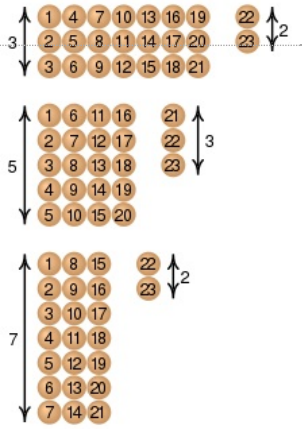
# Théorème des restes chinois

En mathématiques, le **théorème des restes chinois** est un résultat d'arithmétique modulaire traitant de résolution de systèmes de congruences. Ce résultat, initialement établi pour $\mathbb{Z}/n\mathbb{Z}$, se généralise en théorie des anneaux. Ce théorème est utilisé en théorie des nombres.

## Fragments d'histoire

### Exemple de Sun Zi



Exemple de Sun Zi : il y a 23 objets.

La forme originale du théorème apparait sous forme de problème dans le livre de Sun Zi, le *Sunzi suanjing* **(en)**, datant du IIIe siècle[1]. Il est repris par le mathématicien chinois Qin Jiushao dans son ouvrage le *Shùshū Jiǔzhāng* (« Traité mathématique en neuf chapitres ») publié en 1247. Le résultat concerne les systèmes de congruences (voir arithmétique modulaire).

> *Soient des objets en nombre inconnu. Si on les range par 3 il en **reste** 2. Si on les range par 5, il en **reste** 3 et si on les range par 7, il en **reste 2**. Combien a-t-on d'objets ?*

Cette énigme est parfois associée au général Han Xin **(en)** comptant son armée[2].

La résolution proposée par Sun Zi pour ce problème est la suivante :

> *Multiplie le reste de la division par 3, c'est-à-dire 2, par 70, ajoute-lui le produit du reste de la division par 5, c'est-à-dire 3, avec 21 puis ajoute le produit du reste de la division par 7, c'est-à-dire 2 par 15. Tant que le nombre est plus grand que 105, retire 105.*

Mais la solution n'explique qu'imparfaitement la méthode utilisée. On peut cependant remarquer que :

- 70 a pour reste 1 dans la division par 3 et pour reste 0 dans les divisions par 5 et 7 ;
- 21 a pour reste 1 dans la division par 5 et pour reste 0 dans les divisions par 3 et 7 ;
- 15 a pour reste 1 dans la division par 7 et pour reste 0 dans les divisions par 3 et 5.

Le nombre 233 ($2 \times 70 + 3 \times 21 + 2 \times 15$) a bien alors pour restes respectifs 2, 3 et 2 dans les divisions par 3, 5 et 7. Enfin, comme 105 ($3 \times 5 \times 7$) a pour reste 0 dans les trois types de division, on peut l'ôter ou l'ajouter autant de fois que l'on veut sans changer les valeurs des restes. La plus petite valeur pour le nombre d'objets est alors de 23.

On retrouve ce problème presque à l'identique en 1202 dans le *Liber Abbaci* de Fibonacci[3] dans le chapitre XII qui concerne les problèmes et énigmes où l'on trouve également le problème des lapins de la suite de Fibonacci. Le problème avait aussi été étudié par Ibn al-Haytham (Alhazen) – voir l'article Mathématiques arabes – dont Fibonacci a pu lire les œuvres.

Euler[4] s'est également intéressé à cette question, ainsi que Gauss[5].

### Astronomie

Selon Ulrich Libbrecht **(de)**[6], la motivation de ce type de calcul chez les Chinois serait l'astronomie. On peut en effet penser que les Chinois, férus de calculs astronomiques, puissent être intéressés par des concordances de calendrier et qu'ils aient été amenés très tôt à s'intéresser à des questions du type :

> *Dans combien de jours la pleine lune tombera-t-elle au solstice d'hiver ?*

Si la question se pose alors qu'il reste 6 jours avant le solstice d'hiver et 3 jours avant la pleine lune, la question se traduit par :

> *Existe-t-il un entier x tel que le reste de la division de x par 365 donne 6 et le reste de la division de x par 28 donne 3 ?*

### Comptage de paquets

Mais selon Daumas et al.[7], il s'agirait plus probablement de problèmes associés à des comptages par paquets, peut-être d'origine divinatoire.

Enfin, il serait dommage de ne pas présenter ce problème concernant des pirates et un trésor, très fréquemment cité pour illustrer le théorème des restes chinois :

> *Une bande de 17 pirates possède un trésor constitué de pièces d'or d'égale valeur. Ils projettent de se les partager également, et de donner le reste au cuisinier chinois. Celui-ci recevrait alors 3 pièces. Mais les pirates se querellent, et six d'entre eux sont tués. Un nouveau partage donnerait au cuisinier 4 pièces. Dans un naufrage ultérieur, seuls le trésor, six pirates et le cuisinier sont sauvés, et le partage donnerait alors 5 pièces d'or à ce dernier. Quelle est la fortune minimale que peut espérer le cuisinier s'il décide d'empoisonner le reste des pirates ?*

La réponse est 785. Les nombres 17, 11 et 6 étant premiers entre eux deux à deux, les solutions sont distantes d'un multiple de 1122 ($17 \times 11 \times 6$) ; par ailleurs 785 vérifie bien l'énoncé : $785 = 17 \times 46 + 3 = 11 \times 71 + 4 = 6 \times 130 + 5$. Il s'ensuit que 785 est bien le plus petit des nombres possibles[8].

L'arithmétique modulaire a rendu ce type de problème plus facile à résoudre.

## Système de congruences d'entiers

### Théorème

Soient $n_1$, ..., $n_k$ des entiers deux à deux premiers entre eux, c'est-à-dire que PGCD ($n_i$ , $n_j$) = 1 lorsque $i \neq j$. Alors pour tous entiers $a_1$, ..., $a_k$, il existe un entier $x$, unique modulo $n = \prod_{i=1}^{k} n_i$, tel que

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ &\cdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

## Algorithme

Une solution $x$ peut être trouvée comme suit. Pour chaque $i$, les entiers $n_i$ et $\hat{n}_i = \frac{n}{n_i} = n_1 \ldots n_{i-1} n_{i+1} \ldots n_k$ sont premiers entre eux. D'après le théorème de Bachet-Bézout on peut calculer l'inverse $v_i$ de $\hat{n}_i$ modulo $n_i$. Pour cela, on peut utiliser l'algorithme d'Euclide étendu et obtenir des entiers $u_i$ et $v_i$ tels que $u_i n_i + v_i \hat{n}_i = 1$. Si on pose $e_i = v_i \hat{n}_i$, alors nous avons

$e_i \equiv 1 \pmod{n_i}$ et $e_i \equiv 0 \pmod{n_j}$ pour $j \neq i$.

Une solution particulière de ce système de congruences est par conséquent

$$x = \sum_{i=1}^{k} a_i e_i \ ,$$

et les autres solutions sont les entiers congrus à $x$ modulo le produit $n$.

## Exemple

L'exemple de Sun Zi, présenté plus haut dans la section histoire, se réduit à

$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

on obtient alors

- $n = 3 \times 5 \times 7 = 105$
- $n_1 = 3$ et $\hat{n}_1 = 5 \times 7 = 35$ , or $2\hat{n}_1 \equiv 1 \pmod{3}$ donc $e_1 = 70$
- $n_2 = 5$ et $\hat{n}_2 = 3 \times 7 = 21$ , or $\hat{n}_2 \equiv 1 \pmod{5}$ donc $e_2 = 21$
- $n_3 = 7$ et $\hat{n}_3 = 3 \times 5 = 15$ , or $\hat{n}_3 \equiv 1 \pmod{7}$ donc $e_3 = 15$

une solution pour $x$ est alors $x = 2 \times 70 + 3 \times 21 + 2 \times 15 = 233$

et les solutions sont tous les entiers congrus à 233 modulo 105, c'est-à-dire à 23 modulo 105.

## Généralisation à des nombres non premiers entre eux

Les systèmes de congruences peuvent être résolus même si les $n_i$ ne sont pas premiers entre eux deux à deux. Le critère précis est le suivant :

> une solution $x$ existe si et seulement si $a_i \equiv a_j \pmod{\mathrm{PGCD}(n_i, n_j)}$ pour tous $i$ et $j$. L'ensemble des solutions $x$ forme alors une classe de congruence modulo le PPCM des $n_i$.

Exemple : le système $x \equiv -1 \bmod 4$ et $x \equiv -1 \bmod 6$ équivaut à : $x + 1$ multiple de 4 et 6 c'est-à-dire de PPCM(4, 6) = 12, ou encore : $x \equiv -1 \bmod 12$.

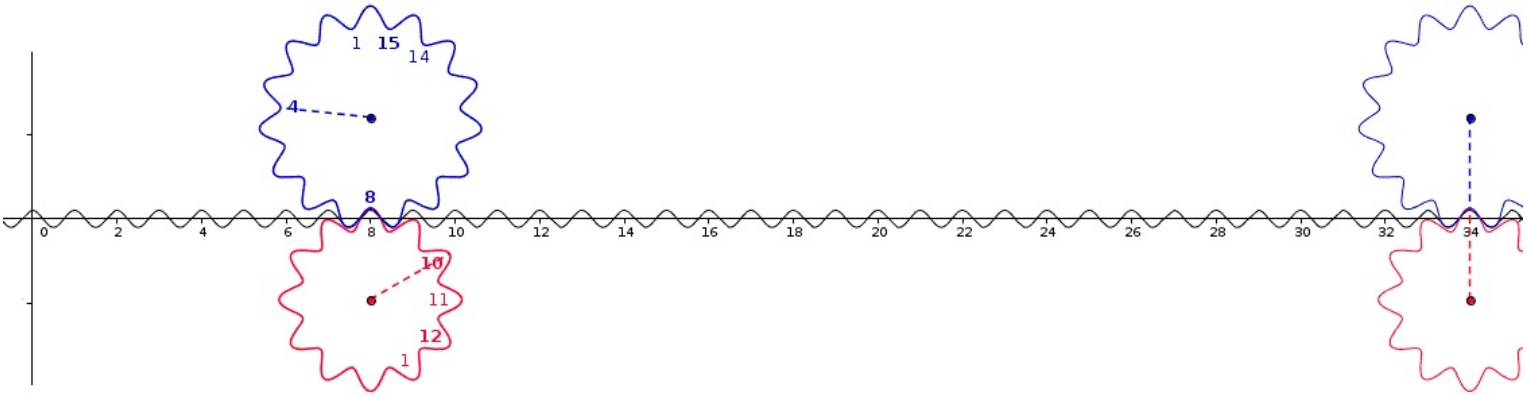
Une méthode de résolution de tels systèmes est la méthode chinoise, qui consiste à se ramener à des modules premiers entre eux deux à deux (dans l'exemple ci-dessus : les modules 4 et 3). Une autre est la méthode des substitutions successives.

## Interprétation mécanique

La résolution du système $\begin{cases} x \equiv r \pmod{a} \\ x \equiv s \pmod{b} \end{cases}$ , d'inconnue $x$ , passe par le calcul du PPCM de $a$ et $b$.

Une roue dentée comportant $a$ dents s'engrène dans une autre roue dentée comportant elle $b$ dents. Combien de dents doivent passer pour que sa $r$-ième dent vienne en coïncidence avec la $s$-ième dent ?

Le PPCM des deux nombres $a$ et $b$ est ce qui permet de comprendre le comportement périodique de ce système : c'est le nombre de dents séparant deux contacts de même congruence. On peut donc trouver la solution, s'il y en a une, dans l'intervalle $[1, \mathrm{PPCM(a, b)}]$. Il y a une solution si PGCD($a$, $b$) divise $r - s$ .




Pour cet engrenage, $\begin{cases} x \equiv 4 \ (mod\ 15) \\ x \equiv 10 \ (mod\ 12) \end{cases}$ , PPCM(12,15)=60 , pour x ∈ [1,60] , la solution est x = 34 .

On peut comprendre simplement pourquoi le calcul sur des roues dentées fait intervenir de l'arithmétique modulaire, en remarquant que l'ensemble des dents d'une roue en comptant $n$ peut être paramétré par l'ensemble des racines $n$-ièmes de l'unité, qui a une structure de groupe naturellement isomorphe à celle de $\mathbb{Z}/n\mathbb{Z}$.

# Résultat pour les anneaux

## Dans les anneaux Z/*n*Z

Le théorème chinois a également une version plus abstraite : si $n_1$, ..., $n_k$ sont deux à deux premiers entre eux alors, en notant $n$ le PPCM des $n_i$, c'est-à-dire dans le cas présent le produit des $n_i$, l'application (à valeurs dans l'anneau produit)

$$\begin{array}{rccc} \phi : & \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z} \\ & \alpha[n] & \longmapsto & (\alpha[n_1], \ldots, \alpha[n_k]) \end{array}$$

est un isomorphisme d'anneaux.

Par exemple, la table suivante[9] compare $\mathbb{Z}/15\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ et chaque paire d'éléments de $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ apparaît exactement une et seule fois :

| x | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| x mod 3 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 | 0 | 1 | 2 |
| x mod 5 | 0 | 1 | 2 | 3 | 4 | 0 | 1 | 2 | 3 | 4 | 0 | 1 | 2 | 3 | 4 |

Pour le montrer, on remarque d'abord que les deux ensembles finis $\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$ ont le même nombre d'éléments. Comme $\phi$ est un morphisme d'anneaux, il suffit donc de démontrer qu'il est injectif pour en déduire que c'est un isomorphisme. Pour cela, il suffit de montrer que son noyau est réduit à 0 : si $\alpha \equiv 0 \mod n_i$ pour $i = 1, \ldots, k$, c'est-à-dire si $\alpha$ est un multiple de chaque $n_i$, alors $\alpha \equiv 0 \mod n$, c'est-à-dire $\alpha$ est un multiple du produit $n_1$, ..., $n_k$. Ceci résulte de l'hypothèse que les $n_i$ sont premiers entre eux deux à deux.

Dans le cas où les $n_i$ ne sont pas deux à deux premiers entre eux, le morphisme ci-dessus n'est qu'injectif. Il existe une solution au problème initial si et seulement si les données sont dans l'image, c'est-à-dire que le pgcd de $n_i$ et $n_j$ divise $a_i - a_j$ pour tout couple $(i, j)$.

## Dans un anneau principal

Pour un anneau principal $R$, le théorème des restes chinois prend la forme suivante : Si $r_1$, ..., $r_k$ sont des éléments de $R$ qui sont premiers entre eux deux à deux, et $r$ désigne le produit $r_1 \ldots r_k$, alors le morphisme d'anneaux

$$\begin{array}{rccc} f : & R/rR & \longrightarrow & R/r_1R \times \cdots \times R/r_kR \\ & x \bmod rR & \longmapsto & (x \bmod r_1R, \cdots, x \bmod r_kR) \end{array}$$

est un isomorphisme.

L'isomorphisme inverse peut être construit comme ceci. Pour chaque $i$, les éléments $r_i$ et $r$ / $r_i$ sont premiers entre eux et par conséquent, il existe des éléments $u_i$ et $v_i$ dans $R$ tels que

$$u_i r_i + v_i \frac{r}{r_i} = 1$$

Fixons $e_i = v_i\, r$ / $r_i$. On a :

$$e_i \equiv 1 \pmod{r_i} \quad \text{et} \quad e_i \equiv 0 \pmod{r_j}$$

pour $j \neq i$.

Alors l'inverse de $f$ est le morphisme construit à l'aide des idempotents $e_i$ (mod $r$) :

$$\begin{array}{rccc} g: & R/r_1R \times \cdots \times R/r_kR & \longrightarrow & R/rR \\ & (a_1 \bmod r_1R, \cdots, a_k \bmod r_kR) & \longmapsto & \sum_{i=1}^{k} a_i e_i \bmod rR\,. \end{array}$$

#### Exemple des polynômes

Le théorème des restes chinois permet de résoudre explicitement tout système de congruences dans l'anneau euclidien $R = K[X]$ des polynômes sur un corps $K$, c'est-à-dire tout système de la forme.

$$\forall i \in \{0, \ldots, n\}, P \equiv A_i \pmod{R_i}$$

où les données sont des polynômes $R_i$ deux à deux premiers entre eux et des polynômes $A_i$, et l'inconnue est le polynôme $P$.

L'interpolation lagrangienne correspond au cas particulier où les $R_i$ sont de la forme $X - x_i$ et les $A_i$ sont constants, et fournit la solution $P$ de degré $\leq n$ . Plus explicitement, si $x_0$, $x_1$, ... , $x_n$ sont $n + 1$ éléments de $K$ distincts deux à deux, on prend pour $E_i$ les polynômes interpolateurs de Lagrange, définis par :

$$E_i = \frac{(X - x_0)(X - x_1)\ldots(X - x_{i-1})(X - x_{i+1})\ldots(X - x_n)}{(x_i - x_0)(x_i - x_1)\ldots(x_i - x_{i-1})(x_i - x_{i+1})\ldots(x_i - x_n)}.$$

Pour $j$ différent de $i$, $E_i$ est divisible par $R_j$, de sorte que $E_i \equiv 0$ modulo $R_j$. Par ailleurs, modulo $R_i$, $X \equiv x_i$, de sorte que $E_i \equiv 1$ modulo $R_i$.

Pour $n + 1$ éléments quelconques $y_0$, $y_1$, ... , $y_n$ de $K$, dire qu'un polynôme $P$ est tel que $P(x_i) = y_i$ pour tout $i$, est équivalent à dire que $P \equiv y_i$ modulo $R_i$. Un tel polynôme $P$ est donné par

$$P = \sum_{i=0}^{n} y_i E_i,$$

ce qu'on peut vérifier par un calcul direct.

### Pas dans les anneaux factoriels

Le théorème des restes chinois n'a pas lieu en toute généralité dans les anneaux factoriels. Considérons par exemple l'anneau factoriel $\mathbb{Z}[X]$. Soit $p$ un nombre premier. Alors $p$ est irréductible dans $\mathbb{Z}[X]$, et est par conséquent premier dans cet anneau. Maintenant, posons $a_1 = 0$, et $a_2 = 1$, tous deux éléments de $\mathbb{Z}[X]$. Posons aussi $n_1 = p$ et $n_2 = X$.

S'il existait un élément $a$ de $\mathbb{Z}[X]$ tel que $a = a_1 \bmod n_1$ et $a = a_2 \bmod n_2$, alors $a$ serait un polynôme dont les coefficients sont multiples de $p$, mais qui serait aussi égal à 1 + (un multiple de $X$) ; cela ne se peut.

### Dans les corps munis de valuations indépendantes

Le théorème des restes chinois s'étend de plusieurs façons aux corps munis d'un certain nombre de valuations indépendantes[10,11], tels que les anneaux factoriels (et *a fortiori* principaux), les anneaux de Dedekind etc. On le trouve alors sous le nom de « théorème d'approximation faible (en) » :

*Soient* $v_1, v_2, \ldots v_n$ *des valuations discrètes indépendantes d'un corps* K , $a_1, a_2, \ldots a_n$ *des éléments de* K, *et* $k_1, k_2, \ldots, k_n$ *des entiers relatifs. Alors il existe* $x \in K$ *tel que* $v_i(x - a_i) = k_i$ *pour tout* i.

Le théorème reste vrai pour les valuations non discrètes, en remplaçant les $k_i$ par des éléments du groupe des valeurs des $v_i$[10].

Le théorème ne suppose pas que les $a_i$ soient éléments d'un anneau, ni que les $k_i$ soient positifs. Par contre, même si les valuations sont issues d'un anneau (intègre) $A$, $x$ ne peut être supposé élément de $A$.

Voyons ce que le théorème signifie pour les rationnels en général lorsque les $k_i$ sont positifs, les valuations en jeu étant les valuations $p$ adiques. Si $q$ dénote un nombre rationnel, convenons ici, par homologie avec le cas entier, que $q$ est multiple d'un entier $n$ si le numérateur de $q$ l'est, et si le dénominateur de $q$ est premier avec $n$. Convenons encore de noter $q_1 = q_2 \bmod n$ si $q_1$-$q_2$ est multiple de $n$ (on peut facilement vérifier que les principes de base des congruences fonctionnent encore pour cette définition étendue, à quelques adaptations près).

Le théorème d'approximation faible implique[12] alors que si $n_1$, $n_2$, ... $n_r$ sont $r$ entiers premiers deux à deux, et $q_1$, $q_2$, ... $q_r$ sont $r$ rationels, alors il existe un rationnel $q$ tel que $q = q_i \bmod n_i$ pour tout $i$ (ce qui est loin de se déduire trivialement du théorème des restes chinois[13]).

On va maintenant faire voir que ce théorème implique le théorème des restes chinois dans $\mathbb{Z}$, et même dans les anneaux principaux. En fait, il est même un peu plus général, car il fournit un élément $x$ de valuation $p_i$-adique exactement égale aux $k_i$.

Supposons donc que $A$ soit un anneau principal, de corps de fractions $K$. Avec les notations du début de l'article, si les $n_i$ sont décomposés en produit de puissances de facteurs premiers $p_{ij}^{c_{i,j}}$, on voit facilement, en répétant éventuellement les $a_i$ correspondants, qu'il suffit de supposer que $n_i$ est une puissance d'un certain élément premier $p_i$, disons $p_i^{c_i}$.

En notant $v_i$ les valuations $p_i$-adiques correspondantes, le théorème d'approximation faible dit qu'il existe un élément $x$ de $K$ tel que $v_i(x - a_i) = c_i$ pour tout $i$. Notons $x = r/s$, où $r$ et $s$ sont des éléments de $A$ premiers entre eux. On a donc

$$\frac{r}{s} - a_i = p_i^{c_i} q,\ q \in K,$$

les numérateurs et dénominateurs de $q$ n'étant pas multiples de $p_i$. Multiplions cette équation par $s$, puis regardons la modulo $p_i^{c_i}$ :

$$sa_i = r \bmod p_i^{c_i}.$$

Cela implique que $s$ n'est pas multiple de $p_i$ pour tout $i$, puisque $r$ est premier avec $s$. Il existe donc $t$ dans $A$ tel que $st = 1 \bmod p_1^{c_1} \cdots p_n^{c_n}$ . En multipliant la congruence précédente par $t$, on obtient $a_i = rt \bmod p_i^{c_i}$ pour tout $i$; donc $rt$ satisfait aux conditions du théorème des restes chinois.

Observons pour finir que le théorème d'approximation faible n'est pas englobé par le théorème chinois dans les anneaux généraux, exposé dans la section suivante, car les idéaux premiers associés aux valuations ne réalisent pas nécessairement la condition de Bezout; un exemple simple est l'anneau factoriel $\mathbb{Z}[X]$, où l'on a les ideaux premiers $< p >$ et $< X >$, $p$ un nombre premier quelconque, mais $< p > + < X > \neq \mathbb{Z}[X]$.

### Résultat pour les anneaux généraux

Si $R$ est un anneau et $I_1$, ..., $I_k$ des idéaux bilatères de $R$ deux à deux premiers entre eux (ce qui signifie que $I_i + I_j = R$ lorsque $i \neq j$), on démontre (par récurrence sur $k$)[14] que le morphisme

$$\begin{array}{ccc} R/(I_1 \cap \cdots \cap I_k) & \longrightarrow & R/I_1 \times \cdots \times R/I_k \\ x \bmod I_1 \cap \cdots \cap I_k & \longmapsto & (x \bmod I_1, \cdots, x \bmod I_k) \end{array}$$

est un isomorphisme et que l'idéal intersection de ces idéaux est égal à la somme de tous leurs produits dans n'importe quel ordre :

$$I_1 \cap \cdots \cap I_k = \sum_{\sigma \in \mathfrak{S}_k} I_{\sigma(1)} \cdots I_{\sigma(k)}.$$

Si l'anneau est commutatif, tous ces produits sont égaux et l'intersection des $I_i$ est simplement égale à leur produit. Mais s'il ne l'est pas, pour deux idéaux bilatères $I$ et $J$ premiers entre eux, en général[15] $I \cap J \neq IJ$, et l'on a seulement $I \cap J = IJ + JI$, d'où l'expression ci-dessus, avec une somme indexée par le groupe symétrique.

Si $R$ est un anneau commutatif général, rien n'autorise à supposer que les idéaux sont co-premiers, même si $R$ est intègre et que ces idéaux sont premiers. Cependant, on peut se demander si le théorème chinois généralisé (c.-à-d. qui ne suppose pas les $n_i$ premiers entre eux, mais impose des conditions sur les $a_i$) aurait lieu.

C'est justement le cas des anneaux de Prüfer (en) et en réalité, cette propriété les caractérise. Plus précisément[16],[17], pour qu'un anneau commutatif intègre soit de Prüfer, il faut et il suffit qu'un système de congruences $x = x_i \bmod I_i$ admette des solutions dès que $x_i \equiv x_j \bmod (I_i + I_j)$.

Évidemment, si les idéaux $I_i$ sont co-premiers, l'idéal $I_i + I_j$ est $R$ tout entier, donc la condition sur $x_i$ et $x_j$ est toujours vérifiée, et le système de congruence a une solution $x$. On retrouve bien le théorème chinois, tel qu'exposé au début de cette section.

## Applications

Des applications du théorème des restes chinois se rencontrent dans la branche diophantine de la théorie des congruences.

Le théorème suivant peut être vu soit comme une application du théorème des restes chinois, soit comme une généralisation de ce théorème.

Soit $P_i(x_1, x_2, \ldots, x_n) \equiv 0 \bmod m_i$ ($i$ = 1,2, ... k) un système de $k$ congruences, où les $P_i$ sont des polynômes de $n$ variables, et où les modules $m_i$ sont premiers deux à deux. Alors ces congruences sont conjointement solvables si et seulement si chacune d'entre elles est solvable séparément; plus précisément, si $m$ est le produit des modules $m_i$, chaque n-uplet ($x_1, x_2, \ldots, x_n$) où $x_i$ est une solution de la i-ème congruence, détermine bijectivement un n-uplet ($y_1, y_2, \ldots, y_n$) modulo $m$ satisfaisant toutes les congruences à la fois.

De plus, si l'on convient d'appeler "primitive" une solution ($x_1, x_2, \ldots, x_n$) d'une congruence telle que chacun des $x_i$ soit premier avec le module $m_i$, alors le théorème précédent reste vrai si on le restreint aux solutions primitives: Les congruences sont conjointement primitivement solvables si et seulement si chacune d'entre elles l'est séparément, et il y a bijection entre les n-uplets de solutions primitives modulo $m_i$, et ceux de solutions primitives conjointes modulo $m$.

La preuve de ce théorème est simple : une solution conjointe induit évidemment une solution pour chaque équation séparément, et inversement, à partir de telles solutions, on reconstruit une solution conjointe avec le théorème des restes chinois.

Évidemment, si $P_i(x) = x - a_i$, on retrouve le théorèmes des restes chinois.

Un autre théorème notoire est le suivant :

Soit $P(x_1, x_2, \ldots, x_n) \equiv 0 \bmod m$ une congruence, où $P$ est un polynôme de $n$ variables, et supposons que $m$ soit le produit de $k$ modules $m_i$ premiers deux à deux. Alors cette congruence est solvable (resp. primitivement solvable) modulo $m$ si et seulement si elle est solvable (resp. primitivement solvable) modulo chaque $m_i$. À nouveau, il y a bijection entre les solutions de la première congruence modulo $m$ et les k-uplets de solutions de congruences modulo chaque $m_i$. La preuve est similaire à celle du théorème précédent.

Grâce à ce dernier théorème, la solution d'une congruence modulo $m$ se réduit a celle des solutions modulo chacune des puissances maximales de facteurs premiers composant $m$.

Parmi les nombreuses applications du théorème des restes chinois à la théorie des nombres, citons encore la démonstration de la multiplicativité de l'indicatrice d'Euler.

### Une méthode connexe

On a vu qu'une des applications majeures du théorème des restes chinois résidait dans le fait que la résolution d'une congruence modulo un nombre $m$, produit de deux nombres $m_1$ et $m_2$, se réduisait à la résolution de cette même congruence modulo $m_1$ et $m_2$, lorsque $m_1$ et $m_2$ sont premiers entre eux. Typiquement, les $m_i$ sont des puissances de nombres premiers, le théorème chinois étant poussé le plus loin possible. Cela simplifie déjà considérablement les problèmes théoriques et pratiques, mais comment réduire la question plus encore ? La technique suivante est déjà utilisée par Gauss dans les *Disquisitiones arithmeticae*. Pratiquée avec habileté, le plus souvent par le biais d'une descente infinie, elle permet une analyse fine des cas où les nombres $m_1$ et $m_2$ ne sont pas premiers entre eux, et de ramener finalement la question aux moduli premiers.

Soit $P(x_1, x_2, \dots x_n) \equiv 0 \mod m$ une congruence, où $P$ est un polynôme de $n$ variables, et $m$ est le produit de $m_1$ et $m_2$, non nécessairement premiers entre eux. La résolution de cette congruence équivaut à la résolution *successive* de $P(x'_1, x'_2, \dots, x'_n) \equiv 0 \mod m_1$ puis de $Q(x''_1, x''_2, \dots, x''_n) \equiv 0 \mod m_2$ où le polynôme $Q$ à coefficients entiers est égal à

$$Q(X_1, \dots, X_n) = \frac{1}{m_1} P(m_1 X_1 + x'_1, \dots, m_1 X_n + x'_n).$$

L'ensemble des solutions est alors $\{(x_i) = (x'_i + m_1 x''_i),\ (x'_i) \in S_1,\ (x''_i) \in S_2\}$, où $S_1$ et $S_2$ sont les ensembles de solutions des congruences ci-dessus resp.

**Démonstration et exemples**

Si la proposée a une solution $x_i$ modulo $m$, alors cette solution est évidemment une solution modulo $m_1$. On peut donc poser $x_i = x'_i + m_1 x''_i$, où $(x'_i)$ est une solution de la proposée modulo $m_1$, et $x''_i$ est un nombre entier déterminé par $x'_i$ et $x_i$. Ainsi, les $x''_i$ vérifient $R(x''_i) = 0 \mod m$, avec $R = P(x'_i + m_1 X_i)$. Mais il est facile de voir que tous les coefficients du polynôme $R$ sont multiples de $m_1$. On peut donc simplifier cette dernière congruence par $m_1$, ce qui donne $Q(x''_i) = 0 \mod m_2$ (notations de l'énoncé).

Réciproquement, supposons qu'il existe une solution de la congruence $P(x_i) = 0 \mod m_1$, et une autre de la congruence $Q(x''_i) = 0 \mod m_2$, $Q$ étant défini à partir de $P$ et $(x_i)$ comme précédemment. Alors en remontant l'argument précédent, on voit que $(x_i = x'_i + m_1 x''_i)$ est une solution de la proposée.

**Exemples :**

- Donnons-nous un nombre premier impair $p$, un entier positif $n$, et un nombre $a$ premier avec $p$. Soit à démontrer (sans utiliser de racine primitive modulo $p$) que $a$ est résidu quadratique modulo $p^n$ si c'est un résidu quadratique modulo $p$ (la réciproque est triviale).

On suppose par récurrence le résultat vrai pour $n = N > 0$, puisqu'il est trivialement vérifié pour $n = 1$. En faisant

$$P(X) = X^2 - a, \quad m_1 = p^n \quad \text{et} \quad m_2 = p$$

dans le lemme ci-dessus, on obtient d'abord

$$P(x') = x'^2 - a \equiv 0 \mod p^n,$$

qui a bien une solution $x'$ par l'hypothèse de récurrence, d'ailleurs première avec $p$ puisque $a$ l'est. Puis

$$Q(x'') = p^N x''^2 + 2x'x'' + \frac{x'^2 - a}{p^N} \equiv 0 \mod p,$$

qui n'est autre qu'une équation linéaire modulo $p$, et a donc une solution $x''$ puisque $p$ est premier avec $2x'$. Donc la congruence $x^2 - a \equiv 0$ a lieu pour le modulo $m_1 m_2 = p^{n+1}$, et pour tout modulo $p^k$ en général.

- Tout entier $a$ congru à 1 modulo 8 est résidu quadratique modulo $2^n$, $n \in \mathbb{N}$ (réciproque immédiate pour $n > 2$ et $a$ impair).

La séparation $m_1 = 2^{n-1}$ et $m_2 = 2$ mène à une tautologie. Mais en observant que le résultat est immédiat pour $n \leq 3$, les carrés impairs étant toujours congrus à 1 modulo 8, on prend la séparation $m_1 = 2^{n-2}$ et $m_2 = 4$, et on suppose le résultat vrai pour tout $n < N$, avec $N > 3$. Soit donc $n = N$. L'hypothèse d'induction fournit une solution $x'$, forcément impaire, de

$$x'^2 - a \equiv 0 \mod 2^{n-1},$$

et c'est a plus forte raison une solution modulo $m_1$. On a d'autre part, avec les notations du lemme,

$$Q(x'') = 2^{n-2} x''^2 + 2x'x'' + \frac{x'^2 - a}{2^{n-2}} \equiv 2x'x'' + \frac{x'^2 - a}{2^{n-2}} \mod 4 \equiv 0 \iff x'x'' + \frac{x'^2 - a}{2^{n-1}} \equiv 0 \mod 2.$$

Et comme $x'$ est impair, on a bien une solution $x''$ modulo $m_2$ qui permet de conclure.

- Soit $p$ un nombre premier impair, $a \in \mathbb{Z}$ un nombre premier avec $p$, $n$ un entier positif, et $f$ une forme quadratique entière d'une ou plusieurs variables: sous forme matricielle, $f(\mathbf{x}) = \frac{1}{2}\mathbf{x}^T M \mathbf{x}$. On suppose $\det(M) \not\equiv 0 \mod p$. Alors la congruence $f(\mathbf{x}) \equiv a \mod p^n$ est solvable si (et seulement si) la congruence $f(\mathbf{x}) \equiv a \mod p$ l'est.

On prend $P(\mathbf{x}) = \frac{1}{2}\mathbf{x}^T M \mathbf{x} - a$, et la séparation $m_1 = p^n$, $m_2 = p$. Supposons le résultat vrai pour $n = N$.

L'hypothèse d'induction fournit une solution $\mathbf{x}'$, forcément non nulle, de $P(\mathbf{x}') \equiv 0 \mod p^n$, et on a, avec les notations du lemme,

$$Q(\mathbf{x}'') = \frac{P(\mathbf{x}')}{p^n} + \mathbf{x}'^T M \mathbf{x}'' + \frac{1}{2} p^n \mathbf{x}''^T M \mathbf{x}'' \equiv 0 \mod p, \quad \text{ou bien} \quad \mathbf{x}'^T M \mathbf{x}'' \equiv -\frac{P(\mathbf{x}')}{p^n} \mod p.$$

Cette dernière congruence, linéaire en $\mathbf{x}''$, aura une solution si $\mathbf{x}'^T M \not\equiv 0$ modulo $p$. Mais cela a lieu puisque $\mathbf{x}' \not\equiv 0$ et que $M$ est inversible modulo $p$. Donc la congruence proposée a une solution modulo $p^{n+1}$, et pour tous les moduli $p^k$ en général.

Observons encore que le théorème des restes chinois peut être vu comme un corollaire de ce lemme, en réduisant la question par induction au cas de deux facteurs $m_1 := n_1$ et $m_2 := n_2$, et en appliquant la méthode précédente au polynôme $P(X) = n_2(X - a_1) + n_1(X - a_2)$ (avec les notations du début de l'article).

## Utilisations

Le théorème des restes chinois est largement utilisé en arithmétique et en algèbre, notamment sous sa forme générale dans l'arithmétique des corps, que ce soit au cours de démonstrations théoriques aussi bien que dans des cas pratiques.

Dans le domaine de l'algorithmique, il est par exemple utilisé dans l'algorithme RSA en cryptographie, et il intervient aussi dans l'algorithme de Silver-Pohlig-Hellman pour le calcul du logarithme discret. Il intervient dans l'algorithme de test de primalité de Agrawal et Biswas, développé en 1999[18].

Il permet de représenter de grands nombres entiers comme n-uplets de restes de divisions euclidiennes. Sous cette forme, des opérations comme l'addition ou la multiplication peuvent se faire en parallèle en temps constant (pas de propagation de retenue). Par contre, la comparaison ou la division ne sont pas triviales.

## Notes et références

1. Selon A. Zachariou, le théorème des restes chinois aurait été découvert antérieurement par les Grecs (Paulo Ribenboim, Nombres premiers et records, PUF, 1re éd., 1994, p. 24).
2. (en) Man-Keung Siu, « "Algorithmic mathematics" and "Dialectics mathematics" (http://hkumath.hku.hk/~mks/ALGDIA.pdf) », *Proc. 2d International Conference on the Teaching of Mathematics*, 2002, p. 6.
3. (la) Leonardus « Pisanus », *Liber Abbaci (http://www.mdz-nbn-resolving.de/urn/resolver.pl?urn=urn:nbn:de:bvb:12-bsb10525679-8)*, Tipogr. delle Scienze Matematiche e Fisiche, 1857, p. 304 (S. 311).
4. (la) L. Euler, « Solutio problematis arithmetici (http://eulerarchive.maa.org/docs/originals/E036.pdf) de inveniendo numero, qui per datos numeros divisus relinquat data residua », *Commentarii academiae scientiarum Petropolitanae*, vol. 7, 1740, p. 46-66, ou bien *Opera Omnia*, Series 1, vol. 2, p. 18-32.
5. (la) C. F. Gauss, *Disquisitiones arithmeticae (https://gallica.bnf.fr/ark:/12148/bpt6k994003/f27.image.r=.langFR)*, 1801, p. 23, §32. Reproduction de la traduction *Recherches arithmétiques*, Gabay, 1989, p. 15.
6. (en) Ulrich Libbrecht, *Chinese Mathematics in the Thirteenth Century*, 1973.
7. Denis Daumas, Michel Guillemot, Olivier Keller, Raphaël Mizrahi et Maryvonne Spiesser, Le théorème des restes chinois (http://culturemath.ens.fr/content/le-th%C3%A9or%C3%A8me-des-restes-chinois-textes-commentaires-et-activit%C3%A9s-pour-l%E2%80%99arithm%C3%A9tique-au-lyc%C3%A9e), Textes, commentaires et activités pour l'arithmétique au lycée, sur le site CultureMath (http://www.math.ens.fr/culturemath/index.html) de l'ENS, § 1. Le problème des restes chinois : Questions sur ses origines (http://www.math.ens.fr/culturemath/materiaux/irem-toulouse11/questions-sur-les-origines.html#r3).
8. Louis Frécon, *Arithmétiques*, Publibook, 2016 (lire en ligne (https://books.google.com/books?id=EZU2DQAAQBAJ&pg=PA121)), p. 121.
9. (en) Dexter C. Kozen, *Theory of Computation*, Springer-Verlag, coll. « Texts in Computer Science », 2006 (ISBN 9781846282973, lire en ligne (https://www.springer.com/gp/book/9781846282973)), p. 86, Supplementary Lecture B, Chinese Remaindering
10. (en) Moshe Jarden (en), « Intersections of local algebraic extensions of a Hilbertian field », dans A. Barlotti et al., *Generators and Relations in Groups and Geometries*, Dordrecht, Kluwer, coll. « NATO ASI Series C » (no 333), 1991 (lire en ligne (http://www.math.tau.ac.il/~jarden/Articles/paper56.pdf)), p. 343-405, p. 17 du pdf, prop. 4.4, 4.5 et rmk 4.6.
11. (en) J. W. S. Cassels et A. Fröhlich, *Algebraic Number Theory*, Academic Press, 1967, 366 p. (ISBN 978-0-9502734-2-6), p. 48.
12. Les $n_i$ sont produits de puissances $p_{i,j}^{c_{i,j}}$ où les $p_{i,j}$ sont des facteurs premiers distincts. En appliquant le thm. d'approximation faible aux valuations $p_i$-adiques $v_{i,j}$ correspondantes, on obtient un $x$ tel que $v_{i,j}(x - q_i) = c_{i,j}$. Donc $x - q_i$ est multiple de $p_{i,j}^{c_{i,j}}$ pour tout $j$, et donc de $n_i$.
13. Preuve directe: notons $q_i = a_i / b_i$, et $c_{i,j}$ = P.G.C.D.($n_i$, $b_j$). Pour tout $i$, le théorème chinois fournit des nombres entiers $e_i$ tels que $e_i = 1 \bmod n_i$ et $e_i = 0 \bmod n_k c_{k,i}$, pour tout $k \neq i$. Alors $q = \sum_i q_i e_i$ satisfait à la question.
14. N. Bourbaki, *Algèbre, chapitres 1 à 3*, Springer, 2007 (ISBN 978-3-540-33849-9), p. A I.105 et 103.
15. Un contre-exemple dans l'anneau des matrices triangulaires supérieures de taille 2 est proposé en exercice dans Bourbaki 2007, p. A I.151.
16. (en) Pete L. Clark, « Commutative Algebra » (http://alpha.math.uga.edu/~pete/integral2015.pdf), sur *alpha.math.uga.edu*, 2015, p. 345-348, Th. 21.1 et 21.6.
17. (en) László Fuchs (en) et Luigi Salce, *Modules over Non-Noetherian Domains*, AMS, 2001 (lire en ligne (https://books.google.com/books?id=gK_yBwAAQBAJ&pg=PA91)), chap. III (« Prüfer Domains »), p. 91-96, Th. 1.1 + ex. 1.9 et 1.10.
18. Manindra Agrawal et Somenath Biswas, « Primality and Identity Testing via Chinese Remaindering », *Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society, fOCS '99, 1999, p. 202– (ISBN 9780769504094, lire en ligne (http://dl.acm.org/citation.cfm?id=795665.796517), consulté le 9 juillet 2019)

## Voir aussi

### Articles connexes

- Théorème de Bachet-Bézout
- Système couvrant

### Bibliographie


- Michel Demazure, *Cours d'algèbre. Primalité. Divisibilité. Codes.*, Cassini, coll. « Nouvelle bibliothèque mathématique », 1997 (ISBN 978-2842250003)
- Ronald Graham, Donald Knuth et Oren Patashnik (trad. Alain Denise), *Mathématiques concrètes : Fondations pour l'informatique*, Paris, Vuibert, 2003, 2e éd., xiv+688 (ISBN 978-2-7117-4824-2)


### Liens externes

- **(en)** Chinese Remainder Theorem (http://www.cut-the-knot.org/blue/chinese.shtml) sur cut-the-knot

---