ミレニアム大学入試の背景を探る (3)

宮川　幸隆

§1. 単位加法半群ℕの部分半群

ℤを有理整数環とする．n を正整数とし，
$a_1,\ a_2,\ \cdots\cdots,\ a_n,\ c\in\mathbb{Z}$ とするとき，

$c|a_1$ かつ $c|a_2$ かつ …… かつ $c|a_n$
$\iff a_1\in(c)$ かつ $a_2\in(c)$ かつ … かつ $a_n\in(c)$
$\iff (a_1,\ a_2,\ \cdots\cdots,\ a_n)\subseteqq(c)$

であるから，$(a_1,\ a_2,\ \cdots\cdots,\ a_n)=d$ とすると，(d) は $(a_1,\ a_2,\ \cdots\cdots,\ a_n)\subseteqq(d)$ なる最小の**単項イデアル**であり，ℤは**単項イデアル整域**であるから，

$$(a_1,\ a_2,\ \cdots\cdots,\ a_n)=(d)$$

である．ただし，ここに $(a_1,\ a_2,\ \cdots\cdots,\ a_n)$ は，$\boldsymbol{a_1,\ a_2,\ \cdots\cdots,\ a_n}$ **から生ずる (ℤの) イデアル**および $a_1,\ a_2,\ \cdots\cdots,\ a_n$ の **G.C.D.** (最大公約数) $d(>0)$ を表す．以上の考察によって，次の定理が成り立つ：

定理 1　$a_1,\ a_2,\ \cdots\cdots,\ a_n,\ k\in\mathbb{Z}$,
$(a_1,\ a_2,\ \cdots\cdots,\ a_n)=d$　のとき，
$\exists x_1,\ \exists x_2,\ \cdots\cdots,\ \exists x_n\in\mathbb{Z}$：
s.t. $k=x_1a_1+x_2a_2+\cdots\cdots+x_na_n$
$\iff d|k$

イデアル

$$(a_1,\ \cdots\cdots,\ a_n)$$
$$=\{x_1a_1+\cdots\cdots+x_na_n|x_1,\ \cdots\cdots,\ x_n\in\mathbb{Z}\}$$

は**加法群ℤの部分群**であるが，ℕを非負整数全体の集合，$a_1,\ \cdots\cdots,\ a_n\in\mathbb{N}$ とするとき，

$$\langle a_1,\ \cdots\cdots,\ a_n\rangle$$
$$=\{x_1a_1+\cdots\cdots+x_na_n|x_1,\ \cdots\cdots,\ x_n\in\mathbb{N}\}$$

は**単位加法半群ℕの部分半群**である．何となれば，

$x,\ y\in\langle a_1,\ \cdots\cdots,\ a_n\rangle$,
$x=x_1a_1+\cdots\cdots+x_na_n$；　$x_1,\ \cdots\cdots,\ x_n\in\mathbb{N}$
$y=y_1a_1+\cdots\cdots+y_na_n$；　$y_1,\ \cdots\cdots,\ y_n\in\mathbb{N}$

とするとき，

$$x+y=(x_1+y_1)a_1+\cdots\cdots+(x_n+y_n)a_n$$
$$\in\langle a_1,\ \cdots\cdots,\ a_n\rangle,$$
$$0=0\cdot a_1+\cdots\cdots+0\cdot a_n\in\langle a_1,\ \cdots\cdots,\ a_n\rangle$$

であるからである．

定理 1 によれば，

$$x_1a_1+\cdots\cdots+x_na_n\ (x_1,\ \cdots\cdots,\ x_n\in\mathbb{Z})$$

の形に表される整数は $a_1,\ \cdots\cdots,\ a_n$ の G.C.D の倍数に他ならないが，$a,\ b\in\mathbb{N}-\{0\}$, $(a,\ b)=1$ とするとき，

$$ma+nb\ (m,\ n\in\mathbb{N})$$

の形に表される非負整数について次の定理が成り立つ：

定理 2　$a,\ b\in\mathbb{N}-\{0\}$, $(a,\ b)=1$ とするとき，
$$ma+nb\ (m,\ n\in\mathbb{N})$$
の形で，$(a-1)(b-1)$ 以上の整数はすべて表せて，更に，$0,\ 1,\ 2,\ \cdots\cdots,\ (a-1)(b-1)-1$ のうち丁度半分だけが $\langle a,\ b\rangle$ の要素となる．

証明　$k\in\mathbb{Z}$ のとき，

$$k\notin\langle a,\ b\rangle \Longrightarrow (a-1)(b-1)-1-k\in\langle a,\ b\rangle$$

を示そう：実際，$(a,\ b)=1$ であるから，定理 1 により $x,\ y$ の一次不定方程式

$$ax+by=k \qquad ①$$

は整数解をもつ．その一組を解を $(x,\ y)=(x_0,\ y_0)$ とすれば，一般解は $(x,\ y)=(x_0+bt,\ y_0-at)$ である．さて，

$$k=xa+yb\quad(x,\ y\in\mathbb{Z})$$

とするとき，$k\notin\langle a,\ b\rangle$ から，

$$x<0 \text{ or } y<0$$

である．

I）$x<0$ のとき，
上の考察から，$x=x_0+bt\ (t\in\mathbb{Z})$ の形に表されているが，$x_0+bt<0$ を満たす最大の t を t_0 とし，$x_1=x_0+bt_0$, $y_1=y_0-at_0$ とおく．
いま，$-b\leqq x_1<0$ である．何となれば，もし，$x_1<-b$ であるとすれば，$x_1+b<0$ となって t_0 の最大性に反するからである．このとき，

$$(a-1)(b-1)-1-k$$
$$=ab-a-b-ax_1-by_1$$
$$=(-x_1-1)a+(a-1-y_1)b$$

で，$-x_1-1\geqq 0$ である．さて，$a-1-y_1\geqq 0$ ならば，$(a-1)(b-1)-1-k\in\langle a,\ b\rangle$ であるから，$a-1-y_1<0$，すなわち，

$$y_1\geqq a$$

と仮定する．このとき，y_1 を a で割ったときの商を q，余りを r とすると，

$$y_1=aq+r,\ q\geqq 1,\ 0\leqq r<a$$

であるから，

$$k=x_1a+y_1b=x_1a+(aq+r)b$$
$$=(x_1+qb)a+rb$$

となって，$x_1+qb\geqq x_1+b\geqq 0$，$r\geqq 0$ とから

$$k\in\langle a,\ b\rangle$$

となり，$k\notin\langle a,\ b\rangle$ に反する．

II） $y<0$ のとき，

①の一般解は $(x,\ y)=(x_0-bt,\ y_0+at)$ とも表せるから，Ｉ）の場合と同様にして

$$(a-1)(b-1)-1-k\in\langle a,\ b\rangle$$

を示せる．

負の整数 k は明らかに $k\notin\langle a,\ b\rangle$ を満たすから，定理の前半は成り立つ．次に，$k\in\mathbb{Z}$ のとき，

$$k\in\langle a,\ b\rangle \Longrightarrow (a-1)(b-1)-1-k\notin\langle a,\ b\rangle$$

を示そう：実際，

$$(a-1)(b-1)-1-k\in\langle a,\ b\rangle$$

ならば，$\langle a,\ b\rangle$ が半群であることから，

$$(b-1)a-b\in\langle a,\ b\rangle$$

とならねばならないが，x，y の一次不定方程式

$$ax+by=(b-1)a-b$$

の一般解は $(x,\ y)=(b-1+bt,\ -1-at)$ であり，

$$b-1+bt\geqq 0 \Longrightarrow t\geqq\frac{1-b}{b}=\frac{1}{b}-1$$
$$\Longrightarrow t\geqq 0\ [\because\ \ b\geqq 1,\ t\in\mathbb{Z}]$$
$$\Longrightarrow -1-at\leqq -1\ [\because\ \ a>0]<0,$$
$$-1-at\geqq 0 \Longrightarrow t\leqq -\frac{1}{a}$$
$$\Longrightarrow t\leqq -1\ \ [\because\ \ a\geqq 1,\ t\in\mathbb{Z}]$$
$$\Longrightarrow b-1+bt\leqq -1\ [\because\ \ b>0]<0$$

となるから矛盾が生ずる．

以上で，定理の後半も示された．

§2. 大阪大学・前期・理系のミレニアム入試問題

2000年の大学入試問題に，§1の「単位加法半群$\mathbb{N}$の部分半群」の内容を背景に持つ，大阪大学・前期・理系の入試問題が現れました．その問題とは次のようなものです：

> どのような負でない２つの整数 m と n をもちいても
>
> $$x=3m+5n$$
>
> とは表すことができない正の整数 x をすべて求めよ．

解説 3，$5\in\mathbb{N}-\{0\}$，$(3,\ 5)=1$ であるから，定理２によって，$(3-1)(5-1)=8$ 以上の整数はすべて

$$3m+5n\ (m,\ n\in\mathbb{N}) \qquad ②$$

の形に表せます．更に，0，1，2，……，7 のうち丁度半分の４個だけが②の形に表せるのですが，それらは 0，3，5，6 であることが明らかですので，求めるべきすべての正整数 x は

1，2，4，7

となるのです．

(静岡県立三島北高等学校)

ミレニアム大学入試の背景を探る (4)

宮川　幸隆

本稿では，2000年の京都大学・後期・文系の入試問題の背景を探ります．その問題とは次のようなものです：

> 複素数 α は $|\alpha|=1$ を満たしている．このとき，$|\alpha^m+\alpha^{-m}|>1$ となる自然数 m が存在することを示せ．

解説　$|\alpha|=1$ から，

$$\alpha=\cos\theta+i\sin\theta$$

とおけて，

$$\alpha^m=\cos m\theta+i\sin m\theta,$$
$$\alpha^{-m}=\cos m\theta-i\sin m\theta$$

から，

$$|\alpha^m+\alpha^{-m}|=2|\cos m\theta|$$

$\cos m\theta$ は $\cos\theta$ の m 次の多項式として表せて

$$\cos m\theta=T_m(\cos\theta)$$

とすると，多項式 T_m は**チェビシェフの多項式**と呼ばれます．

$$\cos 1\theta=\cos\theta=T_1(\cos\theta)$$

から

$$T_1(x)=x$$

ですが，cos の 2 倍角の公式から

$$\cos 2\theta=2\cos^2\theta-1=T_2(\cos\theta)$$

ですから，

$$T_2(x)=2x^2-1$$

です．cos の加法定理から，

$$\cos(m+1)\theta=\cos m\theta\cos\theta-\sin m\theta\sin\theta,$$
$$\cos(m-1)\theta=\cos m\theta\cos\theta+\sin m\theta\sin\theta$$

なので，これらを辺々加えて

$$\cos(m+1)\theta+\cos(m-1)\theta=2\cos m\theta\cos\theta$$
$$\therefore\quad \cos(m+1)\theta=2T_m(\cos\theta)\cos\theta-T_{m-1}(\cos\theta)$$

となり，$\cos m\theta$ が $\cos\theta$ の m 次の多項式として表せて，チェビシェフの多項式は，漸化式

$$T_{m+1}(x)=2xT_m(x)-T_{m-1}(x)\quad(m=2,\ 3,\ \cdots\cdots)$$

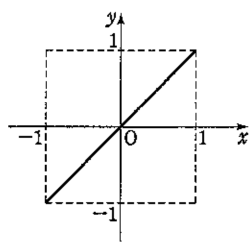
と初期条件 $T_1(x)=x$，$T_2(x)=2x^2-1$ によって定義されることが帰納法によって示されました．

$$T_3(x)=2xT_2(x)-T_1(x)$$
$$=2x(2x^2-1)-x=4x^3-3x$$

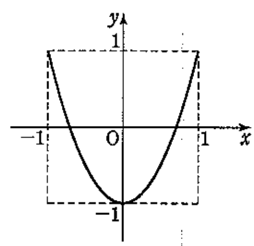
から，cos の 3 倍角の公式が導かれます．4 倍角，5 倍角，6 倍角，…… の公式も同様に導けます．

さて，$y=T_1(x)$，$y=T_2(x)$，$y=T_3(x)$ のグラフは下のようになり，

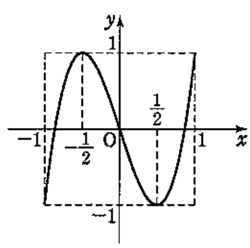
$T_1(x)=x$



$T_2(x)=2x^2-1$



$T_3(x)=4x^3-3x$



$$-1\leqq x<-\frac{1}{2},\ \frac{1}{2}<x\leqq 1\ \text{のとき}\quad |T_1(x)|>\frac{1}{2},$$

$$-\frac{1}{2}<x<\frac{1}{2}\ \text{のとき}\quad |T_2(x)|>\frac{1}{2},$$

$$x=\pm\frac{1}{2}\ \text{のとき}\quad |T_3(x)|=1>\frac{1}{2}$$

ですから，$|\alpha^m+\alpha^{-m}|>1$ となる自然数 m が，

$$1\leqq m\leqq 3$$

の範囲に存在することがわかります．

（静岡県立三島北高等学校）