§.2 整数

§.2.1 約数と倍数

<u>Def.</u> (約数, 倍数)

0でない整数 a が整数 b を割り切るとき
($b = ac$ とかける $c \in \mathbb{Z}$ が存在するとき)
a を b の約数, b は a の倍数といい
$a \mid b$ とかく. //

<u>Eg</u> (例) ◦ $a = 6$, $b = 24$ のとき
$6 \mid 24$ である ($24 = 6 \times 4$)
◦ $a = 6$, $b = 25$ のとき
$6 \nmid 25$ である.

<u>Def.</u> (素数)

1と自分自身以外に約数をもたない正の整数であって1でないものを素数という. //

<u>Eg</u> 2, 3, 5, 7, 11, 13, 17, 19, 23, …

<u>Prop.</u> (命題)

素数は無限個存在する. //

Pf. (証明)　　　　　　　　調べてみて下さい

素数は有限個であると仮定する。
ここで全ての素数を小さい順に
並べる。

$$p_1 < p_2 < p_3 < \cdots < p_n$$

ここで次の数を考える

$$N = \underbrace{p_1 p_2 \cdots p_n}_{\text{全ての素数の積}} + 1 \in \mathbb{Z}$$

Nの定ぎから　$p_i \nmid N$　$(i=1,2,\cdots,n)$

したがって素数の定ぎより　Nは素数。
ところが　$N \neq p_i$　$(i=1,2,\cdots,n)$ より
仮定に反する。ゆえに素数は無限個　□

Thm (定理)

任意の $n \in \mathbb{Z}$ は　$n = \pm p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$
($p_1, p_2, \cdots, p_r$ は相異なる素数)

の形にかける。これを n の素因数分解という。
また $p_1, p_2, \cdots, p_r$ のことを n の素因数という。

//

Eg　$504 = 2^3 3^2 7$

$$\begin{array}{r|l} 2 & 504 \\ 2 & 252 \\ 2 & 126 \\ 7 & 63 \\ 3 & 9 \\ & 3 \end{array}$$

Def

$a,b,d \in \mathbb{Z}$ において $d \mid a$ かつ $d \mid b$ のとき
d を a,b の公約数といい，その中で最大のものを
最大公約数という．　　$\gcd(a,b)$ とかく．

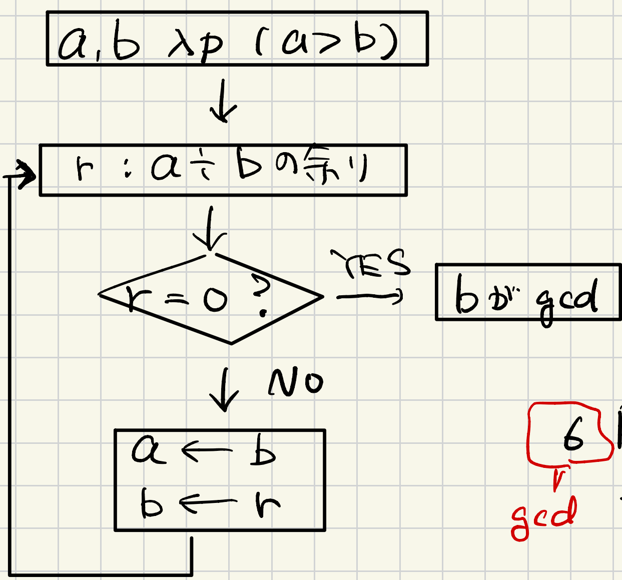
greatest common divisor

Eg　$\gcd(1800, 3780) = 2^2 \cdot 3^2 \cdot 5 = 180$.

$$\begin{cases} 1800 = 2^3 \cdot 3^2 \cdot 5^2 \\ 3780 = 2^2 \cdot 3^3 \cdot 5 \cdot 7 \end{cases}$$

§2.2　ユークリッドの互除法

アルゴリズム



例1　$a = 3780$
　　$b = 1800$

$3780 \div 1800 = 2$, $3780 - 3600 = \boxed{180}$

$1800 \div \boxed{180} = 10$, $1800 - 1800 = 0$

$\boxed{180}$ = gcd.

例2　$a = 282$
　　$b = 222$

$282 \div 222 = 1$, $282 - 222 = 60$

$222 \div 60 = 3$, $222 - 180 = 42$

$60 \div 42 = 1$, $60 - 42 = 18$

$42 \div 18 = 2$, $42 - 36 = \boxed{6}$

$18 \div \boxed{6} = 3$, $18 - 18 = 0$

gcd

ベズーの定理

$a, b \in \mathbb{Z}$ に対して x と y の方程式

$$ax + by = \gcd(a, b) \quad \leftarrow \text{ベズーの等式}$$

は整数解をもつ。 $\square$

Eg $282x + 222y = 6$ は整数解をもつ

◎ 互除法の逆算

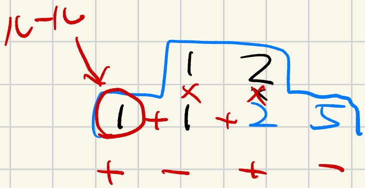
例

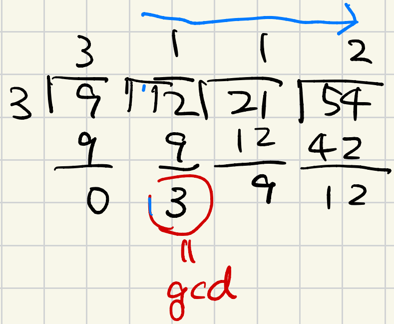
$$\begin{aligned}
282 &= 222 \times 1 + 60 &\longleftrightarrow\quad 60 &= 282 - 222 \times 1 \quad ④\\
222 &= 60 \times 3 + 42 &\longleftrightarrow\quad 42 &= 222 - 60 \times 3 \quad ③\\
60 &= 42 \times 1 + 18 &\longleftrightarrow\quad 18 &= 60 - 42 \times 1 \quad ②\\
42 &= 18 \times 2 + 6 &\longleftrightarrow\quad 6 &= 42 - 18 \times 2 \quad ①\\
18 &= 6 \times 3 + 0
\end{aligned}$$

$$\begin{aligned}
6 &\overset{①}{=} 42 - 18 \times 2\\
&\overset{②}{=} 42 - (60 - 42 \times 1) \times 2\\
&= 60 \times (-2) + 42 \times 3\\
&\overset{③}{=} 60 \times (-2) + (222 - 60 \times 3) \times 3\\
&= 222 \times 3 + 60 \times (-11)\\
&\overset{④}{=} 222 \times 3 + (282 - 222 \times 1) \times (-11)\\
&= 282 \times \underbrace{(-11)}_{= x} + 222 \times \underbrace{14}_{= y}
\end{aligned}$$

安藤式 Euclid 互除法の逆算法

$54x + 21y = 3$ の整数解を1つ求めよ.





$$\begin{cases} x = 2 \\ y = -5 \end{cases}$$

$54 \times 2 + 21 \times (-5)$

$= 108 - 105 = 3$ OK

§.2.3 mod 計算 ～13:40

<u>Def</u>

$a, b \in \mathbb{Z}$ と $n \in \mathbb{N}$ に対して

$$a \equiv b \pmod n \overset{\text{Def.}}{\iff} n \mid (a-b)$$

このとき a と b は n を法として合同という. $\square$

$$a \equiv b \pmod n \iff n \mid (a-b)$$

$$\iff a - b = nc \quad (c \in \mathbb{Z})$$

$$\iff a = nc + b$$

ここで a を n で割った余りを r とすると

$(a = nk + r)$