方数であることが証明できる．

【解説】

(1)

$a$ が奇数のとき，$b$ も奇数だとすると，$a^2$ も $b^2$ も 4 で割ると 1 余るので，$a^2+b^2$ は 4 で割ると 2 余る数である．平方数を 4 で割った余りは 0 か 1 なので，4 で割ると 2 余る数は平方数にはならない．よって，$a^2+b^2=c^2$ は成立しないので，$a$, $b$ が共に奇数であるということはありえない．つまり，$a$ が奇数ならば，$b$ は偶数であることがわかる．このとき，$a^2+b^2$ は奇数になるので，$c$ は奇数である．

(2)

$a^2+b^2=c^2$ より，

$$\left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right)=\left(\frac{b}{2}\right)^2 \quad \cdots ①$$

である．(1) より，$a$, $c$ が奇数，$b$ は偶数なので，$\dfrac{c+a}{2}$, $\dfrac{c-a}{2}$, $\dfrac{b}{2}$ はいずれも自然数である．

$\dfrac{c+a}{2}$ と $\dfrac{c-a}{2}$ が互いに素であることを証明する．

$\dfrac{c+a}{2}$ と $\dfrac{c-a}{2}$ 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，

$$\frac{c+a}{2}=pm,\quad \frac{c-a}{2}=pn$$

となる．これより，

$$a=p(m-n),\quad c=p(m+n)\quad \cdots②$$

となるので，$a$ も $c$ の $p$ の倍数である．

さて，②を $a^2+b^2=c^2$ に代入すると，$b^2=4p^2mn$，つまり

$$\left(\frac{b}{p}\right)^2=4mn$$

だから，$b$ もまた $p$ の倍数となり，$a$, $b$ は互いに素であることに矛盾する．

よって，$\dfrac{c+a}{2}$ と $\dfrac{c-a}{2}$ が互いに素であることが示された．

したがって，☒より，$\dfrac{c+a}{2}$ と $\dfrac{c-a}{2}$ は共に平方数であるので，$\dfrac{c+a}{2}=d^2$，つまり，$c+a=2D^2$ となる $d$ が存在する．

■

**発展 5**

上の問題では，ピタゴラス数の重要な性質が背景にある．ピタゴラス数とは

$$x^2+y^2=z^2\quad \cdots①$$

をみたす自然数の組のことである．この式は，『ピタゴラスの定理 (3 平方の定理)』で有名であり，この式をみたす自然数の組として，(3, 4, 5) や (5, 12, 13) などを即座に思い出す人もいるだろう．これらがピタゴラス数である．

そこで問題になるのが，「ピタゴラス数を具体的に求めるには，どうすればよいのか」という問題であり，同時に「そうやって求めた数の組以外にはピタゴラス数はないのか」という問題も浮かび上がる．

これらについて考えてみよう (前半部分は京大の問題と全く同じである)．

まず，①をみたす自然数の組の一つを $(a,\ b,\ c)$ とすると，

$$a^2+b^2=c^2$$

である．$a$, $b$, $c$ に共通の素因数 $p$ が存在したとすると，

$$a=pa',\ b=pb',\ c=pc'$$

とおけ，

$$(pa')^2+(pb')^2=(pc')^2$$

$$\therefore\quad (a')^2+(b')^2=(c')^2$$

となる．つまり，$(a,\ b,\ c)$ が解ならば，$(a',\ b',\ c')$ も解になるので，始めから，$a$, $b$, $c$ を互いに素であると設定してもよい．

以下，互いに素な自然数解の組 $(a,\ b,\ c)$ で考える．

(ここからしばらく，前出の京大の問題に同じなので略記)

$a^2+b^2=c^2$ より，$a$ と $b$ の偶奇性は一致しないので，$a$ を奇数，$b$ を偶数としてよく，したがって $c$ は奇数となる．このとき，

$$\left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right)=\left(\frac{b}{2}\right)^2\quad \cdots②$$

と変形でき，$\dfrac{c+a}{2}$, $\dfrac{c-a}{2}$, $\dfrac{b}{2}$ はいずれも自然数で，$\dfrac{c+a}{2}$ と $\dfrac{c-a}{2}$ が互いに素である．よって，$\dfrac{c+a}{2}$ と $\dfrac{c-a}{2}$ は共に平方数になるので，

$$\frac{c+a}{2}=m^2,\quad \frac{c-a}{2}=n^2$$

とおける．よって，

$$a=m^2-n^2,\ c=m^2+n^2$$

となり，さらに，

$$b=2mn$$

となる．

$\dfrac{c+a}{2}$ と $\dfrac{c-a}{2}$ が互いに素なので，$m$ と $n$ も互いに素である．また，$c$ が奇数なので，$m$ と $n$ の偶奇性は一致しない．

したがって，以上をまとめると，次の重要な命題を得る．

**☆ピタゴラス数の重要命題☆**

$m$, $n$, $k$ を整数とする．

$$①\ \begin{cases} a=k(m^2-n^2)\\ b=2kmn\\ c=k(m^2+n^2)\end{cases}$$

とおけば，

$$a^2+b^2=c^2\quad \cdots②$$

である．逆に，②を満たす整数の組 $(a,\ b,\ c)$ が与えられたとき，その最大公約数を $k$ とすると，①のように書け，その際，$m$ と $n$ は互いに素で，一方は偶数，他方は奇数である．

これで，ピタゴラス数が完全に判明した．

□

---

## 京大入試問題 11

$a,\ b,\ p,\ q$ はすべて自然数で，$\dfrac{p^2+q^2}{a}=\dfrac{pq}{b}$ 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．

[1998 年後期文系]

---

【考え方】

(1) は問題ないと思う．(2) が難しい．まずは，問題の式が比例式であることに注目して，

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

とおいて，$a=\dfrac{p^2+q^2}{k}$, $b=\dfrac{pq}{k}$ とし，$\sqrt{a+2b}$ に代入して計算しようと試みるが $\cdots$

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

となり，$\sqrt{a+2b}$ は自然数にならない．というか，$\sqrt{k}$ とは何であろうか？こんなものが残ってしまっては，自然数どころの話ではない．なんとか，ならないだろうか．ここで大胆な仮説を立てる．$\sqrt{k}$ を消去したい $\cdots$ ならば $k$ が平方数？ $\cdots$ いやいや，平方数だけでは $\dfrac{p+q}{\sqrt{k}}$ は自然数にはならない．では，$k=1$ であることが言えないだろうか．そのためには，(1) がヒントになっているのだが，その真意に気付くであろうか？(1) で「$pq$ が $b$ で割り切れる」ということは，$\dfrac{pq}{b}$ が約分可能であることを意味している．ならば，$\dfrac{p^2+q^2}{a}=\dfrac{pq}{b}$ を限界までどんどん約分していって，式の値 (つまり $k$) が 1 になることを示せないだろうか．

また，具体的な数字を当てはめて証明の方針を考えることもできる．

いま，$p=6$, $q=8$ とでも設定してみよう．このとき，$p^2+q^2=100$, $pq=48$．$pq$ は $b$ で割り切れるから，$b=12$ とでもしてみよう．このとき，

$$\frac{100}{a}=\frac{48}{12}$$

より，$a=25$. したがって，

$$\frac{100}{25}=\frac{48}{12}$$

いったい，この等式は何なのか？　両辺を約分すると $4=4$ となり式の値は 4 なのだが，両辺の 100 と 48 を約すると

$$\frac{25}{25}=\frac{12}{12}$$

となり，式の値は 1 になっているではないか！

【解説】

(1)

$$\frac{p^2+q^2}{a}=\frac{pq}{b}\quad\cdots①$$

☒より，

$$apq=b(p^2+q^2)$$

よって，$a,\ b$ が互いに素だから，$pq$ が $b$ で割り切れる．

(2)

$p$ と $q$ の最大公約数を $g$ とおくと，

$$p=gp_1,\quad q=gq_1\ \ (p_1\text{と}\ q_1\text{は互いに素})$$

となり，これを☒に代入して，

$$\frac{p_1^2+q_1^2}{a}=\frac{p_1q_1}{b}\quad\cdots☒$$

☒と同じ形になるので，(1) より，

$$p_1q_1\text{は}\ b\ \text{で割り切れる．}$$

☒より，

$$ap_1q_1=b(p_1^2+q_1^2)$$

であり，$b(p_1^2+q_1^2)$ は $p_1q_1$ で割り切れるが，$p_1$ と $q_1$ が互いに素のとき，$p_1^2+q_1^2$ と $p_1q_1$ は互いに素だから，

$$b\ \text{は}\ p_1q_1\text{で割り切れる．}$$

したがって，$b=p_1q_1$. よって，☒の値は 1 である．よって，

$$a=p_1^2+q_1^2,\quad b=p_1q_1$$

なので，$\sqrt{a+2b}=p_1+q_1$ となり，$\sqrt{a+2b}$ は自然数．

■

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 $0 \leqq r < b$) 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．

証明終

***Remark* 29**

一般に，$a,\ b$ の最大公約数を $(a,\ b)$ と表記することがある．例えば，

$$(8,\ 12) = 4, \qquad (5,\ 7) = 1$$

などと書く．$(5,\ 7) = 1$ は 5 と 7 が互いに素であることを意味している．つまり，「$a,\ b$ が互いに素である」ということを単に「$(a,\ b) = 1$ である」と表現する．座標と混同しないように (大丈夫だと思うが)．この表記方法を用いると，上のユークリッドの互除法は

$$(a,\ b) = (b,\ a - bq)$$

とシンプルに表現できる．

□

具体例で検証する方がわかりやすいだろう．

---

例 **19**

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，

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

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，

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

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．

---

## 練習問題 33

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．

[2002 年同志社大 (商)]

【解説】

(1)

$20853 = 7 \times 9 \times 331$

$3843 = 7 \times 9 \times 61$

だから，最大公約数は 63 である．

(2)

$$\begin{aligned}&(20853,\ 3843)\\ =&(3843,\ 1638)\\ =&(1638,\ 567)\\ =&(567,\ 504)\\ =&(504,\ 63)\\ =&63\end{aligned}$$

よって，最大公約数は 63 である．

■

このように，ユークリッドの互除法は具体的に最大公約数を求める場合に有効である．では，入試問題ではどのような例で登場するのだろうか．次の問題を見てほしい．

この問題は (1) が (2) のヒントになっていて，(2) は (1) の結果を利用して証明するのだが，(1) はまさにユークリッドの互除法の基本原理そのものである．

(1) なしで，いきなり (2) だけ出題されたら，ユークリッドの互除法を知らない人はお手上げだろう．

## 練習問題 34

(1) 自然数 $a,\ b,\ c,\ d$ に，$\dfrac{b}{a} = \dfrac{c}{a} + d$ 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．

[2000 年大阪市大前期理系]

【考え方】

(1) は，「ユークリッドの互除法より明らか」とするわけにはいかないだろう．つまり，「$\dfrac{b}{a} = \dfrac{c}{a} + d$ より，$b = ad + c$ で，これは，$b$ を $a$ で割ったら商が $d$，余りが $c$ であることを意味しており，ユークリッドの互除法により，$b$ と $a$ の最大公約数は $a$ と $c$ の最大公約数に等しい．よって，$a$ と $c$ が互いに素ならば，$a$ と $b$ も互いに素である $\cdots$」と．しかし，「$a$ と $c$ が互いに素ならば，$a$ と $b$ も互いに素である」ことを示すだけなので，ユークリッドの互除法なんか意識しなくても，普通に考えれば証明できる．

(2) は，(1) の結果を利用するが，この問題はユークリッドの互除法の意識があると，解決が早い．

【解説】

(1)

$\dfrac{b}{a} = \dfrac{c}{a} + d$ より，$b - ad = c$．$a$ と $b$ が互いに素でないと仮定すると，$a$ と $b$ に共通の素因数 $p$ が存在するので，$b - ad$ は $p$ で割り切れる．よって，$c$ も $p$ で割り切れることになるので，$a$ と $c$ も互いに素ではない．

(2)

$$\frac{28n+5}{21n+4} = \frac{7n+1}{21n+4} + 1 \cdots ①$$

であり，さらに，

$$\frac{21n+4}{7n+1} = \frac{1}{7n+1} + 3 \cdots ②$$

となる．

②より，$7n+1$ と 1 は互いに素だから，(1) より，$21n+4$ と $7n+1$ は互いに素である．よって，①より，$21n+4$ と $7n+1$ は互いに素だから，(1) より，$21n+4$ と $28n+5$ も互いに素である．

■

### ***Remark*** **30**

$a,\ b$ の最大公約数を $(a,\ b)$ と表し，ユークリッドの互除法を用いると，

$$(a,\ c) = (b,\ b - ad) = (a,\ b)$$

と表現できるので，

$$(a,\ c) = 1 \implies (a,\ b) = 1$$

であることは，簡単に証明できる．

□

## 練習問題 35

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

【考え方】

$4x + 9y$ と $3x + 7y$ が互いに素であることを証明すればよい．つまりは，上の問題の (2) の方法をそのまま真似ればよい．はたしてユークリッドの互除法以外で証明できるだろうか．

【解説】

***Remark* 31**

$a,\ b$ の最大公約数を $(a,\ b)$ と表し，ユークリッドの互除法を用いると，

$$\begin{aligned}(4x+9y,\ 3x+7y) &= (3x+7y,\ x+2y)\\ &= (x+2y,\ y)\\ &= (y,\ x)\end{aligned}$$

と表現できるので，

$$(x,\ y)=1 \implies (4x+9y,\ 3x+7y)=1$$

であることは，簡単に証明できる．

□

## 5　有理数解をもつ方程式

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

このタイプの問題は，入試ではほとんどが 2 次方程式か 3 次方程式の場合で出題されるが，京都大では一般の $n$ 次方程式の場合が出題された (96 年後期文系)．しかし，基本的な証明の方法は，2 次方程式や 3 次方程式の場合と本質的に同じであるので，特別に構える必要はない．よって，2 次方程式や 3 次方程式の手法を確実にマスターすることが大切である．

まずは，2 次方程式，3 次方程式の場合から始めよう．証明方法は全く同じであることに気付くであろう．

---

**例 20**

$p,\ q$ を整数とし，$f(x)=x^2+px+q$ とおく．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．

---

**【考え方】**

まずは，問題文を定式化せねばならない．つまり，有理数 $a$ を $a=\dfrac{n}{m}$ $(m,\ n$ は互いに素) とおくとき，

$$f\left(\frac{n}{m}\right)=0 \implies m=1$$

であることを示せばよい．

**【解説】**

有理数 $a$ を $a=\dfrac{n}{m}$ $(m,\ n$ は互いに素) とおく．$x=a$ が $f(x)=0$ の解だから，$f(a)=0$ が成立する．つまり，

$$\left(\frac{n}{m}\right)^2+p\left(\frac{n}{m}\right)+q=0$$

したがって，

$$\begin{aligned}n^2+pmn+qm^2&=0\\ n^2&=-m(pn+qm)\end{aligned}$$

だから，$n^2$ は $m$ で割り切れることになるが，$m,\ n$ は互いに素なので，$m=1$ でなければならない．

したがって，$a=\dfrac{n}{1}=n$ となるので，有理数 $a$ は整数である．

■

---

**練習問題 36**

$a,\ b,\ c$ 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．

[2002 年神戸大前期理系]

---

**【考え方】**

先程の問題と同様，有理数解を $x=\dfrac{n}{m}$ とおいて，$m=1$ を示せばよい．

**【解説】**

$f(x)=x^3+ax^2+bx+c$ とおく．$f(x)=0$ が有理数解 $x=\dfrac{n}{m}$ $(m,\ n$ は互いに素) をもつとき，$f\left(\dfrac{n}{m}\right)=0$ より，つまり，

$$\left(\frac{n}{m}\right)^3+a\left(\frac{n}{m}\right)^2+b\left(\frac{n}{m}\right)+c=0$$

したがって，

$$\begin{aligned}n^3+amn^2+bm^2n+cm^3&=0\\ n^3&=-m(an^2+bmn+cm^2)\end{aligned}$$

だから，$n^3$ は $m$ で割り切れることになるが，$m,\ n$ は互いに素なので，$m=1$ でなければならない．

したがって，有理数解は $\dfrac{n}{1}=n$ となるので，有理数解は整数である．

■

---

**練習問題 37**

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 $\dfrac{q}{p}(p,\ q$ 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．

[1998 年岡山大 C 日程 (情工)]

【考え方】

今度は，同じ 3 次方程式でも 3 次の係数が 1 ではない場合であるが，証明の手法はこれまでと全く同じである．

【解説】

$f(x)=ax^3+bx^2+cx+d$ とおく．$f(x)=0$ が有理数の解 $\dfrac{q}{p}$ ($p$, $q$ は互いに素) をもつとき，$f\left(\dfrac{q}{p}\right)=0$ より，つまり，

$$a\left(\frac{q}{p}\right)^3+b\left(\frac{q}{p}\right)^2+c\left(\frac{q}{p}\right)+d=0$$

したがって，

$$aq^3+bpq^2+cp^2q+dp^3=0$$
$$aq^3=-p(aq^2+bpq+cp^2)$$

だから，$aq^3$ は $p$ で割り切れることになるが，$p$, $q$ は互いに素なので，$a$ が $p$ で割り切れなければならない．

よって，題意は証明された．

■

これまでに取り上げた，2 次方程式，3 次方程式の場合は，一般に，$n$ 次方程式の場合にも拡張されて，次のようにまとめることができる．

☆整数係数の整方程式の有理数解☆

整数係数の整方程式

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0=0\ (a_n\neq 0)$$

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．

難しそうに書かれてはいるが，高次方程式を因数分解して解いたときを思い出してほしい．解の候補として考えた数が，まさに $\dfrac{a_0\text{の約数}}{a_n\text{の約数}}$ ではなかっただろうか．

## 京大入試問題 12

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

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

を考える．

(1) 方程式 $f(x)=0$ が整数解 $\alpha$ を持てば，$\alpha$ 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．

[1996 年後期文系]

【考え方】

(1) はこれまでの 2 次方程式，3 次方程式でとった手法と同様である．$p$ が素数であることに注意しよう．

(2) は対偶をとる．つまり，「方程式 $f(x)=0$ は整数解を持つ」と仮定するわけだが，このとき，(1) の結果をそのまま利用できることになる．

【解説】

(1)

$f(\alpha)=0$ より，

$$\alpha^n+pa_{n-1}\alpha^{n-1}+\cdots+pa_i\alpha^i+\cdots+pa_0=0$$

$$\therefore \alpha^n=-p(a_{n-1}\alpha^{n-1}+\cdots+a_i\alpha^i+\cdots+a_0)$$

$a_{n-1}\alpha^{n-1}+\cdots+a_i\alpha^i+\cdots+a_0$ は整数なので，右辺は $p$ の倍数になる．

よって，$p$ は素数だから $\alpha^n$ も $p$ の倍数になるので，$\alpha$ は $p$ で割り切れる．

(2)

$f(x)=0$ は整数解を持つと仮定すると，(1) より，その整数解は $p$ の倍数になるので，$kp$($k$ は整数) とおける．このとき，$f(kp)=0$ より，

$$k^np^n+pa_{n-1}k^{n-1}p^{n-1}+\cdots+pa_1kp+pa_0=0$$

$$\therefore a_0=-(k^np^{n-1}+pa_{n-1}k^{n-1}p^{n-2}+\cdots+pa_1k)$$

右辺は $p$ の倍数だから，左辺も $p$ の倍数になる．

よって，$a_0$ は $p$ で割り切れる．

したがって，$a_0$ 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が示された．

■

これまで，方程式が有理数解をもつ場合を考えてきたが，今度は，方程式が整数解をもつ場合を考えよう．これも 2 次方程式，3 次方程式の場合がほとんどである．

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 21**

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．

---

【考え方】

解の公式を用いて，

$$x=\frac{3a\pm\sqrt{9a^2-8a+12}}{2}$$

と，解を具体的に求めて，「これが整数になるには，√の中が平方数になればよいので $\cdots$」と考える人が多い．理屈は正しいのだが，この方法ではなかなか $a$ の値を特定することは難しい ($9a^2-8a+12=m^2$ となる，整数 $a$, $m$ を求めよ，という問題に帰着する)．また，「ルートの中が 0 になればよいので $\cdots$」などと全く的外れな解釈をとる人もいる．

いずれにしても，この問題では，解と係数の関係を利用するに限る．

【解説】

2 つの整数解を $\alpha$, $\beta(\alpha\leqq\beta)$ 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，

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

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

■

***Remark* 32**

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．

□

---

**練習問題 38**

$p$ を素数とする．$x$ に関する 2 次方程式

$$px^2+(5-p^2)x-3p=0$$

が整数の解をもつのは $p=2$ のときに限ることを示せ．

[1996 年千葉大前期]

---

【考え方】

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 $\alpha$, $\beta(\alpha\leqq\beta)$ とする」とはおけないのである！ (2 つとも整数解とは限らない．整数解と分数解かもしれない)．このことは，$x^2$ の係数にも関係がある．この問題では $x^2$ の係数が 1 ではないので，2 つの解が「整数＆分数」の可能性があるのだ．

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．

【解説】

$f(x)=px^2+(5-p^2)x-3p$ とおく．整数解を $x=m$ とおくと，$f(m)=0$ だから，

$$pm^2+(5-p^2)m-3p=0$$

つまり，

$$5m=p(-m^2+mp+3)\quad\cdots\boxtimes$$

よって，$5m$ が素数 $p$ で割り切れるので，5 または $m$ が素数 $p$ で割り切れる．

5 が素数 $p$ で割り切れるとき，$p=5$ なので，このとき，もとの方程式は $x^2-4x-3=0$ となって，解は $x=2\pm\sqrt{7}$ で整数ではない．

$m$ が素数 $p$ で割り切れるとき，$m=kp$ とおけば，$\boxtimes$より，

$$5k=kp^2-k^2p^2+3$$
$$\therefore k(5-p^2+kp^2)=3$$

$k$, $5-p^2+kp^2$ は整数なので，

| $k$ | 1 | -1 | 3 | -3 |
|---|---|---|---|---|
| $5-p^2+kp^2$ | 3 | -3 | 1 | -1 |

の各場合を考えると，

$k=1$, $5-p^2+kp^2=3$ のとき，$5=3$ より矛盾．

$k=-1$, $5-p^2+kp^2=-3$ のとき，$p^2=4$ より, $p=2$.

$k=3$, $5-p^2+kp^2=1$ のとき，$p^2=-2$ より矛盾．

$k=-3$, $5-p^2+kp^2=-1$ のとき，$p^2=\frac{3}{2}$ より矛盾．

したがって，以上より，$f(x)=0$ が整数解をもつのは，$p=2$ の場合に限る．

■

---

**練習問題 39**

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．

[2003 年大阪大後期理系]

【考え方】

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 $\cdots$」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．

【解説】

解と係数の関係より，

$$\begin{cases} (n-1)+n+(n+1)=-p \\ (n-1)n+n(n+1)+(n+1)(n-1)=q \\ (n-1)n(n+1)=r \end{cases}$$

となるので，

$$\begin{cases} p=-3n \\ q=3n^2-1 \\ r=-n^3+n \end{cases}$$

となる．$p>q>r$ より，

$$-3n>3n^2-1>-n^3+n$$

$-3n>3n^2-1$ より，$3n^2+3n-1<0$

$$\therefore \quad \frac{-3-\sqrt{21}}{6}<n<\frac{-3+\sqrt{21}}{6}$$

$$\therefore -1.26\cdots<n<0.26\cdots$$

これを満たす整数 $n$ は $n=-1,\ 0$ である．

$n=0$ のとき，$3n^2-1>-n^3+n$ は成立しない．

$n=-1$ のとき，$3n^2-1>-n^3+n$ は成立する．

したがって，$n=-1$ であり，このとき，$p=3,\ q=2,\ r=0$ である．

■

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．

## 練習問題 40

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 $3a+2b\leqq 0$ が成り立つ

[1996 年大阪大前期理系]

【考え方】

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

【解説】

$X^2+aX+b=0$ の 2 つの解を $\alpha,\ \beta$ $(2\leqq\alpha\leqq\beta)$ とおくと，

$$\alpha+\beta=-a,\quad \alpha\beta=b \quad \cdots ☒$$

これを条件 (ロ) の式に代入すると，

$$-3(\alpha+\beta)+2\alpha\beta\leqq 0$$

したがって，

$$(2\alpha-3)(2\beta-3)\leqq 9$$

$2\leqq\alpha\leqq\beta$ に注意すると，

$\alpha=2$ のとき，$\beta=2,3,4,5,6$

$\alpha=3$ のとき，$\beta=3$

の場合が考えられる．これら各場合を☒に代入して計算すると，$(a,\ b)$ の組が確定する．

| $a$ | $-4$ | $-5$ | $-6$ | $-7$ | $-8$ | $-6$ |
|---|---|---|---|---|---|---|
| $b$ | 4 | 6 | 8 | 10 | 12 | 9 |

■

最後に，有理数解に関する応用問題を 2 問紹介しておく．いずれも整数特有の性質を用いているので重要な問題である．

## 応用問題 12

整数 $a,\ b$ を係数とする 2 次式

$$f(x)=x^2+ax+b$$

を考える．$f(\alpha)=0$ となるような有理数 $\alpha$ が存在するとき，以下のことを証明せよ．

(1) $\alpha$ は整数である．

(2) 任意の整数 $l$ と任意の自然数 $n$ に対して，$n$ 個の整数

$$f(l),\ f(l+1),\ \cdots,\ f(l+n-1)$$

のうち少なくとも 1 つは $n$ で割り切れる．

[1980 年大阪大文系理系]

【考え方】

(1) は問題ないだろう．例 33 と全く同じであるので解答も省略する．

(2) は難問．(1) をうまく利用するのだが，(2) との関連になかなか気付かないだろう．(1) は，$f(x)=0$ は整数解 $\alpha$ をもっていることを主張している．つまり，$f(\alpha)=0$ だから $f(\alpha)$ は $n$ で割り切れることになる．

ここで，$\alpha$ に $n$ を加えた，$\alpha+n$ を考えると，

$$\begin{aligned} f(\alpha+n) &= (\alpha+n)^2+a(\alpha+n)+b \\ &= \alpha^2+2\alpha n+n^2+a\alpha+an+b \\ &= \alpha^2+a\alpha+b+n(2\alpha+n+a) \\ &= f(\alpha)+n(2\alpha+n+a) \end{aligned}$$

$f(\alpha)$ は $n$ で割り切れるので，$f(\alpha+n)$ も $n$ で割り切れることになる．

同様にして，$\alpha+2n$, $\alpha+3n$, $\cdots$ もすべて $n$ で割り切れることがわかるので，一般に，$f(\alpha+kn)$ ($k$ は整数) が $n$ で割り切れることになる．つまり，$\alpha$ から間隔 $n$ でずらしていった整数 $\beta$ において，必ず $f(\beta)$ は $n$ で割り切れるのである．

ここで，

$$l,\ l+1,\ \cdots,\ l+n-1$$

が連続する $n$ 個の整数であることに注目すれば，$\alpha$ から間隔 $n$ でずらしていったとき，必ず，いずれかの整数にヒットすることがわかるであろう．このことを意識しないと，以下の解答は理解できないかもしれない．

【解説】

(2) 連続する $n$ 個の整数

$$l,\ l+1,\ \cdots,\ l+n-1$$

を $n$ で割った余りは，0 から $n-1$ が順不同で 1 回ずつ現れるので，この中に，$\alpha$ を $n$ で割った余りと同じものがただ一つ存在する．このような数を $\beta$ とおく．つまり，

$$\beta-\alpha \text{は } n \text{ の倍数}$$

いま，

$$\begin{aligned} f(\beta)-f(\alpha) &= (\beta^2-\alpha^2)+a(\beta-\alpha) \\ &= (\beta-\alpha)(\beta+\alpha+a) \end{aligned}$$

$\beta-\alpha$ は $n$ の倍数だから，$f(\beta)-f(\alpha)$ は $n$ の倍数．$f(\alpha)=0$ より，$f(\beta)$ は $n$ の倍数．

■

## ***Remark*** 33

上の問題の結果を一般化すれば，整数係数の多項式 $f(x)$ が整数解 $\alpha$ をもつとき

$$f(\alpha+n)-f(\alpha) \text{ は } n \text{ で割り切れる．}$$

ことがわかる．このことは合同式を用いて表現すれば，より一層明確になる．

$$f(\alpha+n)\equiv f(\alpha) \pmod{n}$$

となる．

□

## 応用問題 13

整数を係数とする n 次の整式

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

について，次の (1)(2) を証明せよ．

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

(2) ある自然数 $k(>1)$ に対して，$k$ 個の整数

$$f(1),\ f(2),\ \cdots,\ f(k)$$

のどれもが $k$ で割り切れなければ，方程式 $f(x)=0$ は有理数の解をもたない．

[1982 年九州大文系]

【考え方】

先ほどの大阪大で出題された 2 年後に，$n$ 次式の場合で出題された．大阪大の問題を経験していれば，なんでもない問題だが，初見だと厳しい問題である．(2) は大阪大の問題の対遇になっていることに注意しよう．

【解説】

(2)

対偶を証明する．

方程式 $f(x)=0$ は有理数解 $\alpha$ をもつならば，(1) より，$\alpha$ は整数になる．$\alpha$ を $k$ で割った余りを $r$ とおく．いま，$1\leq r\leq k$ と設定しておく．このとき，

$$r-\alpha \text{は } k \text{ の倍数}$$

いま，

$$\begin{aligned} & f(r)-f(\alpha) \\ =&(r^n-\alpha^n)+a_1(r^{n-1}-\alpha^{n-1})+\cdots+a_{n-1}(r-\alpha) \\ =&(r-\alpha)\times(\text{整数}) \end{aligned}$$

$r-\alpha$ は $k$ の倍数だから，$f(r)-f(\alpha)$ は $k$ の倍数．$f(\alpha)=0$ より，$f(r)$ は $k$ の倍数．したがって，

$$f(1),\ f(2),\ \cdots,\ f(k)$$

の中に，必ず一つ $k$ で割り切れるものが存在する．

したがって，対偶が証明されたので，もとの命題も証明された．

【別解 1】

対偶によらずに直接証明してみよう．

任意の整数 $N$ は

$$N = kl + r \quad (l \text{ は整数}, r = 1, 2, \cdots, k)$$

と表現でき，

$$N^i = (kl + r)^i \equiv r^i \pmod{k}$$

が成立するので，

$$f(N) \equiv f(r) \pmod{k}$$

$f(r) \not\equiv 0 \pmod{k}$ より，$f(N) \not\equiv 0 \pmod{k}$ なので，$f(x)$ は任意の整数で 0 にはならない，すなわち，整数解をもたない．(1) より，整数解をもたないということは有理数解をもたないということだから，題意は証明された．

■

## 6 ${}_pC_k$ 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．

整数問題では主に 基本性質① が利用される．基本性質① 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☆

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

基本性質② ${}_nC_k = {}_{n-1}C_{k-1} + {}_{n-1}C_k$

**証明**

いずれも，${}_nC_k = \dfrac{n!}{k!(n-1)!}$ を用いて証明できる．

証明終

***Remark* 34**

上の性質は組合せ論的に解釈することもできる．つまり，基本性質① を $k\ {}_nC_k = n\ {}_{n-1}C_{k-1}$ と変形すれば，この式は，$n$ 人の中から代表者 1 人を含む $k$ 人を選ぶ選び方の総数を表しており，基本性質② は，$n$ 人の中から $k$ 人を選ぶ選び方を，特定の 1 人を含む場合と含まない場合に分けて数えることを表している．

□

☆二項係数の性質①☆

素数 $p$ について，

${}_pC_k$ $(k = 1,\ 2,\ \cdots\ p-1)$ は $p$ の倍数

**証明**

基本性質① より，

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

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

証明終

この性質から，次の重要な結果が得られる．

☆二項係数の性質①からわかること☆

$(a+b)^p$ と $a^p + b^p$ のそれぞれを $p$ でわった余りは等しい．

つまり，

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

が成立する。

**証明**

二項定理より

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

${}_pC_k$ $(k = 1,\ 2,\ \cdots\ p-1)$ は $p$ の倍数だから，$\displaystyle\sum_{k=1}^{p-1} {}_pC_k\ a^{p-k}b^k$ は $p$ で割り切れる．したがって，$(a+b)^p$ と $a^p + b^p$ のそれぞれを $p$ でわった余りは等しい．つまり，

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

が成立する。

証明終

**例 22**

$p$ 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．

[2006 年早稲田大 (政経)]

【考え方】

上の☆二項係数の性質①からわかること☆ を用いれば，$(n+1)^p - n^p - 1$ が $p$ で割り切れることは明らかであるが，ここでは，きちんと $(n+1)^p$ を二項展開して証明しておこう．このような計算を面倒くさがってはいけない．

【解説】

二項定理より

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

だから，

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

となる．${}_p\mathrm{C}_k$ $(k = 1,\ 2,\ \cdots\ p-1)$ は $p$ の倍数であるから，右辺は $p$ の倍数．よって，$(n+1)^p - n^p - 1$ が $p$ で割り切れる．

■

***Remark* 35**

☆二項係数の性質①からわかること☆より，合同式を用いて解答すると，驚くほど簡単な証明になる．

$$\begin{aligned}(n+1)^p &\equiv n^p + 1^p \equiv n^p + 1 \pmod{p} \\ \therefore\ (n+1)^p - n^p - 1 &\equiv 0 \pmod{p}\end{aligned}$$

よって，$(n+1)^p - n^p - 1$ が $p$ で割り切れる．

□

次の問題は『フェルマーの小定理』が背景にある．『フェルマーの小定理』は後ほど紹介するが，この定理を知っていれば，すぐに答えはわかる．

**練習問題 41**

$p$ を 5 以上の素数とする．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．

【考え方】

$3^p = (2+1)^p = (1+1+1)^p$ と，どんどん二項展開していく．

【解説】

$$\begin{aligned}3^p &= (2+1)^p \\ &= \sum_{k=0}^{p} {}_p\mathrm{C}_k \ 2^k \\ &= 1 + \sum_{k=1}^{p-1} {}_p\mathrm{C}_k \ 2^k + 2^p \\ &= 1 + \sum_{k=1}^{p-1} {}_p\mathrm{C}_k \ 2^k + (1+1)^p \\ &= 1 + \sum_{k=1}^{p-1} {}_p\mathrm{C}_k \ 2^k + \sum_{k=0}^{p} {}_p\mathrm{C}_k 1^p \\ &= 1 + \sum_{k=1}^{p-1} {}_p\mathrm{C}_k \ 2^k + 1 + \sum_{k=1}^{p-1} {}_p\mathrm{C}_k + 1 \\ &= 3 + \sum_{k=1}^{p-1} {}_p\mathrm{C}_k + \sum_{k=1}^{p-1} {}_p\mathrm{C}_k \ 2^k\end{aligned}$$

${}_p\mathrm{C}_k$ $(k = 1,\ 2,\ \cdots\ p-1)$ は $p$ の倍数であるから，$\displaystyle\sum_{k=1}^{p-1} {}_p\mathrm{C}_k$，$\displaystyle\sum_{k=1}^{p-1} {}_p\mathrm{C}_k \ 2^k$ は $p$ で割り切れる．

よって，$3^p$ を $p$ で割ったときの余りは 3 である．

このとき，$3^p - 3 = 3(3^{p-1} - 1)$ は $p$ で割り切れるが，$p$ は 5 以上の素数だから，$3^{p-1} - 1$ が $p$ で割り切れる．よって，$3^{p-1}$ を $p$ で割ったときの余りは 1 である．

■

***Remark* 36**

☆二項係数の性質①からわかること☆より，合同式を用いて解答すると，

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

$3^p$ を $p$ で割ったときの余りは 3 である．さらに，

$$3^p - 3 \equiv 3(3^{p-1} - 1) \equiv 0 \pmod{p}$$

であり，$3 \not\equiv 0 \pmod{p}$ より，

$$3^{p-1} - 1 \equiv 0 \pmod{p}$$

よって，$3^{p-1}$ を $p$ で割ったときの余りは 1 である．

□

## 京大入試問題 13

$a$，$b$ 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．

[1995 年前期理系]

【考え方】

まずは，何を示せばよいのかを考えよう．この問題の場合，「$d$ を $2p$ で割った余りが 1 であること」つまり，「$d-1$ が $2p$ で割り切れること」を示せばよい．ここで，$p$ が $p > 2$ なる素数であることから，「$d-1$ が 2 でも $p$ でも割り切れること」を示すことになる．

まずは「積の形をつくる」という大原則を思い出そう．すると，$a^p - b^p$ の因数分解を考えるのではないだろうか．

【解説】

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

が素数 $d$ に等しく，$p > 2$, $a > b \geqq 1$ より，

$$a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + ab^{p-2} + b^{p-1} > 1$$

だから，

$$\begin{cases} a - b = 1 \\ a^{p-1} + a^{p-2}b + a^{p-3}b^2 + \cdots + ab^{p-2} + b^{p-1} = d \end{cases}$$

となる．よって，$a = b + 1$ を $a^p - b^p = d$ に代入して，

$$\begin{aligned} d &= (b+1)^p - b^p \\ &= \sum_{k=0}^{p} {}_p\mathrm{C}_k \ b^k - b^p \\ &= 1 + \sum_{k=1}^{p-1} {}_p\mathrm{C}_k \ b^k \end{aligned}$$

ここで，${}_p\mathrm{C}_k$ $(k = 1,\ 2,\ \cdots\ p-1)$ は $p$ の倍数であるから，$\displaystyle\sum_{k=1}^{p-1} {}_p\mathrm{C}_k \ b^k$ は $p$ で割り切れるので，$d-1$ は $p$ で割り切れることがわかる．

また，$b+1$ と $b$ は偶奇が異なるから，$(b+1)^p - b^p$ は必ず奇数になるので，$d-1$ は偶数であることもわかる．

$p$ が $p > 2$ なる素数であることから，$d-1$ が 2 でも $p$ でも割り切れること，すなわち，$d-1$ が $2p$ で割り切れることになる．

したがって，$d$ を $2p$ で割ると 1 余る．

■

次に紹介する☆二項係数の性質②☆ は，とりたてて暗記する必要はないが，知っていると，ごく稀に便利なことがある．

> ☆二項係数の性質②☆
> 素数 $p$ と整数 $m$ について，
>
> ${}_{pm}\mathrm{C}_p$ が $p$ で割り切れる
>
> $\Longleftrightarrow$ $m$ が $p$ で割り切れる

証明

基本性質① より，

$$p\,{}_{pm}\mathrm{C}_p = pm\ {}_{pm-1}\mathrm{C}_{p-1}$$

つまり，

$${}_{pm}\mathrm{C}_p = m\ {}_{pm-1}\mathrm{C}_{p-1}$$

が成立する．

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

となるので，${}_{pm-1}\mathrm{C}_{p-1}$ の分子の各項は連続する $p-1$ 個の整数 $pm-1,\ pm-2,\ \cdots,\ pm-p+1$ の積であり，いずれも $p$ で割り切れないので，${}_{pm-1}\mathrm{C}_{p-1}$ は $p$ で割り切れない．よって，${}_{pm-1}\mathrm{C}_{p-1}$ は $p$ と互いに素となり，

${}_{pm}\mathrm{C}_p$ が $p$ で割り切れる

$\Longleftrightarrow$ $m$ が $p$ で割り切れる

が成立する．

終

この☆二項係数の性質②☆ が背景にあるのが，次の京都大学の入試問題である．別に☆二項係数の性質②☆ を知らなくても解けるのだが，やはり知っていると，証明の道筋がはっきりして明確であろう．

## 京大入試問題 14

$n$ が相異なる素数 $p$，$q$ の積，$n = pq$ ，であるとき，$(n-1)$ 個の数 ${}_n\mathrm{C}_k$ $(1 \leqq k \leqq n-1)$ の最大公約数は 1 であることを示せ．

[1997 年前期理系]

【考え方】

「$(n-1)$ 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．まずは，特別な数に注目して，最大公約数の候補を考えよう．例えば，${}_{pq}\mathrm{C}_1 = pq$ の約数は $1,\ p,\ q,\ pq$ だから，最大公約数も，$1,\ p,\ q,\ pq$ のいずれかであることがわかる．

あとは，残り $(n-2)$ 個の数のそれぞれの約数と共通な約数が 1 であること，つまり，共通約数が $p$ や $q$, $pq$ にはならないこと，を証明すればよい．

そのためには，$p$ で割り切れない，または，$q$ で割り切れない数の存在を具体的に示せばよいのだが，どの数なのか見当がつかないかもしれない．しかし，これも特別な数に注目すれば，うまく示せる．では，どの数を選ぶのか，と言われると，対象となりそうなものは限られてくるだろう．

いずれにしても，具体的に計算できそうな項に注目することがポイントである．

【解説】

${}_{pq}\mathrm{C}_1 = pq$ の約数は $1,\ p,\ q,\ pq$ だから，最大公約数は，$1,\ p,\ q,\ pq$ のいずれかである．

$$\begin{aligned}&{}_{pq}\mathrm{C}_p\\ =&q{}_{pq-1}\mathrm{C}_{p-1}\\ =&q\frac{(pq-1)(pq-2)\cdots(pq-p+1)}{(p-1)!}\end{aligned}$$

ここで，分子は連続する $p-1$ 個の整数 $pq-1,\ pq-2,\ \cdots,\ pq-p+1$ の積であり，これらはいずれも $p$ の倍数ではなく，$p$ と $q$ は相異なる素数なので，${}_{pq}\mathrm{C}_p$ は $p$ の倍数ではない．同様にして，${}_{pq}\mathrm{C}_q$ は $q$ の倍数ではない．

よって，最大公約数が $p,\ q,\ pq$ になることはありえないので，最大公約数は 1 となる．

■

***Remark* 37**

☆二項係数の性質②☆ より，

$${}_{pq}\mathrm{C}_p\text{が}p\text{で割り切れる}$$
$$\Longleftrightarrow q\text{が}p\text{で割り切れる}$$

が成立する．しかし，$p$ と $q$ が相異なる素数だから，$q$ が $p$ で割り切れることはないので，

$${}_{pq}\mathrm{C}_p\text{は}p\text{で割り切れない}$$

ことがわかる．同様にして，

$${}_{pq}\mathrm{C}_q\text{は}q\text{で割り切れない}$$

こともわかる．

□

***Remark* 38**

それでは，${}_{pq}\mathrm{C}_p$ を $p$ で割った余りはどうなるのであろうか．

一般に，${}_{pq}\mathrm{C}_k$ $(1 \leqq k \leqq pq-1)$ で $k$ が $p$ の倍数のとき，${}_{pq}\mathrm{C}_k$ と ${}_q\mathrm{C}_{\frac{k}{p}}$ は $p$ で割った余りは同じになる．つまり，

$${}_{pq}\mathrm{C}_k \equiv_q {}\mathrm{C}_{\frac{k}{p}} \pmod p$$

が成立する．このことから，

$${}_{pq}\mathrm{C}_p \equiv_q \mathrm{C}_1 \equiv q \pmod p$$

となるので，${}_{pq}\mathrm{C}_p$ を $p$ で割った余りは $q$ であることがわかる．

このことを使えば，☆二項係数の性質②☆ も簡単に説明がつく．つまり，

$${}_{pm}\mathrm{C}_p \equiv_m \mathrm{C}_1 \equiv m \pmod p$$

だから，

${}_{pm}\mathrm{C}_p$が $p$ で割り切れる $\Longleftrightarrow$ $m$ が $p$ で割り切れる

のは明白．

□

# 7　完全剰余系

整数問題の攻略 (基礎編) の最後は，完全剰余系について解説する．

”完全剰余系”などと仰々しく言われると，とても難しそうな気がするが，その内容は極めてシンプルである．美しさすら感じる．

しかし，完全剰余系をテーマにした問題は，整数問題の中でも難問の部類に属し，主に難関大学で頻繁に取り上げられてきた．

これから，完全剰余系に関する重要な性質をいくつか紹介していくが，いきなり一般的な内容に踏み込む前に，まずは具体的な数値で”意味”を確認してほしい．

具体例での考察が，整数問題を攻略する上で，もっとも基本かつ重要な考え方なのである．

それでは，完全剰余系の話を始めよう．

まずは，整数を余りで分類したときのことを思い出してほしい．

全ての整数は $n$ で割ったときの余りによって $n$ 個のグループに分類される．つまり，全ての整数は，$\mod n$ に対して，

$$0,\ 1,\ 2,\ \cdots,\ n-1$$

のいずれかの整数と合同になる．このような $n$ 個の整数の集合

$$\{0,\ 1,\ 2,\ \cdots,\ n-1\}$$

を法 $n$ に関する完全剰余系という．

***Remark* 39**

正確に表現すると，$n$ で割ったときの余りによって分類された $n$ 個のグループを法 $n$ に関する剰余類といい，この $n$ 個の剰余類の各々から，1 つずつ代表元を選んで作った整数の組のことを，法 $n$ に関する完全剰余系というのである．

例えば $n=5$ とき,

$$\{0,1,2,3,4\}$$

や

$$\{-2,-1,0,1,2\}$$

はいずれも法 5 に関する完全剰余系である．

一般に, 完全剰余系の選び方は無数にあるのだが，ここでは，始めの例，つまり，0 から $n-1$ までの整数の組を法 $n$ に関する完全剰余系ということにする

□

***Remark* 40**

上のように表記すると，完全剰余系とは単なる $n$ 個の整数の集まりなのか, と思うかもしれないが，　mod $n$ **で考えている**ということが重要なのである．たとえば，次のような 5 つの整数の集合を考えてみよう

$$\{0,1,2,3,4\}$$

この集合の中の数字 $0,1,2,3,4$ だけを使って，加法，減法，乗法をいろいろおこなってみよう．すると，計算結果が, 0,1,2,3,4 以外の数字になることがある (例えば，$3+4,\ 1-4,\ 2\times 3,$ など)．つまり，もとの集合に属する整数以外の数が出てきてしまう．

しかし，　mod 5 でみれば (つまり，　mod 5 で計算すれば)，計算結果は, 0,1,2,3,4 のいずれかの整数に必ずなるので，常にもとの集合に属することがわかる．

このように，ある演算による計算結果が常に元の集合に属することを，「集合がその演算に関して閉じている」という．

この場合，集合 $\{0,1,2,3,4\}$ は　mod 5 で，加法，減法，乗法に関して閉じている，ということになる．これが，完全剰余系の基本概念である．

□

完全剰余系とはどういうものなのかがわかったところで，完全剰余系に関する基本定理を紹介する．この定理は非常に重要で，これをテーマにした入試問題は数多くある．

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欲しい．なお，2008 年の奈良県立医科大学でこれと証明方法が同じ問題が出題された (後ほど紹介する)．

**☆完全剰余系の基本定理☆**
法 $n$ に関する完全剰余系の各元に，$n$ と互いに素な整数 $a$ をかけても，また法 $n$ に関する完全剰余系となる．

つまり，こういうことである．

法 $n$ に関する完全剰余系

$$\{0,\ 1,\ 2,\ \cdots,\ n-1\}$$

の各元に $n$ と互いに素な整数 $a$ をかけ,

$$\{0a,\ 1a,\ 2a,\ \cdots,\ (n-1)a\}$$

とすると，これもまた法 $n$ に関する完全剰余系になる，すなわち $n$ 個の整数 $ka(k=0,\ 1,\ 2,\ \cdots,\ n-1)$ を $n$ で割った余りには，0 から $n-1$ までの整数が 1 回ずつすべて (順不同で) 現れる，ということ．言い換えると，

**☆完全剰余系の基本定理☆**
$a,\ n$ が互いに素であるとする．このとき，$n$ 個の相異なる整数

$$0a,\ 1a,\ 2a,\ 3a,\ \cdots,\ (n-1)a$$

を $n$ で割った余り全体は，0 から $n-1$ までの全ての整数である
つまり，$n$ で割った余りには，0 から $n-1$ までの整数が 1 回ずつすべて (順不同で) 現れる．

本当にこんなことがおこるのだろうか．まずは具体的な数字で確認してみよう．

---

**例 23**

$n=8$ とする．つまり，法 8 に関する完全剰余系

$$\{0,1,2,3,4,5,6,7\}$$

を考える．

8 と互いに素な数として，$a=3$ をとり，完全剰余系の基本定理 (以下，単に「基本定理」とよぶ) を確認する．

$0\times3,\ 1\times3,\ 2\times3,\ 3\times3,\ 4\times3,\ 5\times3,\ 6\times3,\ 7\times3$ を 8 で割った余りを求めると，

$$\begin{aligned}0\times3=0&\longrightarrow \text{余り } 0\\ 1\times3=3&\longrightarrow \text{余り } 3\\ 2\times3=6&\longrightarrow \text{余り } 6\\ 3\times3=9&\longrightarrow \text{余り } 1\\ 4\times3=12&\longrightarrow \text{余り } 4\\ 5\times3=15&\longrightarrow \text{余り } 7\\ 6\times3=18&\longrightarrow \text{余り } 2\\ 7\times3=21&\longrightarrow \text{余り } 5\end{aligned}$$

確かに，余りは 0, 1, 2, 3, 4, 5, 6, 7 が 1 回ずつ現れている．

次に，8 と互いに素でない数として，$a=6$ をとり，基本定理を確認する．

$0\times6,\ 1\times6,\ 2\times6,\ 3\times6,\ 4\times6,\ 5\times6,\ 6\times6,\ 7\times6$ を 8 で割った余りを求めると，

$$\begin{aligned}0\times6=0&\longrightarrow \text{余り } 0\\ 1\times6=6&\longrightarrow \text{余り } 6\\ 2\times6=12&\longrightarrow \text{余り } 4\\ 3\times6=18&\longrightarrow \text{余り } 2\\ 4\times6=24&\longrightarrow \text{余り } 0\\ 5\times6=30&\longrightarrow \text{余り } 6\\ 6\times6=36&\longrightarrow \text{余り } 4\\ 7\times6=42&\longrightarrow \text{余り } 2\end{aligned}$$

となり，余りは 0, 1, 2, 3, 4, 5, 6, 7 が 1 回ずつ現れることはない．

---

---

**例 24**

7 は素数だから，$1\leqq n\leqq 6$ の全ての整数 $n$ と互いに素である．よって，下の表で全ての横の段には， mod 7 でみたときに 0 から 6 までの数字が 1 回ずつ現れている．

| × | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
|---|---|---|---|---|---|---|---|
| 1 | 0 | 1 | 2 | 3 | 4 | 5 | 6 |
| 2 | 0 | 2 | 4 | 6 | 1 | 3 | 5 |
| 3 | 0 | 3 | 6 | 2 | 5 | 1 | 4 |
| 4 | 0 | 4 | 1 | 5 | 2 | 6 | 3 |
| 5 | 0 | 5 | 3 | 1 | 6 | 4 | 2 |
| 6 | 0 | 6 | 5 | 4 | 3 | 2 | 1 |

---

それでは基本定理を証明しよう．

この証明方法が重要なので，しっかりと理解してほしい．

**☆完全剰余系の基本定理☆**

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

$$0a,\ 1a,\ 2a,\ 3a,\ \cdots,\ (n-1)a$$

を $n$ で割った余り全体は，0 から $n-1$ までの全ての整数である

つまり，$n$ で割った余りには，0 から $n-1$ までの整数が 1 回ずつすべて (順不同で) 現れる．

**証明**

$n$ 個の整数 $ka(k=0,\ 1,\ 2,\ \cdots,\ n-1)$ を $n$ で割った余りは, $n$ 個の整数 $0,\ 1,\ 2,\ \cdots, n-1$ のいずれかの数である．よって，$n$ 個の余りが全て異なることを示せばよい．

$k_1,\ k_2\ (0\leqq k_1<k_2\leqq n-1)$ として，$k_1a,\ k_2a$ を $n$ で割った余りが同じであると仮定すると，

$$\begin{aligned}k_1a&=nq_1+r\\ k_2a&=nq_2+r\\ \therefore\quad (k_2-k_1)a&=n(q_2-q_1)\end{aligned}$$

$a$, $n$ 互いに素より，$k_2-k_1$ は $n$ の倍数である．ところが，$0\leqq k_1<k_2\leqq n-1$ より，$1\leqq k_2-k_1\leq n-1$ だから，$k_2-k_1$ は $n$ の倍数にはならない．よって，矛盾．

したがって，$n$ 個の数 $ka(k=0,\ 1,\ 2,\ \cdots,\ n-1)$ を $n$ で割った余りは全て異なるので，題意は証明された．

証明終

***Remark* 41**

上の基本定理では，法 $n$ に関する完全剰余系で考えているので，

$$\{0a,\ 1a,\ 2a,\ \cdots,\ (n-1)a\}$$

という，$n$ 個の整数について述べているが，$a$ と $n$ が互いに素であるので，$0a$ を $n$ で割った余りは明らかに 0 であり，$1a,\ 2a,\ \cdots,\ (n-1)a$ を $n$ で割った余りは明らかに 0 ではないので，初めから $0a$ の場合を除外して，次のように表現する場合もある．

> $a,\ n$ が互いに素であるとする．このとき，$n-1$ 個の相異なる整数
>
> $$1a,\ 2a,\ 3a,\ \cdots,\ (n-1)a$$
>
> を $n$ で割った余り全体は，1 から $n-1$ までの全ての整数である
> つまり，$n$ で割った余りには，1 から $n-1$ までの整数が 1 回ずつすべて (順不同で) 現れる．

書物によっては，こちらの方を基本定理として扱っているものもある．どちらの方を基本定理とするべきか，などという議論は全くナンセンスである．特に，どちらというふうに限定せずに，臨機応変に考えていきたい．

□

---

## 練習問題 42

$p,\ q$ を互いに素な正整数とする．

(1) 任意の整数 $x$ に対して，$p$ 個の整数

$$x-q,\ x-2q,\ \cdots,\ x-pq$$

を $p$ で割った余りは全て相異なることを証明せよ．

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

[2008 年奈良県立医大前期]

---

**【考え方】**

(1) は，基本定理の証明方法をそのまま適応すればよい．

(2) は，$x = pa + qb$ より $x - bq = pa$ だから，$x - bq$ が $p$ で割り切れることになる．このことと (1) との関係が読み取れるだろうか．

正しい論述をしてほしい．

**【解説】**

(1)

背理法で証明する．

$x - kq$ と $x - lq(1 \leqq k < l \leqq p)$ を $p$ で割った余りが等しいとすると，

$$x - kq = p\alpha + r$$
$$x - lq = p\beta + r$$
$$\therefore\ \ (l-k)q = p(\alpha - \beta)$$

$p,\ q$ 互いに素より，$l-k$ は $p$ の倍数である．ところが，$1 \leqq k < l \leqq p$ より，$1 \leqq l-k \leqq p-1$ だから，$l-k$ は $p$ の倍数にはならない．よって，矛盾．

したがって，$p$ 個の数 $x - kq(k = 1,\ 2,\ \cdots,\ p)$ を $p$ で割った余りは全て異なる

(2)

$x > pq$ より $p$ 個の整数 $x - kq(k = 1,\ 2,\ \cdots,\ p)$ は全て正の整数である．

任意の正の整数を $p$ で割った余りは，$0,\ 1,\ ,\cdots,\ p-1$ のいずれかである．

(1) より，$p$ 個の整数 $x - kq(k = 1,\ 2,\ \cdots,\ p)$ を $p$ で割った余りは全て異なり，かつ，余りは $p$ 個の整数 $0,\ 1,\ ,\cdots,\ p-1$ のいずれかであることから，$x - kq(k = 1,\ 2,\ \cdots,\ p)$ の中に，$p$ で割って余りが 0 であるものが必ず 1 つ存在する．このときの $k$ を $b$ とし，$p$ で割ったときの商を $a$ とすれば，

$$x - bq = pa$$

となる．すなわち，$x = pa + qb$ となる正整数 $a,\ b$ が存在する．

よって，題意は証明された．

■

さて，基本定理から，次の 2 つの重要なことが導かれる．

> **☆基本定理からわかる重要性質☆**
>
> $a,\ b$ が互いに素
> $\Longleftrightarrow$ $ax + by = 1$ となる整数 $x,\ y$ が存在する．

**証明**

($\Longrightarrow$) の証明

$a,\ b$ が互いに素のとき，基本定理より，$ka(k = 0,\ 1,\ 2,\ \cdots, b-1)$ 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，$k = x,\ -q = y$ とおいて題意は成立する．

($\Longleftarrow$) 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，

$$ax + by = 1$$
$$pa'x + pb'y = 1$$
$$p(a'x + b'y) = 1$$

$p$ は素数なので，この式は矛盾である．

証明終

***Remark* 42**

上にあげた**基本定理からわかること①**を互いに素であること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 25**

$a$ を 2 以上の自然数とするとき，$a$, $a^2+1$ は互いに素であることを**基本定理からわかること①**を利用して示せ．

---

【解説】

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

■

***Remark* 43**

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．よって，$a$, $a^2+1$ は互いに素である．

記号で書くと，

$$(a^2+1,\ a) = (a,\ 1) = 1$$

この，ユークリッドの互除法による証明も一つと数えると，$a$, $a^2+1$ は互いに素である証明をこれまでに 4 つ紹介したことになる．**練習問題 39** と合わせて確認しておこう．いずれも大切な証明方法である．

□

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，各自で取り組んでみよう．

---

**練習問題 43**

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．

[2002 年明治大 (商)]

---

【解説】

まず**完全剰余系の基本定理**を証明し，次に**基本定理からわかること⊠**を証明する．全く同じなので省略する．

かなりの長丁場である．私立文系の入試問題としては厳しすぎる．

■

***Remark* 44**

さて，$ax + by = 1$ を $\mod b$ でみると，

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

となるので，**基本定理からわかること①**は，

$a$, $b$ が互いに素
$\Longrightarrow ax \equiv 1 \pmod{b}$ となる整数 $x$ が存在する．

となる．つまり，

> $a$, $b$ が互いに素のとき，1 次合同方程式
>
> $$ax \equiv 1 \pmod{b}$$
>
> には必ず解が存在する．法 $b$ で考えたときは，整数解の個数は 1 個である．

となる．具体的にどのような解になるかはまだわからないが，少なくとも解が存在することは保障されたわけである．

□

**発展 6**

なお，一般的には次のようになる．興味のある人は，証明を考えてみよう．

1 次合同方程式

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

には必ず解が存在するための必要十分条件は，$a$ と $b$ の最大公約数を $d$ とするとき，$d$ が $c$ を割り切ること，である．さらに，法 $b$ で考えたとき，この 1 次合同方程式の整数解の個数は $d$ 個である．

となる．つまり，先ほどの条件に当てはめると，$a$, $b$ が互いに素のとき，$a$ と $b$ の最大公約数は $d = 1$．このとき，1 は $c$ を割り切るので解が必ず存在する．さらに，解の個数は 1 個である．

□

それでは，$a$, $b$ が互いに素であるとき，$ax + by = 1$ となる整数 $x$, $y$ を実際に求めてみよう．

---

**例 26**

$3x + 5y = 1$ を満たす整数 $x$, $y$ を求めよ．

---

**【考え方】**

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．

**【解説】**

$x = 2$, $y = -1$ が解の 1 つだから，

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

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．

■

***Remark* 45**

合同式を利用すると，次のような解答になる．

$3x + 5y = 1$ を　mod 5 でみると，

$$3x \equiv 1 \pmod{5}$$

となる．この両辺に 2 をかけると，

$$6x \equiv 2 \pmod{5}$$

$6 \equiv 1 \pmod{5}$ だから，

$$x \equiv 2 \pmod{5}$$

となる．つまり，$x = 5k + 2$ である．

□

上の例の解答に不安を感じる人もいるだろう．なぜ，1 組の解が簡単に見つかるのか，見つからない場合はどうするのか．また，合同式を利用した解答では，両辺に 2 を掛ける，とあるが，なぜ 2 なのか，と．

解は必ず存在することはわかったものの，実際に解を求めるには，少し工夫が必要なようである．

実は，この背景には，すでに紹介したユークリッドの互除法がある．ユークリッドの互除法を利用すれば，$ax + by = 1$ の整数解 $x$, $y$ を 1 組求めることができる．しかし，入試ではユークリッドの互除法を利用しないと解が求められないような問題は出題されない (つまり，簡単に 1 組見つかる) ので，ここで詳しくは説明しないでおく．

$\cdots$ と，タカをくくっていたら東大で次のような問題が出題された．解を 1 組うまく見つけられるだろうか．

---

## 応用問題 14

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．

[2005 年東京大前期文理共通]

---

**【考え方】**

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

**【解説】**

$a^2 - a$ が 10000 で割り切れることから，

$$a(a-1) = 2^4 5^4 k$$

となる．

ところで，$a$ と $a-1$ は互いに素である (なぜなら，互いに素でないと仮定すると共通の素因数 $p$ が存在することになり，$a = pm$, $a - 1 = pn$ より $p(m-n) = 1$ となるので矛盾)．したがって，$a$ は奇数であることから

$$a = 5^4 x, \quad a - 1 = 2^4 y \quad (x,\ y \text{ は整数})$$

となるので，

$$625x - 16y = 1$$

となる．これをみたす整数 $x$, $y$ を求める．$625 = 16 \times 39 + 1$ であるから，$x = 1$, $y = 39$ が解の 1 組なので，

$$625x - 16y = 1$$
$$625 \cdot 1 - 16 \cdot 39 = 1$$

の辺々を引くと，

$$625(x-1) - 16(y-39) = 0$$
$$625(x-1) = 16(y-39)$$

となる．625 と 16 は互いに素だから，$x - 1 = 16k$ とおけ，このとき，$y - 39 = 625k$ となる．したがって，$x = 16k + 1$, $y = 625k + 39$ と定まる．

よって，$a = 5^4 x = 625(16k+1)$ となり，$a$ は 3 以上 9999 以下の奇数だから，

$$3 \leqq 625(16k+1) \leqq 9999$$

これをみたす $k$ は $k = 0$ であるので，$a = 625$ となる．

■

## ***Remark*** **46**

合同式を利用すれば，

$$625x - 16y = 1$$

を　mod 16 でみると，$625 = 16 \times 39 + 1$ であるから，$625 \equiv 1$ なので，

$$x \equiv 1 \pmod{16}$$

したがって，$x = 16k + 1$ と定まる

□

またさらに，次のことが言える．

> **☆基本定理からわかること②☆**
> $a$, $b$ が互いに素であるとき，$ax + by$($x$, $y$ は整数) は任意の整数値をとることができる．つまり，$ax + by$ 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，「基本定理からわかること①」より，

$$ax + by = 1$$

となる整数 $x$, $y$ 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，

$$a(cx) + b(cy) = c$$

が得られる．

証明終

もし，「$a$, $b$ 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ことを証明せよ」といわれたら，まず**基本定理**を証明し，次に**基本定理からわかること①**を証明し $\cdots$ と，かなり息の長い議論をせねばならない．

しかし，実際に入試で出題されるとすれば，$a$, $b$ が具体的な数値で与えられることが多く，この場合には，上のような長い議論をするのは実戦的ではない．

次のように，解答すれば十分であろう．

---

## 練習問題 44

$7x + 11y$($x$, $y$ は整数) は任意の整数値をとることができることを証明せよ．

---

**【考え方】**

やはり，$7x + 11y = 1$ とみたす解を 1 組求めねばならない．

**【解説】**

$x$, $y$ が整数の時，$7x + 11y$ も整数である．

さらに ($x = -3$, $y = 2$ が $7x + 11y = 1$ をみたすことを調べた上で)，任意の整数 $m$ に対して，$x = -3m$, $y = 2m$ とおくと，

$$7(-3m) + 11(2m) = m$$

となるので，$7x + 11y$ はすべての整数をとることができる．

■

---

## 応用問題 15

$xy$ 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 $\dfrac{2}{5}$ の任意の直線はこれらの円のどれかと共有点をもつという．このような性質をもつ実数 $r$ の最小値を求めよ．

[1991 年東京大前期理系]

【考え方】

まずは傾きが $\dfrac{2}{5}$ の任意の直線を設定し，と円 $(x-m)^2+(y-n)^2=r^2$ と共有点をもつための条件を考えよう．しかし，問題はここからで，☆基本定理からわかること☒☆を知らないと全く先に進まないだろう．

【解説】

傾きが $\dfrac{2}{5}$ の直線を

$$2x-5y=a \quad (a \text{ は定数})$$

とおくと，これが円 $(x-m)^2+(y-n)^2=r^2$ と共有点をもつための条件は

$$r \geqq \frac{|2m-5n-a|}{\sqrt{2^2+(-5)^2}}=\frac{|2m-5n-a|}{\sqrt{29}}$$

ここで，$m$，$n$ がすべての整数値をとるとき $2m-5n$ はすべての整数値をとることができる．なぜならば，任意の整数 $a$ に対して，$m=3a$，$n=a$ とおけば，

$$2(3a)-5(a)=a$$

となるからである．

したがって，$a$ にもっとも近い整数を $N$ とすれば，

$$|2m-5n-a| \geqq |N-a|$$

となので，

$$r \geqq \frac{|N-a|}{\sqrt{29}} \quad \cdots ①$$

である．$|N-a| \leqq \dfrac{1}{2}$ より，任意の実数 $a$ に対して，①が成立するための $r$ の条件は，

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

となるので，求める $r$ の最小値は $r=\dfrac{1}{2\sqrt{29}}$ である．

■