担当教員: 柳田 伸太郎　研究室: A441　E-mail:yanagida@math.nagoya-u.ac.jp

解答 (整数と多項式の互除法)

作成日: 10/26/2016 更新日: 11/01/2016 Version: 0.2

問題 1. a/b を超えない最大の整数を q とすると $q \le a/b < q+1$. 従って $r := a - qb$ とおくと $0 \le r < b$. また $a = qb + r = q'b + r'$, $0 \le r, r' < b$ だとすると $|q - q'|b = |r - r'|$. もし $q \neq q'$ なら $|r - r'| \ge b$ となるが、$0 \le r, r' < b$ より $|r - r'| < b$ だから矛盾。

問題 2. $a, b \in n\mathbb{Z}$ は $a = pn$, $b = qn$ $(p, q \in \mathbb{Z})$ と書ける。よって $a + b = (p+q)n$ だから $a + b \in n\mathbb{Z}$. また $r \in \mathbb{Z}$ について $ra = (rp)n$ だから $ra \in n\mathbb{Z}$.

問題 3. I を $\mathbb{Z}$ のイデアルとする。$I = \{0\}$ はイデアルだが $I = 0\mathbb{Z}$ と書けるから $n = 0$ として主張は正しい。そこで $I \neq \{0\}$ と仮定する。

$0 \neq a \in I$ とする。$-1 \in \mathbb{Z}$ だから $-a = (-1)a \in I$. 従って I は必ず正の整数を含む。そこで I に含まれる正の整数のうち最小のものを $n > 0$ とする。$n\mathbb{Z} \subset I$ は直ちに従う。また任意の $a \in I$ に対して $a = qn + r$, $0 \le r < n$ と書くと、n の取り方から $r = 0$ がわかるので $a = qn \in n\mathbb{Z}$ となり $I = n\mathbb{Z}$ も分かる。

また $n, m \ge 0$ が $n\mathbb{Z} = m\mathbb{Z}$ を満たすとすると、$n = qm$, $m = pn$ $(p, q \in \mathbb{Z})$ と書ける。$n, m \ge 0$ より $p, q \ge 0$. また $n = pqn$ となるので $p = q = 1$ が従う。つまり $n = m$.

問題 4.

(1) $a, b \in I$, $r \in \mathbb{Z}$ とする。$a = \sum_{i=1}^{s} n_i a_i$, $b = \sum_{i=1}^{s} m_i a_i$ $(n_i, m_i \in \mathbb{Z})$ と書けて $a + b = \sum_{i=1}^{s} (n_i + m_i) a_i$ より $a + b \in I$. また $ra = \sum_{i=1}^{s} (rn_i) a_i$ だから $ra \in I$. 従って I は $\mathbb{Z}$ のイデアル。

(2) $I = d\mathbb{Z}$ とすると任意の $i = 1, \dots, s$ に対して $a_i \in I$ だから $d | a_i$. また $e | a_i$ $(i = 1, \dots, s)$ と仮定し $a_i = p_i e$ と書く。$d \in I$ だから $d = \sum_{i=1}^{s} n_i a_i$ となる $n_i \in \mathbb{Z}$ $(i = 1, \dots, s)$ が取れる。よって $d = \sum_{i=1}^{s} (n_i p_i) e$ より $e | d$.

(3) $d' \ge 0$ が定理 2 の性質 (1), (2) を満たすと仮定する。$d = \sum_{i=1}^{s} n_i a_i$ と書くと性質 (1) より $d' | d$. また $d | a_i$ と d' が性質 (2) を満たすことから $d | d'$. 特に $d' = pd$, $d = p'd'$ とかける。よって $d = pp'd$. $d = 0$ なら $d' = pd = 0$. $d \neq 0$ なら $pp' = 1$ から $d = d'$.

問題 5. $d := \gcd(a_1, \dots, a_s)$ とすると問題 4 のイデアル I に対して $I = d\mathbb{Z}$. よって $d = \gcd(a_1, \dots, a_s) = 1$ と仮定すると $1 = d \in I$ から $1 = \sum_{i=1}^{s} n_i a_i$ となる整数 n_i が取れる。逆にこの式を仮定すると、問題 4 のイデアル I に対して $1 \in I$ が成り立つから、$d := \gcd(a_1, \dots, a_s)$ とけば $1 \in I = d\mathbb{Z}$. これから $d = 1$ が分かる。

問題 6. $d := \gcd(a, b)$, $e := \gcd(b, a - qb)$ とおく。$d | a$, $d | b$ より $d | (a - qb)$ なので $d | e$. また $a = (a - qb) + qb$ と $e | (a - qb)$, $e | qb$ より $e | a$. よって $e | d$. d と e は非負整数だから $d = e$.

問題 7. $d := \gcd(a_1, \dots, a_s)$, $e := \gcd(a_1, \gcd(a_2, \dots, a_s))$ とする。$d | a_i$ $(i = 2, \dots, s)$ より $d | \gcd(a_2, \dots, a_s)$. また $d | a_1$ より $d | e$. 更に $e | \gcd(a_2, \dots, a_s)$ と $e | a_1$ より $e | a_i$ が任意の $i = 1, \dots, s$ に対して成り立つ。よって $e | d$ となるから $d = e$.

担当教員: 柳田 伸太郎　研究室: A441　E-mail:yanagida@math.nagoya-u.ac.jp

問題 8. (1) 正の整数 $r_0 = a$ より小さな正の整数は有限個であり、ステップ (2)(b) で $r_{l+1} < r_l$ となることから、有限回の手続きの後ステップ (2)(a) に必ず到達する。

(2) 最終的にステップ (2)(a) に到達した時点で得られている非負整数列を $r_0 = a > r_1 = b > r_2 > \cdots > r_n > r_{n+1} = 0$ と表すと、問題 6 の主張から $\gcd(a,b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_n, r_{n+1}) = \gcd(r_n, 0) = r_n$.

問題 9. $I = \{ax + by \mid x, y \in \mathbb{Z}\}$ とすると問題 4 より $I = d\mathbb{Z}$. すると「方程式 $(\star)$ の解が存在する」 $\iff$ $c \in I$ $\iff$ $c \in d\mathbb{Z}$ $\iff$ $d|c$.

問題 10. (1) 仮定から $ax_o + by_o = c$, $ax + by = c$ なので、辺々引いて $a(x - x_o) + b(y - y_o) = 0$. また $\gcd(a,b) = 1$ より $ka + lb = 1$ となる $k, l \in \mathbb{Z}$ が取れる (問題 5)。よって $(x - x_o) = (x - x_o)(ka + lb) = -kb(y - y_o) + lb(x - x_o)$ となるが、右辺は b で割れるので $b|(x - x_o)$. 同様に $(y - y_o) = ka(y - y_o) - la(x - x_o)$ から $a|(y - y_o)$ が分かる。

(2) (x, y) を方程式 $(\star)$ の整数解とする。設問 (1) から $(x - x_o) = bs$, $(y - y_o) = at$ と書ける。仮定から $a, b > 0$ に注意すると再び設問 (1) より $0 = a(x - x_o) + b(y - y_o) = abs + bat$ となるから $s + t = 0$. よって $x = x_o + bs$, $y = y_o - as$ と書ける。逆にこのような $x, y \in \mathbb{Z}$ が与えられれば $ax + by = ax_o + by_o + abs - bas = c$ となるので (x, y) は $(\star)$ の整数解。

問題 11. 各 Q_i は $\begin{pmatrix} q & 1 \\ 1 & 0 \end{pmatrix}$ の形の行列 (但し $q \in \mathbb{Z}$) なので、整数成分の逆行列 $\begin{pmatrix} 0 & 1 \\ 1 & -q \end{pmatrix}$ を持つ。従って Q も逆行列を持ち $Q^{-1} = Q_n^{-1} \cdots Q_1^{-1}$ の各成分も整数。また Q_i 達の定義から $Q^{-1} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ なので、これと $(c, 0)$ の積をとると

$$c = (c,0) \begin{pmatrix} 1 \\ 0 \end{pmatrix} = (c,0) Q^{-1} \begin{pmatrix} a \\ b \end{pmatrix} = (x_o, y_o) \begin{pmatrix} a \\ b \end{pmatrix} = ax_o + by_o$$

となり、(x_o, y_o) は方程式 $(\star)$ の整数解であることが分かる。

問題 12. $s \in \mathbb{Z}$ を任意として (1) $x = -7 + 3s$, $y = 21 - 8s$. (2) $x = -17 + 35s$, $y = 35 - 72s$.

問題 13. (1) $f = 0$ または $g = 0$ のときは $fg = 0$ より与式は $-\infty = -\infty$ で成り立つ。

$f, g \neq 0$ のときは $m := \deg(f)$, $n := \deg(g)$ とおけば $f = a_m x^m + a_{m-1} x^{m-1} + \cdots$, $g = b_n x^n + b_{n-1} x^{m-1} + \cdots$ $(a_m, b_n \neq 0)$ と書けて、fg の最項次数の項は $a_m b_n x^{m+n}$ だから $\deg(fg) = n + m$ となる.

(2) $fg \neq 0$ なら同様に a_m, b_n を置き $d := \max\{m, n\}$ とする。$\deg(f + g) \leq d$ となるから与式が成り立つ. $f = 0$ ならば $f + g = g$ から明らか。$g = 0$ も同様。

(3) $fg = 0$ ならば (1) より $\deg(f) + \deg(g) = -\infty$. ここでもし f, g 両方とも 0 でないとすると左辺は 0 以上であり矛盾する。

問題 14. $\deg(f) \geq \deg(g)$ と仮定する。$m := \deg(f)$, $n := \deg(g)$ とおけば $L(f) = a_m x^m$, $L(g) = b_n x^n$ $(a_m, b_n \neq 0)$ と書ける。$c := a_m / b_n$ とおくと $m \geq n$ より $q := cx^{m-n}$ は 0 でない多項式であり $qL(g) = L(f)$. 逆に $L(f) = qL(g)$ となる多項式 $q \neq 0$ が存在するな

担当教員: 柳田 伸太郎　研究室: A441　E-mail:yanagida@math.nagoya-u.ac.jp

ら、問題 13 (1) より $\deg(f)=\deg(L(f))=\deg(q)+\deg(L(g))=\deg(q)+\deg(g)$. ここで $q\neq 0$ だから右辺は $\deg(g)$ 以上である。

問題 15. $0\leq\deg(g)\leq\deg(f)$ と仮定し $L(f)=qL(g)$ となる $q\neq 0$ をとる。$f=L(f)+f'$, $g=L(g)+g'$ と書くと f',g' は多項式で $\deg(f')<\deg(f)$, $\deg(g')<\deg(g)$. 従って $r=f-qg=L(f)+f'-qL(g)-qg'=f'-qg'$. ここで $\deg(f')\leq\deg(f)-1$, $\deg(qg')=\deg(q)+\deg(g')\leq\deg(q)+\deg(g)-1=\deg(f)-1$ だから $\deg(r)\leq\deg(f)-1$.

問題 16. 問題 15 より各ステップで得られる多項式 r_{l+1} について $\deg(f)>\deg(r_l)>\deg(r_{l+1})$. よって数回後に $\deg(g)\geq 0$ より小さな次数の多項式が現れることになり、手続きは終了する。終了時の多項式の列を $r_0,r_1,\dots,r_n,r_{n+1}$ とすると、$r_0=f$ かつ

$$\deg(f)=\deg(r_0)>\deg(r_1)>\cdots>\deg(r_n)\geq\deg(g)>\deg(r_{n+1}).$$

また各 $l=0,\dots,n$ について多項式 $q_l\neq 0$ があって $L(r_l)=q_lL(g)$, $r_{l+1}=r_l-q_lg$. よって

$$\begin{aligned}f=r_0=r_1+q_0g&=r_2+q_1g+q_0g\\&=\cdots\\&=r_n+q_{n-1}g+\cdots+q_0g\\&=r_{n+1}+q_ng+q_{n-1}g+\cdots+q_0g.\end{aligned}$$

よって $q:=q_0+\cdots+q_n$, $r:=r_{n+1}$ とすれば $f=qg+r$, $\deg(r)<\deg(g)$.

問題 17. $f=q_1g+r_1=q_2g+r_2$, $\deg(r_i)<\deg(g)$ だとする。特に $\deg(r_2-r_1)=\deg(q_1-q_2)+\deg(g)$. もし $q_1\neq q_2$ なら $\deg(q_1-q_2)+\deg(g)\geq\deg(g)$ だが、一方仮定から $\deg(r_2-r_1)<\deg(g)$ だから矛盾。よって $q_1=q_2$ でありそれから $r_1=r_2$ も従う。

問題 18. (1) $q=x^8+x^5+x^2-2$, $r=x^2-1$. (2) $q=2ix^2-x+1-2i$, $r=5x-4+2i$.

問題 19. $g,h\in\langle f\rangle$, $p\in\mathbb{C}[x]$ とする。$g=qf$, $h=rf$ となる $q,r\in\mathbb{C}[x]$ が取れる。$g+h=(q+r)f$ だから $g+h\in\langle f\rangle$. また $pg=(pq)f$ より $pg\in\langle f\rangle$.

問題 20. $I\subset\mathbb{C}[x]$ をイデアルとする。$I=\{0\}$ の時は明らか。そこで $I\neq\{0\}$ とする。

f を I に含まれる 0 でない多項式のうち次数が最小のものとする。$f\in I$ であり I がイデアルだから任意の $h\in\mathbb{C}[x]$ に対して $hf\in I$. よって $\langle f\rangle\subset I$. 次に任意の $g\in I$ を f で割り $g=qf+r$, $q,r\in\mathbb{C}[x]$, $\deg(r)<\deg(f)$ とする。このとき $qf\in\langle f\rangle\subset I$ だから $r=g-qf\in I$. もし $r\neq 0$ とすると $0\leq\deg(r)<\deg(f)$ となり、f の取り方と矛盾する。従って $r=0$. 特に $g=qf\in\langle f\rangle$。以上より $I=\langle f\rangle$.

また $\langle f\rangle=\{0\}$ ならば $0=1\cdot f$ より $f=0$. そこで $\langle f\rangle\neq\{0\}$ として $\langle f\rangle=\langle g\rangle$ と仮定する。$f=pg$, $g=qf$ となる多項式 p,q が取れるので $f=pqf$. 問題 13 (3) より $f=0$ または $pq=1$. $\langle f\rangle\neq\{0\}$ と仮定しているから $pq=1$. 問題 13 (1) より $\deg(p)+\deg(q)=0$. つまり $\deg(p)=\deg(q)=0$ となるから p, q は 0 でない複素数。従って g は f の複素数倍。

問題 21. (1) 問題 4(1) と同様なので省略。
(2) 設問 (1) と問題 20 により $I=\langle f\rangle$ となる多項式 $f\in I$ が存在する。$f_i\in I=\langle f\rangle$

担当教員: 柳田 伸太郎　研究室: A441　E-mail:yanagida@math.nagoya-u.ac.jp

$(i=1,\dots,s)$ より $f_i=p_if$ と書ける。つまり f_i は f で割れる。また $g\in\mathbb{C}[x]$ が f_i $(i=1,\dots,s)$ を割るとすると $f_i=q_ig$ と書ける。また $f\in I$ だから $f=\sum_{i=1}^s h_if_i$ とすると $f=(h_1q_1+\cdots+h_sq_s)g$ となるから f は g で割れる.
(3) 多項式 g が定理 4 の条件 (1), (2) を満たすとし、$I=\langle f\rangle$ となる f を取る。このとき f も g も定理 4 の条件 (1), (2) を満たしている。従って f は g で割れ、g は f で割れる。従って $I=\langle f\rangle=\langle g\rangle$.
(4) まず f_i のうちどれかは 0 ではないから $I\neq\{0\}$. $I=\langle f\rangle$ となる f を取ると $f\neq0$ で f は設問 (2) から定理 4 の条件 (1), (2) を満たす。そこで $f=a_0+\cdots+a_mx^m$, $a_m\neq0$ $(\deg(f)=m)$ 書ける。$g:=f/a_m$ とおくと g は定理 4 の三つの条件を満たす。
また h が定理 4 の三つの条件を満たすと仮定する。このとき設問 (3) より $I=\langle g\rangle=\langle h\rangle$ が成り立つ。よって問題 20 より $h=cg$ となる 0 でない複素数 c が存在する。ところが g と h の最高次数の項の係数は 1 であるから $c=1$ である.

問題 22. $f:=\gcd(f_1,\dots,f_s)$ とすると問題 21 の $\mathbb{C}[x]$ のイデアル I は $\langle f\rangle$ と等しい。従って特に $\gcd(f_1,\dots,f_s)=1$ ならば $1\in I$ だから $1=m_1f_1+\cdots+m_sf_s$ となる多項式 m_i が存在する。一方このような m_i が存在するなら $1\in I$. $f:=\gcd(f_1,\dots,f_s)$ とおくと $1\in\langle f\rangle=I$ となるから $1=pf$ となる多項式 p が存在する。$\deg(p)+\deg(f)=0$ となるから p も f も定数。f の最高次数の項の係数は 1 だから $f=1$.

問題 23. (1) $p:=\gcd(f,g)$, $r:=\gcd(g,f-qg)$ とすると $f=ps$, $g=pt$ となる多項式 s,t が存在するが、$f-qg=(s-qt)p$ より p は g と $f-qg$ 両方を割る。従って p は r を割る。また $g=rs'$, $f-qg=rt'$ となる多項式 s',t' を取ると $f=qg+rt'=(qs'+t')r$ より r は f,g を割る。従って r は p を割る。
よって $r=ap$, $p=br$ となる多項式 a, b がある。このとき $p(ab-1)=0$ だから $p=0$ または $ab=1$. ところが $g\neq0$ だから $p\neq0$. よって $ab=1$. 次数計算により a,b は共に定数。しかし r,p の最高次数の係数が 1 だから $a=b=1$. よって $r=p$ である。
(2) $f:=\gcd(f_1,\dots,f_s)$, $h:=\gcd(f_2,\dots,f_s)$, $g:=\gcd(f_1,h)$ とおく。このとき f は f_1 を割る。また $f_2,\dots,f_s$ も f で割れるから h は f で割れる。よって g は f で割れる。また g は f_1 を割る。更に h は g で割れる。そこで $f_i=p_ih$ とおくと分かるように f_i $(i=2,\dots,s)$ は g で割れる。よって f は g で割れる。あとは (1) と同様で $f=g$ が分かる。

問題 24. 問題 23 より $\gcd(f,g)=\gcd(r_1,r_2)=\gcd(r_2,r_3)=\cdots=\gcd(r_n,r_{n+1})$ となる。ここで $r_{n+1}=0$ である。従って一般に $r\neq0$ に対して $\gcd(r,0)=cr$ となる複素数 c が存在することを示せば良い。ところが $s:=\gcd(r,0)$ とおくと s は r を割る。そこで $r=as$ (a は多項式) と書くと、r は r 自身を割り更に 0 も割る $(0=0\cdot r)$. よって r は s を割る。あとは問題 23 と同様の議論で s が r の複素数倍だと分かる。

問題 25.

(1) $\gcd(f,g)=x-1$　　(2) $\gcd(f,g)=x+2i$