

OS - juinEx. 1

$$\begin{cases} x \equiv 6 \pmod{14} \\ x \equiv 12 \pmod{15} \\ x \equiv 16 \pmod{17} \end{cases} \Leftrightarrow \begin{cases} x \equiv 6 \pmod{2} \Leftrightarrow x \equiv 0 \pmod{2} \\ x \equiv 6 \pmod{7} \\ x \equiv 12 \pmod{5} \Leftrightarrow x \equiv 2 \pmod{5} \\ x \equiv 12 \pmod{3} \Leftrightarrow x \equiv 0 \pmod{3} \\ x \equiv 16 \pmod{17} \end{cases}$$

$$\Leftrightarrow \begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 6 \pmod{7} \\ x \equiv 2 \pmod{5} \\ x \equiv 0 \pmod{3} \\ x \equiv 16 \pmod{17} \end{cases}$$

$$M = 2 \cdot 7 \cdot 5 \cdot 3 \cdot 17 = 3570$$

$$M_2 = 2 \cdot 5 \cdot 3 \cdot 17 = 510, \quad M_3 = 2 \cdot 7 \cdot 3 \cdot 17 = 714$$

$$\text{et } M_4 = 2 \cdot 7 \cdot 5 \cdot 3 = 210.$$

$$* \quad \underbrace{510}_{490+20} x \equiv 1 \pmod{7} \Leftrightarrow 6x \equiv 1 \pmod{7} \quad \text{donc } x_2 = 6$$

$$* \quad \underbrace{714}_{170+540} x \equiv 1 \pmod{5} \Leftrightarrow 4x \equiv 1 \pmod{5} \quad \text{donc } x_3 = 4$$

$$* \quad \underbrace{210}_{170+40} x \equiv 1 \pmod{17} \Leftrightarrow 6x \equiv 1 \pmod{17} \quad \text{donc } x_4 = 3$$

$$\text{Ainsi } x = 6 \cdot 510 \cdot 6 + 2 \cdot 714 \cdot 4 + 16 \cdot 210 \cdot 3 = 34152 \equiv 2022 \pmod{3570}$$

$$S = \{2022 \pmod{3570}\}$$

Ou plus directement:

$$\begin{cases} x \equiv 6 \pmod{14} \\ x \equiv 12 \pmod{15} \\ x \equiv 16 \pmod{17} \end{cases} \quad \text{pgcd}(14, 15) = \text{pgcd}(14, 17) = \text{pgcd}(15, 17) = 1$$

$$M = 14 \cdot 15 \cdot 17 = 3570, \quad M_1 = 15 \cdot 17 = 255, \quad M_2 = 14 \cdot 17 = 238, \quad M_3 = 14 \cdot 15 = 210$$

$$* \quad 255x \equiv 1 \pmod{14} \Leftrightarrow 3x \equiv 1 \pmod{14} \quad \text{donc } x_1 = 5$$

$$* \quad 238x \equiv 1 \pmod{15} \Leftrightarrow 13x \equiv -2x \equiv 1 \pmod{15} \quad \text{donc } x_2 = 7$$

$$* \quad 210x \equiv 1 \pmod{17} \Leftrightarrow 6x \equiv 1 \pmod{17} \quad \text{donc } x_3 = 3$$

$$\text{Donc } x = 6 \cdot 5 \cdot 255 + 12 \cdot 7 \cdot 238 + 16 \cdot 3 \cdot 210 = 37722 \equiv 2022 \pmod{3570}$$

Problème 2

On a $589 = 19 \cdot 31$, $e = 7$.

On cherche d tel que $7d \equiv 1 \pmod{18 \cdot 30}$

$$540 = 7 \cdot 77 + 1 \text{ donc } d = -77 + 540 = 463$$

or il faut calculer $61^{463} \pmod{589}$

d	r	n	$61^{2^n} \pmod{589}$	Contributions
463	1	0	61	61
231	1	1	187	187
115	1	2	218	218
57	1	3	404	404
28	0	4	63	—
14	0	5	435	—
7	1	6	156	156
3	1	7	187	187
1	1	8	218	218

$$\text{donc } m = 61 \cdot 187 \cdot 218 \cdot 404 \cdot 156 \cdot 187 \cdot 218 \equiv$$

$$\equiv 61 \cdot 218 \cdot \underbrace{404^2}_{\equiv 63} \cdot 156 \equiv 123 \pmod{589}$$

Le rendez-vous est fixé au n° 123 Baker Street.

Problème 3

a) Commençons par résoudre $\overbrace{r^2 + r - 12}^{(r+4)(r-3)} = 0$, donc la solution de l'EHA est $y = C_1 e^{-4x} + C_2 e^{3x}$.

On cherche ensuite une solution particulière de l'équation différentielle

On essaie avec $y_p = a \cos(2x) + b \sin(2x)$

On a $y_p' = -2a \sin(2x) + 2b \cos(2x)$

$y_p'' = -4a \cos(2x) - 4b \sin(2x)$ donc

$$\begin{aligned} y_p'' + y_p' - 12y_p &= (-4a + 2b - 12a) \cos(2x) + \\ &+ (-4b - 2a - 12b) \sin(2x) = \\ &= (-16a + 2b) \cos(2x) + (-2a - 16b) \sin(2x) \end{aligned}$$

donc
$$\begin{cases} -16a + 2b = 0 & \Rightarrow b = 8a \\ -2a - 16b = 65 & \Rightarrow -130a = 65 \Rightarrow a = -\frac{1}{2} \end{cases}$$

or $b = -4$ Donc la solution générale est

$$y = -\frac{1}{2} \cos(2x) - 4 \sin(2x) + C_1 e^{-4x} + C_2 e^{3x}$$

b) $(4x^2 + 1) \cdot y' = (1 + 4x) \cdot y$ donc

$$\begin{aligned} \frac{y'}{y} &= \frac{1+4x}{4x^2+1} \quad \text{donc} \quad \ln(|y|) = \int \frac{1}{\underbrace{4x^2+1}_{(2x)^2+1}} dx + \\ &+ \int \frac{4x}{4x^2+1} dx = \frac{1}{2} \arctan(2x+1) + \frac{1}{2} \ln(4x^2+1) \end{aligned}$$

donc
$$y = e^{\frac{1}{2} \arctan(2x+1)} \cdot \sqrt{4x^2+1} \cdot C$$

Ex. 4

$$f: \mathbb{C} \rightarrow \mathbb{C}, \quad f(z) = \underbrace{\frac{1}{13}(5+12i)}_a z + \underbrace{4-32i}_b$$

a) Comme $|a| = \frac{1}{13} \sqrt{5^2 + 12^2} = 1$, il s'agit bien d'une isométrie propre.

C'est donc une translation ou une rotation, mais comme $a \neq 1$, c'est une rotation.

Calculons son centre (donc son PF): $f(z) = z$.

$$\frac{1}{13}(5+12i)z + 4-32i = z \quad (\Leftrightarrow)$$

$$\left(1 - \frac{1}{13}(5+12i)\right)z = 4-32i$$

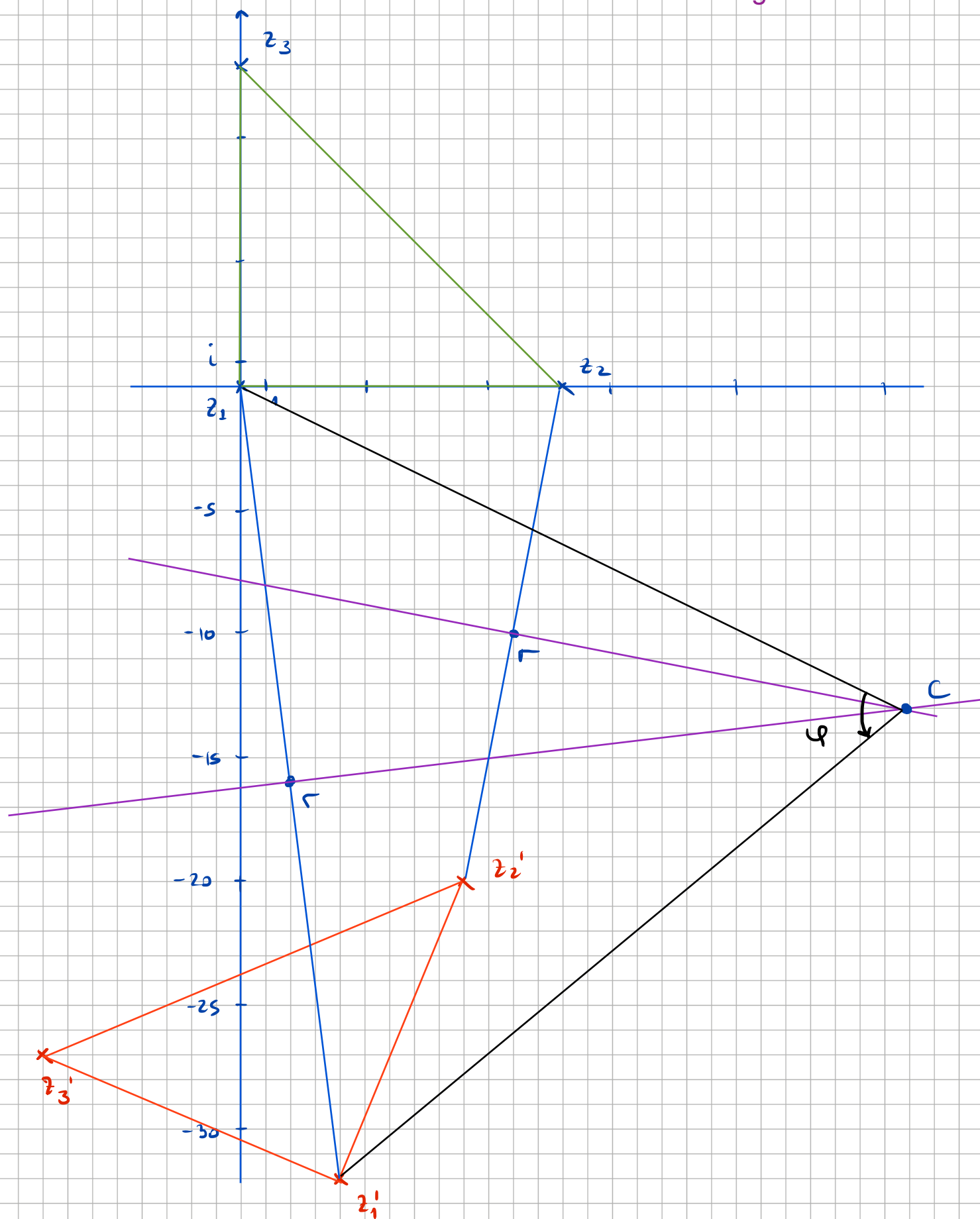
$$\begin{aligned} \frac{1}{13}(8-12i) \quad \text{donc} \quad z &= \frac{4-32i}{8-12i} \cdot 13 \cdot \frac{8+12i}{8+12i} = \\ &= \frac{\overbrace{13 \cdot 4 \cdot 4}^{208} (1-8i)(2+3i)}{\underbrace{64 + 144}_{208}} = 2 + 3i - 16i + 24 = \\ &= 26 - 13i. \end{aligned}$$

De plus, $a = \frac{1}{13}(5+12i)$, donc $\cos(\varphi) = \frac{5}{13}$
 $\Rightarrow \varphi \approx 67,38^\circ$.

C'est une rotation de centre $26-13i$ et d'angle $\varphi \approx 67,38^\circ$.

b) On calcule $f(0) = 4-32i$, $f(13) = 5+12i + 4-32i = 9-20i$ et $f(13i) = 5i-12 + 4-32i = -8-27i$.

Le centre de rotation est sur la médiatrice de $z_1 z_1'$ et sur celle de $z_2 z_2'$.



Problème 5

$$a) P_3(x) = f(a) + f'(a)(x-a) + \frac{f''(a)}{2!} (x-a)^2 + \frac{f'''(a)}{3!} (x-a)^3$$

$$f'(x) = -6 \sin(6x), \quad f'\left(\frac{\pi}{6}\right) = 0$$

$$f''(x) = -36 \cos(6x), \quad f''\left(\frac{\pi}{6}\right) = 36$$

$$f'''(x) = 216 \sin(6x), \quad f'''\left(\frac{\pi}{6}\right) = 0$$

$$\text{donc } P_3(x) = -1 + 18 \cdot (x - \frac{\pi}{6})^2$$

$$b) P_3\left(\frac{1}{2}\right) = -1 + 18 \left(\frac{1}{2} - \frac{\pi}{6}\right)^2 \approx -0,9899757602$$

$$(\cos(3) \approx -0,9899924966)$$

Problème 1

a) $m = 322$ Pour le décrypter, il faut calculer $322^{13} \bmod 493$.

13	1	322	287
6	0	154	38
3	1	52	-35
1	1	239	239

Donc $\equiv 475 \equiv (-18)$
 $322^{13} \equiv 322 \cdot 52 \cdot 239 \equiv$
 $\equiv 135 \bmod 493$.

b) On décrypte ensuite la signature $S = 287$, en calculant $287 \bmod 493$

$$S = \underbrace{287 \cdot (-35)}_{-185} \cdot 239 \equiv 155 \bmod 493.$$

Pour vérifier l'authenticité, on calcule $155^7 \bmod 437$ et on regarde si c'est égal à 135

$$155^7 \equiv 155 \cdot \underbrace{155^2}_{-10} \cdot \underbrace{155^4}_{100} \equiv -155000 \equiv 135 \bmod 437.$$

Comme $135 = m$, le message est fiable.

Problème 2

$$\text{Si } \underline{n=1} : 1^2 - 1 = 0 \text{ et } \frac{(1-1) \cdot 1 \cdot 2}{3} = 0$$

$$\text{Si } \underline{n=2} : 1^2 - 1 + 2^2 - 2 = 2 \text{ et } \frac{1 \cdot 2 \cdot 3}{3} = 2$$

Supposons ensuite l'égalité vraie pour n (HR) et calculons

$$\begin{aligned} & 1^2 - 1 + 2^2 - 2 + \dots + n^2 - n + (n+1)^2 - (n+1) \stackrel{\text{HR}}{=} \\ &= \frac{(n-1) \cdot n \cdot (n+1)}{3} + n^2 + 2n + \cancel{1} - n - \cancel{1} = \\ &= \frac{1}{3} ((n-1) \cdot n \cdot (n+1) + 3n(n+1)) = \frac{1}{3} (n(n+1)(\underbrace{n-1+3}_{=n+2})) \\ &= \frac{(n+1)-1 \cdot (n+1)(n+1+1)}{3} \quad \text{d'où le résultat.} \end{aligned}$$

Problème 3

a) On a
$$\begin{cases} u_0 = \sqrt{2} \\ u_{n+1} = \sqrt{1+u_n} \end{cases}, n \geq 0$$

b) Si la suite converge vers L , alors $L = \sqrt{1+L}$
donc $L^2 - L - 1 = 0$

donc $L \in \left\{ \frac{1 \pm \sqrt{5}}{2} \right\}$ et comme $L > 0$,

on en déduit que $L = \frac{1+\sqrt{5}}{2}$.

c) Vérifions que cette suite est croissante.

On définit la fonction f par $f(x) = \sqrt{1+x}$

Comme $f'(x) = \frac{1}{2\sqrt{1+x}} > 0$ pour tout $x > -1$,

la fonction est croissante.

Comme $u_0 = \sqrt{2} > 1$ et $u_{n+1} = f(u_n)$, la suite est croissante.

Montrons qu'elle est majorée par $\frac{1+\sqrt{5}}{2}$ par récurrence sur n .

$$u_0 = \sqrt{2} \approx 1,41 < 1,62 \approx \frac{1+\sqrt{5}}{2}$$

Si $u_n \leq \frac{1+\sqrt{5}}{2}$, alors $u_{n+1} = \sqrt{1+u_n} \leq$

$$\leq \sqrt{1 + \frac{1+\sqrt{5}}{2}} = \sqrt{\frac{1}{2}(3+\sqrt{5})} \text{ qui est } \leq \frac{1+\sqrt{5}}{2}$$

$$\Leftrightarrow \frac{1}{2}(3+\sqrt{5}) \leq \frac{1}{4}(1+2\sqrt{5}+5) = \frac{1}{2}(3+\sqrt{5})$$

ce qui est vrai.

La suite est croissante et majorée, elle est donc convergente.

Problème 4

On a
$$S = \sum_{i=1}^{3000} i = \frac{3000 \cdot 3001}{2} = 4\,501\,500$$

Calculons ensuite la somme des multiples de 7 et de 11 inférieurs à 3000 :

$$S_7 = 7 \cdot \sum_{i=1}^{\lfloor 3000/7 \rfloor} i = 7 \cdot \sum_{i=1}^{428} i = 7 \cdot \frac{428 \cdot 429}{2} = 642\,642$$

et
$$S_{11} = 11 \cdot \sum_{i=1}^{\lfloor 3000/11 \rfloor} i = 11 \cdot \sum_{i=1}^{272} i = 11 \cdot \frac{272 \cdot 273}{2} = 408\,408$$

Puis la somme des multiples de 77 inférieurs à 3000

$$S_{77} = 77 \cdot \sum_{i=1}^{\lfloor 3000/77 \rfloor} i = 77 \cdot \sum_{i=1}^{38} i = 77 \cdot \frac{38 \cdot 39}{2} = 57\,057$$

Le résultat cherché est

$$S - S_7 - S_{11} + S_{77} = 3\,507\,507$$

Problème 5

a) $u_k = \frac{5}{k(k+2)}$ (on a $\lim_{n \rightarrow \infty} u_k = 0$).

b) On a $\frac{5}{2} \left(\frac{1}{k-1} - \frac{1}{k+1} \right) = \frac{5}{2} \cdot \frac{\overbrace{k+1-k+1}^{=2}}{(k-1)(k+1)} =$

$= \frac{5}{(k-1)(k+1)}$ ou

utiliser plutôt
cette version :

$\frac{5}{2} \left(\frac{1}{k} - \frac{1}{k+2} \right) = \frac{5}{2} \left(\frac{k+2-k}{k(k+2)} \right) = \frac{5}{k(k+2)}$

c) $S_k = \underbrace{\frac{5}{1 \cdot 3}}_{u_1} + \underbrace{\frac{5}{2 \cdot 4}}_{u_2} + \underbrace{\frac{5}{3 \cdot 5}}_{u_3} + \dots + \underbrace{\frac{5}{k \cdot (k+2)}}_{u_k} =$

$= \frac{5}{2} \cdot \left(\sum_{i=1}^k \frac{1}{i} - \sum_{i=1}^k \frac{1}{i+2} \right) = \frac{5}{2} \cdot \left(\sum_{i=1}^k \frac{1}{i} - \sum_{i=3}^{k+2} \frac{1}{i} \right) =$

$= \frac{5}{2} \cdot \left(1 + \frac{1}{2} + \sum_{i=3}^k \frac{1}{i} - \sum_{i=3}^k \frac{1}{i} - \frac{1}{k+1} - \frac{1}{k+2} \right) =$

$= \frac{5(3(k+1)(k+2) - 2(k+2) - 2(k+1))}{4(k+1)(k+2)} = \frac{5(3k^2 + 5k)}{4(k+1)(k+2)}$

k^e Somme
partielle

d) Donc $\lim_{k \rightarrow \infty} S_k = \frac{15}{4}$

Problème 6

Posons $x = \text{nombre de bouteilles}$, $x \leq 1000$.

$$\begin{cases} x \equiv 23 \pmod{6} \\ x \equiv 2 \pmod{35} \end{cases} \Leftrightarrow \begin{cases} x \equiv 5 \pmod{6} \\ x \equiv 2 \pmod{35} \end{cases} \Leftrightarrow \begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \end{cases}$$

$$\Leftrightarrow \begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 2 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases}$$

$$N = 2 \cdot 3 \cdot 5 \cdot 7 = 210$$

On résout 1) $105x \equiv 1 \pmod{2} \Rightarrow x_1 = 1$

$$2) \underbrace{70x \equiv 1 \pmod{3}}_{\equiv 1 \pmod{3}} \Rightarrow x_2 = 1$$

$$3) 42x \equiv 1 \pmod{5} \Leftrightarrow 2x \equiv 1 \pmod{5} \Rightarrow x_3 = 3$$

$$4) \underbrace{30x \equiv 1 \pmod{7}}_{\equiv 2 \pmod{7}} \Rightarrow x_4 = 4$$

$$\text{Donc } x \equiv 1 \cdot 105 \cdot 1 + 2 \cdot 70 \cdot 1 + 2 \cdot 42 \cdot 3 + 2 \cdot 30 \cdot 4 \equiv$$

$$\equiv 737 \pmod{210} \Rightarrow \text{au maximum, il y a}$$

$$737 + 210 = \underline{\underline{947 \text{ bouteilles}}}$$

Problème 1

x = nombre de pièces. On a alors

$$\begin{cases} x \equiv 17 \pmod{26} \\ x \equiv 4 \pmod{13} \\ x \equiv 9 \pmod{14} \end{cases} \Leftrightarrow \begin{cases} x \equiv 17 \equiv 4 \pmod{13} \\ x \equiv 1 \pmod{2} \\ x \equiv 4 \pmod{13} \\ x \equiv 2 \pmod{7} \\ x \equiv 1 \pmod{2} \end{cases} \Leftrightarrow \begin{cases} x \equiv 4 \pmod{13} \\ x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{7} \end{cases}$$

On applique le thm chinois : $M = 13 \cdot 2 \cdot 7 = 182$,
 $M_1 = 14$, $M_2 = 91$, $M_3 = 26$.

On résout $14x \equiv 1 \pmod{13}$, donc $x_1 = 1$.

$91x \equiv 1 \pmod{2}$, donc $x_2 = 1$ et $\underset{\equiv 5}{26}x \equiv 1 \pmod{7}$ $\cdot 4$

$\underset{\equiv -4}{20x} \equiv 4 \pmod{7}$ donc $x_3 = -4$.

$$\text{Ainsi } x = 4 \cdot 1 \cdot 14 + 1 \cdot 1 \cdot 91 + 2 \cdot (-4) \cdot 26 = -61 \equiv 121 \pmod{182}.$$

Comme $600 \leq x \leq 700$, on a $x = 667$.

Problème 2

a) $e_3 = 5$ et $(p_3 - 1)(q_3 - 1) = 10 \cdot 22 = 220$ n'est pas
 on a $253 = 11 \cdot 23$

premier à 5, donc e_3 n'est pas inversible mod 220
 Il ne sera donc pas possible de trouver d_3 .

b) On a $n = 8$, donc Julien envoie $8^5 \pmod{133} = 50$.
 Il envoie $C = 50$.

c) Il faut la clé de décryptage de Julien. On résout
 $63x \equiv 1 \pmod{220}$.

$$220 = 3 \cdot 63 + 31$$

$$63 = 2 \cdot 31 + 1$$

$$(1, -5)$$

$$\text{donc } 1 = 63 - 2(220 - 3 \cdot 63)$$

$$= 7 \cdot 63 - 2 \cdot 220 \text{ et } d_3 = 7.$$

Pour décrypter, Julien calcule $148^7 \bmod 253$ et $185^7 \bmod 253$.

7	1	148	185
3	1	146	70
1	1	64	93

$$\text{donc } 148^7 \equiv \underbrace{148 \cdot 146 \cdot 64}_{\equiv 103} \equiv \underbrace{14}_{\equiv m} \bmod 253 \quad \text{et}$$

$$185^7 \equiv \underbrace{185 \cdot 70 \cdot 93}_{\equiv -48} \equiv \underbrace{70}_{\equiv 5} \bmod 253$$

Le nouveau rendez-vous est à 14h et

$$70^5 \equiv 14 \bmod 133, \text{ donc Julien peut s'y fier.}$$

Problème 5,

$$\text{a) } x_0 = 1, \quad x_1 = \frac{2}{5}, \quad x_2 = \frac{1 + \frac{2}{5}}{\frac{2}{5} + 3} = \frac{7}{19} \approx 0,368$$

$$\text{et } x_4 = \frac{1 + \frac{7}{19}}{\frac{7}{19} + 3} = \frac{26}{71} \approx 0,366$$

$$\text{b) On procède par récurrence : } x_0 = 1 > 0 \text{ et, si } x_n > 0, \text{ alors } x_{n+1} = \frac{1 + \overset{>0}{x_n}}{\underset{>0}{2x_n+3}} > 0.$$

$$\text{d) On a } x_1 - x_0 = \frac{2}{5} - 1 = -\frac{3}{5} < 0.$$

Supposons que $x_{n+1} - x_n \overset{HR}{< 0}$ et calculons

$$\begin{aligned} x_{n+2} - x_{n+1} &= \frac{1 + x_{n+1}}{2x_{n+1} + 3} - \frac{1 + x_n}{2x_n + 3} = \\ &= \frac{(1 + x_{n+1})(2x_n + 3) - (1 + x_n)(2x_{n+1} + 3)}{(2x_{n+1} + 3)(2x_n + 3)} = \\ &= \frac{2x_n + 3 + 2x_{n+1}x_n + 3x_{n+1} - 2x_{n+1} - 3 - 2x_nx_{n+1} - 3x_n}{(2x_{n+1} + 3)(2x_n + 3)} \\ &= \frac{2(x_n - x_{n+1}) - 3(x_n - x_{n+1})}{(2x_{n+1} + 3)(2x_n + 3)} = \frac{\overset{<0 \text{ par HR}}{x_{n+1} - x_n}}{\underset{>0}{(2x_{n+1} + 3)} \underset{>0 \text{ vu b)}}{(2x_n + 3)}} < 0 \end{aligned}$$

d'où le résultat. Donc la suite est décroissante.

c) La suite est décroissante vu c), et bornée par 0, vu b), donc elle est convergente.

Appelons L la limite, alors $L = \frac{1+L}{2L+3}$ car

$$2L^2 + 2L - 1 = 0, \quad L = \frac{-2 \pm \sqrt{12}}{4} = \frac{-1 \pm \sqrt{3}}{2}$$

$$L > 0, \text{ donc } L = \frac{\sqrt{3}-1}{2} \approx 0,366025.$$

Problème 4

a) Si $p=1$, $u_n = \frac{n+1}{2(n+2)} n$ et $\lim_{n \rightarrow \infty} u_n = \infty \neq 0$ donc la série diverge.

b) Si $p=-1$, $u_n = \frac{n+1}{2(n+2)} \cdot \frac{1}{n}$. (comparable à la série harmonique)

$$\text{On a } u_n = \frac{n+1}{2(n+2)} \cdot \frac{1}{n} \geq \frac{n+1}{4(n+1)} \cdot \frac{1}{n} = \frac{1}{4} \cdot \frac{1}{n}$$

$\frac{2n+4}{2n+4} \leq \frac{4n+4}{4n+4}$

dont la série diverge, car la série harmonique diverge, donc la série diverge par le critère de comparaison.

c) Si $p < -1$, $p = -k$ avec $k > 1$, et

$$u_n = \frac{n+1}{2(n+1)} \cdot \frac{1}{n^k}, \quad k > 1 \text{ (comparable à la série de Riemann)}$$

$$u_n = \frac{n+1}{2(n+2)} \cdot \frac{1}{n^k} \leq \frac{n+2}{2(n+2)} \cdot \frac{1}{n^k} = \frac{1}{2} \cdot \frac{1}{n^k}, \quad k > 1$$

dont la série converge (Riemann, $\alpha = k > 1$), donc la série converge par le critère de comparaison.

Problème 3

a) $(1-x^2) \cdot y' - 2xy = x^2, \quad x \in]-1; 1[.$

Donc $y' - \frac{2x}{1-x^2} \cdot y = \frac{x^2}{1-x^2}.$

Sol. de l'éq. homogène associée :

$$y = c \cdot e^{-\int \frac{2x}{1-x^2} dx} \quad \text{et} \quad \int \frac{2x}{1-x^2} dx = -\ln(\overset{>0}{1-x^2})$$

$$= \ln\left(\frac{1}{1-x^2}\right)^{(2)}$$

Donc $y_{(1)} = c \cdot \frac{1}{1-x^2}.$

Sol. particulière : on pose $y = C(x) \cdot \frac{1}{1-x^2}$ et

on remplace :

$$C'(x) \cdot \frac{1}{1-x^2} + C(x) \frac{-2x}{(1-x^2)^2} - \frac{2x}{1-x^2} \cdot \frac{C(x)}{1-x^2} = \frac{x^2}{1-x^2}$$

$$C'(x) = x^2 \quad \text{donc} \quad C(x) = \frac{1}{3} x^3.$$

et $y = c \cdot \frac{1}{1-x^2} + \frac{1}{3} x^3 \cdot \frac{1}{1-x^2}.$

Problème 3

$$b) \quad y'' + 2y' + 5y = e^{3x}$$

Pol. $y^2 + 2y + 5 = 0$, $\Delta = 4 - 20 = -16$

Sol. : $\frac{-2 \pm 4i}{2} = -1 \pm 2i$

Sol. eq. homogène : $y = e^{-x} (c_1 \cos(2x) + c_2 \sin(2x))$

Sol. particulière : $y_p = ae^{3x}$,

$y_p' = 3ae^{3x}$ or $y_p'' = 9ae^{3x}$

donc $e^{3x} = (9a + 6a + 5a)e^{3x}$

donc $a = \frac{1}{20}$.

Sol générale : $y = \frac{1}{20} e^{3x} + e^{-x} (c_1 \cos(2x) + c_2 \sin(2x))$
 $c_1, c_2 \in \mathbb{R}$

Problème 1

a) $x^2 - 6x + 5 = (x-5)(x-1)$

donc $\frac{4x-7}{x^2-6x+5} = \frac{A}{x-5} + \frac{B}{x-1}$

soit $4x-7 = A(x-1) + B(x-5)$ donc $\begin{cases} 4 = A+B \\ -7 = -A-5B \end{cases}$

d'où $B = \frac{3}{4}$ et $A = \frac{13}{4}$

Donc $\int \frac{4x-7}{x^2-6x+5} dx = \frac{13}{4} \ln|x-5| + \frac{3}{4} \ln|x-1| + C$

b) $A = \int x \cdot \cos^2(3x) dx ; \frac{1}{3} x \cdot \cos(3x) \cdot \sin(3x) +$

$f'(x) = \cos(3x), g(x) = x \cdot \cos(3x)$

$f(x) = \frac{1}{3} \sin(3x), g'(x) = \cos(3x) - \frac{1}{3} x \sin(3x)$

$-\frac{1}{3} \int \sin(3x) \cdot \cos(3x) dx - \frac{1}{9} \int x \cdot \underbrace{\sin^2(x)}_{=1-\cos^2(x)} dx =$

$= \underbrace{\frac{1}{3} x \cos(3x) \sin(3x) - \frac{1}{3} \cdot \frac{1}{2} \sin^2(3x) \cdot \frac{1}{3}}_{=B} - \frac{1}{9} \cdot \frac{1}{2} x^2 + \frac{1}{9} \underbrace{\int x \cdot \cos^2(3x) dx}_A$

donc $\frac{8}{9} A = B \Rightarrow A = \frac{9}{8} B$

Par conséquent, $A = \frac{3}{8} x \cos(3x) \sin(3x) - \frac{1}{16} \sin^2(3x) - \frac{1}{16} x^2 + C$

c) $x^4 - 2x^3 - 8x^2 = x^2(x^2 - 2x - 8) = x^2(x-4)(x+2)$

donc $\frac{13x^2-6x+8}{x^4-2x^3-8x^2} = \frac{A}{x} + \frac{B}{x^2} + \frac{C}{x-4} + \frac{D}{x+2}$

$\Rightarrow 13x^2 - 6x + 8 = A(x^3 - 2x^2 - 8x) + B(x^2 - 2x - 8) + C(x^3 - 4x^2) + D(x^3 + 2x^2)$

$\begin{cases} A+C+D=0 \\ -2A+B-4C+2D=13 \\ -8A-2B=-6 \\ -8B=8 \end{cases}$ donc $A=1$
donc $B=-1$

d'où $\begin{cases} C+D=-1 \\ -4C+2D=16 \end{cases} \Leftrightarrow -2C+D=8$ donc $C=-3, D=2$

$\Rightarrow \int = \ln|x| + \frac{1}{x} - 3 \ln|x-4| + 2 \ln|x+2| + C$

Problème 2

$$a) \quad x^4 y^2 dy = -3(x^6 + x^3 + 1) \cdot y^3 dx$$

$$\int \frac{1}{y} dy = \int \left(-3x^2 - \frac{3}{x} - \frac{3}{x^4} \right) dx$$

$$\text{donc } \ln(|y|) = -x^3 - 3\ln(|x|) + \frac{1}{x^3} + C$$

$$\text{donc } y = e^{-x^3 + \frac{1}{x^3}} \cdot e^{\ln(1/|x|^3)} \cdot e^C$$

$$\Rightarrow y = k \cdot \frac{1}{|x|^3} \cdot e^{-x^3 + \frac{1}{x^3}}$$

$$b) \quad y' + \frac{3}{x} \cdot y = x^3 + 2x^2$$

$$\text{On résout d'abord } y' + \frac{3}{x} \cdot y = 0 \Leftrightarrow \frac{y'}{y} = -\frac{3}{x}$$

$$\hookrightarrow \text{Solution: } y = C \cdot e^{-\int \frac{3}{x} dx} = C \cdot e^{-3\ln(|x|)} \\ = C \cdot \frac{1}{|x|^3}$$

On cherche ensuite une solution particulière de l'éq.

$$y' + \frac{3}{x} \cdot y = x^3 + 2x^2$$

$$\text{facteur intégrant: } e^{\int \frac{3}{x} dx} = e^{3\ln(|x|)} = x^3$$

$$\Rightarrow \underbrace{y' \cdot x^3 + y \cdot (3x^2)}_{(y \cdot x^3)'} = x^3 + 2x^2$$

$$\Rightarrow y \cdot x^3 = \frac{1}{4}x^4 + \frac{2}{3}x^3 + C$$

$$\text{donc } y = \frac{1}{4}x + \frac{2}{3} + \frac{C}{x^3}$$

$$\Rightarrow \text{Solution: } y = \frac{1}{4}x + \frac{2}{3} + \frac{C}{x^3}$$

$$c) \quad y'' - 5y' + 6y = e^{2x} + 5e^{4x} \quad (*)$$

$$\text{Eq. caractéristique: } r^2 - 5r + 6 = (r-2)(r-3)$$

$$\Rightarrow \text{sol. gén. de } y'' - 5y' + 6y: y = C_1 e^{2x} + C_2 e^{3x}$$

$$\text{Sol. particulière de } (*): a e^{2x} + b e^{4x} =: y_p(x)$$

$$y_p'(x): 2a e^{2x} + 4b e^{4x} \text{ et } y_p''(x) = 4a e^{2x} + 16b e^{4x}$$

$$\Rightarrow e^{2x} + 5e^{4x} = \underbrace{(4a - 10a + 6a)}_0 e^{2x} + \underbrace{(16b - 20b + 6b)}_{=12b} e^{4x}$$

Problème car e^{2x} est une sol. de l'éq. homogène associée (pb de résonance)

On cherche une sol. de $y'' - 5y' + 6y = e^{2x}$ de la forme $y_p = axe^{2x}$.

Donc $y_p' = ae^{2x} + 2axe^{2x}$ et $y_p'' = \underbrace{2ae^{2x} + 2ae^{2x} + 4axe^{2x}}_{4ae^{2x}}$

$$\Rightarrow e^{2x} = e^{2x}(4ax + 4a - 5a - 10ax + 6ax)$$

$$= e^{2x}(-a) \quad \text{donc } a = -1.$$

$\Rightarrow$ Sol. générale : $y = c_1 e^{2x} + c_2 e^{3x} + x e^{2x} + \frac{5}{2} e^{4x}$.

Problème 3

a) $7x + 48y = 1 \quad \begin{cases} 48 = 6 \cdot 7 + 6 \\ 7 = 6 \cdot 1 + 1 \end{cases} \quad \text{donc}$

$$1 = 7 - 6 = 7 - (48 - 6 \cdot 7) = -1 \cdot 48 + 7 \cdot 7.$$

Sol. : $\begin{cases} x = 7 + 48k \\ y = -1 - 7k \end{cases}, \quad k \in \mathbb{Z}.$

b) $\varphi(133) = \varphi(7 \cdot 19) = 6 \cdot 18 = 108 \quad 108 = 9 \cdot 11 + 9$

On résout $11x + 108y = 1$: $11 = 9 + 2$

$$9 = 4 \cdot 2 + 1$$

donc $1 = 9 - 4 \cdot 2 = 9 - 4(11 - 9) =$

$$= 5 \cdot 9 - 4 \cdot 11 = 5(108 - 9 \cdot 11) - 4 \cdot 11 = 5 \cdot 108 - 49 \cdot 11$$

Sol. : $\begin{cases} x = -49 + 108k \\ y = 5 - 11k \end{cases}, \quad k \in \mathbb{Z}.$

c) d_A : sol. de $7x \equiv 1 \pmod{4 \cdot 12 \stackrel{=48}{}}$ donc $d_A = \underline{7} \pmod{48}$.

d_B : sol. de $11x \equiv 1 \pmod{6 \cdot 18 \stackrel{=108}{}}$ donc $d_B = \underline{-49 + 108} \pmod{108} = \underline{59} \pmod{108}$.

d) $S = m^{d_A} = 27^7 \pmod{65}$

$$27^2 \equiv 14 \pmod{65}, \quad 27^4 \equiv 196 \equiv 1 \pmod{65}$$

donc $27^7 \equiv 27 \cdot 14 \equiv 53 \pmod{65}$. Donc $\underline{S = 53}$.

e) Le message codé est $(M^M \bmod 133; s^M \bmod 133)$
avec $M=27$ et $s=53$.

M	1	$27 \bmod 133$	$53 \bmod 53$
5	1	64	16
2	0	106	-10
1	1	64	100

donc $27^M \equiv 27 \cdot 64^2 \equiv 27 \cdot 106 \equiv 69 \bmod 133$ et

$53^M \equiv 53 \cdot 16 \cdot 100 \equiv 79 \bmod 133$.

Elle envoie $(69, 79)$.

f) Bernt va calculer $69^{59} \bmod 133$. Il devrait obtenir 27
puis $79^{59} \bmod 133$. Il devrait obtenir 53 et
vérifier si $53^7 \equiv 27 \bmod 65$ pour en connaître l'authenticité.

Problème 4

(A) $f(z) = \underbrace{\frac{1}{5}(3-4i)}_{=: a} \cdot \bar{z} + \underbrace{(-9-3i)}_b$ (similitude indirecte)

a) c'est le cas si $|a|=1$ et qu'il n'y a pas de point fixe.

$|a| = \frac{1}{5} \sqrt{3^2 + (-4)^2} = 1$: donc c'est une isométrie.

De plus, $f(z) = z \Leftrightarrow \frac{1}{5}(3-4i)(x-yi) - 9-3i = x+yi \cdot 1.5$
avec $z = x+yi$

$\Leftrightarrow 3x - 3yi - 4xi - 4y - 45 - 15i = 5x + 5yi$

$\Leftrightarrow (-2x - 4y - 45) + (-8y - 4x - 15)i = 0$

$\Leftrightarrow \begin{cases} 2x + 4y = -45 \\ 4x + 8y = -15 \end{cases}$ et ce système n'a pas de solution.

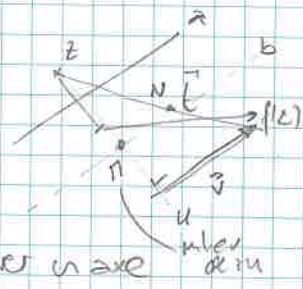
b) $z_1' = f(z_1) = f(0) = -9-3i$

$z_2' = f(z_2) = f(5) = 3-4i - 9-3i = -6-7i$

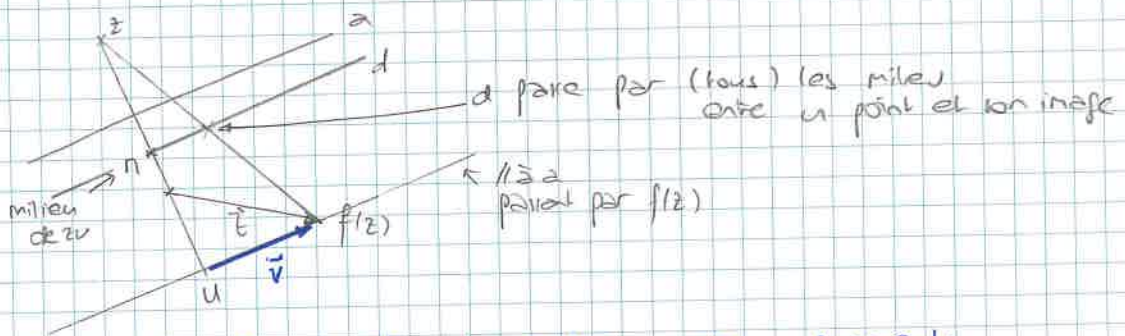
$z_3' = f(z_3) = f(5i) = -3i - 4 - 9-3i = -13-6i$.

c) Sur f. axe. (de sym) et un vect. de translation // à l'axe.

$\vec{v}$: image d'un point de b. (par N = lieu de $[z f(w)]$ et // à $\vec{a}$)



c) On veut un vecteur de translation $\parallel$ à l'axe de symétrie



Soit π_1 , π_2 et π_3 les milieux des segments $[z_1 z'_1]$, $[z_2 z'_1]$ et $[z_3 z'_1]$. Alors l'axe d cherché passe par π_1 , π_2 et π_3 .

Soit $\tilde{z}_2$ le symétrique de z_2 par rapport à d ,

$$\text{alors } \vec{v} = \overrightarrow{\tilde{z}_2 z'_2}$$

d) On a $M_1 = \frac{1}{2}(0 + (-9 - 3i)) = -\frac{9}{2} - \frac{3}{2}i$, $\pi_1(-\frac{9}{2}; -\frac{3}{2})$

$$M_2 = \frac{1}{2}(5 - 6 - 7i) = -\frac{1}{2} - \frac{7}{2}i, \pi_2(-\frac{1}{2}; -\frac{7}{2}), \overrightarrow{\pi_1 \pi_2} = \begin{pmatrix} 4 \\ -2 \end{pmatrix}$$

$$\text{donc (d): } \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1/2 \\ -7/2 \end{pmatrix} + k \begin{pmatrix} 4 \\ -2 \end{pmatrix} \Leftrightarrow \begin{cases} x = -\frac{1}{2} + 4k \\ y = -\frac{7}{2} - 2k \end{cases}$$

$$\text{On a } x + 2y = -\frac{15}{2} \Leftrightarrow 2x + 4y + 15 = 0$$

Soit n : normale à d , passant par $z_2(5; 0)$

$$(n): 2x - y = 10$$

$$\pi \in n \cap d:$$

$$\pi(\frac{5}{2}; -5)$$

$$\pi = \begin{cases} 2x + 4y = -15 \\ 2x - y = 10 \end{cases} \quad 5y = -25, y = -5$$

$$\overrightarrow{O\tilde{z}_2} = \overrightarrow{O\pi} + \tilde{z}_2 \pi = \begin{pmatrix} 5/2 \\ -5 \end{pmatrix} + \begin{pmatrix} -5/2 \\ -5 \end{pmatrix} = \begin{pmatrix} 0 \\ -10 \end{pmatrix}, \tilde{z}_2(0; -10)$$

$$\vec{v} = \overrightarrow{\tilde{z}_2 z'_2} = \begin{pmatrix} -6 \\ 3 \end{pmatrix}$$

(B) MAS :

Il faut construire les images de a, b, α et β .

[α] : Demi-cercle passant par Ω le centre de γ .
Donc α' est une droite qui passe par les points
 $P, P' \in \gamma \cap \alpha$. une portion de droite.

Appelons A et $\tilde{A}$ les extrémités de a et déterminons leurs images A' et $\tilde{A}'$.

A' : $M = \text{milieu de } [A\Omega], T_A \in \text{Car}(M; A) \cap \gamma$.
 $A' \in \text{per}_{(A\Omega)}(T_A)$

Idem pour

$\tilde{A}'$: $N = \text{milieu de } [\tilde{A}\Omega], T_{\tilde{A}} \in \text{Car}(N; \tilde{A}) \cap \gamma$.
 $\tilde{A}' \in \text{per}_{(\tilde{A}\Omega)}(T_{\tilde{A}})$

$\Rightarrow \alpha' = \text{droite } (PP')$ sauf le segment $[A'\tilde{A}']$.

[$\Rightarrow$] : l'image de a est une portion de cercle (qui passe par A' et $\tilde{A}'$, et par $Q \in a \cap \gamma$).

$C \in \text{médiane de } [A'\tilde{A}']$ et celle de $[Q\tilde{A}']$

Image de a = arc de cercle, centre en C , entre $\tilde{A}'$ et A' .

[β] : Image de β = portion de droite passant par Q et L' l'image de L (où $b = [QL]$).

En fait $L' = C$ ($Q = \text{milieu de } [L\Omega]$, donc $P = T_L$).

$\beta' = [QC]$ (l'image du centre)

[b] : l'image de b est une portion de cercle, passant par Q et C et R' , l'image de R , le milieu de b .

d) L'axe de symétrie passe par les points M_1 et M_2 , milieux respectifs des segments $[Z_1 Z_1']$ et $[Z_2 Z_2']$

$$m_1 = \frac{1}{2} (0 + 1 - 9 - 3i) = -\frac{9}{2} - \frac{3}{2}i, \quad M_1 \left(-\frac{9}{2}; -\frac{3}{2}\right)$$

$$M_2 = \frac{1}{2} (5 - 6 - 7i) = -\frac{1}{2} - \frac{7}{2}i, \quad M_2 \left(-\frac{1}{2}; -\frac{7}{2}\right)$$

$$\star \text{ Axe: } \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} -1/2 \\ -7/2 \end{pmatrix} + k \begin{pmatrix} 4 \\ -2 \end{pmatrix} \Leftrightarrow \begin{cases} x = -\frac{1}{2} + 4k \\ y = -\frac{7}{2} - 2k \end{cases}$$

$$\text{donc } x + 2y = -\frac{15}{2} \Leftrightarrow 2x + 4y + 15 = 0.$$

$\star$ Vecteur de translation:

Le comité des footballeurs de Chamblandes est parvenu à trouver un terrain pour créer un terrain de football synthétique, de 105 m de long et 68 m de large.

Le premier jour, ils commencent par couvrir 1500 m^2 . Chaque jour qui suit, ils couvrent les trois quarts de la surface posée la veille. Parviendront-ils à finir le terrain (justifier) ?

La surface du terrain vaut $105 \cdot 68 = 7140$

$$1500 \left(1 + \frac{3}{4} + \left(\frac{3}{4} \right)^2 + \cdots \right) = \lim_{n \rightarrow \infty} \sum_{k=0}^n 1500 \left(\frac{3}{4} \right)^k = 1500 \frac{1}{1 - \frac{3}{4}} = 6000 < 7140.$$

1. Étudier la convergence de $\frac{1}{\ln(2)} - \frac{1}{\ln(3)} + \frac{1}{\ln(4)} - \frac{1}{\ln(5)} + \dots + \frac{(-1)^k}{\ln(k)} + \dots$
 2. Étudier la croissance de la fonction $f(x) = \ln(x) - x$ puis montrer que $\ln(x) < x - 1$ si $x > 1$.
 3. Étudier la convergence absolue de $\frac{1}{\ln(2)} - \frac{1}{\ln(3)} + \frac{1}{\ln(4)} - \frac{1}{\ln(5)} + \dots + \frac{(-1)^k}{\ln(k)} + \dots$
 4. Prouver que la fonction $f(x) = \frac{x}{(x^2 + 1)^p}$ est décroissante si $p > \frac{1}{2}$ pour $x > \frac{1}{2p-1}$.
 5. Étudier la convergence des séries $\sum_{n=1}^{\infty} \frac{n}{(n^2 + 1)^p}$ avec $p \in]\frac{1}{2}; \infty[$ grâce au critère de l'intégrale.
-

1. $f(x) = \ln(x)$ est croissante donc la série $u_n = \frac{1}{\ln(n)}$ est décroissante.
On a $\lim_{n \rightarrow \infty} \frac{1}{\ln n} = 0$ et la série est alternée donc elle converge.
2. $f'(x) = \frac{1}{x} - 1 = \frac{1-x}{x}$ qui est négative à partir de $x = 1$. De plus $f(1) = \ln 1 - 1 = -1$ ainsi $\ln x - x < -1$ ce qui donne $\ln x < x - 1$ qui nous donne finalement $\ln x + 1 < x$.
3. Elle ne converge pas absolument car $\frac{1}{\ln(x+1)} > \frac{1}{x}$. Donc la somme terme à terme des valeurs absolues des termes de la série est supérieure terme à terme à la série harmonique qui diverge.
4. $f'(x) = \frac{(x^2 + 1)^p - x p (x^2 + 1)^{p-1} 2x}{(x^2 + 1)^{2p}} = \frac{(x^2 + 1)^{p-1} [x^2 + 1 - 2px^2]}{(x^2 + 1)^{2p}}$
 $f'(x) = \frac{1 - x^2(2p-1)}{(x^2 + 1)^{p+1}} = \frac{(1 - x\sqrt{2p-1})(1 + x\sqrt{2p-1})}{(x^2 + 1)^{p+1}}$ qui est négative avec nos conditions.
5. $I(p) = \int_1^{\infty} \frac{n \, dn}{(n^2 + 1)^p} = \frac{1}{2} \int_1^{\infty} \frac{2n \, dn}{(n^2 + 1)^p}$ avec $p \in]\frac{1}{2}; \infty[$.
Si $p \neq 1$ on a $I(p) = \frac{(n^2 + 1)^{2(1-p)}}{1-p} \Big|_1^{\infty}$ qui diverge si $p \in]\frac{1}{2}; 1[$ et converge si $p > 1$.
 $I(1) = \frac{\ln(n^2 + 1)}{2} \Big|_1^{\infty} = \infty$ donc diverge.
Au final la série converge uniquement si $p > 1$.

1. Déterminer le polynôme de Taylor de degré cinq de la fonction $f(x) = e^x$ pour $a = 0$.
 2. Utiliser le résultat précédent pour estimer e .
 3. Sachant que $e < 3$, quelle est l'imprécision de cette estimation ?
-

1. $P_5(x) = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \frac{x^4}{4!} + \frac{x^5}{5!}$.
2. $e \approx P_5(1) = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \frac{1}{5!} = \frac{240 + 60 + 20 + 5 + 1}{120} = \frac{326}{120} = \frac{163}{60} = 2,7\overline{16}$.
3. $R_5(1) \leq \frac{e^c}{6!}$ où $c \in [0, 1]$ et comme $e \leq 3$ nous avons donc $R_5(1) \leq \frac{3}{6!} = \frac{1}{240} \approx 0,0041$.

Déterminer tous les points à coordonnées entières situés sur la droite $637x - 119y = 35$ et à l'intérieur du disque de rayon 150 centré à l'origine.

$$\begin{aligned} 637 &= 119 \cdot 5 + 42 & \implies & 42 = 637 - 119 \cdot 5 \\ 119 &= 42 \cdot 2 + 35 & \implies & 35 = 119 - 42 \cdot 2 \\ 42 &= 35 \cdot 1 + 7 & \implies & 7 = 42 - 35 \cdot 1 \\ 35 &= 7 \cdot 5 \end{aligned}$$

$\text{pgcd}(637; 119) = 7$ divise 35 : l'équation diophantienne admet une infinité de solutions.

$$\begin{aligned} 7 &= 42 - 35 \cdot 1 \\ &= 42 - (119 - 42 \cdot 2) \cdot 1 = 119 \cdot (-1) + 42 \cdot 3 \\ &= 119 \cdot (-1) + (637 - 119 \cdot 5) \cdot 3 = 637 \cdot 3 - 119 \cdot 16 \end{aligned}$$

Donc $637x - 119y = 35$ admet la solution particulière $(15; 80)$.

La solution générale est $\begin{cases} x = 15 - \frac{-119}{7}k = 15 + 17k \\ y = 80 + \frac{637}{7}k = 80 + 91k \end{cases} \quad (k \in \mathbb{Z})$

Cherchons pour quelles valeurs de k ces points sont à l'intérieur du disque $x^2 + y^2 \leq 150^2$:

$$(15 + 17k)^2 + (80 + 91k)^2 \leq 150^2$$

$$8570k^2 + 15\,070k - 15\,875 \leq 0$$

$$\Delta = 15\,070^2 - 4 \cdot 8570 \cdot (-15\,875) = 771\,299\,900$$

$$k_1 = \frac{-15\,070 - \sqrt{771\,299\,900}}{2 \cdot 8570} \approx -2,5 \quad \text{et} \quad k_2 = \frac{-15\,070 + \sqrt{771\,299\,900}}{2 \cdot 8570} \approx 0,741$$

En conclusion, trois points satisfont les conditions posées :

$$k = -2 \text{ donne } (-19; -102);$$

$$k = -1 \text{ donne } (-2; -11);$$

$$k = 0 \text{ donne } (15; 80).$$

Trois paysans partagent équitablement leur production de riz, qu'ils vont vendre dans différents marchés, où l'on use de sacs contenant respectivement 83 onces, 110 onces et 135 onces.

Lorsqu'ils se retrouvent, ils se félicitent d'avoir réussi à vendre tous les sacs qu'ils pouvaient, si bien qu'il reste 32 onces au premier paysan, 70 onces au deuxième et 30 onces au dernier. Combien d'onces, au minimum, les paysans ont-ils produit ?

Si x désigne le nombre d'onces que chaque paysan emporte au marché, il s'agit de résoudre le système de congruences :

$$\begin{cases} x \equiv 32 \pmod{83} \\ x \equiv 70 \pmod{110} \\ x \equiv 30 \pmod{135} \end{cases}$$

Comme $110 = 5 \cdot 22$ et $135 = 5 \cdot 27$, on observe d'abord que :

$$\begin{cases} x \equiv 32 \pmod{83} \\ x \equiv 70 \pmod{110} \\ x \equiv 30 \pmod{135} \end{cases} \iff \begin{cases} x \equiv 32 \pmod{83} \\ x \equiv 70 \pmod{22} \\ x \equiv 70 \pmod{5} \\ x \equiv 30 \pmod{5} \\ x \equiv 30 \pmod{27} \end{cases} \iff \begin{cases} x \equiv 32 \pmod{83} \\ x \equiv 4 \pmod{22} \\ x \equiv 0 \pmod{5} \\ x \equiv 3 \pmod{27} \end{cases}$$

avant de pouvoir appliquer le théorème chinois des restes.

$$M = 83 \cdot 22 \cdot 5 \cdot 27 = 246\,510$$

$$M_1 = \frac{246\,510}{83} = 2970, M_2 = \frac{246\,510}{22} = 11\,205, M_3 = 42\,302, M_4 = 9130.$$

$$\begin{aligned} 1. \quad 2970x &\equiv 1 \pmod{83} &\iff -18x &\equiv 1 \pmod{83} \\ 83 &= 18 \cdot 4 + 11 &\implies 11 &= 83 - 18 \cdot 4 \\ 18 &= 11 \cdot 1 + 7 &\implies 7 &= 18 - 11 \cdot 1 \\ 11 &= 7 \cdot 1 + 4 &\implies 4 &= 11 - 7 \cdot 1 \\ 7 &= 4 \cdot 1 + 3 &\implies 3 &= 7 - 4 \cdot 1 \\ 4 &= 3 \cdot 1 + 1 &\implies 1 &= 4 - 3 \cdot 1 \\ 3 &= 1 \cdot 3 \end{aligned}$$

$$\begin{aligned} 1 &= 4 - 3 \cdot 1 = 4 - (7 - 4 \cdot 1) \cdot 1 = 7 \cdot (-1) + 4 \cdot 2 = 7 \cdot (-1) + (11 - 7 \cdot 1) \cdot 2 = 11 \cdot 2 + 7 \cdot (-3) = \\ &= 11 \cdot 2 + (18 - 11 \cdot 1) \cdot (-3) = 18 \cdot (-3) + 11 \cdot 5 = 18 \cdot (-3) + (83 - 18 \cdot 4) \cdot 5 = 83 \cdot 5 - 18 \cdot 23 \end{aligned}$$

On a trouvé, grâce à l'algorithme d'Euclide, $x \equiv 23 \pmod{83}$

$$\begin{aligned} 2. \quad 11\,205x &\equiv 1 \pmod{22} &\iff 7x &\equiv 1 \pmod{22} \quad | \cdot (-3) &\iff x &\equiv -3 \pmod{22} \\ 3. \quad 42\,302x &\equiv 1 \pmod{5} &\iff 2x &\equiv 1 \pmod{5} \quad | \cdot 3 &\iff x &\equiv 3 \pmod{5} \\ 4. \quad 9\,130x &\equiv 1 \pmod{27} &\iff 4x &\equiv 1 \pmod{27} \quad | \cdot 7 &\iff x &\equiv 7 \pmod{27} \end{aligned}$$

La solution du système de congruences est donc :

$$32 \cdot 2970 \cdot 23 + 4 \cdot 11\,205 \cdot (-3) + 0 \cdot 42\,302 \cdot 3 + 3 \cdot 9130 \cdot 7 \equiv 24\,600 \pmod{246\,510}$$

Les paysans ont produit, au minimum, 73 800 onces de riz.

Alice a pour clé publique $(407, 7)$, alors que Bob a pour clé publique $(1763, 13)$.

1. Quel message crypté faut-il envoyer à Alice pour lui transmettre le message 18 ?
2. Sachant que Bob a choisi deux nombres premiers p et q très proches l'un de l'autre, quelle signature (qu'on ne demande pas de crypter) fera croire à Alice que Bob en est l'auteur ?

1. Il s'agit de calculer $18^7 \bmod 407$:

x	reste r	n	$18^{2^n} \bmod 407$	contribution
7	1	0	18	18
3	1	1	$18^2 \equiv -83$	-83
1	1	2	$(-83)^2 \equiv -30$	-30

$$18^7 \equiv 18 \cdot (-83) \cdot (-30) \equiv 50 \bmod 407$$

Le message crypté est donc 50.

2. $\sqrt{1763} \approx 41,99$ mène rapidement à $1763 = 41 \cdot 43$.

$$\text{Donc } \varphi(1763) = 40 \cdot 42 = 1680.$$

Pour trouver la clé privée de Bob, cherchons une solution particulière à l'équation diophantienne $13x + 1680y = 1$:

$$1680 = 13 \cdot 129 + 3 \quad \implies \quad 3 = 1680 - 13 \cdot 129$$

$$13 = 3 \cdot 4 + 1 \quad \implies \quad 1 = 13 - 3 \cdot 4$$

$$3 = 1 \cdot 3$$

$$1 = 13 - 3 \cdot 4 = 13 - (1680 - 13 \cdot 129) \cdot 4 = 13 \cdot 517 + 1680 \cdot (-4)$$

Bob a pour clé privée $d_B = 517$.

La signature du message est donc $18^{517} \bmod 1763$:

x	reste r	n	$18^{2^n} \bmod 1763$	contribution
517	1	0	18	18
258	0	1	$18^2 \equiv 324$	
129	1	2	$324^2 \equiv 959$	959
64	0	3	$959^2 \equiv 1158$	
32	0	4	$1158^2 \equiv 1084$	
16	0	5	$1084^2 \equiv 898$	
8	0	6	$898^2 \equiv 713$	
4	0	7	$713^2 \equiv 625$	
2	0	8	$625^2 \equiv 1002$	
1	1	9	$1002^2 \equiv 857$	857

$$18^7 \equiv 18 \cdot 959 \cdot 857 \equiv 201 \bmod 1763$$

La signature, non cryptée du message, est ainsi 201.