剰余系をテーマとした問題

剰余類と剰余系

m で割った余りが r ($r=0,1,2,\cdots,m-2,m-1$) であるような整数全体の集合を C_r で表すと, 整数の集合 Z は, $C_0, C_1, C_2, \cdots, C_{m-2}, C_{m-1}$ の m 個の部分集合に分類できる。この各部分集合を m を法とする剰余類という。

$C_0, C_1, C_2, \cdots, C_{m-2}, C_{m-1}$ の各剰余類を,
それぞれ $0,1,2,\cdots,m-2,m-1$ で代表させたとき,
その集合 $Z_m=\{0,1,2,\cdots,m-2,m-1\}$ を
m を法とする剰余系という。

代表は, 0 から連続する m 個の整数である必要はない。

「剰余系」という表現を用いる代わりに

例題１ m, n を整数とする。(以後, このことを $m, n\in Z$ と表す)
$m+n$, mn の偶奇を, m, n の偶奇について調べよ。

① m が偶数, n が偶数のとき

$m=2h$, $n=2k$ ($h, k\in Z$) と表すことが出来るので
$m+n=2h+2k=2(h+k)$
$mn=2h\times 2k=2\times(2hk)$
$h+k$, $2hk\in Z$ なので　$m+n$ は偶数, mn は偶数である。

② m が偶数, n が奇数のとき

$m=2h$, $n=2k+1$ ($h, k\in Z$) と表すことが出来るので
$m+n=2h+(2k+1)=2(h+k)+1$
$mn=2h\times(2k+1)=2\times\{h(2k+1)\}$
$h+k$, $h(2k+1)\in Z$ なので　$m+n$ は奇数, mn は偶数である。

③ m が奇数, n が偶数のとき

$m=2h+1$, $n=2k$ ($h, k\in Z$) と表すことが出来るので
$m+n=(2h+1)+2k=2(h+k)+1$
$mn=(2h+1)\times 2k=2\times\{k(2h+1)\}$
$h+k$, $k(2h+1)\in Z$ なので　$m+n$ は奇数, mn は偶数である。

④ m が奇数, n が奇数のとき

$m=2h+1$, $n=2k+1$ ($h, k\in Z$) と表すことが出来るので
$m+n=(2h+1)+(2k+1)=2(h+k+1)$
$mn=(2h+1)\times(2k+1)=4hk+2h+2k+1=2(2hk+h+k)+1$
$h+k+1$, $2hk+h+k\in Z$ なので　$m+n$ は偶数, mn は奇数である。

教科書の発展では「合同式」として次のように表現されている

$a\equiv 0 \pmod 2$, $b\equiv 0 \pmod 2$ $\Longrightarrow$ $a+b\equiv 0 \pmod 2$, $ab\equiv 0 \pmod 2$
$a\equiv 0 \pmod 2$, $b\equiv 1 \pmod 2$ $\Longrightarrow$ $a+b\equiv 1 \pmod 2$, $ab\equiv 0 \pmod 2$
$a\equiv 1 \pmod 2$, $b\equiv 0 \pmod 2$ $\Longrightarrow$ $a+b\equiv 1 \pmod 2$, $ab\equiv 0 \pmod 2$
$a\equiv 1 \pmod 2$, $b\equiv 1 \pmod 2$ $\Longrightarrow$ $a+b\equiv 0 \pmod 2$, $ab\equiv 1 \pmod 2$

以上のことは次のように表現できる

$A=\{\cdots,-4,-2,0,2,4,6,\cdots\}$
$B=\{\cdots,-3,-1,1,3,5,7,\cdots\}$　とする。

A の要素の一つを a, B の要素の一つを b として a を「偶数」, b を「奇数」と表す。ただし, 複数回現れる「偶数」,「奇数」は必ずしも同じ要素を表しているわけではない。

偶数, 奇数についての和, 積は次の表のようになる。

和	偶数	奇数
偶数	偶数	奇数
奇数	奇数	偶数

積	偶数	奇数
偶数	偶数	偶数
奇数	偶数	奇数

次へのＳＴＥＰとするために

$A=\{\,2k\,|\,k\in Z\,\}$, $B=\{\,2k+1\,|\,k\in Z\,\}$

A の要素の一つを a, B の要素の一つを b として a を０, b を１と表す。ただし, 複数回現れる０, １は必ずしも同じ要素を表しているわけではない。

０, １についての和, 積は次の表のようになる。

和	0	1
0	0	1
1	1	0

積	0	1
0	0	0
1	0	1

３で割ったときの余りについて

$A=\{\,3k\,|\,k\in Z\,\}$, $B=\{\,3k+1\,|\,k\in Z\,\}$, $C=\{\,3k+2\,|\,k\in Z\,\}$

A の要素の一つを a, B の要素の一つを b, C の要素の一つを c として a を０, b を１, c を２と表す。ただし, 複数回現れる０, １, ２は必ずしも同じ要素を表しているわけではない。

０, １, ２についての和, 積は次の表のようになる。

和	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

積	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

これを利用して解答する場合の表現方法

例題２ $a, b, c\in Z$, $a^2+b^2=c^2$ のとき

a, b の少なくとも一方は 3 の倍数であることを示せ。

解答
<表現方法の説明>
2 の倍数を偶数, 2 で割って 1 余る数を奇数, 偶数, 奇数の和, 積について

偶数 + 奇数は奇数
偶数 × 奇数は偶数
と表すように

3 で割り切れる数を０, 3 で割って 1 余る数を１, 3 で割って 2 余る数を２とする。０, １, ２の和, 積については次の表の通りである。

和	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

積	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

以上<表現方法の説明>

<背理法を用いた証明>
a, b はともに０でないと仮定する。

０ × ０ ≡ ０ ，１ × １ ≡ １ ，２ × ２ ≡ １ より

a, b がともに０でないとき, a^2, b^2 は１となって

$a^2+b^2\equiv$ １ ＋ １ ≡ ２　である。

これは　$c^2\equiv$ ０　または　$c^2\equiv$ １　であることに反する。

よって　a, b の少なくとも一方は０

すなわち

$a, b, c\in Z$, $a^2+b^2=c^2$ のとき
a, b の少なくとも一方は 3 の倍数である。

２０１２年・関西大学

a, b, c を正の整数とする。$a^2+b^2=c^2$ を満たすとき,
a, b, c の積 abc が 3 の倍数であることを示せ。

2005年・一橋大学

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。

2007年・千葉大学

n を奇数とする。次の問いに答えよ。
(1) n^2-1 は 8 の倍数である。
(2) n^5-n は 3 の倍数である。
(3) n^5-n は 120 の倍数である。

フェルマーの小定理をテーマとした問題

2006年・早稲田大学

次の問いに答えよ。ただし, 正の整数 n と整数 k ($0 \leqq k \leqq n$) に対して ${}_n\mathrm{C}_k$ は正の整数である事実を使ってよい。
(1) m が 2 以上の整数のとき ${}_m\mathrm{C}_2$ が m で割り切れるための必要十分条件を求めよ。
(2) p を 2 以上の素数とし, k を p より小さい正の整数とする。このとき ${}_p\mathrm{C}_k$ は p で割り切れることを示せ。
(3) p を 2 以上の素数とする。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。

2010年・大阪大学

p は素数, r は正の整数とする。
(1) x_1 , x_2 , $\cdots$, x_r についての式

$(x_1+x_2+\cdots+x_r)^p$ を展開したときの単項式

$x_1^{p_1}\cdot x_2^{p_2}\cdot\cdots\cdot x_r^{p_r}$ の係数を求めよ。

(2) x_1 , x_2 , $\cdots$, x_r が正の整数のとき

$(x_1+x_2+\cdots+x_r)^p-(x_1^p+x_2^p+\cdots+x_r^p)$ は

p で割り切れることを示せ。

(3) r は p で割り切れないとする。

このとき $r^{p-1}-1$ は p で割り切れることを示せ。

よく利用する性質

互いに素な整数 a , b と整数 c について
bc が a で割り切れる。$\Longrightarrow$ c が a で割り切れる。

フェルマーの小定理

補助定理

自然数 n と p (ただし $p \geqq 2$) が互いに素であるとき,

n , $2n$, $3n$, $\cdots$, $(p-1)n$, $p\,n$ の p 個の整数を

p で割った余りはすべて異なる。

＜背理法による証明＞
hn , kn $(p>h>k>0)$ を p で割った余りが等しいと仮定する。

このとき　$hn=lp+r$, $kn=mp+r$ とおけるので

$$hn-kn=(lp+r)-(mp+r)$$
$$(h-k)\,n=(l-m)\,p$$

ここで　n と p は互いに素なので, $(h-k)$ は p で割り切れ

$(h-k)$ の値は 0, $\pm p$, $\pm 2p$, $\pm 3p$, $\cdots$ のいずれかに一致する。

これは　$(h-k)$ が $0<h-k<p$ であることに矛盾する。

よって　自然数 n と p (ただし $p \geqq 2$) が互いに素であるとき,

n , $2n$, $3n$, $\cdots$, $(p-1)n$, $p\,n$ の p 個の整数を

p で割った余りはすべて異なる。

フェルマーの小定理

自然数 n が素数 p と互いに素であるとき,

n^{p-1} を p で割った余りは常に 1 である。

＜証明＞
補助定理により

n , $2n$, $\cdots$, $(p-1)n$, pn を p で割った余りはすべて異なり,
p で割り切れるものは pn だけなので

$n=q_1p+r_1$, $2n=q_2p+r_2$, $3n=q_3p+r_3$,
$\cdots$, $(p-1)n=q_{p-1}p+r_{p-1}$　　とすると

$r_1\times r_2\times r_3\times\cdots\times r_{p-1}=1\times2\times3\times\cdots\times(p-1)$　　が成立する。

$$n\times 2n\times\cdots\times(p-1)n=(q_1p+r_1)\times(q_2p+r_2)\times\cdots\times(q_{p-1}p+r_{p-1})$$

$$(p-1)\,!\times n^{p-1}=q_1q_2\cdots q_{p-1}\,p^{p-1}+\cdots+\left(\sum_{i=1}^{p-1}\frac{q_i}{r_i}\times r_1r_2\cdots r_{p-1}\right)p+r_1r_2\cdots r_{p-1}$$

$$(p-1)\,!\times n^{p-1}=q_1q_2\cdots q_{p-1}\,p^{p-1}+\cdots+\left(\sum_{i=1}^{p-1}\frac{q_i}{r_i}\times r_1r_2\cdots r_{p-1}\right)p+(p-1)\,!$$

$$(p-1)\,!\times\left(n^{p-1}-1\right)=q_1q_2\cdots q_{p-1}\,p^{p-1}+\cdots+\left(\sum_{i=1}^{p-1}\frac{q_i}{r_i}\times r_1r_2\cdots r_{p-1}\right)p$$

ここで右辺は p で割り切れ, $(p-1)!$ と p は互いに素であるので

$n^{p-1}-1$ は p で割り切れる。

よって

自然数 n が素数 p と互いに素であるとき,

n^{p-1} を p で割った余りは常に 1 である。
ことが証明できた。

格子点をテーマとした問題

互いに素な整数の性質

a , b , x , $y\in Z$ とする。

a , b が互いに素である $\Longrightarrow$ $ax+by=1$ を満たす x , y が存在する

$ax+by=1$ を満たす x , y が存在する $\Longrightarrow$ a , b は互いに素である

例題３　a , b が異なる正の整数で, x , y が $ax+by>0$ を満たしながら, あらゆる整数値をとって変わるときの $ax+by$ の最小値を d, そのときの x , y の値の組の 1 つを x_0 , y_0 とする。このとき, 次のことを証明せよ。

(1) x , y が整数のとき $ax+by$ は d の倍数である。
(2) d は a と b の最大公約数である。

(1)　＜証明＞

$ax_0+by_0=d$

$ax+by$ を d で割ったときの商を　q,
余りを　r $(0\leqq r<d)$　　とすると

$$ax+by=qd+r$$
$$r=ax+by-dq$$
$$r=ax+by-(ax_0+by_0)q$$
$$r=a(x-x_0q)+b(y-y_0q)$$

$X=x-x_0q$, $Y=y-y_0q$ とすると

X , Y は整数で　$aX+bY=r$ $(0\leqq r<d)$

　ここで　$r \neq 0$ と仮定すると　$0 < r < d$ となって

x, y が $ax + by > 0$ を満たしながら, あらゆる整数値をとって変わるときの $ax + by$ の最小値が d であることに矛盾する。

　　よって　$r = 0$　すなわち　$ax + by$ は d の倍数である。

(2)

① d が a と b の公倍数であることを証明する。

＜証明１＞

$x = 1$, $y = 0$ のとき　$ax + by = a$ となり
　(1) から a は d の倍数, d は a の約数となる。

$x = 0$, $y = 1$ のとき　$ax + by = b$ となり
　(1) から b は d の倍数, d は b の約数となる。

　よって　d は a と b の公約数である。

② d は a と b の最大公約数であることを証明する。

＜証明２＞

① より　$a = a_1 d$, $b = b_1 d$ とおける。

　これを　$ax_0 + by_0 = d$　に代入して

$$a_1 d x_0 + b_1 d y_0 = d$$
$$a_1 x_0 + b_1 y_0 = 1$$

a_1 と b_1 の最大公約数を d' とすると　$a_1 = a_2 d'$, $b_1 = b_2 d'$

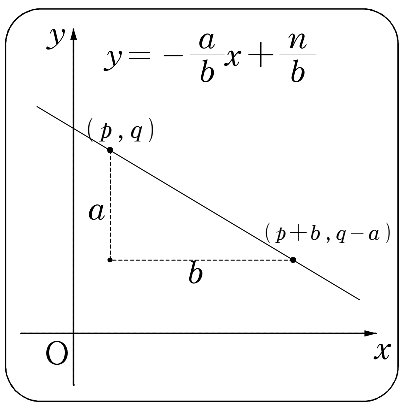
$$a_2 d' x_0 + b_2 d' y_0 = 1$$
$$(a_2 x_0 + b_2 y_0) \times d' = 1$$　となるので

　　$d' = 1$　すなわち　a_1 と b_1 は互いに素である。

「$a = a_1 d$, $b = b_1 d$, a と b は互いに素 」であることから

　　d は a と b の最大公約数である。

$ax + by = n$ をみたす整数 x, y の一般型



$a, b, x, y \in Z$
　(a, b は互いに素である) とする。

格子点 (p, q) $(p, q \in Z)$ が
$ax + by = n$ を満たすとき,
$ax + by = n$ を満たす x, y の一般型は

$$\begin{cases} x = p + bk \\ y = q - ak \end{cases} \quad (k \in Z) \text{ であり,}$$

この形で表現できないものはない。

2007年・上智大学

n を自然数とし, 座標平面上の直線

$$l_n : 3x + 5y = n$$

を考える。x 座標と y 座標がともに 0 以上の整数である l_n 上の点の個数を $N(n)$ とする。たとえば, $N(1) = N(2) = N(4) = 0$ であり, $n = 3$ のとき, 条件を満たす l_3 上の点は $(1, 0)$ のみなので $N(3) = 1$ である。

(1) $N(n) = 2$ を満たす最小の n を求めよ。
(2) $N(n) = 0$ を満たす最大の n を求めよ。

連続する 2 つの整数は互いに素である

2012年・東京大学

n を 2 以上の整数とする。自然数 (1 以上の整数) の n 乗になる数を n 乗数と呼ぶことにする。以下の問いに答えよ。

(1) 連続する 2 個の自然数の積は n 乗数でないことを示せ。
(2) 連続する n 個の自然数の積は n 乗数でないことを示せ。

「整数のこの性質」とはまとめにくい問題

2009年・京都大学

p を素数, n を正の整数とするとき $(p^n)!$ は p で何回割り切れるか。

2012年・奈良県立医大

n を 3 以上の整数とし, n 個の整数 $a_1, a_2, \cdots, a_n$ は以下の 3 条件を満たすとする。

条件 (i) : $a_1 \geqq 2$
条件 (ii) : $a_1 \geqq a_2 \geqq \cdots \geqq a_n$
条件 (iii) : $1 \leqq i < j <\leqq n$ を満たす任意の整数 i, j に対して, 不等式

$$a_i + a_j > 0 \text{ が成り立つ。}$$

このとき, 不等式 $\displaystyle\sum_{i=1}^{n} a_i \geqq n$ が成り立つことを証明せよ。また, この不等式において等号が成り立つ場合の n の値, および n 個の整数の組 $(a_1, a_2, \cdots, a_n)$ をすべて求めよ。

解き終わると問題の構造がよく見えてくる

2008年・早稲田大学

自然数 m, n に対して $f(m, n)$ を

$$f(m, n) = \frac{1}{2}\left\{(m + n - 1)^2 + (m - n + 1)\right\} \text{ で定める。}$$

以下の問に答えよ。

(1) $f(m, n) = 100$ をみたす m, n を 1 組求めよ。
(2) a, b, c, d は整数で, 等式 $a^2 + b = c^2 + d$ をみたすとする。不等式 $-a < b \leqq a$, $-c < d \leqq c$ が成り立つならば, $a = c$, $b = d$ となることを示せ。
(3) 任意の自然数 k に対し, $f(m, n) = k$ をみたす m, n がただ 1 組だけ存在することを示せ。

2012年・早稲田大学

初項を $a_0 \geqq 0$ とし, 以下の漸化式で定まる数列 $\{a_n\}_{n=0,1,2,\cdots}$ を考える。

$$a_{n+1} = a_n - \left[\sqrt{a_n}\right] \quad (n \geqq 0)$$

ただし $[x]$ は x を超えない最大の整数を表す。次の問いに答えよ。

(1) $a_0 = 24$ とする。このとき, $a_n = 0$ となる最小の n を求めよ。
(2) m を 2 以上の整数とし, $a_0 = m^2$ とする。このとき, $1 \leqq j \leqq m$ をみたす j に対して a_{2j-1}, a_{2j} を j と m で表せ。
(3) m を 2 以上の整数, p を $1 \leqq p \leqq m - 1$ をみたす整数とし, $a_0 = m^2 - p$ とする。このとき, $a_k = (m - p)^2$ となる k を求めよ。さらに, $a_n = 0$ となる最小の n を求めよ。

参考書にあった超難問が, そのまま出題されたまれな例

2009年・名古屋市立大学

　n を 4 以上の自然数とする。和が n となる 2 つ以上の自然数の組合せを考え, その積の最大値を $M(n)$ とおく。
　例えば $n = 4$ のとき, 和が n となる自然数の組合せは
$(1, 1, 1, 1)$, $(2, 1, 1)$, $(3, 1)$, $(2, 2)$ があるが, この積の最大値は $2 \times 2 = 4$ のときであるから $M(4) = 4$ となる。次の問に答えよ。

(1) $M(8)$ を求めよ。
(2) $M(12)$ を求めよ。
(3) $M(n)$ を求めよ。