

CORRIGÉ DU CONTRÔLE 2

Exercice 1 : le problème des restes chinois

Étant donné des nombres entiers a_1, a_2, n_1 et n_2 , le problème des restes chinois consiste à chercher un entier x tel que

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$$

Nous commencerons par étudier deux exemples puis proposerons une généralisation.

1. Considérons $n_1 = 15$ et $n_2 = 67$.

(a) Trouver un nombre entier α_1 tel que $67\alpha_1 \equiv 1 \pmod{15}$.

Commençons par réduire 67 modulo 15 : $67 \equiv 7 \pmod{15}$. Pour trouver α_1 , on peut faire un tableau de congruence dans $\mathbf{Z}/15\mathbf{Z}$:

$\bar{\alpha}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\bar{10}$	$\bar{11}$	$\bar{12}$	$\bar{13}$	$\bar{14}$
$7\bar{\alpha}$	$\bar{0}$	$\bar{7}$	$\bar{14}$	$\bar{6}$	$\bar{13}$	$\bar{5}$	$\bar{12}$	$\bar{4}$	$\bar{11}$	$\bar{3}$	$\bar{10}$	$\bar{2}$	$\bar{9}$	$\bar{1}$	$\bar{8}$

On trouve ainsi une solution $\alpha_1 = 13$ puisque $7 \cdot 13 \equiv 1 \pmod{15}$.

On aurait aussi remarquer plus rapidement que $\bar{67} \cdot \bar{2} = \bar{7} \cdot \bar{2} = \bar{14} = -\bar{1}$. Ainsi $\bar{67} \cdot (-\bar{2}) = \bar{1}$. Le nombre -2 est donc aussi solution.

(b) Déterminer l'égalité de Bézout pour $n_1 = 15$ et $n_2 = 67$.

Appliquons l'algorithme d'Euclide :

Divisons 67 par 15 : $67 = 4 \cdot 15 + 7$.

Divisons 15 par 7 : $15 = 2 \cdot 7 + 1$.

On obtient un reste égal à 1, l'algorithme s'arrête. On en déduit sans surprise que 67 et 15 sont premiers entre eux et on obtient l'égalité de Bézout à partir des égalités ci-dessus :

$$1 = 15 - 2 \cdot 7 = 15 - 2(67 - 4 \cdot 15) = -2 \cdot 67 + 9 \cdot 15.$$

Remarque : on aurait aussi pu déduire l'égalité de Bézout de la première question : on a vu que $67 \cdot 13 \equiv 1 \pmod{15}$. Plus précisément, cette relation vient de l'égalité $67 \cdot 13 = 1 + 15 \cdot 58$. Il en découle $67 \cdot 13 - 15 \cdot 58 = 1$, c'est une égalité de Bézout (différente de celle trouvée ci-dessus).

(c) En déduire un nombre entier α_2 tel que $15\alpha_2 \equiv 1 \pmod{67}$.

Réduisons l'égalité ci-dessus modulo 67 : comme $-2 \cdot 67 + 9 \cdot 15 = 1$, on en déduit $9 \cdot 15 \equiv 1 \pmod{67}$. Ainsi $\alpha_2 = 9$ est une solution.

Remarquons qu'en réduisant l'égalité de Bézout modulo 15, on obtient $-2 \cdot 67 \equiv 1 \pmod{15}$. On obtient ainsi une solution $\alpha_1 = -2$ à la question 1. C'est cohérent avec notre réponse précédente puisque $-2 \equiv 13 \pmod{15}$.

- (d) Soient a_1 et a_2 des nombres entiers et $x = 67\alpha_1 a_1 + 15\alpha_2 a_2$.
Que vaut x modulo 15 et modulo 67 ?

Comme $67\alpha_1 \equiv 1 \pmod{15}$, on déduit

$$x \equiv (67\alpha_1)a_1 + 0 \equiv a_1 \pmod{15}.$$

De même, $15\alpha_2 \equiv 1 \pmod{67}$, donc

$$x \equiv 0 + (15\alpha_2)a_2 \equiv a_2 \pmod{67}.$$

- (e) En déduire l'expression (qu'on ne demande pas d'évaluer) d'une solution du problème

$$\begin{cases} x \equiv 2 \pmod{15} \\ x \equiv -1 \pmod{67} \end{cases}$$

Cette solution est-elle unique ?

La question précédente nous fournit une solution à ce problème en prenant $a_1 = 2$ et $a_2 = -1$. Une solution est donc $x = 67 \cdot 13 \cdot 2 + 15 \cdot 9 \cdot (-1)$ (elle vaut 1607).

Cette solution n'est pas unique. L'égalité de Bézout n'est en effet pas unique et nous aurions pu trouver d'autres nombres α_1 et α_2 solutions des questions 1 et 3. La solution x correspondante aurait alors été différente de celle-ci. Par exemple, avec $\alpha_1 = -2$ et $\alpha_2 = 9 + 67 = 76$, on trouve une nouvelle solution $x' = 67 \cdot (-2) \cdot 2 + 15 \cdot 76 \cdot (-1)$ (qui vaut -1408).

2. Considérons maintenant $n_1 = 15$ et $n_2 = 50$. Démontrer que le problème

$$\begin{cases} x \equiv 2 \pmod{15} \\ x \equiv 3 \pmod{50} \end{cases}$$

n'a pas de solution $x \in \mathbf{Z}$.

Ce système n'a pas de solution car 15 et 50 ne sont pas premiers entre eux : ils ont 5 pour facteur commun. Regardons cela en détail :

Supposons par l'absurde qu'une solution $x \in \mathbf{Z}$ existe. On a alors $x \equiv 2 \pmod{15}$ et $x \equiv 3 \pmod{50}$. Traduisons : il existe des entiers k et ℓ tels que $x = 2 + 15k$ et $x = 3 + 50\ell$. Ainsi $2 + 15k = 3 + 50\ell$, donc $15k - 50\ell = 1$. Or 5 divise $15k$ et 50ℓ . Il divise donc leur différence. Donc 5 divise 1, ce qui est absurde. On en déduit que le problème n'a pas de solution $x \in \mathbf{Z}$.

3. Soient n_1 et n_2 des nombres premiers entre eux, et a_1, a_2 des nombres entiers.
En vous appuyant sur la méthode employée dans le premier exemple, démontrer qu'il existe un nombre entier x tel que

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \end{cases}$$

Comme n_1 et n_2 sont premiers entre eux, on peut appliquer le théorème de Bézout : il existe des entiers u et v tels que $n_1u + n_2v = 1$.

Alors on en déduit $n_1u \equiv 1 \pmod{n_2}$ et $n_2v \equiv 1 \pmod{n_1}$.

Posons $x = n_1ua_2 + n_2va_1$.

D'après ce qui précède, on obtient en réduisant x modulo n_2 :

$$x \equiv 0 + (n_2v)a_1 \equiv a_1 \pmod{n_1}.$$

Et de même

$$x \equiv (n_1u)a_2 \equiv a_2 \pmod{n_2}.$$

Nous avons ainsi bien démontré qu'il existait un entier x solution du système de congruences.

Notre preuve contient même la méthode effective pour trouver x : elle repose sur l'égalité de Bézout pour n_1 et n_2 que l'on sait établir grâce à l'algorithme d'Euclide.

L'exemple de la question 2 montre que l'hypothèse « n_1 et n_2 premiers entre eux » est importante. Sans elle, on ne peut pas toujours garantir l'existence d'une solution au système de congruence.

Dernière remarque : le problème des restes chinois s'étend à des systèmes de congruences de plus de deux équations. Il doit son nom au fait qu'on en retrouve la trace dans de très vieux traités de mathématiques chinois.

Exercice 2 : une lemniscate

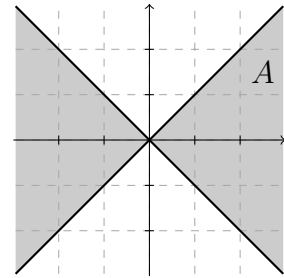
Le but de ce problème est d'étudier l'ensemble

$$E = \{(r \cos(t), r \cos(t) \sin(t)) ; r \in [0, 1], t \in \mathbf{R}\}.$$

1. Soit A l'ensemble représenté ci-contre. Le bord de A est constitué de deux droites qui font partie de A .

Donner, sans justification, une définition mathématique de A .

Remarque : l'utilisation de la valeur absolue peut permettre de définir A simplement.



L'ensemble A est délimité par les droites d'équations $y = x$ et $y = -x$. Mais il faut distinguer deux cas pour décrire les deux parties de A :

$$A = \{(x, y) \in \mathbf{R}^2 \mid x \geq 0 \text{ et } -x \leq y \leq x\} \cup \{(x, y) \in \mathbf{R}^2 \mid x \leq 0 \text{ et } x \leq y \leq -x\}.$$

Nous avons utilisé des inégalités larges car le bord de A fait partie de A . Cette écriture de A peut être simplifiée en utilisant des valeurs absolues :

$$A = \{(x, y) \in \mathbf{R}^2 \mid |x| \geq |y|\}.$$

2. Démontrer $E \subset A$.

Soit $(x, y) \in E$. Par définition de E , il existe $r \in [0, 1]$ et $t \in \mathbf{R}$ tels que $(x, y) = (r \cos(t), r \cos(t) \sin(t))$. On sait que $|\sin(t)| \leq 1$. On en déduit

$$|y| = |r \cos(t) \sin(t)| = |r \cos(t)| |\sin(t)| \leq |r \cos(t)| = |x|.$$

Ainsi le couple (x, y) satisfait l'inégalité définissant A . On en déduit $(x, y) \in A$.
Nous avons bien montré $E \subset A$.

3. Démontrer également que E est inclus dans le disque de centre $(0, 0)$ et de rayon 1.

Ce disque est défini par

$$D = \{(x, y) \in \mathbf{R}^2 \mid x^2 + y^2 \leq 1\}.$$

Reprenons le même raisonnement qu'à la question précédente. Soit $(x, y) = (r \cos(t), r \cos(t) \sin(t))$ un élément de E , avec $r \in [0, 1]$ et $t \in \mathbf{R}$. Alors $x^2 + y^2 = r^2 \cos^2(t) + r^2 \cos^2(t) \sin^2(t)$.
Or $|\cos(t)| \leq 1$ et $|r| \leq 1$. Donc

$$r^2 \cos^2(t) + r^2 \cos^2(t) \sin^2(t) \leq 1 \cdot \cos^2(t) + 1 \cdot 1 \cdot \sin^2(t) = 1.$$

Ainsi $x^2 + y^2 \leq 1$. On en déduit $(x, y) \in D$.
Donc $E \subset D$.

4. Soit f l'application définie sur $\mathbf{R}$ par $f(t) = \cos(t) \sin(t)$. Déterminer son image $f(\mathbf{R})$.

Pour déterminer l'image de f , on peut en faire son étude analytique (dérivée, tableau de variation, etc). Il est plus facile de commencer par exprimer f différemment en reconnaissant une formule trigonométrique : pour tout $t \in \mathbf{R}$, $f(t) = \cos(t) \sin(t) = \frac{1}{2} \sin(2t)$.

On sait que pour tout t , $-1 \leq \sin(2t) \leq 1$. On en déduit que pour tout t , $-\frac{1}{2} \leq f(t) \leq \frac{1}{2}$. Ainsi $f(\mathbf{R}) \subset [-\frac{1}{2}, \frac{1}{2}]$.

D'autre part, la fonction f est une fonction continue sur $\mathbf{R}$. On a $f(\frac{\pi}{4}) = \frac{1}{2}$ et $f(-\frac{\pi}{4}) = -\frac{1}{2}$. D'après le théorème des valeurs intermédiaires, on déduit que toutes les valeurs de l'intervalle $[-\frac{1}{2}, \frac{1}{2}]$ sont prises par la fonction f . On en déduit $[-\frac{1}{2}, \frac{1}{2}] \subset f(\mathbf{R})$.

Par double inclusion, on conclut $f(\mathbf{R}) = [-\frac{1}{2}, \frac{1}{2}]$.

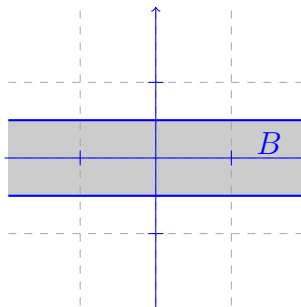
5. En déduire que E est inclus dans un ensemble de la forme $B = \{(x, y) \in \mathbf{R}^2 \mid -b \leq y \leq b\}$, où b est un nombre réel que l'on précisera. Représenter cet ensemble.

Montrons que $E \subset B$ avec $b = \frac{1}{2}$. Soit $(x, y) = (r \cos(t), r \cos(t) \sin(t))$ un élément de E , avec $r \in [0, 1]$ et $t \in \mathbf{R}$. Alors, comme $|r| \leq 1$,

$$|y| = |r \cos(t) \sin(t)| \leq 1 \cdot |f(t)| \leq \frac{1}{2}$$

d'après la question précédente. Ainsi $-\frac{1}{2} \leq y \leq \frac{1}{2}$ et on en déduit que $(x, y) \in B$. Donc $E \subset B$.

L'ensemble B se représente ainsi :



6. Démontrer que le couple $(\frac{\sqrt{3}}{2}, \frac{1}{2})$ n'est pas un élément de E .

Indication : on pourra raisonner par l'absurde et chercher des paramètres r et t correspondant à ce point.

Supposons par l'absurde que $(\frac{\sqrt{3}}{2}, \frac{1}{2}) \in E$. Alors il existe $r \in [0, 1]$ et $t \in \mathbf{R}$ tels que $(\frac{\sqrt{3}}{2}, \frac{1}{2}) = (r \cos(t), r \cos(t) \sin(t))$.

Ainsi $r \cos(t) = \frac{\sqrt{3}}{2}$ et $r \cos(t) \sin(t) = \frac{1}{2}$. En reportant la première égalité dans la seconde, on obtient $\frac{\sqrt{3}}{2} \sin(t) = \frac{1}{2}$, donc $\sin(t) = \frac{1}{\sqrt{3}}$.

Or $\cos^2(t) + \sin^2(t) = 1$ et on sait ici que $\cos(t) > 0$. Donc $\cos(t) = \sqrt{1 - \sin^2(t)} = \sqrt{1 - \frac{1}{3}} = \sqrt{\frac{2}{3}}$.

Enfin, comme $r \cos(t) = \frac{\sqrt{3}}{2}$, on déduit $r = \frac{\sqrt{3}}{2} \sqrt{\frac{3}{2}} = \frac{3}{2\sqrt{2}}$.

Or $3 > 2\sqrt{2}$ (car $9 > 8$), donc $r > 1$. Cela contredit notre hypothèse initiale dans laquelle $r \in [0, 1]$. Nous avons ainsi démontré que le couple $(\frac{\sqrt{3}}{2}, \frac{1}{2})$ n'appartient pas à E .

7. Démontrer que le couple $(\frac{\sqrt{3}}{2}, \frac{1}{4})$ est élément de E .

Il faut reprendre le raisonnement précédent, non pas pour aboutir à une absurdité, mais pour trouver les paramètres r et t qui correspondent au couple $(\frac{\sqrt{3}}{2}, \frac{1}{4})$. Il n'est pas nécessaire de les trouver explicitement, il faut simplement justifier qu'ils existent. Ces calculs constituent le travail d'analyse qui nous permettent de rédiger la synthèse suivantes.

Posons $r = \frac{3}{\sqrt{11}}$. D'autre part, comme $\sin([0, \frac{\pi}{2}]) = [0, 1]$ et $\frac{1}{2\sqrt{3}} \in [0, 1]$, il existe $t \in [0, \frac{\pi}{2}]$ tel que $\sin(t) = \frac{1}{2\sqrt{3}}$.

Alors $\cos(t) > 0$ et $\cos(t) = \sqrt{1 - \sin^2(t)} = \sqrt{1 - \frac{1}{12}} = \frac{\sqrt{11}}{2\sqrt{3}}$.

Alors $r \cos(t) = \frac{3}{\sqrt{11}} \frac{\sqrt{11}}{2\sqrt{3}} = \frac{\sqrt{3}}{2}$ et $r \cos(t) \sin(t) = \frac{\sqrt{3}}{2} \frac{1}{2\sqrt{3}} = \frac{1}{4}$.

Nous avons donc bien montré qu'il existait $r \in [0, 1]$ et $t \in \mathbf{R}$ tels que $(r \cos(t), r \cos(t) \sin(t)) = (\frac{\sqrt{3}}{2}, \frac{1}{4})$. Donc $(\frac{\sqrt{3}}{2}, \frac{1}{4}) \in E$.

8. Sur une grande figure, représenter les éléments de E correspondant aux couples de paramètres (r, t) avec $r \in \{0, \frac{1}{2}, 1\}$ et $t \in \{0, \frac{\pi}{6}, \frac{\pi}{4}, \frac{\pi}{3}, \frac{\pi}{2}\}$.

Notons $g(r, t) = (r \cos(t), r \cos(t) \sin(t))$. Alors, pour tout $t \in \mathbf{R}$, $g(0, t) = (0, 0)$. Et

$g(1, 0) = (1, 0)$, $g(1, \frac{\pi}{6}) = (\frac{\sqrt{3}}{2}, \frac{\sqrt{3}}{4})$, $g(1, \frac{\pi}{4}) = (\frac{\sqrt{2}}{2}, \frac{1}{2})$, $g(1, \frac{\pi}{3}) = (\frac{1}{2}, \frac{\sqrt{3}}{4})$, $g(1, \frac{\pi}{2}) = (0, 0)$,

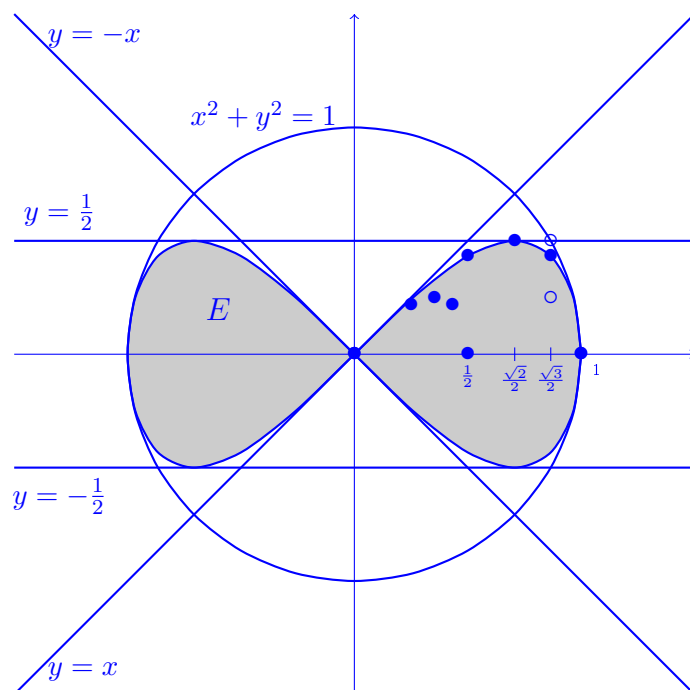
$g(\frac{1}{2}, 0) = (\frac{1}{2}, 0)$, $g(\frac{1}{2}, \frac{\pi}{6}) = (\frac{\sqrt{3}}{4}, \frac{\sqrt{3}}{8})$, $g(\frac{1}{2}, \frac{\pi}{4}) = (\frac{\sqrt{2}}{4}, \frac{1}{4})$, $g(\frac{1}{2}, \frac{\pi}{3}) = (\frac{1}{4}, \frac{\sqrt{3}}{8})$, $g(\frac{1}{2}, \frac{\pi}{2}) = (0, 0)$.

Nous représentons ces 9 éléments de E sur la figure plus bas.

9. Sur cette même figure, représenter l'allure de l'ensemble E , en faisant bien apparaître toutes les propriétés démontrées précédemment.

Nous avons démontré que E est inclus dans A , D et B . Il est donc inclus dans leur intersection. D'autre part, les points calculés précédemment nous donnent une bonne idée de l'allure de E . Il est délimité par la courbe obtenue pour $r = 1$, formée des points de la forme $(\cos(t), \cos(t) \sin(t))$. En faisant varier r entre 0 et 1, nous obtenons tous les points intérieurs à cette courbe. Et pour des raisons de parité et de périodicité, la courbe complète se déduit de ce qu'on obtient pour $t \in [0, \frac{\pi}{2}]$.

On obtient finalement l'ensemble représenté ci-dessous. On remarque bien que le point $(\frac{\sqrt{3}}{2}, \frac{1}{2})$, situé sur le cercle, n'appartient pas à E mais que le point $(\frac{\sqrt{3}}{2}, \frac{1}{4})$ y est bien.



Le terme *lemniscate* est utilisé pour décrire les courbe en forme de 8.