入学年度		学部	学科		組		番号			検	フリガナ	
											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 を正の整数 b に対し

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

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　$\gcd(a, b) = b$

高校で学んだように，この互除法の原理を応用して，２つの数の最大公約数が次のように計算できる．

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

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，「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．残念ながら，証明を理解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，詳しい証明を知りたければ，高校の教科書を見てもらうことにする．

2023 年 4 月 27 日，5 月 11 日

互除法の計算の 3 行目から，

$$29 = 203 - 87 \cdot 2$$

と表せることがわかる．さらに，そのすぐ上の 2 行目より $87 = 696 - 203 \cdot 3$ と表せるので，これを上の式に代入し，

$$29 = 203 - (696 - 203 \cdot 3) \cdot 2 = 696 \cdot (-2) + 203 \cdot 7$$

と表せることがわかる．さらに，その上の行から $203 = 899 - 696 \cdot 1$ と表せるので，

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

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，方程式 $ax + by = d$ を満たす整数解 x, y を求めることが出来る．

いま，a, b が与えられたとき，この x, y を実際に計算するプログラムを書くことを考えて見る．上の計算例をそのままプログラムにしようとすると，互除法の過程，すなわち各段階での商と余りの式を逐一メモリに蓄えておき，最大公約数が求まったあと，それらの式を逆に辿ることが必要となる．そのため，a, b が大きな数である場合，プログラムを実行するのにある程度のメモリが必要となる．しかし，実はもう少し巧妙な方法があり，最大公約数を求めると同時に x, y も求まるアルゴリズムがある．それを見るために，ユークリッドの互除法の証明の過程を振り返って見る．

いま，除法を表す式 (1) において，$a = r_0, b = r_1$ とおき，q, r をそれぞれ q_1, r_2 と書き直すと，

$$r_0 = r_1 q_1 + r_2, \qquad 0 \le r_2 < r_1$$

と表せる．そして，r_1 を r_2 で割ることにより，

$$r_1 = r_2 q_2 + r_3, \qquad 0 \le r_3 < r_2$$

と表せる．さらにこれを繰り返し，

$$\begin{aligned} r_2 &= r_3 q_3 + r_4, & 0 \le r_4 < r_3 \\ r_3 &= r_4 q_4 + r_5, & 0 \le r_5 < r_4 \\ &\vdots & \vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, & 0 \le r_n < r_{n-1} \end{aligned}$$

そして，r_{n+1} が 0 になるとき，すなわち r_n が r_{n-1} を割り切るとき，$r_n = \gcd(a, b)$ となるのであった．この互除法の各段階において

$$ax_k + by_k = r_k$$

をみたす整数 x_k, y_k を見つけていく．そして，$r_{n+1} = 0$ になり互除法が終了したとき，$r_n = \gcd(a, b) = d$ なので，x_n, y_n が求める $ax + by = d$ の整数解となる．まず，$r_0 = a, r_1 = b$ だから，

$$\begin{aligned} a \cdot 1 + b \cdot 0 &= r_0 \\ a \cdot 0 + b \cdot 1 &= r_1 \end{aligned}$$

【裏に続く】

より，$(x_0, y_0) = (1, 0)$，$(x_1, y_1) = (0, 1)$ と定義する．いま，(x_k, y_k) まで定義されているとすると，r_{k+1} は r_k を r_{k-1} で割った余りなので，$r_k = r_{k-1}q_{k-1} + r_{k+1}$，すなわち，

$$r_{k+1} = r_k - r_{k-1}q_{k-1}$$

が成り立つ．したがって，

$$\begin{array}{rlll} & ax_k & + by_k & = r_k \\ -) & ax_{k-1}q_{k-1} & + by_{k-1}q_{k-1} & = r_{k-1}q_{k-1} \\ \hline & a(x_k - x_{k-1}q_{k-1}) & + b(y_k - y_{k-1}q_{k-1}) & = r_k - r_{k-1}q_{k-1} = r_{k+1} \end{array}$$

したがって

$$\begin{cases} x_{k+1} = x_k - x_{k-1}q_{k-1} \\ y_{k+1} = y_k - y_{k-1}q_{k-1} \end{cases}$$

と定義すればよいことがわかる．

そこで，数列 $\{r_n\}, \{q_n\}, \{x_n\}, \{y_n\}$ を上から順次計算していく Excel ファイルを作ってみよう．

理論的には下のような表を作るればよい．ここで，Quotient は商，Mod は余りを表し，これらの関数は Excel に組み込まれている．

n	r_n	q_n	x_n	y_n
0	a	1	1	0
1	b	Quotient(r_0, r_1)	0	1
2	Mod(r_0, r_1)	Quotient(r_1, r_2)	$x_0 - x_1 \cdot q_1$	$y_0 - y_1 \cdot q_1$
3	Mod(r_1, r_2)	Quotient(r_2, r_3)	$x_1 - x_2 \cdot q_2$	$y_1 - y_2 \cdot q_2$
4	Mod(r_2, r_3)	Quotient(r_3, r_4)	$x_2 - x_3 \cdot q_3$	$y_2 - y_3 \cdot q_2$
$\vdots$				
k	Mod(r_{k-2}, r_{k-1})	Quotient(r_{k-1}, r_k)	$x_{k-2} - x_{k-1} \cdot q_{k-1}$	$y_{k-2} - y_{k-1} \cdot q_{k-1}$
$\vdots$				
n	Mod(r_{n-2}, r_{n-1})	Quotient(r_{n-1}, r_n)	$x_{n-2} - x_{n-1} \cdot q_{n-1}$	$y_{n-2} - y_{n-1} \cdot q_{n-1}$
$n+1$	Mod(r_{n-1}, r_n) ← これが 0 になったら終了．すぐ上の x_n, y_n が求めるもの．			

実際の Excel の表には次のページのようにすればよい．第 4 行目（$n = 2$ の行）まで打ち込んだら，それ以下の行は「下方へコピー」と呼ばれる機能を用いると簡単に表が伸ばせる．

	A	B	C	D	E	F
1	n		余り（Remainder）	商（Quotient）		
2	0	(aの値)	=B2	1	1	0
3	1	(bの値)	=B3	= QUOTIENT(C2,C3)	0	1
4	2		= MOD(C2,C3)	= QUOTIENT(C3,C4)	= E2 - E3*D3	=F2- F3*D3
5	3		= MOD(C3,C4)	= QUOTIENT(C4,C5)	= E3 - E4*D4	=F3- F4*D4
6	4		= MOD(C4,C5)	= QUOTIENT(C5,C6)	= E4 - E5*D5	=F4- F5*D5
7	5		= MOD(C5,C6)	= QUOTIENT(C6,C7)	= E5 - E6*D6	=F5- F6*D6
8	6		= MOD(C6,C7)	= QUOTIENT(C7,C8)	= E6 - E7*D7	=F6- F7*D7
9	7		= MOD(C7,C8)	= QUOTIENT(C8,C9)	= E7 - E8*D8	=F7- F8*D8
10	8		= MOD(C8,C9)	= QUOTIENT(C9,C10)	= E8 - E9*D9	=F8- F9*D9
11	9		= MOD(C9,C10)	= QUOTIENT(C10,C11)	= E9 - E10*D10	=F9- F10*D10
12	10		= MOD(C10,C11)	= QUOTIENT(C11,C12)	= E10 - E11*D11	=F10- F11*D11
13	11		= MOD(C11,C12)	= QUOTIENT(C12,C13)	= E11 - E12*D12	=F11- F12*D12
14	12		= MOD(C12,C13)	= QUOTIENT(C13,C14)	= E12 - E13*D13	=F12- F13*D13
15						
16						

2 a) $2x \equiv 1 \pmod{19}$ をみたす整数 x を求めよ．

b) 同様にして，$3x \equiv 1 \pmod{19}, \ldots, 18x \equiv 1 \pmod{19}$ 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．

c) Excel を使って 19 を法としたかけ算の表を作ってみよ．

担当：鍬田 政人 (kuwata.04f@g.chuo-u.ac.jp)