TD 14 - Lundi 30 novembre 2020

Théorème des restes chinois :

Si $m, n \in \mathbb{Z}$, $\text{pgcd}(m,n)=1$, alors

$$\bar{k} \longleftarrow (\bar{a}, \bar{b})$$

$$\varphi : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$\underset{k \bmod (mn)}{\bar{k}} \longmapsto (\underset{k \bmod (m)}{\bar{k}}, \underset{k \bmod (n)}{\bar{k}})$$

est bijective.

Démonstration : $\text{card}\, \mathbb{Z}/mn\mathbb{Z} = mn$

$$\text{card}\,(\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}) = \underbrace{\text{card}\,(\mathbb{Z}/m\mathbb{Z})}_{m}\, \underbrace{\text{card}\,(\mathbb{Z}/n\mathbb{Z})}_{n}$$

$$= mn.$$

Il suffit de mq φ est injective.

Soit $\bar{k}, \bar{\ell} \in \mathbb{Z}/mn\mathbb{Z}$ tq (1) $\bar{k} = \bar{\ell}$ dans $\mathbb{Z}/m\mathbb{Z}$

(2) et $\bar{k} = \bar{\ell}$ dans $\mathbb{Z}/n\mathbb{Z}$

$$\left.\begin{array}{l}(1) \Leftrightarrow m \mid k-\ell \\ (2) \Leftrightarrow n \mid k-\ell\end{array}\right\} \underset{\text{Gauss}}{\overset{\text{pgcd}(m,n)=1}{\Longrightarrow}} mn \mid k-\ell \Leftrightarrow \bar{k} = \bar{\ell} \text{ dans } \mathbb{Z}/mn\mathbb{Z}.$$

- ce qui est intéressant est φ^{-1}.

$\text{pgcd}(m,n) = 1 \Rightarrow \exists\, u, v \in \mathbb{Z}$ tq $mu + nv = 1$. (*)

$(a,b) \in \mathbb{Z}^2$

$$\left[\begin{array}{l} nv \equiv 1 \ [m] \\ \text{et } mu \equiv 1 \ [n] \end{array}\right.$$

On prend $k = bmu + anv$

alors $k \equiv a\underbrace{nv}_{1} \quad [m]$ $\qquad \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}.$

$\in$

$\equiv a \quad [m]$

et $k \equiv bmu \equiv b\ [n]$. $\qquad \varphi(\bar{k}) = (\bar{a}, \bar{b})$

On note N le nombre de moutons

exemple : Un Berger compte ses moutons. Il en a

$0 \leq$ nombre de moutons ≤ 900.

On peut les compter par paquets :

① on fait de 30 ~~~ à la fin il en reste 6
des paquets

② on fait des paquets de 31, il en reste 2.

$$\begin{cases} N \equiv \overset{a}{6} \ [30] \\ N \equiv \underset{b}{2} \ [31] \end{cases}$$

30 et 31 sont premiers entre eux.

$-30 + 31 = 1$ est relation de Bézout.

$um + vn = 1$

$m = 30$
$n = 31$

$$\begin{aligned} N &\equiv -30 \cdot a + 31 \cdot b \quad [mn] \\ &\equiv -180 + 62 \quad [930] \\ &\equiv -118 \quad [930]. \\ &\equiv 812 \quad [930] \end{aligned}$$

812 est le seul nombre congru à 812 modulo 930 et compris entre 0 et 900.

$\rightarrow \boxed{N = 812.}$

équations diophantiennes Diophante

équations faisant intervenir des nombres entiers : $2x + 3y = 1$.

Les solutions sont les relations de Bézout entre 2 et 3.

$x^2 + y^2 = z^2$ $(x,y,z) \in \mathbb{Z}^3$.

solutions = triplets Pythagoriciens

= triangles rectangles qui ont des côtés entiers.

On sait les calculer.

$x^3 + y^3 = z^3$ $(x,y,z) \in \mathbb{Z}^3$.

(E_k) : $x^k + y^k = z^k$ équations de Fermat ($17^{\text{ème}}$ siècle)

$k \geq 3$.

(E_k) n'a pas de solution non triviales pour $k \geqslant 3$
(telle que $xyz \neq 0$)

$\rightarrow$ Grand théorème de Fermat Andrew Wiles ~ 1990.
extrêmement dur.

---

ex (E): $\underbrace{15}_{3 \cdot 5} x^2 - 7y^2 = \underset{\underset{3 \cdot 3}{\shortparallel}}{9}$ Trouver toutes les solutions $(x,y) \in \mathbb{Z}^2$.

Supposons que (x,y) soit solution de (E).

$$-7y^2 \equiv 0 \quad [3].$$
$$\Leftrightarrow -y^2 \equiv 0 \ [3]$$
$$\Leftrightarrow y^2 \equiv 0 \ [3].$$
$$\Leftrightarrow y \equiv 0 \ [3]$$
$$\exists k \in \mathbb{Z} \text{ tq } y = 3k$$

On trouve : $15x^2 - 7 \cdot 3^2 \cdot k^2 = 9$

$\times \frac{1}{3}$: $5x^2 - 7 \cdot \underbrace{3 \cdot k^2}_{} = \underbrace{3}_{}.$ $\leftarrow$

$$5x^2 \equiv 0 \ [3].$$
$$\Leftrightarrow -x^2 \equiv 0 \ [3]$$
$$\Leftrightarrow x^2 \equiv 0 \ [3]$$
$$\Leftrightarrow x \equiv 0 \ [3].$$

$\exists \ell \in \mathbb{Z}$ tq $x = 3\ell$.

$$5 \cdot 3^{\cancel{2}} \cdot \ell^2 - 7 \cdot \cancel{3} \cdot k^2 = \cancel{3}$$
$$\Leftrightarrow 15\ell^2 - 7k^2 = 1. \quad (E')$$

On a montré que (x,y) sol de (E) $\Rightarrow$ $x, y \equiv 0 \ [3]$ et $\left(\frac{x}{3}, \frac{y}{3}\right)$ est sol de de (E').

(E') modulo 3 donne $-k^2 \equiv 1 \quad [3].$
$$\Leftrightarrow k^2 \equiv -1 \ [3]$$
$$\Leftrightarrow \boxed{k^2 \equiv 2 \ [3].}$$

condition nécessaire sur k

Dans $\mathbb{Z}/3\mathbb{Z}$

$\bar{k}$	$\overline{k^2}$
$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$
$\bar{2}$	$\bar{1}$

donc k^2 n'est jamais congru à 2 modulo 3.

Donc (E) n'a pas de solutions en nombres entiers.

Valuation p-adique de n!

Soit $N \in \mathbb{N}$ et p nombre premier, on note

$v_p(N)$ l'unique entier tel que $p^{v_p(N)} \mid N$ et $p^{v_p(N)+1} \nmid N$.

"valuation p-adique de N".

si $N = p^a M$ avec $p \nmid M$, alors $v_p(N) = a$.

Question : $v_p(n!) \overset{?}{=}$ si $n \in \mathbb{N}$.

$$n! = 1 \cdot 2 \cdot 3 \times \dots \times n.$$

$$v_p(n!) = \sum_{k=1}^{n} v_p(k).$$

$E = \{1, \dots, n\}$.

Soit $\alpha \geq 0$.

N_α = nombre d'élts de E divisibles par p^α.

$= \# \{ 1 \leq \underset{\text{"}p^\alpha \ell\text{"}}{k} \leq n \mid p^\alpha \mid k \}$

$= \# \{ \ell \in \mathbb{N} \mid 1 \leq p^\alpha \ell \leq n \}$.

$$\Updownarrow$$

$$\frac{1}{p^\alpha} \leq \ell \leq \frac{n}{p^\alpha}$$

$$= \left[\frac{n}{p^\alpha} \right].$$

M_α = nombre d'élts de E divisible par p^α mais pas par $p^{\alpha+1}$

$$= \left[\frac{n}{p^\alpha}\right] - \left[\frac{n}{p^{\alpha+1}}\right].$$

$$v_p(n!) = \sum_{k=1}^{n} v_p(k)$$

$$= \sum_{\alpha \geq 0} \alpha \cdot \#\{\text{entiers entre } 1 \text{ et } n \text{ de valuations } p\text{-adique } \alpha\}$$

$\#\{\ldots\}$ = $\underbrace{\text{entier divi}}_{\text{entre 1 et } n}$ par p^α mais pas par $p^{\alpha+1}$

$$= \sum_{\alpha \geq 0} \alpha \cdot M_\alpha$$

$$= \sum_{\alpha \geq 1} \alpha\left(\left[\frac{n}{p^\alpha}\right] - \left[\frac{n}{p^{\alpha+1}}\right]\right)$$

$$= \sum_{\alpha \geq 1} \alpha \underbrace{\left[\frac{n}{p^\alpha}\right]} - \underbrace{\sum_{\alpha \geq 1} \alpha \left[\frac{n}{p^{\alpha+1}}\right]}.$$

$$\sum_{\alpha \geq 1} \alpha \left[\frac{n}{p^{\alpha+1}}\right] = \sum_{\beta \geq \cancel{2}\, 1} (\beta - 1) \underbrace{\left[\frac{n}{p^\beta}\right]} \qquad \beta = \alpha + 1$$

$$= \sum_{\alpha \geq 1} \alpha \left[\frac{n}{p^\alpha}\right] - \sum_{\alpha \geq 1} (\alpha - 1)\left[\frac{n}{p^\alpha}\right]$$

$$\boxed{v_p(n!) = \sum_{\alpha \geq 1} \left[\frac{n}{p^\alpha}\right]}$$

somme finie.

<u>Application</u> : combien de zéro y-a-t il tout à droite de l'écriture de 1000!

Ce nombre est la puissance maximale de 10 qui divise 1000!

$10 = 2 \times 5$

$1000! = 10^a \cdot M = 2^a 5^a \cdot M$ avec $10 \nmid M$.

$\Updownarrow$

$\left\{ \begin{array}{l} 2 \nmid M \\ \text{ou} \\ 5 \nmid M. \end{array} \right.$

C'est $\min\left(v_2(1000!),\ v_5(1000!)\right)$

1000 500 250 125 62,5 31,25 15,125
7 3 1 0 0

$v_2(1000!) = 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1$

$v_5(1000!) = 200 + 40 + 8 + 1 = 249.$

1000, 200 40 8 $\left[\frac{8}{5}\right] = 1$ 0 0 0

donc $\boxed{\text{1000! a 249 zéro tout à droite.}}$

Nombres complexes

$\mathbb{C} \ni i \,, \; i^2 = -1$

$x^2 + x + 4 = 0$

$\Delta = -15$

$i \,, \; i^2 = -1$

$\sqrt{\Delta} = \sqrt{-15}$

$= \sqrt{-1} \cdot \sqrt{15}$

$= i\sqrt{15}.$

" On peut réaliser $\mathbb{C}$ dans $\mathcal{M}_2(\mathbb{R})$ "

$\shortparallel$

matrices de taille 2×2

$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ $a, b, c, d \in \mathbb{R}$

$\varphi : \mathbb{C} \xrightarrow{\text{injectif}} \mathcal{M}_2(\mathbb{R})$, pas surjectif. compatible avec $+, \times$.

$a + ib \longmapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

$i \longmapsto \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$

$= -I_2$

$I_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

$\mathbb{C} \simeq \mathbb{R}^2$ (de façon ensembliste). $(a,b).(c,d) \longmapsto (ac-bd, ad+bc)$

$\rightarrow$ il y a une multiplication sur $\mathbb{R}^2$ ...

$\mathbb{R}^3$ Hamilton s'est demandé si il y avait une structure de corps sur $\mathbb{R}^3$.

* La réponse est non.

Sur $\mathbb{R}^4$ oui, les quaternions de Hamilton, mais la multiplication est non commutative $\rightsquigarrow$ "corps non commutatif"
"corps gauche"
"algèbre à division"

$(a,b,c,d) = a + bi + cj + dk.$

$$i^2 = j^2 = k^2 = -1$$
$$ij = k \quad \ldots$$

<u>ex 5.1</u> :

$$z_1 = \frac{3+6i}{3-4i}$$
$$= \frac{(3+6i)(3+4i)}{(3-4i)(3+4i)} = \frac{9-24+i\cdot 30}{9+16}$$
$$= \frac{-15+30i}{25}$$
$$= \frac{-3+6i}{5}$$

$$z_2 = \left(\frac{1+i}{2-i}\right)^2$$
$$= \left(\frac{(1+i)(2+i)}{(2-i)(2+i)}\right)^2 = \left(\frac{1+3i}{5}\right)^2$$
$$= \frac{-8+6i}{25}.$$

$$z = \frac{2+5i}{1-i}$$

$$z_3 = \frac{2+5i}{1-i} + \frac{2-5i}{1+i} = \frac{(2+5i)(1+i)+(2-5i)(1-i)}{2}$$
$$= z + \bar{z} = \frac{-6}{2} = -3.$$
$$= 2\mathrm{Re}(z)$$

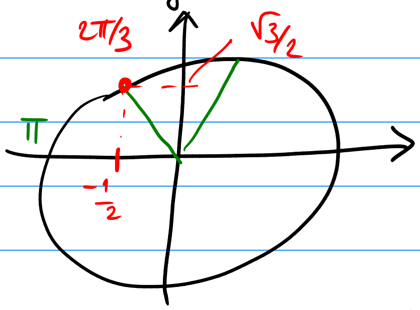
Rq : $z = \dfrac{(2+5i)(1+i)}{2}$ $\quad \boxed{\mathrm{Re}(z) = \frac{-3}{2}.}$

mathématicien suisse → Euler : a dit $e^{i\theta} = \cos\theta + i\sin\theta$.

ex 5.2 :

$$z_1 = 2e^{2i\pi/3} = 2\left(\cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)\right)$$

$$= -1 + i\sqrt{3}.$$

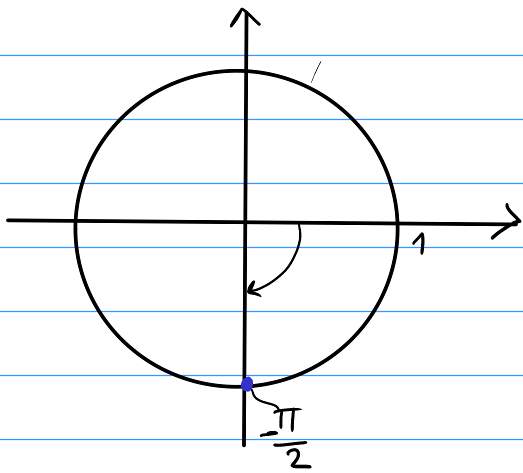


$$z_2 = \left(2e^{i\pi/4}\right)\left(e^{-3i\pi/4}\right)$$

$$= 2e^{i\pi/4 - \frac{3i\pi}{4}} = 2e^{-i\frac{\pi}{2}}.$$

$$\underset{\text{Euler}}{=} \cancel{2\cos\left(-\frac{\pi}{2}\right)}^{=0} + 2i\sin\left(-\frac{\pi}{2}\right)$$

$$= -2i$$

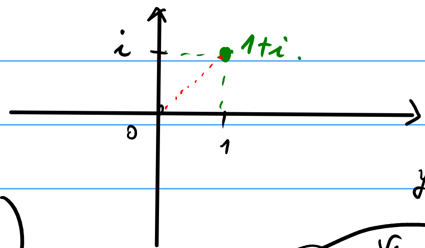


exercice 3

1- $z_1 = 1+i$

$$= |z_1| \cdot e^{i\theta_1}$$

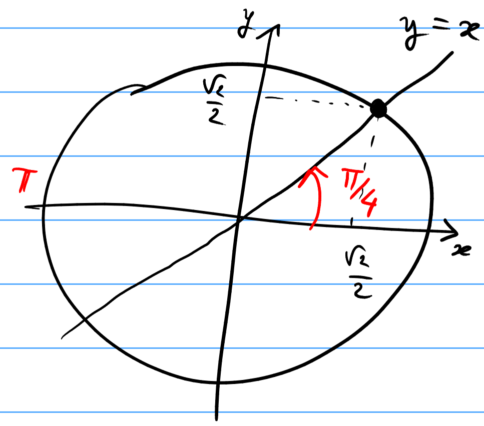
$$= |z_1|\left(\cos\theta_1 + i\sin\theta_1\right)$$



$$|z_1| = \sqrt{1^2 + 1^2} = \sqrt{2}$$

$$\cos\theta_1 + i\sin\theta_1 = \frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}$$

$$= \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}.$$

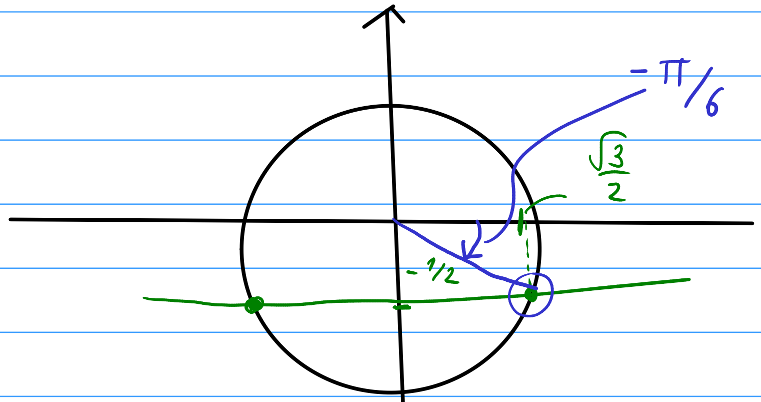


$\theta_1 = \pi/4$.

$z_1 = \sqrt{2}\, e^{i\pi/4}$

$$z_2 = |z_2| e^{i\theta_2} \qquad |z_2| = \sqrt{\sqrt{3}^2 + 1^2} = 2$$

$$\cos\theta_2 + i\sin\theta_2 = \frac{\sqrt{3}}{2} - \frac{1}{2} i$$



$\theta_2 = -\pi/6$

$z_2 = 2 e^{-i\pi/6}$.

2- $z_1 z_2 = (1+i)(\sqrt{3} - i)$

$= (\sqrt{3}+1) + i(\sqrt{3} - 1)$

$z_1 z_2 = 2\sqrt{2}\, e^{i(\pi/4 - \pi/6)}$

$= 2\sqrt{2}\, e^{i\pi/12}$

donc
$$\boxed{\cos\left(\frac{\pi}{12}\right) = \frac{\sqrt{3}+1}{2\sqrt{2}} \qquad \sin\left(\frac{\pi}{12}\right) = \frac{\sqrt{3}-1}{2\sqrt{2}}}$$

<u>ex 5.4</u> ; 1- $z \in \mathbb{C}$ $\quad z = \mathrm{Re}(z) + i\,\mathrm{Im}(z)$

$\bar{z} = \mathrm{Re}(z) - i\,\mathrm{Im}(z)$

$$\frac{z+\bar{z}}{2} = \frac{2\,\mathrm{Re}(z)}{2} = \mathrm{Re}(z).$$

$$\frac{z-\bar{z}}{2i} = \frac{2i\,\mathrm{Im}(z)}{2i} = \mathrm{Im}(z).$$

2- $\mathrm{Re}(e^{i\theta}) = \cos\theta$ (formule d'Euler)

$\underset{\text{par 1-}}{=} \dfrac{e^{i\theta} + \overline{e^{i\theta}}}{2}$

$= \dfrac{e^{i\theta} + e^{-i\theta}}{2}$. $\left(= \mathrm{ch}(i\theta) \right)$

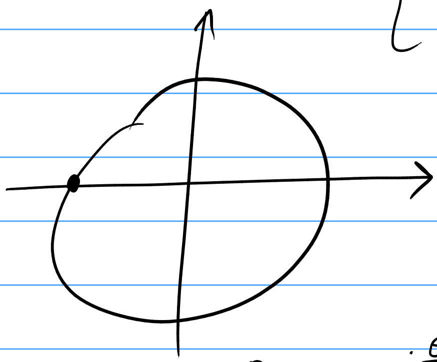
et $\Im(e^{i\theta}) = \sin\theta$ (formule d'Euler)

$$= \frac{e^{i\theta} - e^{-i\theta}}{2i}$$

1-

$$= \frac{e^{i\theta} - e^{-i\theta}}{2i} \quad \left(= \frac{1}{i} \operatorname{sh}(i\theta) \right)$$

ex 5.5 : 1- $1 + e^{i\theta} = 0 \iff \begin{cases} \cos\theta = -1 \\ \sin\theta = 0 \end{cases} \iff \theta = \pi \ [2\pi]$.



donc $\{ \pi + 2k\pi : k \in \mathbb{Z} \}$.

2- $$1 + e^{i\theta} = e^{i\frac{\theta}{2}} \big(\underbrace{e^{i\theta/2} + e^{-i\theta/2}}_{2\cos\left(\frac{\theta}{2}\right)} \big)$$

$$= 2\cos\left(\frac{\theta}{2}\right) e^{i\theta/2}$$

et $\left(\cos\left(\frac{\theta}{2}\right) \overset{?}{\geq} 0 \right)$ $= -2\cos\left(\frac{\theta}{2}\right) e^{i\theta/2} e^{i\pi}$

$$= -2\cos\left(\frac{\theta}{2}\right) e^{i\left(\frac{\theta}{2} + \pi\right)} .$$

$e^{i\pi} = -1$

si $\cos\frac{\theta}{2} \geq 0$, alors

si $\cos\frac{\theta}{2} < 0$

$$\boxed{\begin{aligned} 1 + e^{i\theta} &= 2\cos\frac{\theta}{2} e^{i\theta/2} \\ &= -2\cos\left(\frac{\theta}{2}\right) e^{i\left(\frac{\theta}{2} + \pi\right)} . \end{aligned}}$$