Les entiers

... ces fonctions qui s'ignorent

Un océan semble parfois séparer les cours d'arithmétique et d'analyse. Avec un zeste d'imagination, on peut néanmoins emprunter des passerelles magiques qui joignent les deux rivages. Nous découvrirons ici comment donner aux entiers le cachet de « fonction » et ainsi soudain s'arroger de nouveaux outils autrement hors de portée.

Jimmy Dillies
Georgia Southern University

Nous nous pencherons en particulier sur la technique d'interpolation de Lagrange que nous utiliserons pour résoudre le très ancien et ô combien important théorème des restes chinois.

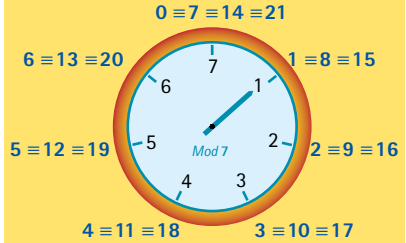
13 = 12 + 1
Treize heures et une heure sont indiquées de la même façon sur un cadran horaire.

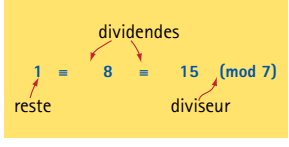
Congruences

Le jeu des congruences, c'est celui des horloges. Une heure, treize heures, ... toutes les douze heures le cadran horaire retrouve le même aspect.

Ainsi, 2 heures et 14 heures sont indiquées au même endroit. Travailler avec des congruences modulo *n*, c'est travailler avec un cadran affichant *n* heures. Ainsi, dans le cas de l'horloge, 2, 14, 26, ... sont indissociables modulo 12.

De la même manière que 1, 8, 15, ... seraient indissociables modulo 7, c'est-à-dire si nos cadrans horaires étaient divisés en 7 heures. On dit que les nombres 1, 8 et 15 sont congruents modulo 7, ce qui s'écrit : $1 \equiv 8 \pmod 7$ et se lit : 1 est congru à 8 modulo 7. Nous retiendrons que ce qui caractérise deux nombres congruents modulo *n*, c'est le reste de la division par *n* qui est identique pour ces deux nombres. Ainsi, 8 et 15 admettent tous deux un reste de 1 suite à une division par 7. Les nombres 8 et 15 tombent donc dans la même classe de congruence.





Nous nommons cette classe de congruence classe de 8 modulo 7, 8 (mod 7), ou de manière équivalente 15 (mod 7). Cela n'est pas important. C'est comme lorsqu'on identifie une équipe de basket : parler de l'équipe de James LeBron, ou parler de l'équipe de Dwyane Wade revient au même. Dans les deux cas, il s'agit de Miami Heat, peu importe le nom du joueur choisi.

Pour les congruences c'est identique. Écrire 3 (mod 12) ou bien 15 (mod 12) c'est simplement parler de la même classe en se référant à des équipiers différents.

Combien existe-t-il de classes de congruence modulo 3 ? Il en existe trois. En effet, un nombre divisé par trois aura toujours un

reste qui sera égal à 0 (c'est le cas lorsque l'on a un multiple de 3), à 1 ou à 2. Tout nombre est donc congruent à l'un de ces trois entiers et ceux-ci ne sont pas congruents entre eux. Pour utiliser l'analogie précédente, il y a trois équipes modulo 3.

Le problème du reste chinois

Combien sommes-nous ?

Voyageons maintenant dans l'espace et le temps pour nous retrouver dans l'empire du milieu au troisième siècle de notre ère.

Dans son opus mathématique, le mathématicien chinois Sun Zi (ou Sun Tzu) pose le problème suivant :

Combien l'armée de Han Xing comporte-t-elle de soldats si, rangés en 2 colonnes, il reste 1 soldat, rangés en 3 colonnes, il reste 1 soldat et, rangés en 5 colonnes il reste 3 soldats ?

S'il n'est pas certain qu'un général arrive à une réponse sans demander à ce que ses troupes soient comptées, Sun Tzu, lui, nous donne la réponse. Malheureusement, il reste évasif quant à la façon utilisée pour y arriver et nous allons donc tenter de trouver nous-mêmes une réponse à ce problème.

En utilisant le langage du paragraphe précédent, nous voyons que le problème est de trouver, étant donné une suite de classes de congruence, un entier qui tombe dans chacune d'entre elles.

Reprenons notre exemple : peut-on trouver un entier p qui soit à la fois congru à 1 modulo 2 (c'est-à-dire un entier impair), à 1 modulo 3 et à 3 modulo 5 ?

En bref, on cherche

$$p \in \mathbb{Z} \text{ tel que } \begin{cases} p \equiv 1 \pmod 2 \\ p \equiv 1 \pmod 3 \\ p \equiv 3 \pmod 5 \end{cases}$$

Si dans ce cas on peut trouver une solution par tâtonnements (ou plus précisément par un crible, voir la figure ci-dessous), il serait intéressant de trouver une méthode plus générale.

Congrus à 1 modulo 2
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ...
Congrus à 1 modulo 3
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ...
Congrus à 3 modulo 5
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 ...

Le plus petit nombre respectant ces trois conditions est 13.

Interpolation de Lagrange

Au lieu d'attaquer directement le problème précédent, nous allons faire un détour par l'analyse et, plus particulièrement, par le monde des polynômes.

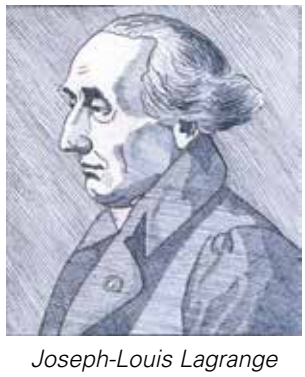
Imaginez que je vous donne N points du plan et que je vous demande de trouver un polynôme dont le graphe traverse ces points. En pratique, je vous donne donc N paires réelles $(x_1, y_1), ..., (x_N, y_N)$ – les x_i étant distincts – et je demande un polynôme f tel que $f(x_i) = y_i$ pour chaque i.

Prenons cet exemple, qui comme nous le verrons est associé au problème des soldats chinois.

Soit les points A(2, 1), B(3, 1) et C(5, 3), peut-on trouver un polynôme dont le graphe passe par ces trois points ?

Une façon tout à fait valable, mais bien fastidieuse, serait de prendre pour f un polynôme général de degré suffisamment grand (dans notre cas le degré 2 suffirait) et de résoudre le système de N équations $\{f(x_i) = y_i\}$, où les coefficients de f sont les inconnues.

La méthode d'interpolation de Lagrange est plus subtile, elle s'attaque au problème morceau par morceau (*Divide et impera* aurait dit Machiavel).



Joseph-Louis Lagrange
1736-1813

Cherchons un polynôme $loc_2(x)$ – car on cherche, en quelque sorte, une solution locale comprenant le point A(2, 1) – qui

a) prend la valeur 1 en $x = 2$ et

b) s'annule en 3 et 5.

On se convainc aisément que

$$loc_2(x) = 1 \cdot \frac{(x-3)(x-5)}{(2-3)(2-5)}$$

fait l'affaire. En effet, le numérateur garantit que la fonction est nulle en 3 et 5 et les autres termes forcent la valeur 1 en $x = 2$. De la même manière, l'on peut trouver des polynômes

$$loc_3(x) = 1 \cdot \frac{(x-2)(x-5)}{(3-2)(3-5)}$$

$$loc_5(x) = 3 \cdot \frac{(x-2)(x-3)}{(5-2)(5-3)}$$

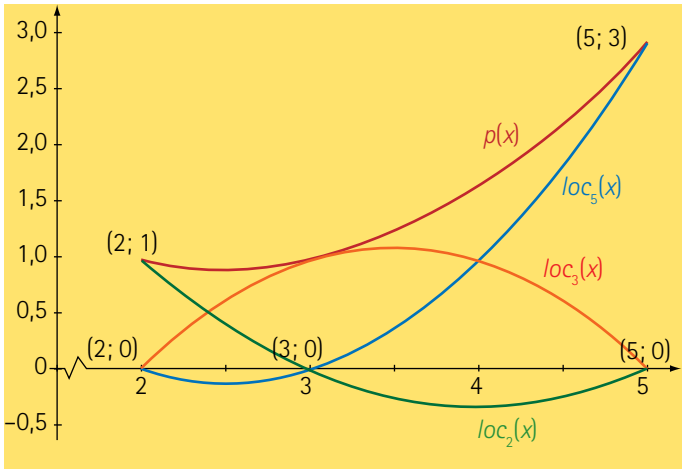
qui se focalisent respectivement sur 3 et 5.

Recollons tout cela

Comme les solutions locales sont nulles en dehors de l'entier auquel on s'intéresse, on peut les recoller sans danger. Le polynôme

$$p(x) = loc_2(x) + loc_3(x) + loc_5(x)$$

prendra les valeurs voulues en 2, 3 et 5.



Les polynômes $loc_{2,3,5}(x)$ et $p(x)$

Voilà, une paire de ciseaux et un peu de colle et l'on a résolu ce problème.

Avant de poursuivre, donnons un petit aperçu de la structure du chemin parcouru. Nous avons d'abord vu la notion de congruence. Puis, nous avons posé le problème de Sun Tzu qui se formule naturellement en termes de congruence. Finalement, nous avons fait un détour par le monde de l'analyse, plus spécifiquement par le monde des polynômes de Lagrange ou comment faire passer un polynôme par un ensemble de points.

Passerelle

Mais quel est donc le lien, me direz-vous, entre l'interpolation de points par des polynômes et le problème original des congruences ?

Revenons au système des congruences et introduisons une nouvelle notation. Notons la classe de congruence d'un entier p modulo n par $p(n)$.

$$p(n) \leftrightarrow p \pmod{n}.$$

Cette notation ingénue a l'avantage d'être une astuce mnémotechnique pour se souvenir des propriétés suivantes des congruences :

$$p(n) + q(n) = (p + q)(n)$$

et $$p(n) \cdot q(n) = (pq)(n).$$

L'on voit ici que d'une certaine manière, prendre un entier modulo n, c'est un peu comme évaluer cet entier à n. On peut donc en quelque sorte oublier que notre entier est un entier, et jouer avec comme s'il s'agissait d'une fonction. Ce n'est pas là une idée si surprenante après tout, car si l'on se souvient un peu de l'arithmétique des polynômes, évaluer un polynôme p en un point a, c'est équivalent à trouver le reste de la division de ce polynôme par $(x - a)$!

Par exemple, considérons $p(x) = x^2 - 9$. Évalué en 1, l'on obtient $p(1) = -8$. On obtient la même réponse en cherchant le reste de la division de $p(x)$ par $(x - 1)$:

$$x^2 - 9 = (x - 1)(x + 1) - 8.$$

Ainsi, évaluer le polynôme en 1 revient à trouver le reste de la division de ce même polynôme par $(x - 1)$. On a une analogie supplémentaire entre le polynôme $(x - n)$ et l'entier n, ce sont les plus petites « fonctions » non-triviales qui s'annulent en n.

Petit lexique à l'usage du voyageur

Polynômes	*Entiers*
$p(x) \in \mathbf{k}[x]$	$p \in \mathbb{Z}$
$x - a$	a
$p(b)$	$p \pmod b$
$(b - a)$	$a \pmod b = a(b)$

Continuant notre analogie nous pouvons réécrire notre problème du reste chinois comme : cherchez un entier p tel que

$$p(2) = 1;$$
$$p(3) = 1$$
et $p(5) = 3$.

La clef du mystère

Ce problème nous est maintenant bien connu. En effet, il s'agit exactement du problème de Lagrange mais dans un monde où les entiers jouent le rôle des polynômes. Ainsi (aidez-vous du petit lexique) la première formule de la page précédente devient dans ce nouveau monde

$$loc_2(x) = 1 \cdot \frac{3 \cdot 5}{3(2) \cdot 5(2)} = 1 \cdot \frac{3 \cdot 5}{1 \cdot 1} = 15.$$

De manière similaire, l'on obtient[1]

$$loc_3(x) = 1 \cdot \frac{2 \cdot 5}{(-1) \cdot (-1)} = 10$$

et

$$loc_5(x) = 3 \cdot \frac{2 \cdot 3}{1} = 18$$

Après recollement, nous obtenons donc comme solution

$$p = 15 + 10 + 18 = 43.$$

Bien entendu, cette solution n'est pas unique, mais c'est là tout le charme de notre passerelle : l'interpolation polynomiale admet elle aussi plusieurs solutions. Ici, tout multiple de $2 \cdot 3 \cdot 5 = 30$ (positif ou négatif) ajouté à p, 43, donnera une autre solution – dont 13 que nous avions trouvé précédemment par inspection. Je laisse au lecteur le soin de traduire cela dans le langage des polynômes.

Conclusion

Si l'arithmétique semble être une branche à part entière des mathématiques, elle se trouve en fait fertilisée par de nombreuses idées venues d'ailleurs. Le lien entre le problème du reste chinois et l'interpolation de Lagrange, qui est de considérer des entiers comme s'ils étaient des fonctions, n'est que le sommet de l'iceberg et il y a sous les profondeurs de nombreux résultats, connus, ou pas encore, qui stimulent la recherche mathématique et permettent aux chercheurs de faire avancer leur connaissance des entiers. En quelque sorte, ce que nous venons de découvrir, c'est l'un des premiers outils de la géométrie arithmétique, un vaste sujet qui nous réserve encore bien des surprises.

---

1. *Pour ces solutions locales, nous avons utilisé au dénominateur $2(3) \cdot 5(3) = (-1) \cdot (-1)$ et $2(5) \cdot 3(5) = (2 \cdot 3)(5) = 6(5) = 1$, c'est-à-dire nous avons tâché d'utiliser des entiers inversibles modulo 2, 3 et 5. C'est une nécessité car nous devons donner un sens à ce quotient modulo ces trois entiers. Nous ne nous y attarderons pas plus ici.*