Des saints, des scélérats et deux théorèmes qui sont vraiment les mêmes

Ezra Brown

Voici une histoire qui mêle comptage de saints, protection de secrets d'espions scélérats, deux cours dos à dos, et façon dont certains étudiants qui suivaient ces deux cours ont remarqué que le théorème des restes chinois (un théorème de théorie des nombres) et le théorème de l'interpolation polynomiale (un théorème d'analyse numérique) sont vraiment les mêmes.

Saviez-vous que ces deux théorèmes sont identiques ?

Le théorème des restes chinois est un des théorèmes fondamentaux de la théorie des nombres. Il énonce que si les entiers positifs $m_1, \ldots, m_n$, sont deux à deux premiers entre eux (c'est-à-dire si jamais deux d'entre eux n'ont un facteur commun sauf 1), alors étant donnés des entiers quelconques $a_1, ..., a_n$, il existe une solution $x = X$ au système de n congruences

$$x \equiv a_i \bmod m_i \text{ pour } 1 \leq i \leq n$$

et que cette solution X est unique à ajout de multiples entiers du produit $m_1 m_2 \ldots m_n$ près. La clef de ce théorème est que si p est un nombre premier fixé et si q est tout premier sauf p, alors il existe des entiers s et t tels que $sp + tq = 1$. Ces conditions nous permettent de construire des formules pour calculer la solution X.

Le théorème d'interpolation polynomiale est l'un des théorèmes fondamentaux de l'analyse numérique. Il énonce que si $x_1, ..., x_n$ sont des nombres réels distincts et si $y_1, ..., y_n$ sont des nombres réels quelconques, alors il existe un polynôme $P(x)$ de degré au plus $n-1$ tel que $P(x_i) = y_i$ pour $1 \leq i \leq n$ et que ce polynôme $P(x)$ est unique. La clef de ce théorème est que si a et b sont des nombres distincts, alors il existe des constantes s et t telles que $s(x-a) + t(x-b) = 1$. Le fait que les x_i soient distincts nous permet de construire une formule de calcul du polynôme $P(x)$; une telle formule ressemble aux formules obtenues à partir du théorème des restes chinois.

Ces deux théorèmes sont les cas particuliers d'une construction dans un contexte plus général et dans cet article, nous décrivons un scénario - notamment deux cours dos à dos - dans lequel les étudiants ont découvert ce fait. On finit en décrivant le contexte général, dans lequel l'idée clef est la possibilité d'écrire 1 d'une façon particulière.

The saints go marching in - combien y en a-t-il ?

Le cours de théorie des nombres démarrait à midi et le sujet du cours était les systèmes de congruence. La classe était mécontente du premier exemple vu au cours précédent. Les étudiants disaient qu'une recherche directe pour trouver le plus petit entier ayant comme restes 2, 3, et 2 lorsqu'on le divise par 3, 5, et 7 (respectivement), serait plus rapide et facile qu'une méthode compliquée. J'approuvais et écrivis au tableau le problème suivant.

Référence : The mathematical association of America, Vol. 46, n° 5, novembre 2015, the College mathematics journal.
Traduction : Denise Vella-Chemla, septembre 2024.

Trouver le plus petit nombre N qui a pour restes $521,607$, et 11 213 lorsqu'on le divise par 193 707 721, 6 695 717 641, et 761 838 257 287, respectivement.

Une recherche exhaustive du plus petit N utilisant des milliards d'ordinateurs, chacun capable de tester un milliard de cas par seconde, prendrait plus de 30 000 ans. Au contraire, un système algébrique informatique résout ce problème en une fraction de seconde. Donc, il vaut mieux utiliser une méthode autre que la recherche brute, n'est-ce pas ?

La classe semblait globalement d'accord avec ça.

Pour illustrer cette méthode, voici un problème qui fait intervenir des diviseurs légèrement plus grand que $3, 5$, et 7 et qui concerne la chanson bien connue "When the Saints Go Marching In." Pour un amoureux des nombres, la phrase "Oh, I want to be in that number"[1] intrigue parce que *personne n'a jamais dit quel est ce nombre.* Ici déterminons ce nombre dans un cas particulier.

Les saints marchent et on connaît quelques faits à leur propos :

- S'ils marchent par lignes de 7, il en reste 3 tout seuls.
- S'ils marchent par lignes de 11, il en reste 1 tout seul.
- S'ils marchent par lignes de 13, il en reste 9 tout seuls.
- Il y a moins de 1000 saints.
- Combien de saints marchent ?

En utilisant la notation des congruences, le problème devient celui de trouver le nombre de saints S tel que

$$S \equiv 3 \bmod 7, \quad S \equiv 1 \bmod 11, \quad S \equiv 9 \bmod 13, \quad S < 1000.$$

À ce point de l'exposé, on peut poser trois questions.

1. Y a-t-il une solution ?
2. Si oui, comment en trouver une ?
3. Si oui, y a-t-il une jolie formule qui donne une solution ?

Prenons ces questions l'une après l'autre. D'abord, l'ensemble des congruences a en effet une solution et cela est garanti par l'un des grands résultats de la théorie des nombres, notamment le théorème des restes chinois (TRC).

Théorème 1 (théorème des restes chinois). *Soient $m_1, ..., m_n$, des entiers deux à deux premiers entre eux (c'est-à-dire que $\gcd(m_i, m_j) = 1$ pour $i \neq j$), et soient $y_1, ..., y_n$ des entiers. Alors le système de congruences*

$$X \equiv y_1 \bmod m_1, \ldots, X \equiv y_n \bmod m_n$$

a une solution $X = S$ qui est unique mod $m_1...m_n$.

[1] traduisible par : "Je veux être du nombre", i.e. je veux être l'un d'entre eux.'

Pour une preuve, voir [2, pp. 38-39], [4, pp. 158-167], ou [5, pp. 235-244], par exemple.

Ce théorème implique qu'une solution S existe, puisque 7, 11, et 13 sont deux à deux premiers entre eux. Voici comment on peut effectivement trouver S. La première congruence, $S \equiv 3 \bmod 7$, implique que 7 divise $S-3$, donc $S = 3+7t$ pour un certain entier t. La substitution dans la seconde congruence et le réarrangement des termes amène à

$$S = 3 + 7t \equiv 1 \bmod 11, \quad \text{donc } 7t \equiv 1 - 3 \equiv 9 \bmod 11.$$

Rappelons que l'algorithme d'Euclide trouve $g = \text{pgcd}(a,b)$ ainsi que les entiers x et y tels que $ax + by = g$. Si $g = 1$, cela implique que $ax \equiv 1 \bmod b$. Donc, x est l'inverse pour la multiplication de a mod b et on écrit $x = a^{-1} \bmod b$. Puisque $\text{pgcd}(7,11) = 1$, on sait que $7x \equiv 1 \bmod 11$ a une solution. Il s'avère que $x = 8$ convient, donc on obtient $t \equiv 8 \cdot 7t \equiv 8 \cdot 9 \equiv 72 \equiv 6 \bmod 11$ de telle façon que $t = 6 + 11u$ et

$$S = 3 + 7(6 + 11u) = 45 + 77u$$

La troisième congruence devient $9 \equiv S \equiv 45 + 77u \bmod 13$; pourtant, $77u \equiv 12u \bmod 13$ et on voit que $u \equiv 3 \cdot 12 \equiv 10 \bmod 13$. Donc, $u = 10 + 13v$ et, puisque $7 \cdot 11 \cdot 13 = 1001$, on obtient notre résultat final, notamment que

$$S = 3 + 7(6 + 11(10 + 13v)) = 3 + 42 + 770 + 7 \cdot 11 \cdot 13v = 815 + 1001v.$$

Ainsi, pour chaque entier v, la quantité $S = 815 + 1001v$ satisfait chacune des trois congruences. Finalement, puisque $S < 1000$, il y a $S = 815$ saints.

Les preuves du TRC fournissent la formule générale suivante pour une solution générale.

Théorème 2 (formule des restes chinois). *Étant donnés des entiers deux à deux premiers entre eux $m_1 ...., m_n$, et des entiers $y_1, ..., y_n$, définissons les nombres M et M_i, M_i^* pour $1 \leq i \leq n$ par*

$$M = m_1 m_2 \ldots m_n, \quad M_i = M/m_i, \quad M_i^* = M_i^{-1} \bmod m_i.$$

Alors $X = y_1 M_1 M_1^* + \ldots + y_n M_n M_n^*$ est une solution du système de n congruences $X \equiv y_i \bmod m_i$, qui est unique modulo M.

Notons que M_i est le produit de tous les m_j pour $j \neq i$ donc $\text{pgcd}(M_i, m_i) = 1$. Il en découle que M_i a un inverse mod m_i, et on note cet inverse M_i^*.

On peut utiliser la formule pour résoudre le problème des saints. Étant donnés $S \equiv 3 \bmod 7, S \equiv 1 \bmod 11$, et $S \equiv 9 \bmod 13$, appelons $m_1 = 7, m_2 = 11$, et $m_3 = 13$. Alors

$$\begin{aligned} M_1 &= 11 \cdot 13 \equiv 4 \cdot 6 \equiv 24 \equiv 3 \bmod 7 \text{ et } M_1^* = 5 \\ M2 &= 7.13 \equiv 7 \cdot 2 \equiv 14 \equiv 3 \bmod 11, \text{ et } M_2^* = 4, \\ M_3 &= 7 \cdot 11 = 77 \equiv 12 \bmod 13 \text{ et } M_3^* = 12, \end{aligned}$$

et $S = 3 \cdot 143 \cdot 5 + 1 \cdot 91 \cdot 4 + 9 \cdot 77 \cdot 12 \equiv 815 \bmod 1001$ comme précédemment. Finalement, on voit que $815 = 3 + 116 \cdot 7 = 1 + 74 \cdot 11 = 9 + 62 \cdot 13$ satisfait chacune des trois congruences.

L'étape-clef pour vérifier la formule est de voir que

$$M_i M_i^* \equiv= \begin{cases} 1 & \mod m_i, \\ 0 & \mod m_j, \quad \text{pour } j \neq i. \end{cases}$$

Sur ce, ce fut la fin du cours. Je promis de donner une preuve au cours suivant, les étudiants se dispersèrent, et certains d'entre eux marchèrent avec moi jusqu'au cours de cryptographie.

Partager des secrets au milieu de personnes indignes de confiance

Le cours de cryptographie commençait à 13 h 30 et le sujet du jour était comment partager un secret en utilisant des régimes de seuil. On commença par l'exemple suivant.

Vous, un milliardaire, avez enfermé vos actifs dans un coffre et vous êtes le seul à en connaître la combinaison. Vous voulez partager votre fortune avec vos sept enfants. Certains d'entre eux sont de bonnes personnes, mais les autres sont des scélérats indignes de confiance. Pour rendre les choses encore pire, ils ne s'entendent pas bien. Vous leur dites que trois d'entre eux ou plus peuvent découvrir le secret en travaillant ensemble. Sinon, votre succession reviendra à votre nièce et à votre neveu préférés, que vos enfants détestent.

Ce que vous, le milliardaire, venez de décrire, c'est un *régime de seuil*.

C'est-à-dire, soient n et w des entiers positifs avec $n \leq w$. Un (n, w)-*régime de seuil* est une façon de partager un nombre secret S entre w participants de telle manière que n'importe quels n d'entre eux puissent aisément reconstruire S mais qu'aucun ensemble de participants d'une taille plus petite ne puisse reconstruire S. Vous, le milliardaire, voulez un $(3, 7)$-régime de seuil ; le secret S est la combinaison du coffre.

Dans un scénario de partage de secret, la personne qui a un secret est le *banquier*, les participants sont les *joueurs*, et on donne à chaque joueur une *part* distincte. Voici un scénario de seuil développé par Adi Shamir (le "S" dans RSA) qui fonctionne comme suit. D'abord, le banquier construit un polynôme $P(x)$ de degré $n-1$ dont le terme constant est le secret S. (Pour vous, le milliardaire, le polynôme est le polynôme quadratique $P(x) = S + ax + bx^2$.) Alors, le banquier donne une part à chacun des w joueurs, la part du $i^{\text{ième}}$ joueur étant un point $(x_i, y_i) = (x_i, P(x_i))$ sur la courbe.

Table 1. Les parts du banquier dans un scénario de seuil $(3, 7)$

Joueur	1	2	3	4	5	6	7
Part	$(1, 9)$	$(2, 13)$	$(3, 23)$	$(4, 39)$	$(5, 61)$	$(6, 89)$	$(7, 123)$

Un appel à volontaires a permis de trouver sept étudiants à qui j'ai octroyé les sept parts de la table 1. J'ai ordonné à trois étudiants de mettre en commun leurs parts et de résoudre les équations résultantes pour le polynôme $S + ax + bx^2$. Les quatre étudiants restant devaient constituer des binômes et faire de même. Les joueurs 1, 4, et 6 ont mis leurs ressources en commun et ont obtenu les équations

$$\begin{aligned} S + a + b &= 9 \\ S + 4a + 16b &= 39 \\ S + 6a + 36b &= 89 \end{aligned}$$

Les doigts se levèrent au-dessus des écrans ; résoudre le système 3×3 résultant a amené le polynôme $11-5x+3x^2$ et le nombre secret s'est avéré être 11. N'importe quel autre ensemble de trois joueurs aurait amené à la même conclusion.

Quand les joueurs 2 et 5 ont essayé ça, leur deux équations à trois inconnues ont amené les équations $S = 10b - 19$ et $a = -7b + 16$. Leur système indéterminé avait de nombreuses solutions et le terme constant S pouvait être vraiment n'importe quoi. Il est arrivé la même chose aux joueurs 3 et 7. Finalement, si quatre joueurs ou plus partageaient leur gain, alors le système résultant serait cohérent et les joueurs apprendraient le secret S.

En général, si n joueurs coopérant mettent en commun leur part, alors ils trouveront le polynôme $P(x)$ et donc son terme constant, qui est le secret S, mais aucun ensemble de moins de joueurs ne peut obtenir aucune information à propos du secret. Ceci est une conséquence du théorème suivant qui concerne le passage d'une courbe polynomiale par un ensemble donné de points.

Théorème 3 (interpolation polynomiale). *Supposons que $(x_1, y_1), ..., (x_n, y_n)$ soient des points du plan, les x_i étant distincts. Il y a un polynôme unique $P(x)$ de degré au plus $n-1$ qui passe par chacun de ces points, i.e., $P(x_i) = y_i$ pour $1 \le i \le n$.*

Pour une preuve, voir [1, pp. 105-116], [5, pp. 309-316], ou [8, pp. 179-199].

Voici comment marche la méthode. Étant donnés les points $(x_1, y_1), ..., (x_n, y_n)$ avec des coordonnées en x distinctes, on veut trouver des nombres réels $a_0, ..., a_{n-1}$ tels que le système d'équations $y_i = P(x_i) = a_0 + a_1 x_i + \ldots + a_{n-1}x_i^{n-1}$ a une solution unique. Le système linéaire résultant $n \times n$ d'inconnues $\{a_i\}$ devient l'équation matricielle $V_n \cdot a = y$, où

$$V_n = \begin{bmatrix} 1 & x_1 & \ldots & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \ldots & x_n^{n-1} \end{bmatrix}, \quad a = \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}, \quad y = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{bmatrix}.$$

Il s'avère que le déterminant de V_n (appelé matrice de Vandermonde) est donné par

$$\det V_n = \prod_{1 \le i < j \le n} (x_j - x_i).$$

Puisque les x_i sont distincts, cette formule signifie que $\det V_n \neq 0$, ce qui fait que le système a une solution unique $\{a_0, ..., a_{n-1}\}$ et que le polynôme résultant est l'unique polynôme de degré au plus $n-1$ qui passe par les points donnés.

Dans une application cryptographique sérieuse, le secret S pourrait être un entier de plusieurs centaines de bits. On choisit un nombre premier q plus grand que le secret, et tous les calculs sont faits sur les entiers modulo q. Les coefficients sont choisis aléatoirement dans l'ensemble $\{1, 2, ..., q\}$, chaque nombre étant choisi avec une probabilité $1/q$. Les x_i sont choisis pour être différents mod q, ce qui implique que la matrice de coefficients V_n du système linéaire $n \times n$ résultant a un déterminant non nul mod q.

Il y a une alternative pour trouver le polynôme $P(x)$ par l'algèbre linéaire, notamment une méthode pas à pas qui mène à une formule pour le polynôme.

D'abord, on trouve une courbe polynomiale $y = P(x)$ qui passe par le point (x_1, y_1). Alors on modifie P de telle façon que la courbe passe à la fois par (x_1, y_1) et par (x_2, y_2). On procède de cette manière jusqu'à ce qu'on ait construit une courbe polynomiale qui passe par tous les points donnés. On donne les détails pour trois points ci-dessous.

Si (x_1, y_1) est un point de la courbe polynomiale $y = P(x)$ alors on a $y_1 = P(x_1)$. Quand on divise un polynôme $P(x)$ de degré positif par $x - x_1$, le processus habituel de division longue produit un quotient $q(x)$ et un reste $r(x)$ et, puisque $x - x_1$ a pour degré 1, le reste est une constante r. Par conséquent $P(x) = r + (x - x_1)q(x)$. Si on substitue $x = x_1$, alors on voit que $r = P(x_1) = y_1$ s'évanouit. Donc, $P(x) = y_1 + (x - x_1)q(x)$ est un polynôme qui passe par (x_1, y_1).

Pour $x = x_2$, on a $y_2 = P(x_2) = y_1 + (x_2 - x_1)q(x_2)$. À nouveau, la supposition que les x_i sont distincts nous permet de diviser les deux côtés de cette équation par $x_2 - x_1$ et donc $q(x_2) = (y_2 - y_1)/(x_2 - x_1)$. Comme auparavant, cela implique $q(x) = q(x_2) + (x - x_2)h(x)$ pour un certain polynôme $h(x)$ et donc

$$\begin{aligned} P(x) &= y_1 + (x - x_1)(q(x_2) + (x - x_2)h(x)) \\ &= y_1 + (x - x_1)\left(\frac{y_2 - y_1}{x_2 - x_1} + (x - x_2)h(x)\right). \end{aligned}$$

Pour le troisième et dernier point, on utilise le fait que $y_3 = P(x_3)$ pour trouver une valeur de $h(x_3)$. En substituant $x = x_3$, on aboutit à l'équation

$$h(x_3) = \frac{1}{x_3 - x_2}\left(\frac{y_3 - y_1}{x_3 - x_1} - \frac{y_2 - y_1}{x_2 - x_1}\right).$$

$P(x)$ passe par les trois points donnés à chaque fois que $h(x_3)$ est comme ci-dessus, et, en particulier, à chaque fois que $h(x)$ est constant avec cette valeur de $h(x_3)$. De cela, on obtient l'équation

$$P(x) = y_1 + (x - x_1)\left(\frac{y_2 - y_1}{x_2 - x_1} + \frac{x - x_2}{x_3 - x_2}\left(\frac{y_3 - y_1}{x_3 - x_1} - \frac{y_2 - y_1}{x_2 - x_1}\right)\right).$$

En effet, $P(x_i) = y_i$ pour $i = 1, 2, 3$. S'il y avait un quatrième point, on écrirait $h(x) = h(x_3) + (x - x_3)k(x)$ et on utiliserait le fait que $y_4 = P(x_4)$ pour mettre (x_4, y_4) sur la courbe.

Un étudiant a dit que la formule ci-dessus pour la solution avait l'air trop embrouillée, et a demandé s'il pouvait y avoir une formule qui paraîtrait plus simple. Cela m'a amené à demander à la classe de prendre cette formule "embrouillée" pour $P(x)$ et à séparer les termes qui contiennent y_1, y_2 et y_3. Ils ont trouvé

$$P(x) = y_1\frac{(x - x_2)(x - x_3)}{(x_1 - x_2)(x_1 - x_3)} + y_2\frac{(x - x_1)(x - x_3)}{(x_2 - x_1)(x_2 - x_3)} + y_3\frac{(x - x_1)(x - x_2)}{(x_3 - x_1)(x_3 - x_2)}$$

On voit que le terme dont le coefficient est y_i est égal à 1 si $x = x_i$ et à 0 si $x = x_j$ pour $j \neq i$. Cette forme du polynôme se généralise comme suit.

Étant donnés n points (x_i, y_i) avec les x_i distincts, définissons les *polynômes d'interpolation de Lagrange* $\mathcal{L}_i(x)$ par

$$\mathcal{L}_i(x) = \prod_{j \neq i} \frac{x - x_j}{x_i - x_j}.$$

Maintenant $\mathcal{L}_i(x_j) = 1$ si $j = i, 0$ pour $j \neq i$ et l'unique polynôme de degré au plus $n - 1$ passant par les n points est égal à $P(x) = y_1\mathcal{L}_1(x) + \ldots + y_n\mathcal{L}_n(x)$. On appelle cette expression la *formule d'interpolation de Lagrange*.

Une étudiante leva la main. "Attendez une minute. N'est-ce pas juste comme le théorème des restes chinois ?".

La connexion

Je lui demandais de poursuivre.

L'étudiante qui suivait également le cours de théorie des nombres continua. "Regardez, lors de l'heure de cours précédente, on a étudié le théorème des restes chinois en théorie des nombres. Vous avez écrit une solution générale. Ici, on étudie le théorème de l'interpolation polynomiale, et à nouveau, vous écrivez une solution générale. Les solutions aux deux problèmes semblent les mêmes. Donc ce nouveau théorème est une version polynomiale du théorème des restes chinois." Le TRC était apparu plus tôt lors du cours de cryptographie, "Ceci est un exemple de plus des nombreuses connexions entre des domaines apparemment différents des mathématiques. En fait, les deux théorèmes sont effectivement le même théorème."

Comment le problème de l'interprétation polynomiale ressemble-t-il à un système de congruences ?

Soient a, b, m des entiers avec $m \neq 0$. La congruence $a \equiv b \bmod m$ est un énoncé que l'entier $a - b$ est un multiple de m.

Soient $y_1 = P(x_1)$. Quand on divise $P(x)$ par $x - x_1$, on obtient un polynôme quotient $q(x)$ et un polynôme reste $r = P(x_1)$. Comme on l'a vu précédemment, cela amène à l'équation $P(x) - y_1 = (x - x_1)g(x)$. On peut écrire cette équation comme une *congruence polynomiale*, notamment $P(x) \equiv y_1 \bmod (x - x_1)$. Cela a du sens, parce qu'une congruence est l'énoncé que la différence de deux quantités est divisible par une troisième quantité.

En fait, la somme, la différence, et le produit des polynômes sont toujours des polynômes. La division de polynômes, comme la division d'entiers, c'est une histoire différente, et donc nous devons fournir quelques définitions. (À ce point, notons que parce que nos polynômes ont leurs coefficients dans un corps arbitraire, on s'attend à ce que notre division polynomiale fasse intervenir non seulement des nombres entiers mais également des nombres rationnels.)

Plus formellement, soient $a(x)$ et $b(x)$ des polynômes avec, disons, des coefficients rationnels et $b(x)$ polynôme non nul. On dit que $b(x)$ divise $a(x)$ si on a $a(x) = b(x)d(x)$ pour un certain polynôme $d(x)$. Par exemple, $c(x) = 2x^3 + 3x^2 - 6x - 35$. Factoriser $c(x) = (x^2 + 4x + 7)(2x - 5)$ montre qu'à la fois $2x - 5$ et $x^2 + 4x + 7$ divisent $c(x)$. D'un autre côté, $c(x) = (x - (3/2))(2x^2 + 6x + 3) - 61/2$

donc $x - (3/2)$ divise effectivement $c(x)$. Pourtant, la différence $c(x) - (-61/2)$ est divisible par $x - (3/2)$ et on peut écrire ce fait en écrivant la congruence

$$c(x) \equiv \frac{-61}{2} \bmod \left(x - \frac{3}{2}\right).$$

De cette algèbre, le théorème des restes chinois nous dit que $c(3/2) = -61/2$ et la congruence précédente nous dit que le polynôme $y = c(x)$ passe par le point $(3/2, -61/2)$.

On dit que $a(x)$ et $b(x)$ sont premiers entre eux si leurs seuls facteurs communs sont des polynômes constants. On peut maintenant réécrire le théorème d'interpolation polynomiale en fonction des congruences.

Théorème 4 (interpolation polynomiale, revisitée). *Supposons que $(x_1, y_1), ..., (x_n, y_n)$ sont des points du plan avec les x_i tous distincts. Soient*

$$P_i(x) = \prod_{j \neq i}(x - x_j) \quad et \quad P_i^* = \frac{1}{\prod_{j \neq i}(x_i - x_j)}.$$

Alors $\mathcal{L}_i(x) = P_i(x)P_i^*$ est l'unique polynôme de degré au plus $n-1$ qui passe par ces n points est donné par

$$P(x) = y_1 P_1(x)P_1^* + \ldots + y_n P_n(x)P_n^*.$$

Pour le théorème des restes chinois, la supposition que les m_j sont deux à deux premiers entre eux est essentielle : elle implique que le produit M_i est premier à m_i. Cela signifie que M_i est inversible mod m_i, un fait qui est la clef pour utiliser la formule des restes chinois.

Pour le théorème d'interpolation polynomiale, la supposition que les x_j sont distincts est essentielle : elle implique que

$$\frac{1}{x_i - x_j}(x - x_j) + \frac{1}{x_j - x_i}(x - x_i) = 1$$

donc les polynômes $x - x_j$ sont premiers entre eux deux à deux. Par conséquent, le produit $P_i(x)$ est inversible mod $(x - x_i)$ et on peut construire les polynômes d'interpolation de Lagrange.

Les polynômes $x - x_1, (x - x_1)(x - x_2), \ldots, (x - x_1)(x - x_2)\ldots(x - x_n)$ qui ont donné la solution étape par étape au problème d'interpolation polynomiale sont les polynômes d'interpolation de Newton, et la formule d'interpolation de Newton pour obtenir la solution est $P(x) = a_0 + (x - x_1)a_1 + \ldots + (x - x_1)\ldots(x - x_{n-1})a_{n-1}$ pour certaines constantes $a_0, \ldots, a_{n-1}$. La représentation par interpolation polynomiale de Newton de la solution au théorème d'interpolation polynomiale correspond à la solution du système de n congruences entières obtenu en satisfaisant les congruences une à une.

La table 2 résume la proche similarité des deux situations. Ces deux théorèmes sont en effet des cas particuliers d'une construction plus générale, donc nous verrons ensuite le contexte général.

Table 2. Comparer les deux problèmes

problème	résoudre $x \equiv a_i \bmod m_i$	résoudre $P(x) \equiv y_i \bmod (x - x_i)$
supposons	pgcd$(m_i, m_j) = 1$ si $i \neq j$	$x_i \neq x_j$ si $i \neq j$
existence	théorème des restes chinois	théorème d'interpolation polynomiale
technique	algorithme d'Euclide	algorithme d'Euclide pour les polynômes
résolution	congruences successives	interpolation par des polynômes de Newton
formule	formule des restes chinois	formule d'interpolation de Lagrange

Quelle est le contexte général ici ?

Le théorème des restes chinois commence avec un système de congruences de la forme $x \equiv a \bmod n$ et fournit les conditions suffisantes pour l'existence d'une solution à ce système. Le contexte général est celui de ces systèmes algébriques familiers qu'on appelle des anneaux.

Soit R un anneau commutatif avec 1 comme élément unité. Rappelons qu'un *idéal* I de R est un sous-ensemble de R qui est fermé selon l'addition et la soustraction et qui est tel que si $a \in I$ et $r \in R$, alors $ra \in I$. L'ensemble $\{ka : k \in R\}$ est l'*idéal engendré par* a, qu'on écrit (a). Par exemple, (3) est l'idéal des entiers multiples de 3 dans l'anneau des entiers et $(x - 5)$ est l'idéal contenant tous les polynômes multiples de $x - 5$ dans l'anneau des polynômes.

Les idéaux A et B sont dits premiers entre eux s'il existe des éléments $a \in A$ et $b \in B$ tels que $a+b = 1$. Dans $\mathbb{Z}$, Les idéaux (118) et (267) sont premiers entre eux parce que $43 \cdot 118 + (-19) \cdot 267 = 1$. Pour les polynômes à coefficients réels, si a et b sont des nombres réels distincts, alors

$$\frac{1}{b-a}(x-a) + \frac{1}{a-b}(x-b) = 1,$$

et ainsi, les idéaux $(x - a)$ et $(x - b)$ sont premiers entre eux.

On doit fournir une définition supplémentaire. Soit I un idéal de R et soient $x, y \in R$. On dit que $x \equiv y \bmod I$ si $x - y$ est un élément de I. Comme dans la relation de congruence mod m pour les entiers et la congruence mod $p(x)$ pour les polynômes sur un corps, la congruence modulo un idéal est une relation d'équivalence.

Avec toute cette terminologie à l'esprit, voici une façon de généraliser nos théorèmes.

Théorème 5 (forme générale du théorème des restes chinois). *Soit R un anneau commutatif avec unité et soient $A_1...., A_n$ des idéaux deux à deux premiers de R. Le système de congruences*

$$X \equiv y_1 \bmod A_1, ..., X \equiv y_n \bmod A_n$$

a une solution commune $X = X_0$ qui est unique modulo l'intersection $A_1 \cap \ldots \cap A_n$.

Preuve. Pour $i < j$, puisque A_i, et A_j, sont premiers entre eux, on peut choisir $a_{ij} \in A_j$, et $a_{ji} \in A_i$ tels que $a_{ij} + a_{ji} = 1$. Alors, pour tout $i \neq j$, on a $a_{ij} \equiv 1 \bmod A_j$ et $a_{ij} \equiv 0 \bmod A_j$ pour tout $j \neq i$. Maintenant choisissons $P_i = \prod_{j \neq i} a_{ij}$ de telle façon que $P_i \equiv 1 \bmod A_i$ et $P_i \equiv 0 \bmod A_j$ pour

tout $j \neq i$. Alors on peut voir que $X_0 = \sum_i y_i P_i$ est une solution du système d'équations donné.

Si X_0' est une autre solution, alors $x_0' - x_0 \equiv 0 \bmod A_i$, pour tout i. Par conséquent $X_0' - X_0 \in A_1 \cap \ldots \cap A_n$, comme souhaité. □

Finalement, on sait que si le plus grand diviseur commun des entiers a et b est égal à 1, alors on peut écrire 1 comme une combinaison linéaire de a et b ; un résultat analogue est vrai pour les polynômes sur un corps. Cette "manière particulière d'écrire 1" est la clef de nos deux théorèmes, et le fait pour des idéaux d'être premier entre eux est la généralisation clef.

Et c'est pourquoi le théorème des restes chinois et le théorème de l'interpolation polynomiale sont vraiment le même théorème.

Coda

Shamir décrit son régime de seuil dans [6] et Stinson donne un excellent traitement de ce cas et d'autres cas de partages de secrets dans [7, pp. 481-515]. Schroeder [5] traite et le théorème des restes chinois et le théorème d'interpolation polynomiale et fournit un traitement extrêmement lisible de nombreuses manipulations en théorie des nombres. Pour un survol général, une bonne source est le texte d'algèbre abstraite de Hungerford [3, pp. 131-132].

Le TRC trouve des applications dans les domaines des codes correcteurs d'erreurs ; dans le domaine de la cryptographie, particulièrement pour l'encryptage, l'authentification, et les protocoles d'accords de clefs ; et dans les algorithmes pour compter le nombre de points de courbes elliptiques pour n'en nommer que trois. Explorer le TRC donne naissance à de très belles mathématiques. Et comme la collègue théoricienne des nombres Theresa Vaughan (1941-2009) me l'a souvent dit, "Vous pouvez faire un long chemin en théorie des nombres avec seulement l'algorithme d'Euclide, le principe des tiroirs et le théorème des restes chinois."

Finalement, la solution du problème pour le cours de théorie des nombres dans lequel intervenaient de grands nombres est $N = 804\,155\,562\,959\,699\,457\,504\,628\,440\,626$. Le logiciel d'algèbre Mathematica sur mon ordinateur a trouvé N en 222 microseconds - en utilisant, bien sûr, le théorème des restes chinois !

Résumé

Le théorème des restes chinois et le théorème d'interpolation polynomiale sont des théorèmes fondamentaux de théorie des nombres et d'analyse numérique, respectivement. Ces deux théorèmes sont des cas particuliers d'une construction dans un contexte plus général et on décrit un scénario à connaître, deux cours accolés dans lequel les étudiants peuvent découvrir ce fait. On termine en décrivant ce contexte général, dans lequel l'idée-clef est la possibilité d'écrire 1 d'une manière particulière.

Références

[1] R. L. Burden, J. D. Faires, Numerical Analysis. Neuvième édition. Brooks et Cole, New York, 2011.
[2] U. Dudley, Elementary Number Theory. Seconde édition. Dover, Mineola, NY, 2008.
[3] T. W. Hungerford, Algebra. Springer, New York, 1974.
[4] K. H. Rosen, Elementary Number Theory and its Applications. Cinquième édition. Pearson/Addison-Wesley, Boston, 2005.
[5] M. Schroeder, Number Theory in Science and Communication. Cinquième édition. Springer, Berlin, 2009.
[6] A. Shamir, How to share a secret, Comm. ACM 22 (1979) 612-613, http://dx.doi.org/10.1145/359168.359176.
[7] D. R. Stinson, Cryptography: Theory and Practice. Troisième édition. CRC, Boca Raton, FL, 2005.
[8] E. Süli, D. Myers, An Introduction to Numerical Analysis. Cambridge Univ. Press, Cambridge, 2003.

Ezra (Bud) Brown a grandi à la Nouvelle-Orléans et a obtenu ses diplômes de l'Université de Rice et de l'Université de l'État de Louisiane. Il travaille à l'Institut polytechnique de Virginie et à l'Université d'État depuis 1969 et est actuellement Professeur Distingué Alumni de mathématiques. Bud est un contributeur fréquent du journal MAA, il a reçu la récompense Pólya en 2000, 2002, et 2006. Il aime chanter (de l'opéra au rock and roll), jouer du piano jazz, résoudre des jeux de mots, et avec son épouse Jo, pratiquer le kayak, le vélo et l'ornithologie.