# Ne léser aucun héritier

*Une mère mathématicienne veut léguer à ses trois enfants son héritage dans un coffre-fort dont elle peut choisir le code. Mais, elle ne fait confiance à aucun des trois. Elle veut être sûre qu'après sa mort ses trois enfants seront présents lors de l'ouverture du coffre et qu'aucun d'eux ne pourra se servir en l'absence des autres. Elle utilise le théorème des restes chinois[1] pour choisir le code.*

**Christiane Rousseau**
Université de Montréal

La mère mathématicienne écrit une lettre personnelle à chacun de ses trois enfants, Alba, Bernardo et Claudia.

À Alba, elle écrit :

*« Le code C est un nombre entier entre 1 et 13 208. Le reste de la division de C par 17 est 3. »*

À Bernardo, elle écrit :

*« Le code C est un nombre entier entre 1 et 13 208. Le reste de la division de C par 21 est 4. »*

À Claudia, elle écrit :

*« Le code C est un nombre entier entre 1 et 13 208. Le reste de la division de C par 37 est 5. »*

Alba toute seule ne peut ouvrir le coffre : tous les nombres 3, 20, ..., 13 195 ont pour reste 3 de la division par 17, et elle sait qu'après trois essais infructueux la serrure va se bloquer. De même pour Bernardo et Claudia.

Alba et Claudia ne peuvent ouvrir le coffre à elles deux. Remarquons que $13 \times 37 = 629$. Tous les nombres 190, $190 + 629 = 819$, $190 + 2 \times 629 = 1\,448$, 2 077, ..., 12 770, ont pour reste 3 de la division par 17, et pour reste 5 de la division par 37.

## Note historique

Le théorème des restes chinois apparaît pour la première fois dans le livre de Sun Zi au III$^{e}$ siècle. Il est ensuite étudié dans le livre de Qin Jiushao en 1247. À cette époque, le problème est étudié simultanément en Europe par Fibonacci et dans le monde arabe par Ibn al-Haytham.

Regardons cette suite : elle est de la forme

$$190 + 629 = 819$$
$$190 + 2 \times 629 = 1\,448$$
$$190 + 3 \times 629 = 2\,077$$
$$\vdots$$
$$190 + 20 \times 629 = 12\,770$$

Parmi ces nombres, se trouve le nombre $190 + 18 \times 629 = 112\,512$. C'est le seul dont le reste de la division par 21 est 4. Le code $C$ est donc

$$C = 11512.$$

Mais, le duo Alba-Claudia n'aurait pas pu le trouver, car elles n'ont pas vu la lettre de Bernardo et ne savent pas que le code est un nombre dont le reste de la division par 21 est 4. De même, les autres duos Alba-Bernardo ou Bernardo-Claudia n'auraient pas pu trouver le code avec leurs seules données.

## Visualiser le théorème des restes chinois

On range des jetons dans une boite. Si on prend une boite de largeur 3, on obtient un nombre entier de rangées et un reste de 2. Si on prend une boite de largeur 5, on obtient un nombre entier de rangées et un reste de 4. Si on prend une boite de largeur 7, on obtient un nombre entier de rangées et un reste de 1. Si on sait qu'on a au plus $3 \times 5 \times 7 - 1 = 104$ jetons, la seule solution est d'avoir 29 jetons.

1. *Voir aussi l'article* « Les entiers… ces fonctions qui s'ignorent » *dans Accromath 9.2.*

## La recette pour construire un tel code

La recette peut fonctionner avec n'importe quel nombre d'héritiers. Nous allons la présenter pour deux héritiers et dans la section problèmes vous pourrez la généraliser et construire un code pour trois héritiers.

On se donne deux entiers $m$ et $n$ relativement premiers. Le reste de la division d'un entier par $m$ est un nombre de l'ensemble $M=\{0, 1, \dots, m-1\}$.

De même, le reste de la division d'un entier par $n$ est un nombre de l'ensemble $N=\{0,1, \dots, n-1\}$. Soit $a\in M$ et $b\in N$. *Le théorème des restes chinois* affirme qu'il existe un unique entier $C$ de l'ensemble $E=\{0,1, \dots, mn-1\}$ tel que

- le reste de la division de $C$ par $m$ est $a$,
- et le reste de la division de $C$ par $n$ est $b$.

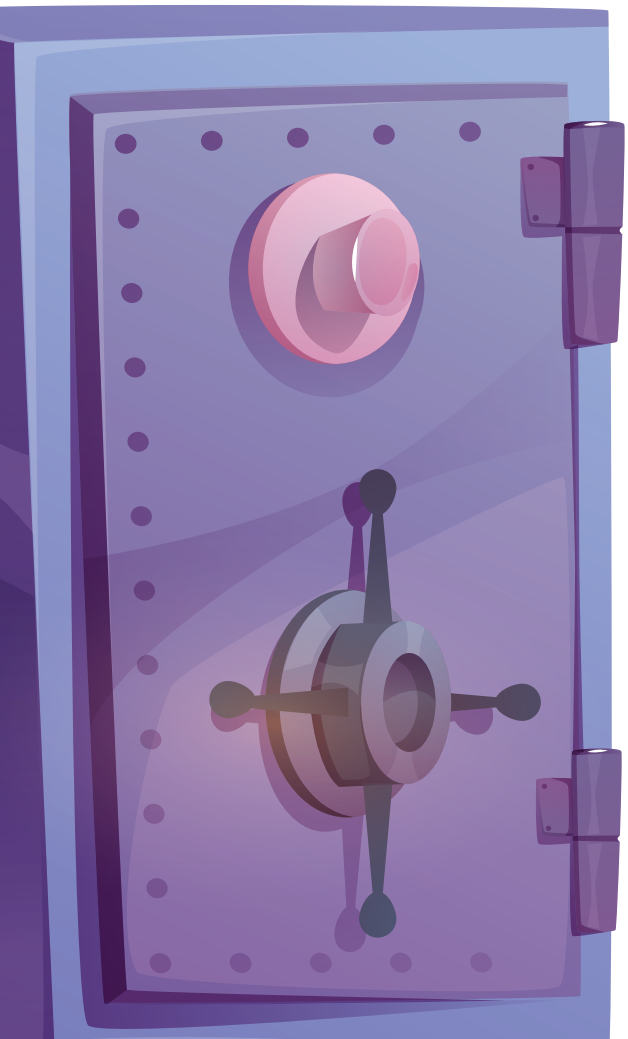
En pratique, on construit

- un premier entier $c$ dont le reste de la division par $m$ est 1 et le reste de la division par $n$ est 0.
- un deuxième entier $d$ dont le reste de la division par $m$ est 0 et le reste de la division par $n$ est 1.

Alors, le nombre $D=ac+bd$ est un nombre dont le reste de la division par $m$ est $a$ et le reste de la division par $n$ est $b$ (voir section problèmes). Cependant, il pourrait arriver que $D \geq mn$. Dans ce cas, l'entier $C$ cherché est le reste de la division de $D$ par $mn$ qui appartient bien à $E$.

Voici un exemple numérique simple dont vous pouvez vérifier les détails. On prend $m=4$ et $n=15$. Les trois multiples de 15 dans $E=\{0, 1, \dots, 59\}$ sont 15, 30 et 45. Les restes de leur division par 4 sont 3, 2, et 1. Donc, on prend $c=45$. Les 14 multiples de 4 dans $E$ sont 4, 8, 12, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56. Les restes de leur division par 15 sont 4, 8, 12, 1, 5, 9, 13, 2, 6, 10, 14, 3, 7, 11. Donc, on prend $d=16$. Alors, $D=45a+16b$. Prenons le cas particulier $a=2$ et $b=6$. Alors, $D=45\times 2+16\times 6=186=3\times 60+6$. Ceci donne le code $C=6$.

Ici on a trouvé $c$ et $d$ à tâtons. Il existe une manière algorithmique de trouver $c$ et $d$ (voir encadré).



### Trouver $c$ et $d$

Rappelons que $m$ et $n$ sont relativement premiers, donc leur PGCD est 1. Le théorème de Bezout affirme qu'il existe deux entiers relatifs $x$ et $y$ tels que

$$1 = PGCD(m; n) = mx + ny \quad (*)$$

Prenons le nombre $ny$: le reste de sa division par $m$ est 1 et le reste de sa division par $n$ est 0. D'autres nombres qui ont cette propriété sont les nombres $ny+kmn$ où $k$ est un entier relatif. En général, on choisit pour $c$ le seul nombre de la forme $ny+kmn$ qui se trouve dans $E$. De même, on choisit pour $d$ le seul nombre de la forme $mx+lmn$ qui se trouve dans $E$.

Ce qui est remarquable c'est que cette méthode extrêmement efficace numériquement remonte à Euclide environ 300 ans av. J.-C. Nous vous invitons à découvrir le théorème de Bezout dans l'article « *Trouver le PGCD de deux entiers* » de ce même numéro.