(indéfini) de 3, à 3 plus un multiple de 5, et à 2 plus un multiple de 7. On résume ces égalités, à un multiple près de 3, 5 ou 7, par le mot « congruence ». En d'autres termes, on dit que x est congru à 2 modulo 3, à 3 modulo 5, et à 2 modulo 7, ce que l'on écrit $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$. Les entiers 3, 5 et 7 sont les « raisons » de ces congruences.

Une chinoiserie ?

Le *Sunzi Sunangjing* explique comment résoudre ces congruences, c'est-à-dire comment trouver les entiers x qui les vérifient. Ce « théorème des restes chinois », comme on le nomme parfois, dit d'ajouter 2×70, 3×21 et 2×15 (cela fait $140 + 63 + 30 = 233$) et de soustraire 105 tant que le résultat est supérieur à 106. Dans cette formule, 70, 21 et 15 ont été choisis parce que 70 est multiple de 5 et de 7 ($70 = 2 \times 5 \times 7$) et est congru à 1 modulo 3 (car $70 = 1 + 69 = 1 + 3 \times 23$), 21 est multiple de 3 et de 7 et est congru à 1 modulo 5, 15 est multiple de 3 et de 5 et est congru à 1 modulo 7. En outre, $105 = 3 \times 5 \times 7$. Dans cet exemple, on trouve donc que x est congru à 23 modulo 105 : trois congruences modulo les nombres premiers 3, 5 et 7 ont été transformées en une seule congruence ayant pour raison le produit $105 = 3 \times 5 \times 7$ de leurs raisons.

Le développement de l'algèbre a permis de comprendre que, dans le calcul des congruences, on peut négliger complètement le multiple indéfini et calculer comme si la raison était nulle. Par exemple, modulo 13, on a $6 \equiv -7$ puisque $6 - (-7) = 13 \equiv 0$; de même, $5 \times 7 \equiv 35 \equiv 3 \times 13 - 4 \equiv -4$. On peut aussi résoudre des équations en congruences ; examinons par exemple la congruence $3x - 5 \equiv 0 \pmod 7$; si l'on multiplie l'équation par 2, on trouve $6x - 10 \equiv 0 \pmod 7$. Mais $6 \equiv -1 \pmod 7$ et $-10 = -14 + 4 \equiv 4 \pmod 7$, si bien que l'équation devient $-x + 4 \equiv 0 \pmod 7$, d'où $x \equiv 4$. Inversement, si $x \equiv 4$, $3x \equiv 12 \equiv 5 \pmod 7$.

Il y a en revanche quelques subtilités nouvelles. Par exemple, 2 et 3 ne sont pas multiples de 6 (ils ne sont pas nuls modulo 6), mais leur produit l'est. Autrement dit, le produit de deux nombres peut être nul (en congruence) sans qu'aucun d'eux ne le soit.

Ce phénomène d'apparence pathologique – un produit égal à zéro alors que les facteurs sont non nuls – ne se présente pas lorsque la raison est un nombre premier, c'est-à-dire un entier positif divisible seulement par 1 et par lui-même. En effet, d'après un résultat d'Euclide, le produit de deux entiers ne peut être multiple d'un nombre premier p sans qu'au moins l'un des deux ne le soit. Pour cette raison, les congruences modulo p, où p est un nombre premier, sont les plus fondamentales en mathématiques.

Ainsi, avec le développement de la théorie des équations et celui de la théorie des nombres, est née peu à peu une théorie des équations polynomiales modulo un nombre premier. Le grand mathématicien allemand Carl Friedrich Gauss avait lui-même largement étudié ce sujet dans lequel, comme le dit Galois lui-même, il s'agit de résoudre une équation en considérant que tout multiple d'un nombre premier donné est nul.

Par exemple, comment résoudre l'équation du nombre d'or, $x^2 - x - 1 = 0$, modulo la raison 7 ou modulo la raison 11 ? On peut commencer par raisonner comme en algèbre classique. Modulo 7, on peut écrire :
$0 = x^2 - x - 1 \equiv x^2 - 8x - 1 \equiv$
$(x - 4)^2 - 17 \equiv (x - 4)^2 - 3 \pmod 7$;
s'il existe une solution entière x de cette congruence, il faut que 3 soit un carré

L'AUTEUR

Antoine CHAMBERT-LOIR
est professeur de mathématiques
à l'Université de Rennes 1.

✔ SUR LE WEB

Pour des détails sur les célébrations du **bicentenaire de la naissance d'Évariste Galois**, voir : http://www.galois.ihp.fr/

Qu'est-ce qu'un corps ?

Un corps est un ensemble muni d'une addition et d'une multiplication, et de deux éléments distincts notés 0 et 1, qui vérifient les axiomes suivants (a, b et c désignent ici des éléments quelconques du corps) :

- $a + b = b + a$ (commutativité de l'addition) ;
- $(a + b) + c = a + (b + c)$ (associativité de l'addition) ;
- $a + 0 = a$; pour tout a, il existe un unique élément b tel que $a + b = 0$, et on le note $-a$;
- $(a \times b) \times c = a \times (b \times c)$ (associativité de la multiplication) ;
- $a \times 1 = 1 \times a = a$; pour tout $a \neq 0$, il existe un unique élément, noté $1/a$ ou a^{-1}, tel que $a \times a^{-1} = a^{-1} \times a = 1$.
- $(a + b) \times c = a \times c + b \times c$ (distributivité de la multiplication par rapport à l'addition).

La soustraction est alors définie par la formule $a - b = a + (-b)$, la division par un élément non nul par la formule $a/b = a \times (1/b)$. Pour tout a, $a \times 0 = 0$, $a \times (-1) = -a$, etc.

Des exemples de corps sont l'ensemble des nombres rationnels (c'est le calcul des fractions appris à l'école élémentaire) ainsi que ceux des nombres réels et complexes. Ces trois corps sont infinis : ils contiennent une infinité d'éléments (par exemple 1, 2, 3, etc.).

On peut faire de l'ensemble {0, 1} un corps avec les lois d'addition et de multiplication données par les tables suivantes :
(où seule la formule $1 + 1 = 0$ n'est pas explicitement forcée par les axiomes ci-dessus). C'est donc un corps à deux éléments ; l'informatique, avec la numération binaire, lui a donné un rôle fondamental.

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Plus généralement, si n est un entier supérieur ou égal à 2, on peut tenter de faire de l'ensemble $\{0, 1, \ldots, n-1\}$ un corps en disant d'abord que la somme (le produit) de deux éléments est le reste de la division par n de leur somme (de leur produit). Cela en fait un « anneau » : la seule propriété qui manque pour en faire un corps est l'existence d'un inverse pour tout élément autre que 0. Lorsque (et seulement lorsque) n est un nombre premier, l'ensemble $\{0, 1, \ldots, n-1\}$ est un corps, que Carl Friedrich Gauss avait étudié en grand détail dans ses *Disquisitiones Arithmeticae* (1798).