1　ユークリッドの互除法

表計算ソフト Excel を用いて，m と n の最大公約数 $d = \gcd(m, n)$ と，$x \cdot m + y \cdot n = d$ となる x, y を求めよう。

1.1　d の求め方

m_k を n_k で割った商を q_k 余りを r_k とする。すなわち

$$m_k = q_k n_k + r_k \tag{1}$$

$$r_k = m_k - q_k n_k \tag{2}$$

(1) より，n_k, r_k の公約数は m_k の約数でもある。
(2) より，m_k, n_k の公約数は r_k の約数でもある。
ゆえに，m_k, n_k の公約数と，n_k, r_k の公約数は一致しており，両者の最大公約数は等しい。

$$\gcd(m_k, n_k) = \gcd(n_k, r_k)$$

$$m_{k+1} = n_k,\ n_{k+1} = r_k \quad \text{とすると} \quad \gcd(m_k, n_k) = \gcd(m_{k+1}, n_{k+1})$$

$m_1 = m, n_1 = n$ から始めて，m_k, n_k $(k = 2, 3, \dots)$ を次々に求めていく。$n_k = 0$ になると，最大公約数が $\gcd(m_k, n_k) = m_k$ とわかる。

例 1.1

k	m_k	n_k	q_k	r_k	d
1	150	27	5	15	?
2	27	15	1	12	?
3	15	12	1	3	?
4	12	3	4	0	?
5	3	0			3

注 1.1　q_k は必要ないけれども，手計算のとき q_k を書いた方が，r_k を計算しやすい。つぎの目標である x, y を求めるときには必要である。

1.2　x, y の求め方

$n_k = 0$ になったときの k を K とおく。

$$d_K = m_K = 1 \cdot M_K + 0 \cdot n_K$$

$$\therefore\ x_K = 1,\ y_K = 0 \quad \text{とおけばよい}$$

これから始めて，x_k, y_k $(k = K-1, K-2, \dots, 1)$ を次々に求めていく。

$$\begin{aligned} d_{k+1} &= x_{k+1} \cdot m_{k+1} + y_{k+1} \cdot n_{k+1} \\ &= x_{k+1} \cdot n_k + y_{k+1} \cdot r_k \\ &= x_{k+1} \cdot n_k + y_{k+1}(m_k - q_k n_k) \\ &= y_{k+1} \cdot m_k + (x_{k+1} - q_k y_{k+1}) n_k \end{aligned}$$

$$\therefore\ x_k = y_{k+1},\ y_k = x_{k+1} - q_k y_{k+1} \quad \text{とすればよい}$$

例 1.2 d, x_k, y_k は下から上へ計算する。

k	m_k	n_k	q_k	r_k	d	x_k	y_k
1	150	27	5	15	3	2	-11
2	27	15	1	12	3	-1	2
3	15	12	1	3	3	1	-1
4	12	3	4	0	3	0	1
5	3	0			3	1	0

注 1.2 y_K は任意の整数でよい。

1.3 Excel で計算する

- B2 に m の値を入れる。
- B3 に `=C2` を入れる。
- B3 を B4〜B20 にコピーする。
- C2 に n の値を入れる。
- C3 に `=E2` を入れる。
- C3 を C4〜C20 にコピーする。
- D2 に `=IF(C2=0,0,QUOTIENT(B2,C2))` を入れる。
- D2 を D3〜D20 にコピーする。
- E2 に `=IF(C2=0,0,MOD(B2,C2))` を入れる。
- E2 を E3〜E20 にコピーする。
- F2 に `=IF(C2=0,B2,F3)` を入れる。
- F2 を F3〜F20 にコピーする。
- G2 に `=IF(B2=0,0,IF(C2=0,1,H3))` を入れる。
- G2 を G3〜G20 にコピーする。
- H2 に `=IF(C2=0,0,G3-D2*H3)` を入れる。
- H2 を H3〜H20 にコピーする。

注 1.3 2 回目からは，B2,C2 に m, n の値を入れるだけでよい。

1.4 x, y の求め方，その 2

上の求め方は，つぎの漸化式にしたがって計算した。

$$\begin{cases} x_K = 1 \\ y_K = 0 \end{cases}$$

$$\begin{cases} x_k = y_{k+1} \\ y_k = x_{k+1} - q_k y_{k+1} \end{cases} \qquad (k = K-1, K-2, \ldots, 1)$$

すなわち

$$\begin{pmatrix} x_K \\ y_K \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$\begin{pmatrix} x_k \\ y_k \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_k \end{pmatrix} \begin{pmatrix} x_{k+1} \\ y_{k+1} \end{pmatrix} \quad (k = K-1, K-2, \ldots, 1)$$

ゆえに

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \cdots\cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_{K-1} \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

ここで

$$\begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \cdots\cdots \begin{pmatrix} 0 & 1 \\ 1 & -q_{k-1} \end{pmatrix}$$

を順々に計算していくと

$$\begin{pmatrix} x_1 \\ y_1 \end{pmatrix} = \begin{pmatrix} a_K & b_K \\ c_K & d_K \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a_K \\ c_K \end{pmatrix}$$

となる。

$$\begin{aligned} \begin{pmatrix} a_k & b_k \\ c_k & d_k \end{pmatrix} &= \begin{pmatrix} a_{k-1} & b_{k-1} \\ c_{k-1} & d_{k-1} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -q_{k-1} \end{pmatrix} \\ &= \begin{pmatrix} b_{k-1} & a_{k-1} - q_{k-1} b_{k-1} \\ d_{k-1} & c_{k-1} - q_{k-1} d_{k-1} \end{pmatrix} \\ &= \begin{pmatrix} b_{k-1} & a_{k-1} - q_{k-1} a_k \\ d_{k-1} & c_{k-1} - q_{k-1} c_k \end{pmatrix} \\ \therefore \begin{pmatrix} a_k \\ c_k \end{pmatrix} &= \begin{pmatrix} b_{k-1} \\ d_{k-1} \end{pmatrix} = \begin{pmatrix} a_{k-2} - q_{k-2} a_{k-1} \\ c_{k-2} - q_{k-2} c_{k-1} \end{pmatrix} \end{aligned}$$

1.5 Excel で計算する

- B2 に m の値を入れる。
- B3 に `=C2` を入れる。
- B3 を B4〜B20 にコピーする。
- C2 に n の値を入れる。
- C3 に `=E2` を入れる。
- C3 を C4〜C20 にコピーする。
- D2 に `=IF(C2=0,0,QUOTIENT(B2,C2))` を入れる。
- D2 を D3〜D20 にコピーする。
- E2 に `=IF(C2=0,0,MOD(B2,C2))` を入れる。
- E2 を E3〜E20 にコピーする。
- F2 に `=IF(C2=0,B2,"")` を入れる。
- F2 を F3〜F20 にコピーする。
- G2 に 1 を入れる。
- G3 に 0 を入れる。
- G4 に `=IF(B4=0,0,G2-D2*G3)` を入れる。
- G4 を G5〜G20 にコピーする。
- H2 に 0 を入れる。
- H3 に 1 を入れる。
- H4 に `=IF(B4=0,0,H2-D2*H3)` を入れる。
- H4 を H5〜H20 にコピーする。

注 1.4 2 回目からは，B2,C2 に m, n の値を入れるだけでよい。