話題提供　:　ユークリッドの互除法について

平成 28 年 2 月
富山県教育委員会小中学校課
児童生徒育成係　主幹
片山　喜美

1　2016 年センター試験

数学Ⅰ・A で

(1) $92x + 197y = 1$ の整数解で x の絶対値が最小のものを求めよ。

(2) $92x + 197y = 10$ の整数解で x の絶対値が最小のものを求めよ

といった問題が出された。

解答例）

(1) 互除法で計算する。

$$
\begin{array}{lrrr}
 & 92 & 197 & \\
2) & & 184 & \\ \hline
 & 92 & 13 & \\
 & 91 & & (7 \\ \hline
 & 1 & &
\end{array}
$$

$$
\begin{array}{rr}
15 & -7 \\ \hline
-14 & \\
1 & -7
\end{array}
$$

従って、
$92 \cdot 15 + 197 \cdot (-7) = 1$

$92x + 197y = 1$, $92 \cdot 15 + 197 \cdot (-7) = 1$ の辺々差し引いて、
$92(x - 15) = -197(y + 7)$ を得る。
$92, 197$ が互いに素であることから、この両辺 $= 92 \times 197n \quad (n \in \mathbb{Z})$ とできる。
従って、一般解は $x = 15 + 197n, y = -7 - 92n$ 。x の絶対値が最小のものは、
$x = 15, y = -7$

(2) $92 \cdot 150 + 197 \times (-70) = 10$
(1) と同様に考えて、一般解は $x = 150 + 197n, y = -70 - 92n$ 。x の絶対値が最小のものは、$n = -1$ として、$x = -47, y = 22$

2　ダイハード３の油分け算

センター試験に一次不定方程式が出題されたと思っていたら、直後に、「ダイハード３」が放映された。

問題

噴水のところで、５ガロンのポリタンクと３ガロンのポリタンクがある。これらを使って、ちょうど4ガロンの水を計って台に載せろ。（さもないと爆弾が爆発する。）

解答例）
暗算で、　$5\cdot 2+3\cdot(-3)=1$ とできるから、$5\cdot 8+3\cdot(-12)=4$
従って、 $4x+3y=4$ の一般解は $x=8+3n,\, y=-12-5n \quad (n\in\mathbb{Z})$

- $n=-2$: $x=2,\, y=-2$ のとき、
（５ガロンのタンクの水量, ３ガロンのタンクの水量）
(0,0) → (5,0) → (2,3) → (2,0) → (0,2) → (5,2) → (4,3)
この手順で５ガロンのタンクに４ガロンの水が残る。
なお、$x=2$ ： ５ガロンのタンクに２度水を入れる。
$y=-2$ ： ３ガロンのタンクから２度水を捨てる。 という動作に対応する。

- $n=-3$: $x=-1,\, y=3$ のとき、
（５ガロンのタンクの水量, ３ガロンのタンクの水量）
(0,0) → (0,3) → (3,0) → (3,3) → (5,1) → (0,1) → (1,0) → (1,3) → (4,0)
この手順で５ガロンのタンクに４ガロンの水が残る。
なお、$x=-1$ ： ５ガロンのタンクから１度水を捨てる。
$y=3$ ： ３ガロンのタンクに３度水を入れる。 という動作に対応する。

3　ユークリッドの互除法を終了するまでの計算回数

簡単な数の場合、ユークリッドの互除法はすぐ終わる。
しかし、長くかかる場合もある。例えば、「 $87x+197y=$ 最大公約数」については、

	87	197	
2)		174	
	87	23	
	69		(3
	18	23	
1)		18	
	18	5	
	15		(3
	3	5	
1)		3	
	3	2	
	2		(1
	1		

77	-34
-68	
9	-34
	27
9	-7
-7	
2	-7
	6
2	-1
-1	
1	-1

従って、 $87 \cdot 77 + 197 \cdot (-34) = 1$

3.1　２つの自然数を与えた時の計算回数

$a > b \geqq 1$ について、ユークリッドの互除法を
$a = r_{-1},\, b = r_0, \quad r_{k-2} = r_{k-1} q_k + r_k$
により進めていく。
すると、 $r_{-1} > r_0 > r_1 > r_2 > \cdots > r_n = d > r_{n+1} = 0$ となる。
このとき、「互除法の計算回数」を $Eu(a,b) = n$ で定義する。

先の例では、
$r_{-1} = 197,\, r_0 = 87,\, r_1 = 23,\, r_2 = 18,\, r_2 = 5,\, r_3 = 3,\, r_4 = 2,\, r_5 = 1,\, r_6 = 0$
$Eu(197, 87) = 5$

また、$N(x) = \max\limits_{a>x} Eu(a,x)$ とおく。
これは、小さいほうの自然数を x とするとき、互除法は最大で何回計算するかということを表す。

補題　$N(x) = \max\limits_{0<b<x} Eu(x,b) + 1$

証明）$Eu(a,x) = Eu(x, r_1) + 1$ より明らか。//

定理　フィボナッチ数列 $\{f_n\}$ を $f_{-1} = 1,\, f_0 = 1, \quad f_{n+2} = f_{n+1} + f_n$ で定める。
$n \geqq 2$ のとき、

(1) $x < f_n$ ならば、$N(x) < n$

(2) $x = f_n$ ならば、$N(x) = n$

証明）

(1) 数学的帰納法による。

- $f_1 = 2,\, f_2 = 3$ であるが、$Eu(2,1) = 0$ より、$N(2) = 0 + 1 = 1$ 。よって、$n = 2$ のときは成立する。
- $x < f_k$ のとき、$N(x) < k \quad (k = 1, 2, \cdots, n)$ が成り立つと仮定する。
  $f_n \leqq x < f_{n+1}$ とする。
  (1) $f_n \leqq r_1 < x$ のとき
  $r_2 = x - r_1 q_2 < f_{n+1} - f_n \cdot 1 = f_{n-1}$
  $Eu(x, r_1) = Eu(r_1, r_2) + 1 \leqq N(r_2) + 1 < (n-1) + 1 = n$ 。よって、$N(x) < n + 1$ //
  (2) $r_1 < f_n$ のとき
  $Eu(x, r_1) \leqq N(r_1) < n$ より、$N(x) < n + 1$ //

(2) $Eu(f_{n+1}, f_n) = n$ より、$N(f_n) \geqq n$ 。また、 $x = f_n < f_{n+1}$ より、$N(f_n) < n+1$ 。
従って、$N(f_n) = n//$

課題　$N(x)$ はどんどん大きくなっていく。それをうまく示せるか？