数学コンクール3月号　解答

$i^2=-1$ より $\mathbb{Z}[i]$ は積について閉じている．$\left(\text{つまり}, z_1, z_2\in\mathbb{Z}[i]\text{ ならば } z_1z_2\in\mathbb{Z}[i]\right)$
係数がすべて $\mathbb{Z}[i]$ に属する多項式 $P(x)$ と2以上の整数 n が

$$P^k(a+bi)\neq 0\ \ (k=1, 2, \cdots\cdots, n-1)\text{ かつ } P^n(a+bi)=0$$

を満たしたとする．

$\alpha_0=a+bi,\ \alpha_k=P^k(a+bi)\ \ (k=1, 2, \cdots\cdots, n)$ とおくと，$\alpha_k\in\mathbb{Z}[i],\ \alpha_n=0$
である．

補題1　$\alpha_0, \alpha_1, \cdots\cdots, \alpha_n$ は相異なる．

証明　仮定より，$\alpha_k\neq 0=\alpha_n\ \ (k=1, 2, \cdots\cdots, n-1)$ である．
　次に，$0\leqq k<l\leqq n-1$ に対し，$\alpha_k=\alpha_l$ であるとすると，

$$\alpha_{k+n-l}=P^{n-l}(\alpha_k)=P^{n-l}(\alpha_l)=\alpha_n=0,\ 0<k+n-l<n$$

　より，矛盾である．（補題1の証明終）

補題2　$\alpha, \beta\in\mathbb{Z}[i]$ が相異なるとき，正の整数 m に対し

$$\frac{P^m(\alpha)-P^m(\beta)}{\alpha-\beta}\in\mathbb{Z}[i]\ \text{ である．}$$

証明　$P^m(x)$ の係数もすべて $\mathbb{Z}[i]$ に属する．したがって，j が正の整数のとき

$$\frac{\alpha^j-\beta^j}{\alpha-\beta}=\alpha^{j-1}+\alpha^{j-2}\beta+\cdots\cdots+\alpha\beta^{j-2}+\beta^{j-1}$$

　であることと，$\mathbb{Z}[i]$ が和と積について閉じていることから従う．（補題2の証明終）

$|\alpha_0|, |\alpha_1|, \cdots\cdots, |\alpha_n|$ のうち最大のものが $d=|\alpha_{n_0}|$ であると仮定する．
$d\leqq(4+2\sqrt{2})|\alpha_0|$ を示したい．
これは $n_0=0, n$ のときは明らかであるから，$1\leqq n_0\leqq n-1$ とする．
以下，$\mathbb{Z}[i]$ から要素0を除いた集合を $\mathbb{Z}[i]^*$ とかく．

補題1, 2より $\dfrac{\alpha_n-\alpha_{n-n_0}}{\alpha_{n_0}-\alpha_0},\ \dfrac{\alpha_n-\alpha_{n_0}}{\alpha_{n-n_0}-\alpha_0}\in\mathbb{Z}[i]^*$　である．

（i）$\left|\dfrac{\alpha_n-\alpha_{n-n_0}}{\alpha_{n_0}-\alpha_0}\right|\geqq\sqrt{2}$ のとき，$|\alpha_{n-n_0}|\geqq\sqrt{2}\,|\alpha_{n_0}-\alpha_0|$　である．

　よって，$d\geqq|\alpha_{n-n_0}|\geqq\sqrt{2}\,|\alpha_{n_0}-\alpha_0|\geqq\sqrt{2}\,(d-|\alpha_0|)$

　より，$d\leqq(2+\sqrt{2})|\alpha_0|$　である．

(ii) $\left|\dfrac{\alpha_n-\alpha_{n_0}}{\alpha_{n-n_0}-\alpha_0}\right| \geqq \sqrt{2}$ のとき, $|\alpha_{n_0}| \geqq \sqrt{2}\,|\alpha_{n-n_0}-\alpha_0|$ である.

一方, $|\alpha_{n-n_0}| \geqq |\alpha_{n_0}-\alpha_0| \geqq d-|\alpha_0|$ である.

よって, $d=|\alpha_{n_0}| \geqq \sqrt{2}\,|\alpha_{n-n_0}-\alpha_0| \geqq \sqrt{2}\,(|\alpha_{n-n_0}|-|\alpha_0|) \geqq \sqrt{2}\,(d-2|\alpha_0|)$

より, $d \leqq (4+2\sqrt{2})|\alpha_0|$ である.

(iii) (i), (ii) 以外のとき

$\alpha_n=0$ であるから $\begin{cases}\alpha_{n_0}-\alpha_0=z\alpha_{n-n_0}\\ \alpha_{n-n_0}-\alpha_0=w\alpha_{n_0}\end{cases}$ $(z, w=\pm 1,\ \pm i)$ とおける.

α_{n-n_0} を消去すると, $(1-zw)\alpha_{n_0}=(1+z)\alpha_0$ となる.

(あ) $1-zw \neq 0$ のとき, $\alpha_{n_0}=\dfrac{1+z}{1-zw}\alpha_0$ となる.

(z, w) は有限通りであり, $d=|\alpha_{n_0}|=|\alpha_0|,\ \sqrt{2}\,|\alpha_0|,\ 0,\ \dfrac{|\alpha_0|}{\sqrt{2}}$ と分かる.

矛盾するものもあるが, 少なくとも $d \leqq \sqrt{2}\,|\alpha_0|$ である.

(い) $1-zw=0$ のとき, $\alpha_0 \neq 0$ より, $1+z=0$ となる.

つまり $z=w=-1$ であり, $\alpha_{n_0}+\alpha_{n-n_0}=\alpha_0$ となる.

ここで, $t=|n-2n_0|$ とおく.

$t=0$ とすると, $n_0=n-n_0$ より, $\alpha_{n_0}=\alpha_{n-n_0}=\dfrac{\alpha_0}{2}$ となるから,

$d=\dfrac{|\alpha_0|}{2}$ である.

$t>0$ とすると, 補題 1, 2 より, $\dfrac{\alpha_n-\alpha_{n-t}}{\alpha_{n-n_0}-\alpha_{n_0}} \in \mathbb{Z}[i]^*$ が従う.

(厳密には, $n-2n_0$ の符号の場合分けを行う)

よって, $d \geqq |\alpha_{n-t}| \geqq |\alpha_{n-n_0}-\alpha_{n_0}|=|\alpha_0-2\alpha_{n_0}| \geqq 2d-|\alpha_0|$

より, $d \leqq |\alpha_0|$ である.

以上より, $k=0, 1, \cdots\cdots, n$ に対し $|\alpha_k| \leqq (4+2\sqrt{2})|\alpha_0|$ が成り立つので, 複素数平面上で中心 0, 半径 $(4+2\sqrt{2})|\alpha_0|$ の円の内部または周上にある $\mathbb{Z}[i]$ の要素の個数を M とおくと, $n+1 \leqq M$ である. よって, $N=M-1$ ととれば題意が成り立つ.