公約数は最大公約数の約数である

みがわり
twitter: @migawari_w

2022 年 12 月 31 日

目次

1 はじめに

「公約数が全て最大公約数の約数になっている」という事実は小中学生の頃に公約数を求める手間を省くテクニックとして使った覚えがあります．先日思い出して証明しようと思ったら，これが思いの他難しく，結局イデアル含む大学数学の内容を使う羽目になってしまいました．

とはいえそれだと証明の議論が長くなってしまいます．そこで「$ax + by = c$ となる c の集合」を考えることで無理やり高校数学範囲にして証明してみました．

問題形式にしたので，自力で証明してみたいと言う方は問題だけ見て証明してみて下さい．

2 問題

a, b は 0 でない整数であるとする．公約数が全て最大公約数の約数であることを示したい．

(1) $ax + by = c$ を満たす x, $y \in \mathbb{Z}$ が存在するような整数 c の集合はある $d \in \mathbb{N}$ が存在して $d\mathbb{Z} = \{dz \mid z \in \mathbb{Z}\}$ と表せることを示せ．

(2) (1) の d は a, b の公約数であることを示せ．

(3) a, b の任意の公約数は (1) の d の約数であることを示せ．また，d は a, b の公約数のうち最大のものであることを示せ．

3　解答

(1) 与えられた集合を U とする．U の元で絶対値が最小かつ正のものを d として $d\mathbb{Z} = U$ を示したい．$d \in U$ より $d = ax_0 + by_0$ なる $x_0, y_0 \in \mathbb{Z}$ が存在する．
($\subset$) 任意の $z \in \mathbb{Z}$ に対し，$dz = a \cdot zx_0 + b \cdot zy_0 \in U$ である．よって $d\mathbb{Z} \subset U$.
($\supset$) $u \in U$ として $x_1, y_1 \in \mathbb{Z}$ として $u = ax_1 + by_1$ と表せる．u を d で割った商を q，余りを r とする．$0 < r < d$ である．$u = qd + r$ より

$$r = u - qd = ax_1 + by_1 - q(ax_0 + by_0) = a(x_1 - qx_0) + b(y_1 - qy_0) \in U$$

であるがこれと d が U の絶対値が最小な元であることから $r = 0$．よって $u \in d\mathbb{Z}$．よって $d\mathbb{Z} \supset U$.
以上より $d\mathbb{Z} = U$ が示された．□

(2) $a = a \cdot 1 + b \cdot 0 \in U = d\mathbb{Z}$，$b = a \cdot 0 + b \cdot 1 \in U = d\mathbb{Z}$ より a, b は d の倍数である．よって d は a, b の公約数である．□

(3) p が a, b の公約数であるとする．$a = pa'$, $b = pb'$ となる $a', b' \in \mathbb{Z}$ が存在する．ここで

$$d = ax_0 + by_0 = p(a'x_0 + b'y_0)$$

であるから p は d の約数である．これより任意の公約数 p に対して

$$d = |d| = |p||a'x_0 + b'y_0| \geq |p| \cdot 1 \geq p$$

であるから d は a, b の公約数のうち最大のものであることが示された．□

4　参考

平林隆一「工学基礎 代数系とその応用」（新・工科系の数学）p.66,67
銀林 浩「初等整数論入門」（ちくま学芸文庫）