

02. GCDとユークリッドの互除法

代数Ⅱ

整数論

- a の倍数全体の集合 (a)
 - $a|b \Leftrightarrow (a) \supseteq (b)$
- イデアル
 - 整数 m の倍数全体の集合
 - $m\mathbb{Z} = \{\dots, -2m, -m, 0, m, 2m\}$

最大公約数と最小公倍数

- 公約数
 - 2つの整数に共通の約数
- 最大公約数(G.C.D.)greatest common divisor
 - $(a, b) = g$
- 公倍数
 - 2つの整数に共通の倍数
- 最小公倍数(L.C.M.)least common multiple
 - $[a, b] = l$

ユークリッドの互除法

- 除法定理を用いる
- アルゴリズム
 - ① $m \geq n$ に対して
 - ② $n=0$ なら m を出力 終了
 - ③ n を m とし, m を n で割った余りを n とし, ②に戻る

例

- 4368と315の最大公約数

$$(4368,315)=(315,273)=(273,42)=(42,21)=(21,0)$$