§4. 整数論

自然数 $a, b \in \mathbb{N}$ に対し、最大公約数を $\gcd(a,b)$ で表す。

定理4.1. $a, b \in \mathbb{N}$ に対し、$\gcd(a,b)$ を次のアルゴリズムで求めることができる

① $x_0 = \max\{a,b\}$, $x_1 = \min\{a,b\}$, $n=1$ とする。

② $n \leftarrow n+1$, $x_n \leftarrow (x_{n-1} \bmod x_{n-2})$ とする。

$x_n > 0$ の間、これをくり返す

③ $x_n = 0$ であり、$x_{n-1} = \gcd(a,b)$ である。

例. $\gcd(456, 123)$ を求める。

① $x_0 = 456$, $x_1 = 123$ である

②-1 $456 = 3 \times 123 + 87$. より $x_2 = 87$

②-2 $123 = 1 \times 87 + 36$ より $x_3 = 36$

②-3 $87 = 2 \times 36 + 15$ より $x_4 = 15$

②-4 $36 = 2 \times 15 + 6$ より $x_5 = 6$

②-5 $15 = 2 \times 6 + 3$ より $x_6 = 3$

②-6 $6 = 2 \times 3 + 0$ より $x_7 = 0$.

$\therefore \gcd(456, 123) = 3$ である。

この方法はユークリッドの互除法とよばれる。

補題 4.2. $\gcd(a,b)$ は次をみたす。

(i) $\gcd(a-b, b) = \gcd(a,b)$

(ii) $\gcd(a,b) = \gcd(b,a)$ (iii) $\gcd(0,b) = b$.

☺(i) $\gcd(a,b)=n$, $\gcd(a-b,b)=m$ とする.

$n|a, n|b$ より, $n|a-b$ $n|b$ である ∴ $m|n$.

一方 $m|a-b$, $m|b$ より $m|(a-b)+b=a$, $m|b$, である ∴ $n|m$

∴ $n=m$ である.

(ii) は明らか.

(iii) 0 は全ての数の倍数なので. 0の約数は全ての整数である.

(注: mがnの倍数 ⇔ $m=kn$ ⇔ nがmの約数)

∴ $\gcd(0,b)$ は bの約数で一番大きいもの. ∴ $\gcd(0,b)=b$. //

定理の証明.

$a>b$ とする $a=kb+r$ とすると.

$\gcd(a,b)=\gcd(a-b,b)=\cdots=\gcd(a-kb,b)=\gcd(r,b)$ がわかる.

これと(ii)より

$\gcd(x_{n+1},x_n)=\gcd(x_n,x_{n-1})$ がわかる.

また. ② より $0\le x_{n+1}<x_n$ であるので. ある $\exists m\in\mathbb{N}$ s.t $x_m=0$ となる. $(x_{m-1}\neq 0)$

このとき $\gcd(a,b)=\gcd(x_0,x_1)=\gcd(x_m,x_{m-1})=\gcd(0,x_{m-1})=x_{m-1}$

となり. 定理が示された //.

定義6.3. 次の漸化式 $a_{n+1}=a_n+a_{n-1}$, $a_0=0, a_1=1$ をみたす数列を

フィボナッチ数列 という.

フィボナッチ数列

1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, … と続く.

定理 6.4

フィボナッチ数列の一般項は.

$$a_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n$$ である.

(:) $n=0$ のときは $a_0 = 0$ である.

$n=1$ のときは. $a_1 = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2} - \frac{1-\sqrt{5}}{2}\right) = 1$ となりみたす

a_n, a_{n-1} のときは成立するとして. a_{n+1} を考える.

$$a_{n+1} = a_n + a_{n-1} = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n + \left(\frac{1+\sqrt{5}}{2}\right)^{n-1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\right)$$

$$= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\left(\frac{1+\sqrt{5}}{2}+1\right) - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\left(\frac{1-\sqrt{5}}{2}+1\right)\right)$$

$$= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n-1}\cdot\left(\frac{1+\sqrt{5}}{2}\right)^2 - \left(\frac{1-\sqrt{5}}{2}\right)^{n-1}\cdot\left(\frac{1-\sqrt{5}}{2}\right)^2\right)$$

$$= \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \left(\frac{1-\sqrt{5}}{2}\right)^{n+1}\right)$$ となる //.

定理 6.5 S を $\max\{a,b\}$ の桁数とすると. ユークリッドの互除法で

② が行われる回数は $6S$ 以下である.

補題 6.6 : $\{x_n\}_{n=0}^{m}$ を. ユークリッド互除法でできる数列とすると.

$x_n \geq a_{m-n}$ である (a_n はフィボナッチ)

(:) $x_m = 0 = a_0$, $x_{m-1} \geq 1 = a_1$ より成立

$x_{n-1} = k_n x_n + x_{n+1} \geq a_{m-n} + a_{m-(n+1)} = a_{m-(n-1)}$ より成立 //

定理の証明.

くり返しの回数は $m-1$ 回であり、補題6.6より

x_0 の桁数 $\geq a_m$ の桁数 $=: t$ なので.

$6t \geq m-1$ を示せばよい. ここで.

$$a_m = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^m - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^m > \frac{1}{\sqrt{5}}\left(\frac{3}{2}\right)^m - 0.3 \quad \text{より}$$

$a_m + 0.3 > \frac{1}{\sqrt{5}}\left(\frac{3}{2}\right)^m$ である

$$\therefore\ t = \lfloor \log_{10}(a_m + 0.3) \rfloor + 1 > 1 + \left\lfloor \log \frac{1}{\sqrt{5}}\left(\frac{3}{2}\right)^m \right\rfloor$$

$$= 1 + \left\lfloor -\frac{1}{2}\log 5 + m(\log 3 - \log 2) \right\rfloor$$

($\log 5 = 0.7$, $\log 3 = 0.477$, $\log 2 = 0.301$)

$$> 1 + \lfloor 0.175(m-2) \rfloor \quad \text{となり.}$$

$t-1 > \lfloor 0.175(m-2) \rfloor$ より $t-1 > 0.175(m-2)$ となり

↑ 整数なので.

$$m-2 < (0.175)^{-1}\cdot(t-1) \leq 5.8(t-1)$$

$\therefore\ m-1 < 6t-5 < 6t$ が導かれる.