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

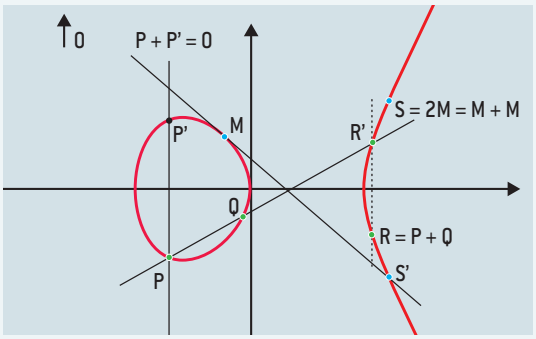
Les courbes elliptiques, qui n'ont pas du tout la forme d'une ellipse, ont été nommées ainsi parce que leurs équations ont un lien avec le calcul de la longueur d'arcs d'ellipses. Une courbe elliptique E est définie par une équation cubique qui peut être mise sous la forme $y^2 = x^3 + ux + v$, où u 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.



la multiplication sur l'addition). C'est un exemple de ce qu'on appelle en mathématiques un corps *(voir l'encadré page 27)*; et comme il n'a qu'un nombre fini d'éléments, on dit que c'est un corps fini.

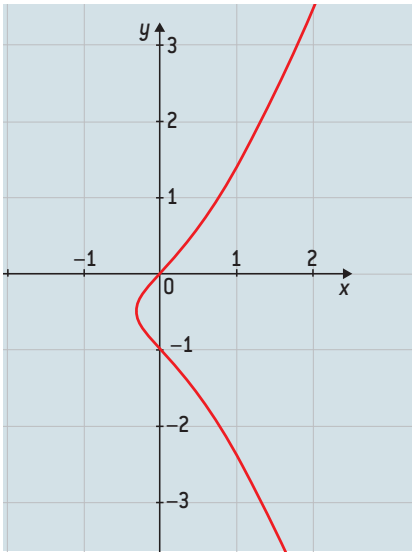
Dans sa note, Galois explique ensuite un certain nombre des propriétés de ces corps finis. Il commence par démontrer que dans un corps fini ayant p^d éléments, tout élément a vérifie $a^{(p^d)} = a$; cela généralise la congruence classique, dénommée « petit théorème de Fermat », selon laquelle $a^p \equiv a \pmod p$ pour tout entier a et tout nombre premier p. Il démontre aussi qu'il existe une « racine primitive » de cette équation $a^{(p^d)} = a$, autrement dit un élément non nul a tel que la suite 0, 1, a, a^2, ..., $a^{(p^d-2)}$ décrive exactement le corps fini.

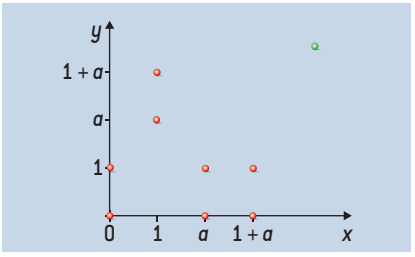
Pour construire un corps fini de « cardinal » p^d, c'est-à-dire ayant p^d éléments, par la méthode expliquée par Galois, il faut partir d'un polynôme F de degré d qui est irréductible modulo p. Galois explique alors qu'un tel polynôme est un facteur modulo p du polynôme $x^{(p^d)} - x$. Peu après, le mathématicien et astronome français Joseph Serret a démontré que l'on peut effectivement trouver un tel facteur, de sorte que, pour chaque puissance p^d d'un nombre premier p, il existe un corps fini de cardinal p^d. Et ce corps est même unique au sens où, pour deux corps finis de même cardinal (obtenus par exemple en suivant la construction de Galois pour deux polynômes F_1 et F_2), on a un dictionnaire reliant un à un les éléments des deux corps qui est compatible avec les règles de calcul (les mathématiciens disent que les deux corps sont isomorphes).

Des corps finis à la cryptographie

Dans les décennies qui ont suivi la note de Galois, plusieurs mathématiciens ont complété les travaux de Galois et formalisé la notion de corps telle qu'elle est présentée dans l'encadré page 27. À la mort de Gauss, en 1855, on a retrouvé un huitième chapitre de ses *Disquisitiones*, qu'il avait écrit en 1797 mais qui n'a été publié par le mathématicien allemand Richard Dedekind qu'en 1863. Dans ce texte, Gauss développait une théorie très proche de celle que Galois avait inventée.

La théorie des corps finis a rapidement montré son importance pour les mathématiques. C'en est aujourd'hui un outil crucial, y compris dans des domaines qui, à première vue, semblent ne pas relever de l'arithmétique tels que la théorie des fonctions automorphes et le programme de Langlands (un grand ensemble de conjectures techniques liant algèbre, théorie des fonctions et théorie des nombres).





2. L'ÉQUATION D'UNE COURBE plane est de la forme $f(x, y) = 0$, à l'instar de l'équation $y^2 + y = x^3 + x^2 + x$ de la courbe elliptique ci-contre. Mais une telle équation peut aussi être considérée dans un corps fini, et non sur le corps des nombres réels. Ainsi, dans le corps à $4 = 2^2$ éléments ($p = 2$, $d = 2$) formés par les polynômes 0, 1, a et $1 + a$ (où l'on a $1 + 1 = 0$ et $a^2 = a + 1$), la courbe elliptique considérée possède huit points *(graphe ci-dessus)* en plus du point 0 à l'infini *(en vert)*.

Les corps finis sont aussi au cœur des télécommunications modernes et des mécanismes intimes du réseau Internet, en particulier dans tout ce qui touche à la sécurité du commerce électronique. Lorsque vous achetez en ligne un livre, un disque ou un appareil photo, vient inévitablement le moment du paiement où il vous faut transmettre votre numéro de carte bancaire. Évidemment, vous aimeriez être certain qu'aucune personne non autorisée ne puisse obtenir ce numéro et l'utiliser à son profit. On est ainsi face à un problème classique de cryptographie : transmettre un message à son destinataire, et que seul ce dernier puisse en avoir connaissance.

Jusque vers 1975, les seuls procédés connus de cryptographie étaient symétriques. L'émetteur et le destinataire conviennent d'un code secret, lequel sert aussi bien à coder un message qu'à le décoder. Dans sa *Vie des douze Césars*, l'historien romain Suétone écrivait à propos de Jules César qu'il « y employait, pour les choses tout à fait secrètes, une espèce de chiffre qui en rendait le sens inintelligible (les lettres étant disposées de manière à ne pouvoir jamais former un mot), et qui consistait, je le dis pour ceux qui voudront les déchiffrer, à changer le rang des lettres dans l'alphabet, en écrivant la quatrième pour la première, c'est-à-dire le d pour le a, et ainsi de suite ». Comme le suggère très bien Suétone, si vous savez comment Jules César procède pour coder un message, vous êtes aussitôt en mesure de déchiffrer un message qu'il a écrit, même si vous n'en êtes pas le destinataire.

Un tel mécanisme n'est pas très utile pour le commerce en ligne puisqu'un site Web ne peut pas matériellement prendre contact avec tous ses clients potentiels et convenir, avec chacun d'entre eux, d'un tel code secret. En 1976, les Américains Whitfield Diffie, Martin Hellman et Ralph Merkle proposèrent un nouveau type de procédé, nommé aujourd'hui cryptographie asymétrique.

Dans ce schéma, n'importe qui est capable de coder des messages, mais seul son destinataire peut les décoder. Pour cela, le destinataire dispose de deux clefs ; l'une est connue de tous et permet de coder les messages, tandis que l'autre, qui permet de décoder les messages, est gardée secrète. En 1978, au MIT, Ronald Rivest, Adi Shamir et Leonard Adleman inventèrent un tel protocole, appelé depuis RSA et très largement utilisé aujourd'hui, y compris dans des consoles de jeu.

Du point de vue mathématique, on peut penser à la cryptographie comme à deux ensembles de symboles, celui des messages et celui des messages codés (un message étant alors une suite de symboles), et à deux applications, l'une qui transforme un symbole en un symbole codé et l'autre qui transforme un symbole codé en un symbole en clair. Dans le schéma de Jules César, les deux ensembles sont les lettres de l'alphabet (latin) ; la fonction qui code un message décale les lettres de trois crans vers la gauche, celle qui décode les décale de trois crans vers la droite.