2018年2月8日

新城門プロジェクト　第3回
整数問題(その1)

基本事項

定義（約数・倍数）2つの整数a, bが，ある整数qを用いて$a = bq$と表せるとき，aをbの倍数，bをaの約数という。

定義（公約数）2つ以上の整数に共通の約数を，それらの整数の公約数という。公約数の中で最大の数を最大公約数という。

定義（素数）2以上の自然数で，1とその数自身以外に正の約数をもたない数を素数という。2以上の自然数で，素数以外の数を合成数という。

基本事項

性質（素数）a, b は整数，p は素数とする。

(1) ab が p の倍数であるならば，a が p の倍数であるか，b が p の倍数である。
(2) $p = ab$ ならば，$(a, b) = (1, p)$ または $(a, b) = (p, 1)$ である。

1　練習問題

nを正の整数とする。

(1) n^2と$2n+1$は互いに素であることを示せ。
(2) n^2+2が$2n+1$の倍数になるnを求めよ。

1.1　用いる定義・性質

定義（互いに素）2つの整数a, bの最大公約数が1のとき，
　a, bは互いに素であるという。
　　つまり，a, bに共通な素因数がないことと同値。

性質（互いに素）a, b, n は整数とする。
　　a, b が互いに素で，an が b の倍数であるならば，n は
　b の倍数である。

1.2　基本問題【6】より

aを整数とするとき，aと$a+1$は互いに素であることを示せ。

【証明1】

直接証明　最大公約数が1であることを示す。

aと$a+1$の最大公約数をgとすると，

$a = g\alpha,\ a+1 = g\beta$ (α, βは互いに素な整数)と表せる。

aを消去すると，$1 = g(\beta - \alpha)$であり，

$\beta - \alpha$は整数で，gが1の正の約数となるから$g = 1$。

よって，a と $a+1$は互いに素である。

1.3　基本問題【6】より

aを整数とするとき，aと$a+1$は互いに素であることを示せ。

【証明2】

背理法　共通な素因数をもつと仮定して矛盾を導く。

aと$a+1$が共通の素因数pをもつとすると，

$a = p\alpha,\ a+1 = p\beta$ (α, βは整数)と表せる。

aを消去すると，$1 = p(\beta - \alpha)$であり，

$\beta - \alpha$は整数で，pが1の約数となるから

pが素数であることに反する。

よって，a と $a+1$は互いに素である。

1.4　(1) 解答　その 1

まず，n と $2n+1$ は互いに素であることを示す。
n と $2n+1$ の最大公約数を g とすると，
$n = g\alpha,\ 2n+1 = g\beta$ (α, β は互いに素な整数) と表せる。
n を消去すると，$1 = g(\beta - 2\alpha)$ であり，
$\beta - 2\alpha$ は整数で，g が 1 の正の約数となるから $g = 1$。
よって，n と $2n+1$ は互いに素であり，
n と $2n+1$ には共通な素因数がない。
このとき，n^2 と $2n+1$ も共通な素因数をもたず互いに素である。

1.5　(1) 解答　その2

n^2 と $2n+1$ が共通の素因数 p をもつとすると,
$n^2 = p\alpha,\ 2n+1 = p\beta$ (α, β は整数) と表せる。
$4n^2 = 4p\alpha,\ 2n = p\beta - 1$ として n を消去すると
$(p\beta - 1)^2 = 4p\alpha$
整理して,
$p(4\alpha + 2\beta - p\beta^2) = 1$
$4\alpha + 2\beta - p\beta^2$ は整数で，p が1の約数となるから
p が素数であることに反する。
したがって，n^2 と $2n+1$ は互いに素である。

1.6　基本問題【3】より

$x^2 - y^2 = 5$ をみたす整数の組 (x, y) をすべて求めよ。

【解答】

$(x + y)(x - y) = 5$ と因数分解すれば,

$x + y,\ x - y$ は5の約数である。

$(x + y, x - y) = (5, 1), (1, 5), (-5, -1), (-1, -5)$ より

$(x, y) = (3, 2), (3, -2), (-3, -2), (-3, 2)$

1.7　基本問題【3】類題

$x^2-2x-y^2=4$ をみたす整数の組 (x,y) をすべて求めよ。

【解答】

$x^2-2x+1-y^2=4+1$

平方完成して,

$(x-1)^2-y^2=5$

$(x-1+y)(x-1-y)=5$ と因数分解すれば,

$x-1+y,\ x-1-y$ は5の約数である。

$(x-1+y, x-1-y)=(5,1),(1,5),(-5,-1),(-1,-5)$

より

$(x,y)=(4,2),(4,-2),(-2,-2),(-2,2)$

1.8　(2) 解答　その1

n^2+2 が $2n+1$ の倍数のとき,

$n^2+2=k(2n+1)$ (k は正の整数) と表せる。

$n^2-2kn=k-2$

k^2 を両辺に加えて

$n^2-2kn+k^2=k^2+k-2$

$(n-k)^2=k^2+k-2$ と変形する。

k^2+k-2 は平方数なので,

これを $k^2+k-2=\ell^2$ (ℓ は非負整数) とおく。

$$k^2 + k - \ell^2 = 2$$

$$\left(k + \frac{1}{2}\right)^2 - \ell^2 = \frac{9}{4}$$

$$(2k+1)^2 - 4\ell^2 = 9$$
$$(2k + 2\ell + 1)(2k - 2\ell + 1) = 9$$
したがって，$2k + 2\ell + 1,\ 2k - 2\ell + 1$ は9の約数である。
$2k + 2\ell + 1 \geqq 2k - 2\ell + 1$ より
$$(2k + 2\ell + 1, 2k - 2\ell + 1) = (9, 1), (3, 3)$$
$$(k, \ell) = (2, 2), (1, 0)$$

$n^2+2=k(2n+1)$ であったから，
$k=2$ のとき，
$n^2+2=2(2n+1)$ を解いて $n=0,4$
n は正の整数だから $n=4$
$k=1$ のとき，
$n^2+2=2n+1$ を解いて $n=1$
したがって，$n=1,4$

1.9　分数が整数となるのは

$\dfrac{3}{n}$ が整数となるのは,

n が 3 の約数のときである。したがって，$n = 3, 1, -1, -3$

$\dfrac{n}{n+1}$ が整数となるのは,

$$\frac{n}{n+1} = \frac{(n+1)-1}{n+1} = 1 - \frac{1}{n+1}$$ より

$n+1$ が 1 の約数のときである。したがって，$n = 0, -2$

1.10　分子の次数を下げる

整数nの多項式$f(n), g(n)$で,
$(f(n)$の次数$) \geqq (g(n)$の次数$)$であるとき,
$f(n)$を$g(n)$で割った商を$q(n)$余りを$r(n)$とすると,
$f(n) = g(n) \cdot q(n) + r(n)$
$(r(n)$の次数$) < (g(n)$の次数$)$

$$\frac{f(n)}{g(n)} = \frac{g(n) \cdot q(n) + r(n)}{g(n)} = q(n) + \frac{r(n)}{g(n)}$$

1.11　(2) 解答　その2

n^2+2が$2n+1$の倍数になるとき，$\dfrac{n^2+2}{2n+1}$は整数である。

$$\frac{n^2+2}{2n+1} = \frac{(2n+1)(\frac{1}{2}n-\frac{1}{4})+\frac{9}{4}}{2n+1} = \frac{1}{2}n - \frac{1}{4} + \frac{\frac{9}{4}}{2n+1}$$

両辺を4倍して $4\cdot\dfrac{n^2+2}{2n+1} = 2n-1+\dfrac{9}{2n+1}$

$2n+1$は奇数なので4とは互いに素であるから，

$4\cdot\dfrac{n^2+2}{2n+1}$が整数であることと，$\dfrac{n^2+2}{2n+1}$が整数であることは同値である。

$$4 \cdot \frac{n^2+2}{2n+1} = 2n - 1 + \frac{9}{2n+1}$$

$\dfrac{n^2+2}{2n+1}$ が整数であるから，$\dfrac{9}{2n+1}$ が整数なので，

$2n+1$ は 9 の約数である。
$2n+1 \geqq 3$ より $2n+1 = 3, 9$
したがって $n = 1, 4$

2　練習問題

$\dfrac{2p-1}{q}, \dfrac{2q-1}{p}$ がともに整数のとき，

整数p, qの組を求めよ。ただし，$p > q > 1$とする。

2.1　解答　その 1

$p > q > 1$ より，$2p - 1 > 0,\ 2q - 1 > 0$ であって

$\dfrac{2p-1}{q},\ \dfrac{2q-1}{p}$ がともに整数であれば，

それぞれは正の整数である。

また，$0 < \dfrac{2q-1}{p} < \dfrac{2q-1}{q} = 2 - \dfrac{1}{q} < 2$ が成り立つので，

$\dfrac{2q-1}{p} = 1$ となる。

このとき，$p = 2q - 1$だから

$$\frac{2p-1}{q} = \frac{2(2q-1)-1}{q} = \frac{4q-3}{q} = 4 - \frac{3}{q}$$

$\dfrac{2p-1}{q}$が整数であるから，$\dfrac{3}{q}$が整数なので，

q は3の約数となり，$q > 1$ より $q = 3$
このとき，$p = 2 \cdot 3 - 1 = 5$

2.2　解答　その２

$\dfrac{2p-1}{q},\ \dfrac{2q-1}{p}$ はともに整数で，$p>q>1$ より

分子の $2p-1,\ 2q-1$ が正の奇数だから，

分母の p, q も奇数，$\dfrac{2p-1}{q},\ \dfrac{2q-1}{p}$ も正の奇数である。

また，$\dfrac{2p-1}{q} > \dfrac{2q-1}{p}$ が成り立つので，

$\dfrac{2p-1}{q} \geqq 3,\ \dfrac{2q-1}{p} \geqq 1$ である。

$$\frac{2p-1}{q} \times \frac{2q-1}{p} = \frac{4pq-2p-2q+1}{pq}$$
$$= 4 - \frac{2p+2q-1}{pq}$$

左辺は奇数の積で3以上，右辺は4未満であるから，

$$\frac{2p-1}{q} \times \frac{2q-1}{p} = 3$$

したがって，$\dfrac{2p-1}{q} = 3,\ \dfrac{2q-1}{p} = 1$ である。

連立方程式を解いて，$p = 5,\ q = 3$

3　練習問題

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

(2) 素数pに対して2^pをpで割った余りを求めよ。

3.1　用いる定義・性質

性質（組合せの総数）$${}_n\mathrm{C}_r = \frac{n!}{r!(n-r)!}$$

定理（二項定理）

$$(a+b)^n = {}_n\mathrm{C}_0 a^n + {}_n\mathrm{C}_1 a^{n-1}b + {}_n\mathrm{C}_2 a^{n-2}b^2 + \cdots + {}_n\mathrm{C}_k a^{n-k}b^k + \cdots + {}_n\mathrm{C}_{n-1} ab^{n-1} + {}_n\mathrm{C}_n b^n$$

性質（素数）pが素数ならば，pは a $(1 \leqq a \leqq p-1)$ と互いに素である。

3.2　(1)解答

$$
\begin{aligned}
{}_r\mathrm{C}_r &= r \cdot \frac{p!}{r!(p-r)!} \\
&= r \cdot \frac{p(p-1)!}{r(r-1)!\{(p-1)-(r-1)\}!} \\
&= p \cdot \frac{(p-1)!}{(r-1)!\{(p-1)-(r-1)\}!} \\
&= p\,{}_{p-1}\mathrm{C}_{r-1}
\end{aligned}
$$

pは素数だから$1 \leqq r \leqq p-1$なる整数rと互いに素である。
したがって，${}_p\mathrm{C}_r$はpの倍数である。

3.3　(2)解答

$$
\begin{aligned}
2^p &= (1+1)^p \\
&= {}_p\mathrm{C}_0 + {}_p\mathrm{C}_1 + {}_p\mathrm{C}_2 + \cdots + {}_p\mathrm{C}_{p-1} + {}_p\mathrm{C}_p \\
&= 1 + {}_p\mathrm{C}_1 + {}_p\mathrm{C}_2 + \cdots + {}_p\mathrm{C}_{p-1} + 1 \\
&= 2 + {}_p\mathrm{C}_1 + {}_p\mathrm{C}_2 + \cdots + {}_p\mathrm{C}_{p-1} \\
&= 2 + (p\text{の倍数})
\end{aligned}
$$

よって，2^p を p で割った余りは $\begin{cases} p=2 \text{のとき} 0 \\ p \neq 2 \text{のとき} 2 \end{cases}$ である。

3.4　(2)の発展

素数pに対して3^pをpで割った余りを求めよ。
素数pに対して4^pをpで割った余りを求めよ。

$\vdots$

素数pに対してa^pをpで割った余りを求めよ。