(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).

Calculer x^a rapidement

✔ **Il existe un algorithme récursif qui permet de calculer très rapidement la puissance entière x^a d'un nombre x. Cet algorithme est fondé sur la numération binaire de l'entier a, et sur le fait que $x^a = (x^2)^{a/2}$ si a est pair, et que $x^a = x\,(x^2)^{(a-1)/2}$ si a est impair. On a par exemple $x^{19} = x\,(x^2)\,(x^{16})$, où x^{16} est calculé par quatre élévations successives au carré : $x^{16} = (((x^2)^2)^2)^2$. On obtient ainsi une méthode de calcul par récurrence qui ne demande qu'environ $2n$ multiplications pour calculer x^a, où n est le nombre de chiffres du développement binaire de a.**

modulo 7 ; or les carrés modulo 7 sont 0, 1, $2^2 = 4$, $3^2 = 9 \equiv 2$, $4^2 \equiv (-3)^2 \equiv 2$, $5^2 \equiv (-2)^2 \equiv 4$ et $6^2 \equiv (-1)^2 \equiv 1$. On constate en particulier que 3 n'est pas un carré modulo 7 et cette équation en congruence n'a donc pas de solution.

Modulo 11, on écrit plutôt :
$0 = x^2 - x - 1 \equiv x^2 - 12x - 1 \equiv (x-6)^2 - 37 \equiv (x-6)^2 - 4 \pmod{11}$.
Par conséquent, $(x-6)^2 \equiv 4 \equiv 2^2$, d'où l'on déduit (comme d'habitude !) que $x - 6 = \pm 2$. On trouve ainsi deux solutions modulo 11, à savoir $x = 4$ et $x = 8$.

Équations polynomiales et congruences

Alors que ses prédécesseurs s'étaient contentés de chercher les solutions entières de congruences polynomiales, Galois s'est intéressé aux espèces de nombres complexes (ou, comme il dit, aux « quantités imaginaires ») que l'on peut définir à partir d'une congruence polynomiale, de la même façon qu'on avait créé les nombres complexes à partir d'une solution « imaginaire » de l'équation $x^2 + 1 = 0$.

Galois considère donc une raison, qui est un nombre premier p et, un polynôme arbitraire $F(x)$ de degré d et à coefficients entiers. Il fait deux hypothèses sur ce polynôme $F(x)$: d'une part, que le coefficient de x^d ne soit pas un multiple de p et, d'autre part, qu'on ne puisse pas factoriser F modulo p, c'est-à-dire qu'il n'existe pas de polynômes F_1 et F_2 tels que $F \equiv F_1 F_2 \pmod{p}$. Galois dit que la congruence $F(x) \equiv 0 \pmod{p}$ est « irréductible ». Par exemple, si $p = 13$, on ne peut pas prendre $F = x^2 + 1$, car $x^2 + 1 \equiv (x-5)(x-8) \pmod{13}$, mais on peut vérifier que le choix $p = 11$ et $F = x^2 + 1$ convient ; il en est de même du choix $p = 13$ et $F = x^2 - 2$, ou encore $p = 7$ et $F = x^2 - x - 1$.

Nous avions introduit un symbole i pour désigner une racine de l'équation $x^2 + 1 = 0$ et vu que l'on pouvait calculer naturellement avec lui. Faisons de même ici : traitons la lettre x, non plus comme une inconnue, mais comme une solution de la congruence $F(x) \equiv 0 \pmod{p}$. Cela donne lieu à un ensemble de p^d « nombres » : tous ceux de la forme :

$$a_0 + a_1 x + \ldots + a_{d-1} x^{d-1},$$

où $a_0, \ldots, a_{d-1}$ sont des entiers compris entre 0 et $p - 1$ (il y a p choix pour chacun des d coefficients, d'où p^d nombres distincts). Ces nombres peuvent être additionnés (on additionne les coefficients de type a_0, ceux de type a_1, etc., en soustrayant p si leur somme dépasse p), ou soustraits. De façon peut-être plus surprenante, on peut aussi les multiplier : si l'on développe le produit de deux nombres de la forme $a_0 + a_1 x + \ldots + a_{d-1} x^{d-1}$, on voit apparaître des puissances de x avec un exposant qui peut dépasser $d - 1$; mais la congruence $F(x) \equiv 0 \pmod{p}$ permet de remplacer x^d par un nombre admissible, x^{d+1} aussi, etc.

Par exemple, si $x^3 + 2x - 1 \equiv 0 \pmod{5}$, alors $x^4 + 2x^2 - x \equiv 0$, et par conséquent $x^4 \equiv -2x^2 + x \equiv 3x^2 + x \pmod{5}$. On en déduit que $x^5 \equiv 3x^3 + x^2 \equiv 3(3x + 1) + x^2 \equiv x^2 + 9x + 3 \equiv x^2 + 4x + 3 \pmod{5}$, etc. Enfin, et c'est là qu'intervient l'hypothèse que la congruence $F(x) \equiv 0$ est irréductible, on peut aussi diviser par tout nombre différent de 0.

On obtient ainsi un ensemble de p^d nombres avec lesquels on peut calculer de façon naturelle : addition, soustraction, multiplication, division par tout élément non nul, ces opérations obéissant aux règles usuelles (commutativité, associativité de l'addition et de la multiplication, distributivité de

L'addition dans une courbe elliptique

Les courbes elliptiques, qui n'ont pas du tout la forme d'une ellipse, ont été nommées ainsi parce que leurs équations ont un lien avec le calcul de la longueur d'arcs d'ellipses. Une courbe elliptique E est définie par une équation cubique qui peut être mise sous la forme $y^2 = x^3 + ux + v$, où u et v sont des nombres réels tels que $4u^3 + 27v^2$ soit non nul (sinon, la courbe a un point singulier).

Une particularité des courbes elliptiques est qu'on peut définir une addition entre leurs points. L'addition de deux points P et Q d'une courbe elliptique E est définie ainsi : si la droite passant par P et Q rencontre la courbe en un troisième point R', le point R = P + Q est le symétrique de R' par rapport à l'axe (horizontal) de symétrie de la courbe. Si la droite passant par P et Q est verticale, on considère que R est à l'infini ; le point à l'infini est défini comme étant le 0 de l'addition. Et quand Q est confondu avec P, la droite tangente à la courbe en P définit le point R = P + P = 2P. Notamment, la somme de trois points P, Q, R est égale au point 0 si et seulement si ces trois points sont alignés.

Muni de cette addition, l'ensemble des points de la courbe elliptique forme un groupe additif (structure algébrique munie d'une addition, supposée associative, où il existe un élément neutre noté 0 et où chaque élément a possède un inverse a' tel que $a + a' = 0$).

Une courbe elliptique peut aussi être considérée sur un corps F différent de celui des nombres réels *(voir la figure 2)*. Dans ce cas, les paramètres u et v sont des éléments de F et le groupe E(F) des points de la courbe elliptique E est formé des solutions (x, y) de l'équation $y^2 = x^3 + ux + v$ considérée dans le corps F, auquel on adjoint un point à l'infini 0.

Signalons que les courbes elliptiques ont joué un rôle central dans la preuve par Andrew Wiles du « grand théorème de Fermat », selon lequel il n'existe pas d'entiers strictement positifs a, b, c tels que $a^n + b^n = c^n$ pour un entier n supérieur à 2.