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

整数と多項式の互除法

作成日: 10/26/2016 更新日: 11/07/2016 Version: 1.0　配布日: 11/10/2016

最大公約数

まず次の定理を思い出そう。

定理 1. 整数 a, b（但し $b > 0$）に対し次を満たす整数 q, r がただ 1 組存在する。

$$a = qb + r, \quad 0 \leq r < b.$$

問題 1. 上記の定理を証明せよ。

二つの整数 a, b に対して $a = qb$ となる整数 q が存在するとき、a は b で整除される、または a は b の倍数、または b は a の約数といい、$b|a$ と表すことにする。

定理 2. 整数 $a_1, \ldots, a_s$ に対して次の性質を持つ非負整数 d が唯一つ存在する：
(1) $d|a_i$ $(i = 1, \ldots, s)$　　(2) $e|a_i$ $(i = 1, \ldots, s)$ ならば $e|d$.
この $d \geq 0$ を $a_1, \ldots, a_s$ の最大公約数といい、$d = \gcd(a_1, \ldots, a_s)$ と書く.

補足 1. 整数 $a_1, \ldots, a_s$ の共通の約数（公約数という）の絶対値の最大値を d とすれば、d が上記の性質を満たすことが示せる。この定義だと上記の性質の (1) は自明だが (2) は証明の必要がある。以下ではイデアルを使って上記のような整数 d の存在を証明する。

定義 1. 整数全体 $\mathbb{Z}$ の空でない部分集合 $I \subset \mathbb{Z}$ は、任意の $a, b \in I$ と $r \in \mathbb{Z}$ に対して $a + b \in I$ かつ $ra \in I$ となっているときイデアルと呼ばれる。

補足 2. 3 年生の代数学の講義で、イデアルはより一般の環に対して定義される。

$\mathbb{Z}$ のイデアルの例として次のようなものがある。

問題 2. 任意の $n \in \mathbb{Z}$ について、n の倍数全体の集合 $n\mathbb{Z}$ は $\mathbb{Z}$ のイデアルであることを示せ。

実は $\mathbb{Z}$ のイデアルは上記の問題のものしかない。

問題 3. $\mathbb{Z}$ の任意のイデアル I に対し、非負整数 n で $I = n\mathbb{Z}$ となるものが唯一つ存在することを示せ（定理 1 を使うと良い）。

以上の準備のもとに最大公約数の存在を証明しよう。

問題 4. 整数 $a_1, \ldots, a_s$ が与えられたとする。これらに対し $\mathbb{Z}$ の部分集合 I を以下で定める。

$$I := \{n_1 a_1 + \cdots n_s a_s \mid n_1, \ldots, n_s \in \mathbb{Z}\}.$$

(1) I は $\mathbb{Z}$ のイデアルであることを示せ.

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

(2) 問 (1) と問題 3 により $I = d\mathbb{Z}$ となる整数 $d \geq 0$ が唯一つ存在する。この d が定理 2 の性質 (1) と (2) を満たすことを示せ。

(3) 定理 2 の性質 (1) と (2) を満たす非負整数は唯一つであることを示せ。

最大公約数の基本的な性質を復習しよう。

問題 5. 整数 $a_1, \ldots, a_s$ について、$\gcd(a_1, \ldots, a_s) = 1$ であることと方程式 $n_1a_1 + \cdots + n_sa_s = 1$ の整数解 $(n_1, \ldots, n_s)$ が存在することが同値であることを示せ。

問題 6. 3 つの整数 a, b, q に対して $\gcd(a, b) = \gcd(b, a - qb)$ が成り立つことを示せ。

問題 7. 任意の整数 $a_1, \ldots, a_s$ $(s \geq 3)$ に対し次の等式を示せ。

$$\gcd(a_1, \ldots, a_s) = \gcd(a_1, \gcd(a_2, \ldots, a_s)).$$

Euclid の互除法

前節では最大公約数の性質を復習した。問題 7 により結局 2 つの整数の最大公約数を求めれば良いことが分かった。それを具体的に求める手続きとして Euclid の互除法がある。正整数 a, b $(a > b)$ が与えられたとして、以下のような手続きを考えよう。

(1) $r_0 = a$, $r_1 = b$ とおき次のステップ (2) に進む。

(2) 非負整数からなる長さが 2 以上の数列 $r_0 > r_1 > \cdots > r_l$ が与えられたとき

(a) $r_l = 0$ なら手続きを終了する。

(b) $r_l > 0$ のとき、r_{l-1} を r_l で割った余りを r_{l+1} とし次のステップ (3) に進む。

(3) 新しく得られた非負整数列 $r_0 > r_1 > \cdots > r_{l+1}$ に対してステップ (2) を行う.

実はこの手続きによって $\gcd(a, b)$ が得られる。

問題 8. 必要なら問題 6 を用いて以下の事実を説明せよ。
(1) 上記の手続きは必ず有限回で終了する。 (2) 上記の手続きで $\gcd(a, b)$ が得られる。

応用: 一次方程式

次の問題を考えよう：正の整数 a, b $(a > b)$ と整数 c が与えられたとき、一次方程式

$$ax + by = c \qquad (\star)$$

が整数解 (x, y) を持つのはどのようなときか？
この問題に対してまず次が分かる。

問題 9. $d := \gcd(a, b)$ としたとき、方程式 $(\star)$ が解を持つためには $d|c$ となることが必要十分であることを示せ。

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

そこで $d := \gcd(a,b)$ とおき $d|c$ と仮定する。方程式 $(\star)$ を d で割ることで、$\gcd(a,b)=1$ のときを考えれば十分であることが分かる。

問題 10. $\gcd(a,b)=1$ と仮定し、(x_o,y_o) を方程式 $(\star)$ の整数解とする。

(1) (x,y) を方程式 $(\star)$ の整数の解とする。このとき $a(x-x_o)+b(y-y_o)=0$ を示せ。またこれを用いて $b|(x-x_o)$, $a|(y-y_o)$ を示せ。

(2) 上記の結果 $x-x_o=bs$, $y-y_o=at$ となる整数 s, t が存在する。このとき $s+t=0$ を示せ。また整数の組 (x,y) が方程式 $(\star)$ の解であるためには

$$x=x_o+bs,\quad y=y_o-as,\quad s\in\mathbb{Z} \tag{$\flat$}$$

と書き表わされることが必要十分であることを示せ。

従って方程式 $(\star)$ の整数解 (x_o,y_o) を 1 組求めれば、あとは式 $(\flat)$ によって全ての解が求まる。最初の解 (x_o,y_o) を求めるには Euclid の互除法が使える。まず正の整数 a, b $(a>b,\ \gcd(a,b)=1)$ に対して互除法で得られる非負整数の単調減少列を

$$r_0=a>r_1=b>r_2>\cdots>r_n>r_{n+1}=0$$

とする。$r_n=\gcd(a,b)=1$ に注意。次に互除法のステップ (2)(a) での商を q_l と書くと

$$\begin{aligned}
r_0&=q_1r_1+r_2 && (0<r_2<r_1)\\
r_1&=q_2r_2+r_3 && (0<r_3<r_2)\\
&\vdots \quad \vdots\\
r_{n-2}&=q_{n-1}r_{n-1}+1 && (0<1<r_{n-1})\\
r_{n-1}&=q_nr_n=q_n
\end{aligned}$$

となる。これらを以下のように行列で表すことができる。

$$\begin{aligned}
\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}r_0\\r_1\end{pmatrix}&=Q_1\begin{pmatrix}r_1\\r_2\end{pmatrix}, && Q_1:=\begin{pmatrix}q_1&1\\1&0\end{pmatrix},\\
\begin{pmatrix}r_1\\r_2\end{pmatrix}&=Q_2\begin{pmatrix}r_2\\r_3\end{pmatrix}, && Q_2=\begin{pmatrix}q_2&1\\1&0\end{pmatrix}\\
&\vdots \quad \vdots\\
\begin{pmatrix}r_{n-2}\\r_{n-1}\end{pmatrix}&=Q_{n-1}\begin{pmatrix}r_{n-1}\\1\end{pmatrix}, && Q_{n-1}:=\begin{pmatrix}q_{n-1}&1\\1&0\end{pmatrix}\\
\begin{pmatrix}r_{n-1}\\1\end{pmatrix}&=Q_n\begin{pmatrix}1\\0\end{pmatrix}, && Q_n:=\begin{pmatrix}q_n&1\\1&0\end{pmatrix}.
\end{aligned}$$

最後の式から順番に前の式に代入していくことで次の式を得る。

$$\begin{pmatrix}a\\b\end{pmatrix}=\begin{pmatrix}r_0\\r_1\end{pmatrix}=Q\begin{pmatrix}1\\0\end{pmatrix},\qquad Q=Q_1Q_2\cdots Q_{n-1}Q_n.$$

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

問題 11. $\gcd(a,b)=1$ のとき、上記の行列 Q は整数成分の逆行列を持つことを示せ。また

$$(x_o, y_o) := (c, 0)Q^{-1}$$

で定義される (x_o, y_o) は方程式 $(\star)$ の整数解であることを示せ。

問題 12. 次の方程式の整数の解 x, y を上の方法で全て求めよ.

(1) $64x + 24y = 56$.　　(2) $72x + 35y = 1$.

多項式の整除

複素数を係数とする変数 x の多項式全体の集合を $\mathbb{C}[x]$ で表す。f の次数を $\deg(f)$ と表す。但し多項式 $0 \in \mathbb{C}[x]$ の次数は $\deg(0) := -\infty$ とする。$\deg(f) = 0$ となるのは f が 0 でない定数のとき、かつそのときに限る。整数全体の集合 $\mathbb{Z}$ のように、$f, g \in \mathbb{C}[x]$ に対して $f \pm g$ や fg はまた $\mathbb{C}[x]$ の元である。また $0 \cdot f = 0$ である。

問題 13. 任意の $f, g \in \mathbb{C}[x]$ に対して次を示せ。

(1) $\deg(fg) = \deg(f) + \deg(g)$.　　(2) $\deg(f+g) \le \max\{\deg(f), \deg(g)\}$.

(3) $fg = 0$ なら f または g は 0.

「割る」という操作をすると「余り」が出るのも $\mathbb{Z}$ のときと似ている。

定理 3. $f, g \in \mathbb{C}[x]$ $(g \neq 0)$ に対し次を満たす $q, r \in \mathbb{C}[x]$ がただ 1 組存在する。

$$f = qg + r, \quad \deg(r) < \deg(g).$$

q を f を g で割ったときの商、r を剰余 (余り) という。

定理 3 は定理 1 より証明が難しい。まず $\deg(f) < \deg(g)$ のときは $q = 0$, $r = f$ とすればよい。また $g \neq 0$ なので $\deg(f) \ge \deg(g) \ge 0$ と仮定しても構わない。

問題 14. $f \in \mathbb{C}[x]$ が $f = \sum_{i=0}^{m} a_i x^i$, $a_m \neq 0$ と書けているとき、$L(f) := a_m x^m$ と定める。$f, g \in \mathbb{C}[x] \setminus \{0\}$ について、$\deg(f) \ge \deg(g)$ となるためには $L(f) = qL(g)$ となる $q \in \mathbb{C}[x] \setminus \{0\}$ が存在することが必要十分であることを示せ。

問題 15. $0 \le \deg(g) \le \deg(f)$ となる $f, g \in \mathbb{C}[x]$ に対し、問題 14 のように $L(f) = qL(g)$ となる 0 でない多項式 q をとり $r := f - qg$ とおく。このとき $\deg(r) < \deg(f)$ を示せ。

$0 \le \deg(g) \le \deg(f)$ となる多項式 f, g に対し以下の手続きを考える：

(1) $r_0 := f$ とおき、問題 15 にある r を r_1 とする。

(2) 多項式の列 $r_0, \dots, r_l$ で $\deg(r_0) > \cdots > \deg(r_l)$ となるものが与えられたとき

　(a) $\deg(r_l) < \deg(g)$ なら操作を終了する。

　(b) $\deg(r_l) \ge \deg(g)$ なら $L(r_l) = q_l L(g)$ となる q_l を取り $r_{l+1} := r_l - q_l g$ とする。

(3) 得られた多項式 $r_1, \dots, r_{l+1}$ に対して上記のステップ (2) を行う.

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

問題 16. $f,\ g$ を多項式で $0 \leq \deg(g) \leq \deg(f)$ となるものとする。このとき上記の操作は有限回の繰り返しで終了することを示せ。また操作が終了したとき、多項式の列 $r_0 = f, \ldots, r_n, r_{n+1}$ で $\deg(r_0) > \cdots > \deg(r_n) \geq \deg(g) > \deg(r_{n+1})$ となるものが得られる。このとき $r := r_{n+1}$ とおくと $f = qg + r$ となる多項式 q が存在することを示せ。

問題 17. 多項式 $f,\ g\ (g \neq 0)$ に対して $q_1, q_2, r_1, r_2 \in \mathbb{C}[x]$ で

$$f = q_1 g + r_1 = q_2 g + r_2, \quad \deg(r_1) < \deg(g),\ \deg(r_2) < \deg(g)$$

を満たすものがあったとする。このとき $q_1 = q_2,\ r_1 = r_2$ となることを示せ。

これで定理 3 の証明が完了した。では具体的な多項式に対して割り算をしてみよう。

問題 18. 次の多項式 $f, g \in \mathbb{C}[x]$ に対して, f を g で割ったときの商 q と余り r を求めよ.
(1) $f = x^{11} - 2x^3 + 1,\ g = x^3 - 1$.　(2) $f = 2ix^4 - x^3 + x^2 + 4x - 3,\ g = x^2 + 1$.

最大公約元と互除法

多項式 f, g に対して、ある多項式 p があって $f = pg$ となるとき、f は g で割れるという。多項式の「最大公約数」にあたるものを整数の場合をまねて次で定義する。

定理 4.　（どれかは 0 でない）$f_1, \ldots, f_s \in \mathbb{C}[x]$ に対して次の 3 つの性質を持つ多項式 $d \in \mathbb{C}[x]$ が唯一つ存在する：

(1) $f_1, \ldots, f_s$ は全て d で割れる。

(2) $f_1, \ldots, f_s$ が全て $g \in \mathbb{C}[x]$ で割れるなら、d は g で割れる。

(3) d の最高次数の項の係数は 1 である。

この d を $f_1, \ldots, f_s$ の最大公約元と呼び、$d = \gcd(f_1, \ldots, f_s)$ と書く。

補足 3.　上記の (3) を仮定せずに複素定数倍の自由度を残して定義する場合もある。

定理 4 を示すため $\mathbb{Z}$ の場合の議論のまねをしよう。$\mathbb{C}[x]$ 内の空でない部分集合 I は、任意の $f, g \in I$ と任意の $h \in \mathbb{C}[x]$ に対して $f + g \in I,\ hf \in I$ をみたすとき、$\mathbb{C}[x]$ のイデアルと呼ばれる。$\mathbb{C}[x]$ のイデアルの例として、$\mathbb{Z}$ のイデアルと同様のものがある。
問題 19. 任意の $f \in \mathbb{C}[x]$ に対して $\langle f \rangle$ を f で割れる多項式全体の集合、つまり

$$\langle f \rangle := \{hf \in \mathbb{C}[x] \mid h \in \mathbb{C}[x]\}$$

とする。このとき $\langle f \rangle$ は $\mathbb{C}[x]$ のイデアルであることを示せ。

実は整数のときと同様の事実が成立する。

問題 20. 任意の $\mathbb{C}[x]$ のイデアル I に対し、$I = \langle f \rangle$ となる $f \in \mathbb{C}[x]$ が存在することを示せ。またそのような f は複素数倍を除き一意的に定まることを示せ。

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

問題 21. $f_1, \dots, f_s \in \mathbb{C}[x]$ をどれかは 0 ではない多項式とする。$I \subset \mathbb{C}[x]$ を次で定める。

$$I := \{h_1 f_1 + \cdots + h_s f_s \mid h_1, \dots, h_s \in \mathbb{C}[x]\}.$$

(1) I は $\mathbb{C}[x]$ のイデアルであることを示せ。

(2) 問 (1) と問題 20 により $I = \langle f \rangle$ となる多項式 f が存在する。このとき f は定理 4 の性質 (1), (2) を満たすことを示せ。

(3) 逆に多項式 g が $f_1, \dots, f_s$ に対して定理 4 の性質 (1), (2) を満たすと仮定する。このとき $I = \langle g \rangle$ が成り立つことを示せ。

(4) $f_1, \dots, f_s$ に対して定理 4 の 3 つの性質を満たす多項式が唯一つ存在することを示せ。

これで多項式 $f_1, \dots, f_s$ の最大公約元が唯一つ存在することが分かった。

問題 22. $f_1, \dots, f_s \in \mathbb{C}[x]$ に対し、$\gcd(f_1, \dots, f_s) = 1$ であることとある $m_1, \dots, m_s \in \mathbb{C}[x]$ が存在して $m_1 f_1 + \cdots + m_s f_s = 1$ となることが同値であることを示せ。

では最大公約元を具体的に計算するにはどうすれば良いだろうか。次の問題のように、最大公倍数と同様の性質を最大公約元は満たすことに注意する。

問題 23. $f, g, q \in \mathbb{C}[x]$ について次を示せ：$g \neq 0$ ならば $\gcd(f, g) = \gcd(g, f - qg)$.

また整数の場合と同様に以下の事実が成立する。

問題 24. $f_1, f_2, \dots, f_s \in \mathbb{C}[x]$ について次を示せ：$f_2 f_3 \cdots f_s \neq 0$ ならば $\gcd(f_1, \dots, f_s) = \gcd(f_1, \gcd(f_2, \dots, f_s))$.

よって最大公約元を求めるためには Euclid の互除法を用いればよいことが分かる。$f, g \in \mathbb{C}[x]$ $(g \neq 0)$ に対し $r_0 := f$, $r_1 := g$ とおく。r_0 を r_1 で割り $r_0 = q_1 r_1 + r_2$ とする。ここで $\deg(r_2) < \deg(r_1)$ に注意。$r_2 \neq 0$ なら r_1 を r_2 で割り $r_1 = q_2 r_2 + r_3$ とする。この場合も $\deg(r_3) < \deg(r_2)$ となる。これを続けて多項式の列 $r_0, r_1, \dots, r_n, r_{n+1}$ で

$$\deg(r_1) > \deg(r_2) > \cdots > \deg(r_n) > \deg(r_{n+1}) = -\infty$$

となるものを得ることができる。

問題 25. 上記において r_n は $f = r_0$ と $g = r_1$ の最大公約元の複素数倍であることを示せ。

問題 26. 以下の f, g に対し最大公約元 $\gcd(f, g)$ を求めよ。

(1) $f = x^{12} - 1$, $g = x^5 - 1$.　(2) $f = ix^5 - 3x^4 - ix^3 - 4x^2 - 2ix - 4$, $g = x^2 + ix + 2$.