

問題 2

(1) ユークリッドの互除法は、最大公約数の問題を解くアルゴリズムであることを説明する。

i) 停止性

$x = x_1, y = x_0$ とし、 x_i を x_{i+1} で割ったときの商を q_{i+1} , 余りを x_{i+2} とする。

このとき $i = 1, 2, \dots, n-2$ のそれぞれについて $x_i = q_{i+1}x_{i+1} + x_{i+2}$ が成り立つ。

ユークリッドの互除法では、余りは割る数より小さく $0 \leq x_{i+2} < x_{i+1}$ より、各 i について $x_{i+1} < x_i$ がいえる。

よって $x_2 > x_3 > \dots \geq 0$ が成り立つので $x_n = 0$ となる n が存在する。

$x_n = 0$ となるときはそこで終了となるから、 $x_n = 0$ となる n が存在することはユークリッドの互除法が有限回で終了することを示している。

ii) 正当性

x_{n-1} が x, y の最大公約数であることを示す。

d を a, b の最大公約数とすると、 d は $x_1 = x, x_2 = y$ の両方を割ることができるので、

$x_3 = x_1 - q_2 x_2$ を割ることができる。さらに d は x_2, x_3 の両方を割ることができるので

$x_4 = x_2 - q_3 x_3$ を割ることができる。続けていくと、 d はすべての x_i を割ることができることがわかる。

従って x_{n-1} も d は割ることができる。

逆に $x_n = 0$ なので $x_{n-2} = q_n x_{n-1}$ であることから x_{n-1} は x_{n-2} を割ることができる。

さらに $x_{n-3} = q_{n-1} x_{n-2} + x_{n-1}$ より、 x_{n-1} は x_{n-3} を割ることができる。

この繰り返しにおいて、 x_{n-1} は全ての x_i を割ることができる、このとき特に $x = x_1, y = x_2$ を割ることができるといえる。

よって x_{n-1} は x, y の公約数で、最大公約数 d の約数となっている。

以上より $x_{n-1} = d$ が言うことができ、 x_{n-1} は x, y の最大公約数である。

(2) x, y ($x \geq y$) で x を y で割った時の商を q , 余りを r とすると $0 \leq r < y$ が成り立つ。

このとき $r < \frac{x}{2}$ であることを示す。

$$x = yq + r \text{ であり}$$

(i) $y \leq \frac{x}{2}$ であるとき

$$0 \leq r < y \text{ より } r < y \leq \frac{x}{2} \quad \therefore r < \frac{x}{2}$$

(ii) $y > \frac{x}{2}$ であるとき

$$2y > x = yq + r \quad \text{--- ①}$$

ここで $0 \leq r < y$ であることから $q = 1$ ($q \geq 2$ だと①は成立しない)。

$$\text{よって } x = y + r$$

$$r = x - y < x - \frac{x}{2}$$

$$= \frac{x}{2}$$

$$\therefore r < \frac{x}{2}$$

$$(i)(ii) \text{ より } r < \frac{x}{2} \quad \text{〃}$$