



## Lemme Chinois

---

### Exercice 1

Soient  $A$  un anneau et  $I$  et  $J$  les idéaux de  $A$  tels que  $I + J = (1)$ . Démontrer que  $I^n + J^m = (1)$  quels que soient entiers positifs non-nuls  $n$  et  $m$ .

[Correction ▼](#)

[002300]

### Exercice 2

Trouver toutes les solutions des systèmes suivantes :

- $$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \\ x \equiv 2 \pmod{11} \end{cases}$$
- $$\begin{cases} x \equiv 997 \pmod{2001} \\ x \equiv 998 \pmod{2002} \\ x \equiv 999 \pmod{2003} \end{cases} .$$

[Correction ▼](#)

[002301]

### Exercice 3

Démontrer que les anneaux suivants sont isomorphes

$$\mathbb{Z}/72\mathbb{Z} \times \mathbb{Z}/84\mathbb{Z} \cong \mathbb{Z}/36\mathbb{Z} \times \mathbb{Z}/168\mathbb{Z}.$$

[Correction ▼](#)

[002302]

### Exercice 4

- Montrer que  $20^{15} - 1$  est divisible par  $11 \times 31 \times 61$ .
- Trouver le reste de la division de  $2^{6754}$  par 1155.

[Correction ▼](#)

[002303]

### Exercice 5

- Quels sont les restes des division de  $10^{100}$  par 13 et par 19 ?
- Quel est le reste de la division de  $10^{100}$  par  $247 = 13 \cdot 19$  ? En déduire que  $10^{99} + 1$  est multiple de 247.

[Correction ▼](#)

[002304]

### Exercice 6

Soit  $C = A \times B$  le produit direct de deux anneaux. Décrire les ensembles des éléments inversibles, des diviseurs de zéro et des éléments nilpotents de l'anneau  $C$ .

**Exercice 7**

1. Déterminer la structure des anneaux quotients suivants :

$$\mathbb{Z}_2[x]/(x^3 + x^2 + x + 1), \quad \mathbb{Z}[x]/(x^2 - 1), \quad \mathbb{Q}[x]/(x^8 - 1).$$

2. Considérons l'anneau quotient  $K[x]/(f^n g^m)$  où  $f$  et  $g$  sont deux polynômes distincts irréductibles sur le corps  $K$ . Décrire les diviseurs de zéro et les éléments nilpotents de l'anneau  $K[x]/(f^n g^m)$ .
3. Quels idéaux a-t-il cet anneau ?
4. Soit  $K$  le corps fini à  $p$  éléments. Trouver le nombre des éléments du groupe multiplicatif de l'anneau  $K[x]/(f^m g^l)$ .
5. Donner une généralisation de la question 4) dans le cas du produit de  $n$  polynômes irréductibles sur un corps fini  $K$  à  $q$  éléments.

Correction ▼

[002306]

**Exercice 8**

Trouver les facteurs multiples des polynômes suivants :

1.  $x^6 - 15x^4 + 8x^3 + 51x^2 - 72x + 27$  ;
2.  $x^6 - 2x^5 - x^4 - 2x^3 + 5x^2 + 4x + 4$ .

Correction ▼

[002307]

**Exercice 9**

Trouver le polynôme  $f \in \mathbb{Z}[x]$  du degré le plus petit tel que

$$\begin{cases} f \equiv 2x \pmod{(x-1)^2} \\ f \equiv 3x \pmod{(x-2)^3} \end{cases} .$$

[002308]

### Correction de l'exercice 1 ▲

$1 \in I+J$  donc  $\exists(x, y) \in I \times J, 1 = x + y$ . En multipliant cette égalité par  $x$ , on obtient  $x^2 + xy = x$ . On en déduit que  $xy \in I$ , donc  $\forall p \in \mathbb{N}; x^p y \in I^p$ , et donc  $\forall(p, q) \in \mathbb{N}^2, x^p y^q \in I^p$ . Par symétrie, on a aussi  $\forall(p, q) \in \mathbb{N}^2, x^p y^q \in J^q$ . Soit maintenant  $(m, n) \in \mathbb{N}^2$ . Notons  $N = 2 \sup(m, n)$ . Alors  $1 = 1^N = (x + y)^N = \sum_{p+q=N} C_N^p x^p y^q$ . Comme :  $(p + q = 2N) \Rightarrow (p \geq n \text{ ou } q \geq m)$ , tous les termes de cette somme sont dans  $I^n$  ou dans  $J^m$ , et donc  $1 \in I^n + J^m$

### Correction de l'exercice 2 ▲

1. 3, 5, 7, 11 sont deux à deux premiers entre eux, donc la solution est unique modulo  $1155 = 3 \cdot 5 \cdot 7 \cdot 11$ .

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \\ x \equiv 2 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv 13 \pmod{15} \\ x \equiv 4 \pmod{7} \\ x \equiv 2 \pmod{11} \end{cases} \Leftrightarrow \begin{cases} x \equiv 88 \pmod{105} \\ x \equiv 2 \pmod{11} \end{cases} \\ \Leftrightarrow \begin{cases} x \equiv 508 \pmod{1155} \end{cases}$$

2. Un diviseur commun de 2001 et 2002 divise leur différence, et donc  $\text{pgcd}(2001, 2002) = 1$ . De même,  $\text{pgcd}(2002, 2003) = 1$ , et comme  $2 \nmid 2001$ ,  $\text{pgcd}(2001, 2003) = 1$ .  
2001, 2002, 2003 sont donc deux à deux premiers entre eux, et la solution est donc unique modulo  $2001 \cdot 2002 \cdot 2003$ .

$$\begin{cases} x \equiv 997 \pmod{2001} \\ x \equiv 998 \pmod{2002} \\ x \equiv 999 \pmod{2003} \end{cases} \Leftrightarrow \begin{cases} x \equiv -1004 \pmod{2001} \\ x \equiv -1004 \pmod{2002} \\ x \equiv -1004 \pmod{2003} \end{cases} \\ \Leftrightarrow x \equiv -1004 \pmod{(2001 \cdot 2002 \cdot 2003)}$$

### Correction de l'exercice 3 ▲

On a  $72 = 8 \cdot 9$  et  $\text{pgcd}(8, 9) = 1$ , donc  $\mathbb{Z}_{72} \simeq \mathbb{Z}_8 \times \mathbb{Z}_9$ . De même,  $\mathbb{Z}_{84} \simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_7$ ,  $\mathbb{Z}_{36} \simeq \mathbb{Z}_4 \times \mathbb{Z}_9$  et  $\mathbb{Z}_{168} \simeq \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_7$ . Donc  $\mathbb{Z}_{72} \times \mathbb{Z}_{84} \simeq \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \simeq \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \simeq \mathbb{Z}_{36} \times \mathbb{Z}_{128}$

### Correction de l'exercice 4 ▲

1. 11, 31, 61 sont premiers donc 2 à 2 premiers entre eux. Ainsi  $20^{15} \equiv 1[11 \cdot 31 \cdot 61] \Leftrightarrow \begin{cases} 20^{15} \equiv 1[11] \\ 20^{15} \equiv 1[31] \\ 20^{15} \equiv 1[61] \end{cases}$
- En utilisant le petit théorème de Fermat, on obtient que, modulo 11 :  $20^{15} \equiv 20^5 \equiv -2^5 \equiv 1[11]$ .
  - $(20^{15})^2 = 20^{30} \equiv 1[31]$ . On en déduit que  $20^{15} \equiv \pm 1[31]$ . Comme  $31 \not\equiv 1[4]$ , d'après le théorème de Wilson,  $x^2 = -1$  n'a pas de solution modulo 31, et donc  $20^{15} \equiv 1[31]$ .  $20^2 \equiv -3[31]$  est premier
  - $20^{15} \equiv (9^2)^{15} \equiv 3^{60} \equiv 1[61]$
2.  $1155 = 11 \cdot 7 \cdot 5 \cdot 3$ . De plus (petit théorème de Fermat)  $2^{6754} \equiv 2^4 \equiv 5[11]$ . De même,  $2^{6754} \equiv 2^4 \equiv 2[7]$ ,  $2^{6754} \equiv 2^2 \equiv -1[5]$ , et  $2^{6754} \equiv 2^0 \equiv 1[3]$ . Or

$$\begin{cases} a \equiv 5[11] \\ a \equiv 2[7] \\ a \equiv 4[5] \\ a \equiv 1[3] \end{cases} \Leftrightarrow \begin{cases} a \equiv 5[11] \\ a \equiv 2[7] \\ a \equiv 4[15] \end{cases} \Leftrightarrow \begin{cases} a \equiv 5[11] \\ a \equiv -26[105] \end{cases} \Leftrightarrow a \equiv 709[1155]$$

Donc le reste de la division de  $2^{6754}$  par 1155 est 709.

**Correction de l'exercice 5 ▲**

13 est premier et  $100 = 12 \cdot 8 + 4$  donc  $10^{100} \equiv 10^4 \equiv (-3)^4 \equiv 3 \equiv -10[13]$ . De même  $10^{100} \equiv 10^{-8} \equiv 2^8 \equiv 9 \equiv -10[19]$ . En utilisant le lemme chinois, on en déduit que  $10^{100} \equiv -10[247]$ . Comme  $\text{pgcd}(10, 247) = 1$ , on peut simplifier cette expression par 10 et on a  $10^{99} \equiv -1[247]$ , et donc  $247|10^{99} + 1$ .

**Correction de l'exercice 6 ▲**

$C = A \times B$ .

$$\begin{aligned} (a, b) \in (A \times B)^\times &\Leftrightarrow \exists (c, d) \in A \times B, (a, b)(c, d) = (1, 1) \\ &\Leftrightarrow \exists (c, d) \in A \times B, ac = 1 \text{ et } bd = 1 \\ &\Leftrightarrow a \in A^\times \text{ et } b \in B^\times \end{aligned}$$

donc  $(A \times B)^\times = A^\times \times B^\times$ .

De même, on obtient que l'ensemble  $\mathcal{D}_{A \times B}$  des diviseurs de 0 de  $A \times B$  est

$$\mathcal{D}_{A \times B} = \mathcal{D}_A \times B \cup A \times \mathcal{D}_B \cup (A \setminus \{0\}) \times \{0\} \cup \{0\} \times (B \setminus \{0\}).$$

Enfin, pour les nilpotents  $\text{Nil}(A \times B) = \text{Nil}(A) \times \text{Nil}(B)$ .

**Correction de l'exercice 7 ▲**

1. En posant  $y = x + 1$ , on a  $\mathbb{Z}_2[x]/(x^3 + x^2 + x + 1) = \{0, 1, x, y, x^2, y^2, xy, xy + 1\}$ . Les tables des opérations sont les suivantes (elles sont symétriques) :

$\oplus$	0	1	x	y	$x^2$	$y^2$	xy	xy + 1
0	0	1	x	y	$x^2$	$y^2$	xy	xy + 1
1		0	y	x	$y^2$	$x^2$	xy + 1	xy
x			0	1	xy	xy + 1	$x^2$	$y^2$
y				0	xy + 1	xy	$y^2$	$x^2$
$x^2$					0	1	x	y
$y^2$						0	y	x
xy							0	1
xy + 1								0

$\otimes$	0	1	x	y	$x^2$	$y^2$	xy	xy + 1
0	0	0	0	0	0	0	0	0
1		1	x	y	$x^2$	$y^2$	xy	xy + 1
x			$x^2$	xy	xy + 1	$y^2$	y	1
y				$y^2$	y	0	$y^2$	xy
$x^2$					1	$y^2$	xy	x
$y^2$						0	0	$y^2$
xy							$y^2$	y
xy + 1								$x^2$

Pour  $\mathbb{Z}[x]/(x^2 - 1)$ ,  $(x - 1)$  et  $(x + 1)$  sont deux idéaux étrangers, et le lemme chinois nous donne  $\mathbb{Z}[x]/(x^2 - 1) \simeq \mathbb{Z}[x]/(x - 1) \times \mathbb{Z}[x]/(x + 1)$ . Or  $\mathbb{Z}[x]/(x + 1) \simeq \mathbb{Z}$  et  $\mathbb{Z}[x]/(x - 1) \simeq \mathbb{Z}$  donc  $\mathbb{Z}[x]/(x^2 - 1) \simeq \mathbb{Z} \times \mathbb{Z}$ .

La factorisation de  $(x^8 - 1)$  sur  $\mathbb{Q}$  est  $(x^8 - 1) = (x - 1)(x + 1)(x^2 + 1)(x^4 + 1)$ . En utilisant le lemme chinois, on obtient que  $\mathbb{Q}[x]/(x^8 - 1) \simeq \mathbb{Q}[x]/(x - 1) \times \mathbb{Q}[x]/(x + 1) \times \mathbb{Q}[x]/(x^2 + 1) \times \mathbb{Q}[x]/(x^4 + 1)$  soit :

$$\mathbb{Q}[x]/(x^8 - 1) \simeq \mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}[i] \times \mathbb{Q}[e^{i\pi/4}].$$

Montrons en effet que  $\mathbb{Q}[x]/(x^2 + 1) \simeq \mathbb{Q}[i]$  : l'application  $\phi : \mathbb{Q}[x]/(x^2 + 1) \rightarrow \mathbb{Q}[i]$  définie par  $\bar{P} \mapsto P(i)$  est un morphisme d'anneau.

— injectivité : Soit  $\bar{P} \in \ker \phi$ . Alors  $P(i) = 0$ . Comme  $P$  est à coefficient rationnels donc réels,  $-i$  est aussi racine de  $P$ . Donc  $x^2 + 1 | P$ .

— surjectivité : Soit  $z = a + ib \in \mathbb{Q}[i]$ . Alors  $z = \phi(ax + b)$ .

De même pour  $\mathbb{Q}[x]/(x^4 + 1) \simeq \mathbb{Q}[e^{i\pi/4}]$ . Considérons le morphisme  $\phi : \mathbb{Q}[x]/(x^4 + 1) \rightarrow \mathbb{Q}[e^{i\pi/4}]$  défini par  $\phi(\bar{P}) = P(e^{i\pi/4})$ .  $\phi$  est bien définie, c'est un morphisme d'anneau.

— injectivité : Soit  $\bar{P} \in \ker \phi$ . Alors  $P(e^{i\pi/4}) = 0$ . Par ailleurs  $X^4 + 1$  est irréductible dans  $\mathbb{Q}$  : sa factorisation sur  $\mathbb{R}$  est  $(x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1)$ , et aucun de ces deux polynômes, même à inversible réel près, n'est rationnel. On en déduit que si  $(x^4 + 1)$  ne divise pas  $P$ , alors  $\text{pgcd}(X^4 + 1, P) = 1$ . Il existerait donc  $U, V \in \mathbb{Q}[x]$ ,  $UP + V(X^4 + 1) = 1$ . En évaluant en  $x = e^{i\pi/4}$ , on obtient une contradiction. Donc  $X^4 + 1 | P$ . (cf. exercice ??).

— surjectivité : Soit  $z = a + be^{i\pi/4} \in \mathbb{Q}[e^{i\pi/4}]$ . Alors  $z = \phi(ax + b)$ .

2. On a  $K[x]/(f^n g^m) \simeq K[x]/(f^n) \times K[x]/(g^m)$ . On en déduit que les diviseurs de 0 sont les polynômes de la forme  $\bar{P}$  où  $P$  satisfait l'une des conditions suivantes :

$$\begin{cases} f^n | P \text{ et } g^m \nmid P & (\{0\} \times K[x]/(g^m) \setminus \{0\}) \\ g^m | P \text{ et } f^n \nmid P & (K[x]/(f^n) \setminus \{0\} \times \{0\}) \\ f | P \text{ et } f^n \nmid P & (\mathcal{D}_{K[x]/(f^n)} \times K[x]/(g^m)) \\ g | P \text{ et } g^m \nmid P & (K[x]/(f^n) \times \mathcal{D}_{K[x]/(g^m)}) \end{cases}$$

Les nilpotents sont donnés par les conditions

$$\begin{cases} fg | P \\ (f^n g^m \nmid P \text{ si on veut exclure } 0) \end{cases}$$

3. Les idéaux de  $K[x]/(f^n)$  sont les idéaux engendrés par les diviseurs de  $f^n$  soit les  $f^k$  pour  $0 \leq k \leq n$ .

La démonstration peut se faire en toute généralité exactement de la même manière que dans  $\mathbb{Z}/n\mathbb{Z}$  : Soit  $\mathcal{D}$  l'ensemble des diviseurs de  $f^n$  (modulo  $K^*$ ). Ici,  $\mathcal{D} = \{f^k, 0 \leq k \leq n\}$ . Soit  $\mathcal{I}$  l'ensemble de idéaux de  $K[x]/(f^n)$ .

On a une flèche de  $\mathcal{D} \rightarrow \mathcal{I}$ , donnée par  $d \mapsto (\bar{d})$ .

— surjectivité Soit  $I \in \mathcal{I}$ .  $I$  est principal : notons  $I = (\bar{h})$ . Soit  $d = \text{pgcd}(f, h)$ , et  $h_1$  le polynôme déterminé par  $h = dh_1$ . Alors  $\text{pgcd}(f, h_1) = 0$  et  $h_1$  est inversible dans le quotient. On en déduit que  $(\bar{h}) = (\bar{d}) = I$  (or  $d \in \mathcal{D}$ ).

— injectivité Soit  $d, d' \in \mathcal{D}$  tels que  $(\bar{d}) = (\bar{d}')$ . On a alors  $d = h_1 d' + h_2 f$  donc  $d' | d$ . De même,  $d | d'$ . On en déduit que  $d \sim d'$ .

Revenons à notre exercice : les idéaux de  $K[x]/(f^n) \times K[x]/(g^m)$  sont donc de la forme  $(f^\alpha) \times (g^\beta)$ . En revenant à  $K[x]/(f^n g^m)$ , on obtient que l'ensemble des idéaux est

$$\{(f^\alpha g^\beta), 0 \leq \alpha, \beta \leq n\}$$

4. Les inversibles de  $K[x]/(f^n)$  sont les (classes des) polynômes premiers avec  $f$ . Le complémentaire est donc formé des multiples de  $f$ , il y en a donc autant que de polynômes de degré  $(nd - 1) - d$  où  $d$  est le degré de  $f$ , soit  $p^{(n-1)d}$ . Il y a donc  $p^{(n-1)d}(p - 1)$  inversibles dans  $K[x]/(f^n)$ .

On en déduit qu'il y en a  $p^{(n-1)d_f + (m-1)d_g}(p - 1)^2$  dans  $K[x]/(f^n g^m)$ , où  $d_f$  et  $d_g$  sont les degrés respectifs de  $f$  et  $g$ .

5. Plus généralement, si les  $f_i$  sont des polynômes irréductibles distincts, dans  $K[x]/(f_1^{n_1} \cdots f_k^{n_k})$  il y a  $p^{\sum (n_i - 1)d_i}(p - 1)^k$  inversibles, où  $d_i$  est le degré de  $f_i$ .

### Correction de l'exercice 8 ▲

Pour obtenir les facteurs multiples, on utilise la remarque suivante :  $g$  est un facteur multiple de  $f$  ssi  $g$  est un facteur commun à  $f$  et à  $f'$  (dérivé formel de  $f$ ).

Ainsi  $\text{pgcd}(f, f')$  est le produit de tous les facteurs multiples de  $f$ , avec exposant diminué de 1 par rapport à  $f$ .  
Ainsi  $f / \text{pgcd}(f, f')$  est le produit de tous les facteurs irréductibles de  $f$ , avec exposant 1 pour tous. Finalement,  
 $\text{pgcd}(\text{pgcd}(f, f'), f / \text{pgcd}(f, f'))$  est le produit de tous les facteurs multiples de  $f$  avec exposant 1.

---