安藤式 Euclid互除法の逆算法

$54x + 21y = 3$ の整数解を1つ求めよ.

ルール

$$\begin{array}{cccc} & 1 & 2 & \\ 1 & +1 & +2 & 5 \\ + & - & + & - \end{array}$$

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

$$\begin{array}{r|r|r|r|r} & 3 & 1 & 1 & 2 \\ 3 & 9 & 12 & 21 & 54 \\ & 9 & 9 & 12 & 42 \\ \hline & 0 & 3 & 9 & 12 \end{array}$$

3 = gcd

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

$= 108 - 105 = 3$ OK

§2.3 mod 計算

～13:40

Def

$a, b \in \mathbb{Z}$ 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. □

$$a \equiv b \pmod n \iff n \mid (a-b)$$
$$\iff a - b = nc \quad (c \in \mathbb{Z})$$
$$\iff a = nc + b$$

ここで a を n で割った余りを r とすると
$(a = nk + r)$

$$nk+r = nc+b$$
$$b = n(k-c)+r$$
ゆえ b を n で割った余りは r.

$\therefore\quad a\equiv b \pmod n \iff$ a と b は n で割った余りが等しい.

$$\mathbb{Z} = \{-2,-1,0,1,2,3,\dots\}$$
$$= \{n \mid n\equiv 0\} \sqcup \{n \mid n\equiv 1\} \sqcup \{n \mid n\equiv 2\} \quad (\mathrm{mod}\,3)$$

mod3 の剰余類という

$\mathbb{Z}$ を class 分け!

Prop.

(i) $n \mid a \iff a\equiv 0 \pmod n$

(ii) $a\equiv b \pmod n \Rightarrow b\equiv a \pmod n$ [反射律]

(iii) $a\equiv a' \pmod n$, $b\equiv b' \pmod n$ ならば

- $a\pm b \equiv a'\pm b' \pmod n$
- $ab \equiv a'b' \pmod n$ $\square$

Eg

4^{10} を 3 で割った余りは?

$$4^{10} = \underbrace{4\cdot 4\cdot \cdots \cdot 4}_{10コ} \equiv \underbrace{1\cdot 1\cdots 1}_{10コ} = 1 \pmod 3$$

Ex. 今日は木曜日. 100日後は何曜日?

mod 7 で考える.

月	火	水	木	金	土	日
			0	1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	…					
≡	≡	≡	≡	≡	≡	≡
4	5	6	0	1	2	3

$$100 = 7 \times 14 + 2 \equiv 0 \cdot 0 + 2 = 2$$

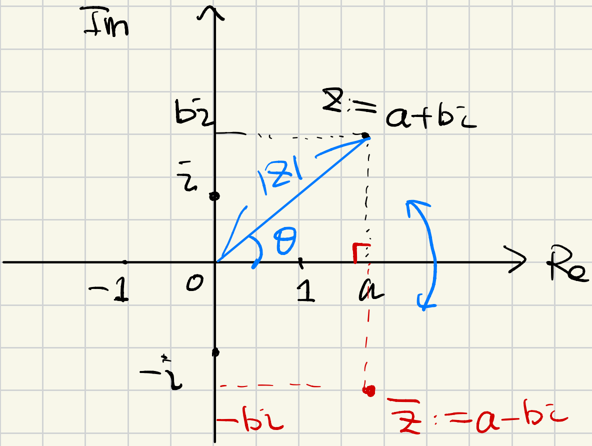
∴ (土)

§3. 複素数

§3.1. 複素数の定義

- ○ 方程式 $x^2 = -1$ の解のうち1つを i ($\notin \mathbb{R}$) とかきこれを虚数単位という.
- ○ $z = a + bi$ ($a, b \in \mathbb{R}$) の形の数を複素数といい a を z の実部, b を z の虚部といい各々 $\mathrm{Re}(z)$, $\mathrm{Im}(z)$ で表す.
- ○ 複素数 z で特に $\mathrm{Im}(z) \neq 0$ であるとき z を虚数という
- ○ 〃 $\mathrm{Re}(z) = 0$, $\mathrm{Im}(z) \neq 0$ のとき z を純虚数という

§3.2. 複素平面と極形式



複素平面 (Gauss 平面) $\mathbb{C}$

- $\bar{z} := a - bi \in \mathbb{C}$

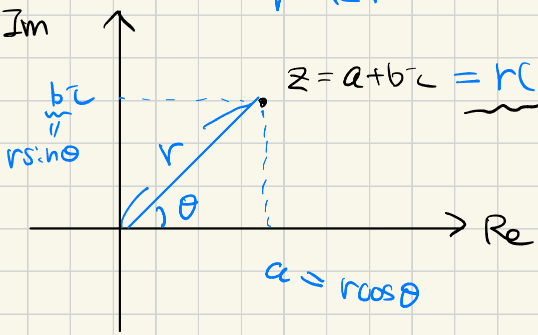
  を z の複素共役という.

- $|z| := \sqrt{a^2+b^2} \in \mathbb{R}$

  を z の絶対値という

- $\theta = \arg(z)$: z の偏角という.

$r = |z|$



$z = a+bi = \underset{\sim\sim\sim\sim\sim\sim\sim\sim}{r(\cos\theta + i\sin\theta)}$

z の極形式という.

<u>Eg.</u> $z = 3 + 3\sqrt{3}\,i$ を <u>極形式に直せ</u>

$$|z| = \sqrt{3^2 + (3\sqrt{3})^2} = 6$$

$$z = 6\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = 6\left(\cos\frac{\pi}{3} + i\sin\frac{\pi}{3}\right) \quad //$$

<u>Ex.</u> $z = 10 - 10i$ を ________ //.

極形式の良い点

$z_1 = r_1(\cos\theta_1 + i\sin\theta_1)$, $z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$

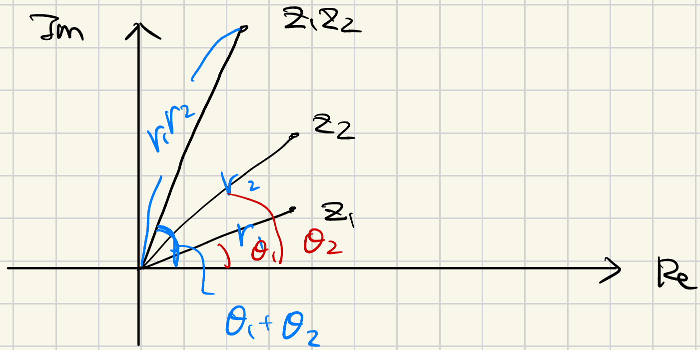
とする.

$$
\begin{aligned}
z_1 z_2 &= r_1 r_2 (\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 \\
&\qquad + i(\cos\theta_1\sin\theta_2 + \sin\theta_1\cos\theta_2)) \\
&= r_1 r_2 (\cos(\theta_1+\theta_2) + i\sin(\theta_1+\theta_2))
\end{aligned}
$$

加法定理

⇝ ・ $|z_1 z_2| = |z_1||z_2|$

・ $\arg(z_1 z_2) = \arg(z_1) + \arg(z_2)$



Thm (ド・モアブル)

$z = r(\cos\theta + i\sin\theta)$ $(r, \theta \in \mathbb{R})$ のとき

$n \in \mathbb{Z}$ に対して

$$z^n = r^n(\cos(n\theta) + i\sin(n\theta)) \quad \square$$