2023/04/20 (2回目)

◎ Euclid の互除法 (ユークリッド ごじょほう)

… 最古のアルゴリズム.

Def $a, b \in \mathbb{N}$ で $b = ka$ となる $k \in \mathbb{N}$ があるとき
- b は a の倍数という.
- a は b の約数という $\Leftrightarrow$ $a \mid b$ とかく

Ex.

$2 \mid 24$, $3 \mid 9$, $5 \nmid 14$ → 5は14の約数でない.

Def $a \in \mathbb{N}$ は $b, c \in \mathbb{N}$ をともに割りてるとき
a を b と c の公約数という.
また, b と c の公約数のうち最大のものを最大公約数という.

Ex. 18と24の公約数は 1, 2, 3, (6) ← 最大公約数. greatest common divisor

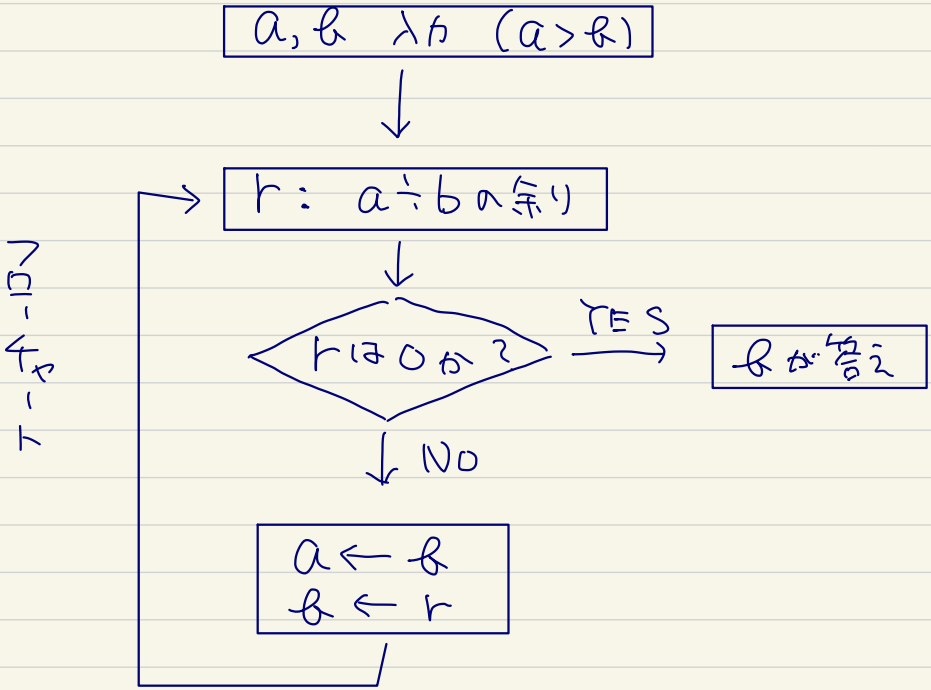
$a, b \in \mathbb{N}$ の最大公約数を $\gcd(a, b)$ で表す.

$a, b \in \mathbb{N}$ が与えられたとき $\gcd(a, b)$ を求めることのできる一連の手続 ⇝ Euclid の互除法.

Ex $\gcd(21, 54) = ?$

$54 = 21 \cdot 2 + 12 \quad \Leftrightarrow \quad 54 - 2 \cdot 21 = 12 \quad \cdots (1)$
$21 = 12 \cdot 1 + 9 \quad \Leftrightarrow \quad 21 - 1 \cdot 12 = 9 \quad \cdots (2)$
$12 = 9 \cdot 1 + (3) \leftarrow \gcd \quad \Leftrightarrow \quad 12 - 1 \cdot 9 = 3 \quad \cdots (3)$
$9 = 3 \cdot 3 + 0 \leftarrow$ 余り 0

アルゴリズム



pf.

求める $g := \gcd(21,54)$ は $g \mid 21$ かつ $g \mid 54$

$\Rightarrow$ (1)より $g \mid 12$ $\Rightarrow$ (2)より $g \mid 9$ $\Rightarrow$ (3)より $g \mid 3$

$\Rightarrow$ $g \leqq 3$.

一方で (3) $\Rightarrow$ (2) $\Rightarrow$ (1) とみれば 3 は 21と54の公約数の1つとわかる.

$\therefore$ $\gcd(21,54) = 3$. ▨

Prop. $a, b \in \mathbb{N}$ とし, $g = \gcd(a,b)$ とする.
このとき $ax + by = g$ を満たす整数解 (x,y) が存在する.

pf Euclidの互除法を逆にたどれば分かる. ▨

Ex. $21x + 54y = 3$ の整数解を1つ求めよ.

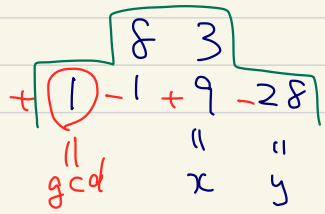
(3) $\Leftrightarrow$ $3 = 12 - 1 \cdot 9$

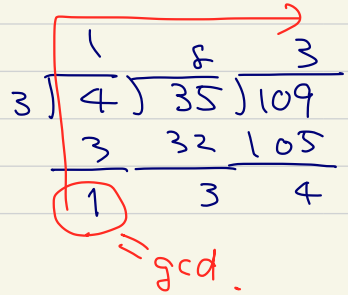
$3 \underset{(2)}{=} 12 - 1(21 - 1 \cdot 12) = 2 \cdot 12 - 1 \cdot 21$

$3 \underset{(1)}{=} 2 \cdot (54 - 2 \cdot 21) - 1 \cdot 21 = 2 \cdot 54 + (-5)21$

$\therefore (x,y) = (-5, 2)$ ▨

Ex. $\gcd(109,35)$ を求めよ. また方程式 $109x + 35y = 1$ の整数解を求めよ.





▨