M3JSB/M3JB/M3TB

本科２期９月度

解答

Ｚ会東大進学教室

選抜東大クラス文系数学

東大文系数学

難関大文系数学Ｔ

１４章　代数（１）

問題

【1】(1) n と $2n+1$ の最大公約数を $d(>0)$ とすると

$n = k_1 d, \quad \cdots\cdots ①$

$2n+1 = k_2 d \quad \cdots\cdots ②$

(ただし k_1, k_2 は互いに素)

と置ける．すると，② − ① × 2 より

$1 = (k_2 - 2k_1)d \qquad \therefore \quad d = 1.$

よって，n と $2n+1$ は互いに素となるから，n^2 と $2n+1$ も互いに素である．

[証明終]

(2) 整式 x^2+2 を整式 $2x+1$ で割ると

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

$\therefore \quad 4(x^2+2) = (2x+1)(2x-1)+9. \quad \cdots\cdots ③.$

n^2+2 が $2n+1$ の倍数であるとすると，

$n^2+2 = k(2n+1)$ (ただし，k は正整数)

と置けるから，③ より

$4k(2n+1) = (2n+1)(2n-1)+9 \qquad \therefore \quad (4k-2n+1)(2n+1) = 9.$

$n \geqq 1$ より $2n+1 \geqq 3$ だから

$2n+1 = 3,\ 9 \quad \therefore \quad n = 1,\ 4.$

このとき，実際に

$1^2+2 = 1\times(2\times1+1), \qquad 4^2+2 = 2\times(2\times4+1)$

となり，条件に適する．よって，

$n = 1$ または 4.　(答)

【2】以下，2 項係数 ${}_n\mathrm{C}_r$ を $\dbinom{n}{r}$ で表す:

$$\binom{n}{r} = \frac{n(n-1)(n-2)\cdots(n-r+1)}{r!} = \frac{n!}{r!(n-r)!}.$$

これにより，2 項定理は次のように書かれる：

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \cdots + \binom{n}{k}a^{n-k}b^k + \cdots + \binom{n}{n-1}ab^{n-1} + b^n$$

$$= \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.$$

また，2 つの整数 a, b について，$a \mid b$ で，「a が b を割り切る」，「b は a で割り切られる」ことを表す．

(1) まず，$k = 1, 2, \cdots, p-1$ について，2 項係数 $\dbinom{p}{k}$ は正整数であり，

$$\binom{p}{k} = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k!} = p\cdot\frac{(p-1)(p-2)\cdots(p-k+1)}{k!}$$

である．ここで $1, 2, \cdots, k < p$ であり，p が素数であることから，2 つの整数 p と $k!$ は互いに素である．従って，この式の最右辺で p と $k!$ が約されることはありえず，第 2 因子が整数でなければならない．それを

$$\frac{(p-1)(p-2)\cdots(p-k+1)}{k!} = m\,(\in \mathbb{Z}^+)$$

と置けば,

$$\binom{p}{k} = mp \Longleftrightarrow p \,\Big|\, \binom{p}{k}$$

が言える．k は 素数 p 未満の任意の正整数であるから，題意が示された．［証明終］

(2) 左辺の $(a+b)^p$ と右辺の $a^p + b^p$ の差が p の倍数であること，つまり

$$p \,\big|\, (a+b)^p - (a^p + b^p)$$

を示す．

2 項定理より

$$\begin{aligned}
&(a+b)^p - (a^p+b^p)\\
&= a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{k}a^{p-k}b^k\\
&\qquad\qquad + \cdots + \binom{p}{p-1}ab^{p-1} + b^p - (a^p+b^p)\\
&= \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \cdots + \binom{p}{k}a^{p-k}b^k + \cdots + \binom{p}{p-1}ab^{p-1}
\end{aligned}$$

を得る．ここで，(1) で示した結果より，係数

$$\binom{p}{1}, \binom{p}{2}, \cdots, \binom{p}{p-1}$$

はすべて p の倍数であるから，$(a+b)^p - (a^p+b^p)$ は p の倍数となる．つまり

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$ ［証明終］

(3) n に関する帰納法による．

(I) $n = 2$ のとき，(2) より成立する．

(II) $n = N$ のときの成立を仮定する：

$$\text{(IH)} \quad (a_1 + a_2 + \cdots + a_N)^p \equiv a_1^p + a_2^p + \cdots + a_N^p \pmod{p}.$$

以下，$(\bmod\ p)$ を固定する．$n = N+1$ のとき,

$$\begin{aligned}
&(a_1 + a_2 + \cdots + a_N + a_{N+1})^p\\
&\equiv \{(a_1 + a_2 + \cdots + a_N) + a_{N+1}\}^p\\
&\equiv (a_1 + a_2 + \cdots + a_N)^p + a_{N+1}^p \qquad \because (2)\\
&\equiv a_1^p + a_2^p + \cdots + a_N^p + a_{N+1}^p \qquad \because (\text{IH})
\end{aligned}$$

となり，このときも成立する．

以上より，2 以上の任意の正整数 n について

$$(a_1 + a_2 + \cdots + a_n)^p \equiv a_1^p + a_2^p + \cdots + a_n^p \pmod{p}.$$ ［証明終］

(4) (3) で得た式で，$a_1 = a_2 = \cdots = a_n = 1$ を代入すると

$$\underbrace{(1+1+\cdots+1)^p}_{n\text{terms}} \equiv \underbrace{1^p + 1^p + \cdots + 1^p}_{n\text{terms}}, \qquad \therefore \quad n^p \equiv n \pmod{p}.$$ ［証明終］

cf. 階差数列を用いた，次のような証明も重要である；

いま，$f(k)=k^p-k$ と定めると

$$
\begin{aligned}
f(k+1)-f(k) &= \{(k+1)^p-(k+1)\}-(k^p-k)\\
&=(k+1)^p-(k^p+1)\\
&=k^p+\binom{p}{1}k^{p-1}+\cdots+\binom{p}{p-1}k+1-(k^p+1)\\
&=\binom{p}{1}k^{p-1}+\binom{p}{2}k^{p-2}+\cdots+\binom{p}{p-1}k.
\end{aligned}
$$

(1) で示したように，ここに現れる 2 項係数はすべて p の倍数であるから

$$p \,\big|\, f(k+1)-f(k) \iff f(k+1)-f(k)\equiv 0 \iff f(k+1)\equiv f(k) \pmod p.$$

従って，任意の正整数 n について

$$f(n)\equiv f(n-1)\equiv f(n-2)\equiv\cdots\equiv f(2)\equiv f(1)=0 \pmod p$$

が成り立つから，

$$n^p-n\equiv 0,\qquad \therefore\quad n^p\equiv n \pmod p.$$ ［証明終］

【3】(1) 2^n 以下の自然数のうち 2^k の倍数であるものの集合を A_k とすると (ただし $k=1,2,\cdots,n$)，A_k の要素の個数$\#A_k$ は

$$\#A_k=\frac{2^n}{2^k}.$$

2^n 以下の自然数のうち 2^{k+1} の倍数であるものの集合を A_{k+1} とすると (ただし $k+1=1,2,\cdots,n$)，A_{k+1} の要素の個数$\#A_{k+1}$ は

$$\#A_{k+1}=\frac{2^n}{2^{k+1}}.$$

任意の正整数 n について，$2^{k+1}\,\big|\,n$ ならば $2^k\,\big|\,n$ であるから，集合の包含関係として

$$A_{k+1}\subset A_k.$$

よって求める個数は，$k=1,2,\cdots,n-1$ のときは

$$\#A_k-\#A_{k+1}=\frac{2^n}{2^k}-\frac{2^n}{2^{k+1}}=2^{n-k-1}.$$

ただし，$n=k$ のときは，$A_{k+1}=\emptyset$ となり，求める個数は $\#A_k=\#A_n=1$ 個.

以上より，

$$\begin{cases} k=1,\ 2,\ \cdots,\ n-1 \text{ のとき，}\quad \dfrac{2^n}{2^k}-\dfrac{2^n}{2^{k+1}}=2^{n-k-1}\text{個,}\\ k=n \text{ のとき，}\quad 1 \text{ 個.}\end{cases}$$ (答)

(2) $N=(2^n)!$ を素因数分解したとき現れる因数 2 の個数は

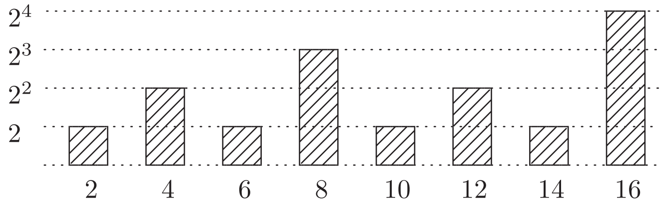
$$
\begin{aligned}
&\sum_{k=1}^{n-1}k\cdot 2^{n-k-1}+n=\sum_{k=1}^{n-1}k\left(\frac{2^n}{2^k}-\frac{2^n}{2^{k+1}}\right)+n\\
=&1\cdot\left(\frac{2^n}{2^1}-\frac{2^n}{2^2}\right)+2\left(\frac{2^n}{2^2}-\frac{2^n}{2^3}\right)+3\left(\frac{2^n}{2^3}-\frac{2^n}{2^4}\right)\\
&\qquad+\cdots+(n-1)\left(\frac{2^n}{2^{n-1}}-\frac{2^n}{2^n}\right)+n\\
=&2^{n-1}+2^{n-2}+2^{n-3}+\cdots+2^1-(n-1)+n\\
=&1+2+2^2+\cdots+2^{n-1}\\
=&2^n-1.
\end{aligned}
$$

従って，$N=(2^n)!$ は 2^{2^n-1} の倍数であるが，2^{2^n} の倍数ではない. ［証明終］

cf. 一般に, n を正整数として, $n!$ の素因数分解は重要である．いま例として, $N=\left(2^4\right)!$

の素因数分解における 2 のべき (累乗の指数) を考えてみよう．
本問の誘導に乗れば，上のような解法になるが，値を求めるだけならば，次のように考えるべきである．図 1 を見られたい．

図 1



16 以下の，2 の倍数を並べて，それぞれを素因数分解したときに，2 で割れる回数を考える．
素因数分解したときに 2^k が現れるならば，2 でちょうど k 回割ることができ，またその逆も成り立つことを考えると，$N=16!$ の素因数分解に現れる 2 のべきは，図 1 の斜線を引かれた正方形の個数に一致することを意味する．
本問の (1) から (2) へという流れは，この個数を，

いくつの正方形からなる長方形が，いくつあるか

と考えてその和を求めることであった．そのせいで，「2^k の倍数ではあるが，2^{k+1} の倍数ではないもの」の個数，つまり『高さが k の長方形の個数』を求めることになったわけである．
考え方を変えて，

少なくても j 回，2 で割り切れるものは N 以下に何個あるか

に着目すると，図 1 で，

- 下から 1 段目には何個の正方形があるか?
- 下から 2 段目には何個の正方形があるか?
- $\cdots$

として数えることにすれば，

$$\left\lfloor\frac{16}{2}\right\rfloor+\left\lfloor\frac{16}{2^2}\right\rfloor+\left\lfloor\frac{16}{2^3}\right\rfloor+\left\lfloor\frac{16}{2^4}\right\rfloor=8+4+2+1=15$$

となる．ここで実数 a について $\lfloor a\rfloor$ は，a を超えない最大の整数を表す．
この線で本問を解きなおしてみよ．

【4】(1) 題意より

$$M = 11x + 2y, \quad \cdots ①$$
$$N = 18x + 5y, \quad \cdots ②$$

$x,\ y$ は互いに素な自然数 $\cdots$ ③

である．①, ②より

$$\begin{cases} 19x = 5M - 2N, & \cdots ④ \\ 19y = 11N - 18M. & \cdots ⑤ \end{cases}$$

④より

$$2N = 5M - 19x.$$

M が 19 で割り切れる，つまり $M = 19m$ となる整数 m が存在する，ならば，$2N = 19(5m - x)$ となるから，

$2N$ は 19 の倍数である

が成り立つ．

2 と 19 は互いに素だから，N は 19 の倍数となり，n を整数として $N = 19n$ とおける．

④, ⑤より

$$\begin{cases} x = 5m - 2n, \\ y = -18m + 11n \end{cases}$$

と表される．$m,\ n$ の公約数を d とすると

$m = kd,\ n = ld \quad (k,\ l : 整数)$

であるから，代入して $x = d(5k - 2l),\ y = d(-18k + 11l)$，よって

d は, $x,\ y$ の公約数

が成り立つ

ところが③より $d = 1$ であるから，$m,\ n$ は互いに素となり，従って M と N の最大公約数は 19 であることが示された． [証明終]

(2) $M + x,\ N + y$ を表すと

$$M + x = 12x + 2y = 2(6x + y),$$
$$N + y = 18x + 6y = 6(3x + y).$$

$6x + y = M' \cdots ①'$，$9x + 3y = N' \cdots ②'$ と置き，$M',\ N'$ の最大公約数 g が 1, 3, 9 のいずれかであることを示す．

①$'$, ②$'$ より

$$\begin{cases} 9x = 3M' - N', \\ 9y = 6N' - 9M' \end{cases}$$

である．ここで

g は $9x,\ 9y$ の公約数であり，

かつ $x,\ y$ は互いに素だから, g は 9 の約数である

が言えるから，g は 1, 3, 9 のいずれかである．

従って，$M + x = 2M',\ N + y = 2N'$ となり，$M + x,\ N + y$ の最大公約数は 2, 6, 18 のいずれかである． [証明終]

【5】(1) $0 \leqq r(b) \leqq 7$ だから

$$0 < a - r(a) < \frac{4}{3}r(b) \leqq \frac{28}{3} = 9 + \frac{1}{3}, \qquad \therefore \quad 0 < a - r(a) \leqq 9.$$

$r(a)$ は a を 8 で割った余りだから, $a - r(a)$ は 8 の倍数であり,

$a - r(a) = 8.$ (答)

従って

$$8 < \frac{4}{3}r(b) \iff 6 < r(b),$$

$$\therefore \quad r(b) = 7 \qquad (\because r(b) = 0,\ 1,\ \cdots,\ 7) \qquad \text{(答)}$$

(2) (1) と同様に考えて

$$\begin{cases} b - r(b) = 8, & \cdots ① \\ r(ab) = 7. & \cdots ② \end{cases}$$

(1) の結果と①より

$b = 15$

$a = 8k + r(a)$ (k : 整数) とおけるので

$ab = 15\{8k + r(a)\} = 8 \times 15k + 15r(a) = 8\{15k + r(a)\} + 7r(a).$

②より

$$r(ab) = r(7r(a)) = 7,$$

$7r(a) - 7 = 7(r(a) - 1)$ は 8 の倍数.

よって, $r(a) = 1$ より

$a = 9.$

以上より

$(a,\ b) = (9,\ 15).$ (答)

添削課題

【1】余弦定理より

$$a^2 = b^2 + c^2 - 2bc\cos 120^\circ \iff a^2 = b^2 + c^2 + bc$$
$$\iff a^2 = (b+c)^2 - bc$$
$$\iff bc = (b+c)^2 - a^2$$
$$\iff bc = (b+c+a)(b+c-a)$$

今, $b \leqq c$ のときを考える.

$b,\ c$ はともに素数であり, また, $b+c+a > c \geqq b \geqq 2$ より

$b+c+a = bc \quad \cdots$① かつ $b+c-a = 1 \quad \cdots$②

① + ② より

$$2(b+c) = bc + 1 \iff bc - 2(b+c) + 1 = 0$$
$$\iff (b-2)(c-2) = 3$$

ここで, $b-2,\ c-2$ は $0 \leqq b-2 \leqq c-2$ をみたす整数であるから

$$(b-2,\ c-2) = (1,\ 3)$$
$\iff (b,\ c) = (3,\ 5)$ (これは $b,\ c$ が素数をみたしている)

これを, ②に代入することにより

$a = 7$

以上より

$(a,\ b,\ c) = (7,\ 3,\ 5)$

$c \leqq b$ のときも同様にして

$(a,\ b,\ c) = (7,\ 5,\ 3)$

が得られる. よって

$(a,\ b,\ c) = (7,\ 3,\ 5),\ (7,\ 5,\ 3)$　　(答)

１５章　代数（２）

問題

【1】(1) $x=2m+1,\ y=2n+1$ ($m,\ n$ は整数) と置く．

$$k = x^2-y^2 = (x+y)(x-y)$$
$$=2(m+n+1)\cdot 2(m-n)$$
$$=4(m-n)(m+n+1). \quad \cdots ①$$

ここで，$m+n$ と $m-n$ の偶奇はつねに一致するから，$m+n+1$ と $m-n$ の偶奇は異なる．

したがって $m+n+1$ と $m-n$ のうち，一方が偶数，他方が奇数である．これと①を合わせて，k は 8 の倍数である．　　　［証明終］

(2) k が 8 の倍数であることが, 方程式 $x^2-y^2=k$ が奇数解をもつための十分条件であることを示す．

$k=8l$ (l は整数) とおくと

$$x^2-y^2=(x+y)(x-y)=8l=4l\cdot 2.$$

連立方程式

$$x+y=4l, \quad x-y=2$$

を解くと

$$x=2l+1, \quad y=2l-1.$$

$x,\ y$ はともに奇数となるので, 奇数解をもつことが示された．

これと (1) を合わせると

方程式 $x^2-y^2=k$ が奇数解をもつ $\iff$ k が 8 の倍数である

が言えるから, 求める必要十分条件は,

k が 8 の倍数であること．　　　(答)

【2】(1) $C(nx)=C(ny)$ より，整数 $nx,\ ny$ の下 2 桁が等しいので

$$nx-ny=n(x-y)=100k$$

をみたす整数 k が存在する．

条件より, n は $100\ (=2^2\cdot 5^2)$ と互いに素であるから，$x-y$ は 100 の倍数である．

これは，x と y の下 2 桁は等しいことを表すから,

$C(x)=C(y)$.　　［証明終］

(2) $0\leqq i<j\leqq 99$ の任意の整数 $i,\ j$ に対し, (1) より

$$C(nx)=C(ny) \implies C(x)=C(y).$$

この対偶命題を作れば

$$C(x)\neq C(y) \implies C(nx)\neq C(ny).$$

$i<j$ より

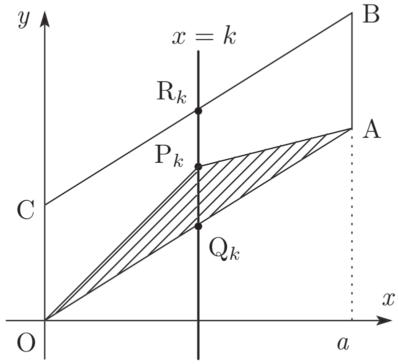
$$C(i)\neq C(j) \implies C(ni)\neq C(nj).$$

従って, $C(nx)$ の値は 0 から 99 の 100 個の異なる値をとる．

よって, $C(nx)=1$ をみたす x が存在する．　［証明終］

【3】題意を図にすると，次の図 1 のようになる．

図 1



(1) k を $1 \leqq k \leqq a-1$ をみたす正整数とし，直線 $x = k$ と線分 OA，線分 CB との交点を，それぞれ Q_k，R_k と定めると

$$\mathrm{Q}_k\left(k,\ \frac{b}{a}k\right),\quad \mathrm{R}_k\left(k,\ \frac{b}{a}k+1\right)$$

となる．

$k = 1, 2, \cdots, a-1$ であるから，k は a の非倍数であり，よって $\dfrac{b}{a}k$ が整数になることはない．従ってまず Q_k が格子点になることはない．

同様にして $\dfrac{b}{a}k+1$ も整数ではないから，R_k も格子点ではない．

開線分 (両端点を含まない線分)$\mathrm{Q}_k\mathrm{R}_k$ を考えると，その長さは 1 であり，Q_k，R_k の y 座標が整数ではないことから，その間にただ 1 個，y 座標 y_k が整数である点が存在する．その点を $\mathrm{P}_k\,(k,\ y_k)$ とすれば，平行 4 辺形 OABC に含まれる格子点は

$$\mathrm{P}_1\,(1,\ y_1),\ \mathrm{P}_2\,(2,\ y_2),\ \cdots,\ \mathrm{P}_{a-1}\,(a-1,\ y_{a-1})$$

であるから，求める個数は $a-1$(個)　　(答)

(2) (1) より，できる 3 角形は

$$\triangle\,\mathrm{OP}_1\mathrm{A},\ \triangle\,\mathrm{OP}_2\mathrm{A},\ \cdots,\ \triangle\,\mathrm{OP}_{a-1}\mathrm{A}$$

であるから，$n = a-1$ である．

$1 \leqq k \leqq a-1$ なる整数 k について，$\mathrm{P}_k\,(k,\ y_k)$，また $\mathrm{A}\,(a,\ b)$ であるから，$\triangle\mathrm{OP}_k\mathrm{A}$ の面積を S_k とすれば

$$S_k = \frac{1}{2}\left|ay_k - bk\right|$$

である．ここで, 点 P_k は不等式 $y > \frac{b}{a}x \iff ay - bx > 0$ をみたすから, $ay_k - bk > 0$ となり，かつ $ay_k - bk$ は整数であることから,

$$ay_k - bk \geqq 1$$

である．この等号が成立するような整数 k が $1 \leqq k \leqq a-1$ に存在するならば,

$$\min S_k = \frac{1}{2}$$

が成り立つ．以下，このような k が存在することを示す．

(1) での考察から，k が定まれば y_k がただ 1 つ定まり，その y_k によって，値 $2S_k = ay_k - bk$ がやはりただ 1 つ定まる．従って，集合 $A = \{1, 2, \cdots, a-1\}$ を定義域とする関数

$f(k) = ay_k - bk$

を考えることができる．

まず，この関数の値域を定める：

$$\frac{b}{a}k < y_k < \frac{b}{a}k + 1 \iff bk < ay_k < bk + a \iff 0 < f(k) = ay_k - bk < a$$

であり，$f(k)$ は整数であるから，次が言える：

$f(k)$ の値域は A の部分集合である：$f(k) \in A = \{1, 2, \cdots, a-1\}$. (#)

次に，関数 $f(k)$ が 1 対 1 の関数であることを示す．関数 $f(k)$ が 1 対 1 であるとは,

$f(i) = f(j) \Rightarrow i = j$

が成り立つことである (**行き先が同じならば出どころも同じ**)．対偶を作ると

$i \fallingdotseq j \Rightarrow f(i) \fallingdotseq f(j)$

となる (**出どころ違えば行き先も違う**).

ここでは前者を使ってみよう．$f(i) = f(j)$ とすると,

$ay_i - bi = ay_j - bj \iff a(y_i - y_j) = b(i - j)$

であるが，a と b は互いに素であるから，$i - j$ は a の倍数である．ところが i, j とも $1 \leqq i \leqq a-1$, $1 \leqq j \leqq a-1$ をみたすから

$-a + 2 \leqq i - j \leqq a - 2$

となり，この範囲の a の倍数は 0 に限る．従って $i = j$ が成り立つ.

よって,

関数 $f(k) = ay_k - bk$ は 1 対 1 の関数である. (†)

(#) と (†) によって，関数 $f(k)$ は

有限集合 A からそれ自身への，1 対 1 の関数である

ことが言えた．つまり,

A の任意の要素 α に対して，$f(k) = \alpha$ となる A の要素 k が存在する.

$\forall \alpha \in A\ \exists k \in A;\ \alpha = f(k)$.

従って，特に $f(k) = 1$ となる k が存在し，その k について

$$S_k = \triangle \mathrm{OP}_k\mathrm{A} = \frac{1}{2}f(k) = \frac{1}{2}$$

となり，このとき考える面積の最小値を得る：

$$\min \triangle \mathrm{OP}_k\mathrm{A} = \frac{1}{2}. \qquad \text{(答)}$$

【4】(1) $\sqrt{5}$ が有理数であるとして

$\sqrt{5} = \dfrac{m}{n}$ (m, n は互いに素な正の整数)

と置く.

分母を払い両辺を 2 乗すると，$5n^2 = m^2$ より，m^2 は 5 の倍数であるが，5 は素数

であるから m が 5 の倍数である．そこで，$m=5m'$ (m'は整数) とおくと

$$5n^2=25m'^2,\quad \therefore\ n^2=5m'^2$$

より，n も 5 の倍数となる．ところがこれは m，n が互いに素であることに反する．

以上より，$\sqrt{5}$ は無理数である．　　　[証明終]

(2) $b=\dfrac{2a+5}{a+2}$ より

$$\sqrt{5}-b=\sqrt{5}-\frac{2a+5}{a+2}=\frac{(2-\sqrt{5})(\sqrt{5}-a)}{a+2}.\ \cdots\cdots ①$$

$2-\sqrt{5}<0$，a は正の有理数であるから

$$(\sqrt{5}-a)(\sqrt{5}-b)=\frac{(2-\sqrt{5})(\sqrt{5}-a)^2}{a+2}<0.$$

よって

$$a<\sqrt{5}<b \text{ または } b<\sqrt{5}<a$$

が成り立ち，$\sqrt{5}$ はつねに a と b の間にある．　　　[証明終]

(3) $2-\sqrt{5}<0$，a は正の有理数であるから，①より

$$\frac{\left|\sqrt{5}-b\right|}{\left|\sqrt{5}-a\right|}=\frac{\sqrt{5}-2}{a+2}.$$

ここで

$$0<\sqrt{5}-2<1,\ a+2>2 \text{ より } \frac{\sqrt{5}-2}{a+2}<1$$

であるから

$$\left|\sqrt{5}-b\right|<\left|\sqrt{5}-a\right|$$

となり，b の方が a より $\sqrt{5}$ に近い．　　　[証明終]

【5】(1) 示すべき命題が成り立つとき，n^7 を 7 で割った余りと，n を 7 で割った余りが等しいから，n^7-n は 7 の倍数である．またこの逆も成り立つ．従って

$$f\left(n^7\right)=f(n)\Longleftrightarrow 7\,\middle|\,n^7-n\Longleftrightarrow n^7\equiv n\pmod 7$$

となるが，次が成り立つことを我々は既に知っている：

任意の素数 p について $n^p\equiv n \pmod p$.

特に $p=7$ とすれば，$n^7\equiv n \pmod 7$ が成り立つから，任意の正整数 n について

$$f\left(n^7\right)=f(n).$$　[証明終]

cf.　「我々は知っている」と書いたが，証明を構成できるかどうかは，定かではない．必ず，もう一度証明しなおしておくこと．

(2) 最も重要なのは，これが $g(n)$ の最大値 $\max g(n)$ を求める問題である，と考えることである．

$f\left(\displaystyle\sum_{k=1}^{7}k^n\right)=G(n)$ とすれば，$g(n)=3G(n)$ であるから，$G(n)$ を最大にする．

また，(1) がどう使われるか，が次に重要である．

本問では，総和記号 $\sum$ は，つねに $k=1$ から $k=7$ に渡る和を表すから，以下 $\sum$

で $\displaystyle\sum_{k=1}^{7}$ を表すことにする．このとき，まず次が成り立つ：

任意の正整数 n について，$G\left(n+6\right)=G\left(n\right)$．

なぜならば，

$\sum k^{n+6}-\sum k^{n}=\sum\left(k^{n+6}-k^{n}\right)=\sum k^{n-1}\left(k^{7}-k\right)$

であり，(1) より任意の正整数 n について $n^{7}-n\equiv 0 \pmod 7$ が成り立つから，k が 1 から 7 まで動くとき

$\sum k^{n+6}-\sum k^{n}\equiv\underbrace{0+0+\cdots+0}_{\text{7terms}}=0 \pmod 7$

である．従って $\sum k^{n+6}$ と $\sum k^{n}$ を 7 で割った余りは等しいから

$G\left(n+6\right)=f\left(\sum k^{n+6}\right)=f\left(\sum k^{n}\right)=G\left(n\right)$

が言えた．n は正整数であるから，これによって n の値を $1\leqq n\leqq 6$ の，ただ 6 通りだけ考えれば十分であることが解る．

以下，$\pmod 7$ を固定する．$4\equiv-3,\ 5\equiv-2,\ 6\equiv-1$ に着目すると，

- n が奇数のとき，

  $\sum k^{n}=1^{n}+2^{n}+\cdots+6^{n}+7^{n}\equiv 1^{n}+2^{n}+3^{n}+(-3)^{n}+(-2)^{n}+(-1)^{n}+0^{n}\equiv 0$

  となるから，$n=1,3,5$ のとき，$G(n)=f\left(\sum k^{n}\right)=0$ である．

- $n=2$ のとき

  $$\begin{aligned}\sum k^{2}&=1^{2}+2^{2}+\cdots+6^{2}+7^{2}\\&\equiv 1^{2}+2^{2}+3^{2}+(-3)^{2}+(-2)^{2}+(-1)^{2}+0^{2}\\&\equiv 2\left(1+4+2\right)+0\equiv 0\end{aligned}$$

  となるから，$n=2$ のとき，$G(2)=f\left(\sum k^{2}\right)=0$ である．

- $n=4$ のとき

  $$\begin{aligned}\sum k^{4}&=1^{4}+2^{4}+\cdots+6^{4}+7^{4}\\&\equiv 1^{4}+2^{4}+3^{4}+(-3)^{4}+(-2)^{4}+(-1)^{4}+0^{4}\\&\equiv 2\left(1+2+4\right)+0\equiv 0\end{aligned}$$

  となるから，$n=4$ のとき，$G(4)=f\left(\sum k^{4}\right)=0$ である．

- $n=6$ のとき

  $$\begin{aligned}\sum k^{6}&=1^{6}+2^{6}+\cdots+6^{6}+7^{6}\\&\equiv 1^{6}+2^{6}+3^{6}+(-3)^{6}+(-2)^{6}+(-1)^{6}+0^{6}\\&\equiv 2\left(1+1+1\right)+0\equiv 6\end{aligned}$$

  となるから，$n=6$ のとき，$G(6)=f\left(\sum k^{6}\right)=6$ である．

以上より，求める最大値は

$\max g(n)=g\left(6\right)=3G\left(6\right)=18.$　　(答)

添削課題

【1】(1) 3 頂点を A, B, C とする.

$\overrightarrow{\mathrm{AB}}=(k,\ l),\ \overrightarrow{\mathrm{AC}}=(m,\ n)$ とおくと, 題意より

$k,\ l,\ m,\ n$: 整数 $\cdots$ ①

$$
\begin{aligned}
(\triangle\,\mathrm{ABC}\ \text{の面積}) &= \frac{1}{2}\cdot\mathrm{AB}\cdot\mathrm{AC}\times\sin\angle\mathrm{BAC}\\
&= \frac{1}{2}|\overrightarrow{\mathrm{AB}}|\cdot|\overrightarrow{\mathrm{AC}}|\sqrt{1-\cos^2\angle\mathrm{BAC}}\\
&= \frac{1}{2}\sqrt{|\overrightarrow{\mathrm{AB}}|^2\cdot|\overrightarrow{\mathrm{AC}}|^2-(\overrightarrow{\mathrm{AB}}\cdot\overrightarrow{\mathrm{AC}})^2}\\
&= \frac{1}{2}\sqrt{(kn-lm)^2}\ =\ \frac{1}{2}|kn-lm|
\end{aligned}
$$

①より, $kn-lm$: 整数 だから

$2\times(\triangle\,\mathrm{ABC}$ の面積$)$: 整数　　[証明終]

(2) 3 頂点 A, B, C の座標がすべて整数の組の正三角形が存在すると仮定する.

$\overrightarrow{\mathrm{AB}}=(k,\ l),\ \overrightarrow{\mathrm{AC}}=(m,\ n)$ とおくと

$k,\ l,\ m,\ n$: 整数 $\cdots$ ②

$2\times(\triangle\,\mathrm{ABC}$ の面積$)=|kn-lm|$: 整数 $\cdots$ ③

したがって

$|\overrightarrow{\mathrm{AB}}|=|\overrightarrow{\mathrm{AC}}|=\sqrt{k^2+l^2}$　　$\because$ 正三角形

$$
\begin{aligned}
2\times(\triangle\,\mathrm{ABC}\ \text{の面積}) &= \mathrm{AB}\cdot\mathrm{AC}\sin 60^\circ\\
&= \frac{\sqrt{3}}{2}(k^2+l^2)\quad\cdots④
\end{aligned}
$$

③, ④より

$\sqrt{3}(k^2+l^2)=2|kn-lm|$

$\sqrt{3}=2\dfrac{|kn-lm|}{k^2+l^2}\quad\cdots$ ⑤

②より, ⑤の右辺は有理数で, 左辺は無理数となり, 不合理.

よって, 3 頂点の座標がすべて整数の組の正三角形は存在しない.　　[証明終]

１６章　代数（３）

問題

【1】整数 a, b について $a \neq 0$ のとき，

- $a \mid b$ で「a は b を割り切る」，「b は a の倍数である」ことを，
- $a \nmid b$ でその否定，「b は a の非倍数である」ことを表す．

(1) 示すべきことは，整数 α について

$$f(\alpha) = 0 \Rightarrow p \mid \alpha$$

である．

$f(x) = 0$ が整数解 α をもつので

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

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

a_k $(k = 0, 1, \cdots, n-1)$，p が整数であることから

(#) の右辺は p の倍数

が成り立つ．よって左辺 α^n も p の倍数であることになり，かつ p は素数であるから，

α は p の倍数

が言えた．　　　［証明終］

(2) 示すべきことは

$$p \nmid a_0 \Rightarrow f(x) = 0 \text{ は整数解をもたない}$$

である．

証明は背理法による．つまり，$p \nmid a_0$ であり，かつ方程式 $f(x) = 0$ が整数解 α をもつとして，矛盾を導く．

$f(x) = 0$ が整数解 α をもつと仮定する．(1) の結果より, その解は k をある整数として $\alpha = kp$ と置ける．これを $f(\alpha) = 0$ に代入して

$$f(kp) = k^n p^n + pa_{n-1}k^{n-1}p^{n-1} + \cdots + pa_1 kp + pa_0 = 0.$$

p で両辺を割って，a_0 について解けば

$$\begin{aligned} a_0 &= -(k^n p^{n-1} + a_{n-1}k^{n-1}p^{n-1} + \cdots + a_1 kp) \\ &= -p(k^n p^{n-2} + a_{n-1}k^{n-1}p^{n-2} + \cdots + a_1 k) \quad \cdots(\dagger) \end{aligned}$$

($\dagger$) の右辺は p の倍数 ($\because$ $n-2 \geqq 0$ より) となり, a_0 は p の倍数となる．

これは仮定 $p \nmid a_0$ に矛盾する．

従って $f(x) = 0$ は整数解をもたないことが示された．　　　［証明終］

【2】条件の不等式が成り立つためには明らかに

$$1-a>0,\ 1-d>0$$

が必要である．よって, 条件は

$$\begin{cases} t<\dfrac{1-a}{b}s, \\ t>\dfrac{c}{1-d}s \end{cases}$$

である．

st 平面で 2 直線

$$t=\frac{1-a}{b}s,\ t=\frac{c}{1-d}s$$

を考える．上の不等式をみたす $(s,\ t)$ が第 1 象限に存在するためには, 2 直線の傾きの大小を比較して

$$\frac{1-a}{b}>\frac{c}{1-d}$$

でなければならない．つまり

$$(1-a)(1-d)-bc>0.$$

ここで, $f(x)=x^2-(a+d)x+(ad-bc)$ とおく．題意は

$$D>0,\ f(-1)>0,\ f(1)>0,\ -1<\text{軸}<1$$

と同値である．ところが

$$\begin{cases} D=(a+d)^2-4(ad-bc)=(a-d)^2+4bc>0, \\ f(1)=1-(a+d)+(ad-bc)=(1-a)(1-d)-bc>0, \\ f(-1)>f(1)>0, \\ 1>\dfrac{a+d}{2}>0 \quad (\because (1-a)+(1-d)>0) \end{cases}$$

なので, これらはすべてみたされている．

よって, 題意が示された．　　　［証明終］

【3】以下，整式 $f(x)$ の次数を $\deg f$ で表す．また，2 つの整式 $p(x), q(x)$ についても，$p(x)$ が $q(x)$ を割り切ることを $p(x) \mid q(x)$ で表す．

(1) $f(x)$ の次数を n とする：$\deg f = n$．このとき $f(x)$ は

$$f(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

と置けて，$a_0 \fallingdotseq 0$ である．x を $1-x$ に変えて

$$f(1-x) = a_0(1-x)^n + a_1(1-x)^{n-1} + \cdots + a_{n-1}(1-x) + a_n$$

となる．題意より，$f(x) = f(1-x)$ は恒等式であるから，最高次の項，つまり n 次の項，の係数について

$$a_0 = a_0(-1)^n \quad \therefore\ 1 = (-1)^n$$

が成り立ち，確かに n は偶数である．　　　[証明終]

(2) 条件式 $f(x) = f(1-x)$ が x についての恒等式であることから，特に $x=1$ のときも成り立つ．よって

$$f(1) = f(0). \qquad \cdots ①$$

いま，$h(x) = f(x) - f(0)$ と定めれば

- $h(1) = f(1) - f(0) = 0 \quad (\because ①)$ より，因数定理から $h(x)$ は $x-1$ を因数にもつ．
- $h(0) = f(0) - f(0) = 0$ より，同様に $h(x)$ は x を因数にもつ．

従って，

$$x-1 \mid h(x),\ x \mid h(x)$$

であり，かつ $x-1$ と x は互いに素であるから，$h(x)$ は $x(x-1)$ で割り切れる．

以上より，$h(x) = f(x) - f(0)$ について，ある整式 $g(x)$ が存在して

$$f(x) - f(0) = x(x-1)g(x)$$

が成り立つことが示された．　　　[証明終]

(3) $h(x) = f(x) - f(0)$ について，$h(1-x)$ を計算してみると，$f(1-x) = f(x)$ を用いて

$$h(1-x) = f(1-x) - f(0) = f(x) - f(0) = h(x) \qquad \cdots ②$$

が成り立つ．ここで (2) より $h(x) = x(x-1)g(x)$ と表されたから，x を $1-x$ に変えると

$$h(1-x) = (1-x)(-x)g(1-x) = x(x-1)g(1-x) \quad \cdots ③$$

である．②と③とから，恒等式として

$$x(x-1)g(x) = x(x-1)g(1-x) \quad \therefore g(x) = g(1-x) \quad \cdots ④$$

が成り立つ．

もし $g(x)$ が定数で，その値が k であれば，(2) の結果より

$$f(x) = x(x-1)k + f(0)$$

となり，$f(0)$ は定数であるから，確かにこのとき $f(x)$ は $x(x-1)$ の 1 次式で表される．

$g(x)$ が定数でないとする．このとき，④は $g(x)$ が題意の $f(x)$ と同じ性質をもつことを意味するから，(1) で示したように $g(x)$ は 2 次以上の偶数次の整式である．

このとき (2) より，ある整式 $g_1(x)$ が存在して

$$g(x) - g(0) = x(x-1)g_1(x)$$

が成り立つ．この左辺を $h_1(x)$ とすると，②と同様に $h_1(x)=h_1(1-x)$ が成り立ち，更に③の $g(x)$ を $g_1(x)$ に，$h(x)$ を $h_1(x)$ に変えた式が成り立つから，④と同様の

$$g_1(x)=g_1(1-x)$$

が恒等式として成立する．

$g_1(x)$ が定数か定数でないかで場合を分けて，この手順を繰り返せば，この手順は $\dfrac{\deg f}{2}=\dfrac{n}{2}$ 回繰り返すことが出来て，そこで停止する．このとき得られた式は，$x(x-1)$ についての $\dfrac{n}{2}$ 次式となるから，題意が証明された．［証明終］

【4】(1) 条件として与えられた 2 式の辺々を加えた

$$f(p)+f(q)=q+p \Longleftrightarrow f(p)+f(q)-(p+q)=0$$

の左辺は，p と q の対称式であるから，基本対称式 $p+q$, pq で表すことが出来る．

実際

$$ap(1-p)+aq(1-q)=q+p \Longleftrightarrow a(p+q)-a\left(p^2+q^2\right)=p+q. \quad \cdots ①$$

また，辺々を引いて出来る式

$$f(p)-f(q)=q-p \Longleftrightarrow f(p)-f(q)+(p-q)=0$$

の左辺は，p と q の交換によって，符号だけを変える (このような式を『交代式』と言う)．

実際

$$ap(1-p)-aq(1-q)+(p-q)=0 \Longleftrightarrow a(p-q)-a(p+q)(p-q)+(p-q)=0.$$

この式で，題意より $p \fallingdotseq q$ であるから，両辺を $p-q(\fallingdotseq 0)$ で割って

$$a-a(p+q)+1=0 \qquad \therefore\ a(p+q)=a+1.$$

これを①に代入する．$p^2+q^2=(p+q)^2-2pq$ を用いて

$$a+1-a\left\{\left(\frac{a+1}{a}\right)^2-2pq\right\}=\frac{a+1}{a}$$

$$\Longleftrightarrow 2apq=1+\frac{1}{a}-(a+1)+a\left(1+\frac{1}{a}\right)^2=2+\frac{2}{a},$$

$$\therefore pq=\frac{1}{a}\left(1+\frac{1}{a}\right).$$

以上より，p と q は

$$p+q=1+\frac{1}{a} \qquad pq=\frac{1}{a}\left(1+\frac{1}{a}\right)$$

をみたすから，t に関する 2 次方程式

$$t^2-\left(1+\frac{1}{a}\right)t+\frac{1}{a}\left(1+\frac{1}{a}\right)=0$$

の 2 解である．p と q が異なる実数であるから，この 2 次方程式の判別式を D として，$D>0$ になる．

$$D=\left(1+\frac{1}{a}\right)^2-4\cdot\frac{1}{a}\left(1+\frac{1}{a}\right)>0$$

$$\Longleftrightarrow \left(1+\frac{1}{a}\right)\left\{\left(1+\frac{1}{a}\right)-\frac{4}{a}\right\}>0$$

$$\Longleftrightarrow \left(1+\frac{1}{a}\right)\left(1-\frac{3}{a}\right)>0.$$

両辺に $a^2(>0)$ をかけて

$$(a+1)(a-3)>0 \qquad \therefore a<-1,\ 3<a. \qquad (答)$$

(2) $f(x)=ax(1-x)$ について $f(x)-x=g(x)$ と置くと，

$$f(x)=g(x)+x$$

であるから，

$$\begin{aligned} f_2(x)-x &= f(f(x))-x \\ &= f(g(x)+x)-x \\ &= a\{x+g(x)\}\{-g(x)-x+1\}-x \end{aligned}$$

$$
\begin{aligned}
&= ag(x)\{-g(x)-2x+1\}+ax(1-x)-x\\
&= g(x)[-a\{g(x)+2x-1\}+1]\\
&\qquad (\because\ ax(1-x)-x=f(x)-x)\\
&= g(x)[-a\{f(x)+x-1\}+1].
\end{aligned}
$$

従って，$f_2(x)-x=f(f(x))-x$ は $g(x)$ つまり $f(x)-x$ で割り切れる：

$f(x)-x \,\big|\, f(f(x))-x.$ 　　［証明終］

(3) $f(x)-x$ を 0 として，方程式 $f(x)-x=0$ を考える．

$f(x)-x=0 \iff ax(1-x)-x=0 \quad \therefore \quad x=0,\ 1-\dfrac{1}{a}.$

この方程式が (i) 重解をもたない場合，(ii) 重解をもつ場合，で場合を分ける．

(i) $f(x)-x=0$ が重解をもたない場合，すなわち，$a\fallingdotseq 1$ の場合．

$f(x)-x=0$ の解を $0=\alpha,\ 1-\dfrac{1}{a}=\beta$ と表すと，

$f(\alpha)-\alpha=0,\quad f(\beta)-\beta=0 \quad \therefore \quad f(\alpha)=\alpha,\ f(\beta)=\beta \qquad (\#)$

が成り立つ．

定義より

$f_2(x)-x=f(f(x))-x$

であるから，(#) により

$f(f(\alpha))-\alpha=f(\alpha)-\alpha=0,\quad f(f(\beta))-\beta=f(\beta)-\beta=0.$

また，同様に (#) を繰り返し用いれば

$f_3(\alpha)-\alpha=f(f(f(\alpha)))-\alpha=f(f(\alpha))-\alpha=f(\alpha)-\alpha=0$

となる．$f_3(\beta)-\beta=0$ も同様に示される．

これをくり返すと，

$f_n(\alpha)-\alpha=0,\ f_n(\beta)-\beta=0$

が成り立つ．よって，$f_n(x)-x$ は $x-\alpha=x$ 及び $x-\beta=x-\left(1-\dfrac{1}{a}\right)$ で割り切れる．

これら 2 つの式は互いに素であるから，$f_n(x)-x$ はこの積

$(x-\alpha)(x-\beta)=x\left\{x-\left(1-\dfrac{1}{a}\right)\right\}=\dfrac{1}{a}x(ax-a+1)$

で割り切れる．ここで

$f(x)-x=ax(1-x)-x=-x(ax-a+1)$

であるから，$f(x)-x=-a(x-\alpha)(x-\beta)$ である．

よって確かに任意の正整数 n について，$f_n(x)-x$ は $f(x)-x$ で割り切れる：

$f(x)-x \,\big|\, f_n(x)-x.$

(ii) $f(x)-x=0$ が重解をもつ場合，すなわち $a=1$ の場合を考える．$f(x)-x=0$ が重解をもつとき，それは 0 である．

題意が成り立つには，$f_n(x)-x$ が x で 2 回割れることが必要かつ十分である．

そこで x^2 を因数にもつことを示す．

まず，$f_n(0)-0$ が 0 である，すなわち $f_n(x)-x$ が x を因数にもつことを示す．

$f(0)=0$ だから，

$$f_2(0)=f(f(0))=f(0)=0,$$
$$f_3(0)=f(f(f(0)))=f(f(0))=f(0)=0,$$
$$\vdots$$
$$f_n(0)=0$$

である．よって，$f_n(x)-x$ は x を因数にもつので，

$$f_n(x)-x=x\left(\frac{f_n(x)}{x}-1\right)$$

と変形できる．従って，題意の成立には

$$\frac{f_n(x)}{x}-1$$

が x でもう一度割れること，つまり x を因数にもつこと，が必要かつ十分である．

これを示すために，

$f_n(x)$ の最低次の項が $+x$ であること $\cdots\cdots(\dagger)$

を示す．

- $n=1$ のとき $f_1(x)=x-x^2$ より成り立つ．
- $n=k$ のとき，$f_k(x)$ の最低次の項が $+x$ であると仮定すると，$g(x)$ を最低次の項が 2 次以上の整式として

  $$f_k(x)=g(x)+x$$

  と表せる．

  $n=k+1$ のとき，

  $$\begin{aligned} f_{k+1}(x) &= f(f_k(x)) \\ &= f(g(x)+x) \\ &= \{g(x)+x\}\{1-g(x)-x\} \\ &= h(x)+x \qquad (h(x)\text{ は最低次が 2 次以上の整式}) \end{aligned}$$

  と表すことができ，このときも成り立つ．

従って，すべての自然数 n に対して $(\dagger)$ が成り立つことが示された．

以上より，題意は示された．　　　［証明終］

添削課題

【1】$F(x)=\{f(x)\}^3-\{g(x)\}^3$, $G(x)=f(x)-g(x)$ とおくと

$$F(x)=G(x)[\{f(x)\}^2+f(x)g(x)+\{g(x)\}^2]$$

$F(x)$ は $(x-a)^2$ で割り切れるから，$G(x)$ が $(x-a)^2$ で割り切れないとすると，$\{f(x)\}^2+f(x)g(x)+\{g(x)\}^2$ $(=H(x)$ とおく$)$ が $(x-a)^2$ で割り切れることになる．このとき，因数定理により $H(a)=0$ であるから

$$\left\{f(a)+\frac{1}{2}g(a)\right\}^2+\frac{3}{4}\{g(a)\}^2=0 \qquad \cdots\cdots ①$$

ここで，$f(x)$, $g(x)$ はともに実数を係数とし，a も実数であるから，$f(a)$, $g(a)$ も実数である．よって，①が成り立つのは

$$f(a)+\frac{1}{2}g(a)=0 \text{ かつ } g(a)=0$$

すなわち

$$f(a)=g(a)=0$$

のときに限る．このとき，因数定理により $f(x)$, $g(x)$ はともに $x-a$ で割りきれるから，$\{f(x)\}^3$, $\{g(x)\}^3$ がともに $(x-a)^3$ で割り切れ

$F(x)$ が $(x-a)^3$で割り切れる

ことになるが，これは $F(x)$ が $(x-a)^3$ では割り切れないという仮定に反する．よって，$G(x)=f(x)-g(x)$ は $(x-a)^2$ で割り切れる．　　　［証明終］

M3JSB/M3JB/M3TB
選抜東大クラス文系数学
東大文系数学
難関大文系数学 T

Z-KAI

会員番号		氏　名	