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.