2 ❦ 拡張ユークリッド互除法

2024年度　総合教育科目演習 I（金曜３限）

入学年度	学部	学科	組	番号	検	フリガナ
	B	1				氏名

自然数を自然数で割る割り算を行い，商と余りを求めることは，小学校で学んだ．これを少し拡張した，整数を正の整数で割る割り算も，自然数の割り算と同様に考えることができる．

一般に、次のことが成り立つ．

整数の除法

整数 a と正の整数 b に対し

(1) $$a = bq + r, \qquad 0 \leq r < 0$$

を満たす整数 q と r 一意的に定まる．

q を，a を b で割ったときの**商 (quotient)**，r をその**余り (remainder)** という．$r = 0$ のとき，a は b で**割り切れる**という．

２つの自然数の最大公約数，最小公倍数についても小学校で学んだ．自然数 a, b に対して，その最大公約数を $\gcd(a, b)$ と書く．さらに，a または b が 0 の場合には，$\gcd(0, b) = b$, $\gcd(a, 0) = a$ と定義し，一般の整数 a, b については，$\gcd(a, b) = \gcd(|a|, |b|)$ と定義する．

ユークリッド互除法の原理

整数 a を正の整数 b で割ったときの商を q，余りを r とすると

$r \neq 0$ のとき　　$\gcd(a, b) = \gcd(b, r)$

$r = 0$ のとき　　$\gcd(a, b) = b$

このユークリッドの互除法の原理を応用して，2 つの数の最大公約数が計算できる．例えば 899 と 696 の最大公約数を求めると

$$\begin{aligned}
899 &= \underline{696} \cdot 1 + \underline{203} & &\gcd(899, 696)\\
\underline{696} &= \underline{203} \cdot 3 + \underline{87} & &= \gcd(696, 203)\\
\underline{203} &= \underline{87} \cdot 2 + \underline{29} & &= \gcd(203, 87)\\
\underline{87} &= \underline{29} \cdot 3 + 0 & &= \gcd(87, 29) = 29
\end{aligned}$$

$\boxed{1}$ 互除法を利用して、次の 2 数の最大公約数を求めよ．

a) 153, 68　　b) 325, 84　　c) 468, 150

互除法の原理の証明は，(1) 式が成り立つとき「a, b の公約数は r を割り切る」ことと「b, r の公約数は a を割り切る」ことを別々に示し，それぞれの組の公約数の最大のものは一致せざるを得ない，という形で示す．恐らく形式的な証明をしても互除法の原理が腑に落ちるというわけにはいかないので，ここでは省略し，詳しい証明は高校の教科書などに譲ることにする．

互除法の計算の各行の「$a = bq + r$」の形の式を $r = a - bq$ の形に書き直し，下のように次々に代入していくことを考える．

$$\begin{aligned}
899 &= 696 \cdot 1 + 203 & &\Rightarrow & \underline{203} &= 899 - 696 \cdot 1\\
696 &= 203 \cdot 3 + 87 & &\Rightarrow & \underline{87} &= 696 - \underline{203} \cdot 3\\
203 &= 87 \cdot 2 + 29 & &\Rightarrow & 29 &= 203 - \underline{87} \cdot 2\\
87 &= 29 \cdot 3 + 0
\end{aligned}$$

すなわち

$$\begin{aligned}
29 &= 203 - \underline{87 \cdot 2}\\
&= 203 - (\underline{696 - 203 \cdot 3}) \cdot 2 = 696 \cdot (-2) + \underline{203 \cdot 7}\\
&\qquad = 696 \cdot (-2) + (\underline{899 - 696 \cdot 1}) \cdot 7 = 899 \cdot 7 + 696 \cdot (-9)
\end{aligned}$$

と表せることがわかる．したがって，

$$899 \cdot 7 + 696 \cdot (-9) = 29$$

これはすなわち，$(x, y) = (7, -9)$ が 1 次不定方程式 $899x + 696y = 29$ の整数解のひとつであるということである．このように，互除法の計算を利用すると，2 つの整数 a, b の最大公約数 d を適当な整数 x, y を用いて，$d = ax + by$ と表すことが出来る．言い換えると，1 次不定方程式

$$ax + by = d \qquad (d \text{ は } a, b \text{ の最大公約数})$$

の整数解 (x, y) を 1 組求めることが出来る．

$\boxed{2}$ 次の 1 次不定方程式の 1 組の整数解を求めよ．

a) $163x + 78y = 1$　　b) $325x + 84y = 1$

ユークリッドの互除法により $899x + 696y = 29$ の解 (x, y) が 1 組求まった．これを用いてこの 1 次不定方程式のすべての解をも求めてみよう．まず，$899x + 696y = 29$ の両辺を 29 で割って，

$$31x + 24y = 1 \tag{2}$$

の解をすべて求めればよいことがわかる．$(x, y) = (7, -9)$ は 1 つの解だから，

$$\begin{array}{rcccl} & 31\,x & + & 24\,y & = 1 \\ -) & 31 \cdot 7 & + & 24 \cdot (-9) & = 1 \\ \hline & 31(x-7) & + & 24(y-(-9)) & = 0 \end{array}$$

これより，

$$31(x - 7) = -24(y + 9) \tag{3}$$

が成り立つ．これは $31(x - 7)$ は 24 の倍数であることを示しているが，31 と 24 は互いに素だｋら，$x - 7$ が 24 の倍数でなければばならない．すなわち，x は整数 k を用いて

$$x - 7 = 24k$$

と表せる．これを (3) に代入して，$31 \times 24k = -24(y + 9)$ となるのから，

$$y + 9 = -31k$$

よって，$899x + 696y = 29$ のすべての解は

$$x = 7 + 24k, \quad y = -9 - 31k, \qquad (k \text{ は整数})$$

であることがわかる．

$\boxed{3}$ 次の 1 次不定方程式の整数解をすべて求めよ．

a) $163x + 78y = 1$　　b) $13x - 5y = 2$

$\boxed{4}$ ある菓子が 5 個入りの箱と 8 個入りの箱で売られている．この 2 種類の箱を購入して，ちょうど 90 個の菓子を用意したい．5 個入りの箱と 8 個入りの箱の組み合わせをすべて求めよ．ただし，1 種類の箱のみを購入してもよいものとする．

$\boxed{5}$ a) $2x \equiv 1 \pmod 7$ をみたす整数 x をすべて求めよ．

b) 同様にして，$3x \equiv 1 \pmod 7, \ldots, 6x \equiv 1 \pmod 7$ をそれぞれ解き，その解の間に何らかのパターンがあるか考えてみよ．