

De la conjecture de Langlands à la carte à puce

Mireille Fouquet, Maître de conférences à l'Univ. Paris-Diderot
 et
Jan Nekovar, Professeur à l'Univ. Pierre et Marie Curie

Les théories mathématiques les plus abstraites sont intimement liées à des technologies omniprésentes dans notre vie quotidienne. C'est le cas des courbes elliptiques.

Des tablettes babyloniennes nous révèlent que les hommes s'intéressent aux relations de type : $a^2 + b^2 = c^2$ entre les nombres entiers depuis l'Antiquité, aussi bien d'un point de vue purement arithmétique que géométrique (il s'agit alors d'un triangle rectangle dont les côtés sont de longueur entière).

On sait écrire toutes les solutions en nombres entiers de cette relation dès le III^e siècle avant notre ère. Cela revient à dire que l'on connaît toutes les solutions rationnelles de l'équation $x^2 + y^2 = 1$. En langage géométrique, on dit que l'on connaît tous les points rationnels sur le cercle. Le cercle est un objet dont on sait tout : il est *élémentaire*. Les courbes elliptiques sont quant à elles les objets *non-élémentaires* les plus simples.

Une courbe elliptique est l'ensemble E des solutions d'une équation cubique à deux variables.

Par exemple : $E : y^2 = x^3 + ax + b$

(dans de nombreux travaux, a et b sont supposés rationnels ou entiers).

Le cercle peut être muni d'une structure de groupe, qui est tout simplement le groupe des rotations du plan de centre 0, ou de façon équivalente le groupe des nombres complexes de module 1. D'une manière analogue, on peut définir une loi de groupe, notée +, sur une courbe elliptique, c'est-à-dire telle que, si A et B sont sur la courbe, A + B soit encore un point de la courbe.

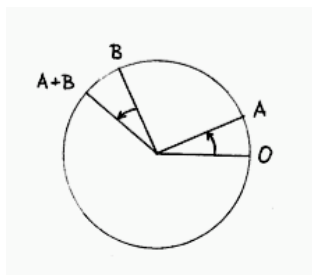


Figure 1 : Loi de groupe sur le cercle

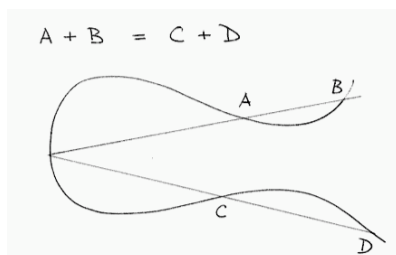


Figure 2 : Loi de groupe sur une courbe elliptique

Ainsi, les courbes elliptiques sont étudiées d'un point de vue algébrique, analytique, arithmétique ou géométrique.

Combien de solutions l'équation E a-t-elle modulo p , p étant un nombre premier ? Quels sont les points rationnels d'une courbe elliptique ?...

Ces questions se sont avérées être une source extrêmement féconde de recherche en mathématiques fondamentales. De nombreux travaux célèbres du XXe siècle leur sont liés : la preuve de la conjecture de Fermat et de la conjecture de Taniyama-Shimura par Wiles, les travaux autour de la conjecture de Langlands, de la conjecture de Sato-Tate, ou encore de la conjecture de Birch et Swinnerton-Dyer, qui est l'un des sept « problèmes du millénaire » à un million de dollars du Clay Mathematics Institute.

Les courbes elliptiques et la cryptographie

Au cœur de nombreux objets de la vie quotidienne – puce de téléphone mobile, carte bleue, carte vitale – ou de gestes devenus banals – achats sur Internet -, se trouvent des systèmes numériques qui identifient les usagers, les protègent des usurpations ou des actes malveillants.

Lors de l'achat d'un billet de train sur Internet, par exemple, la connexion devient *sécurisée*. Comment cela est-il possible ? La première phase de sécurisation consiste à obtenir un secret permettant par la suite de chiffrer et de déchiffrer toutes les communications. Ce secret est partagé uniquement par les deux protagonistes bien que tous leurs échanges d'information soient publics. Pour cela, on fait appel à des opérations algébriques dans un groupe fini, par exemple à la multiplication modulo un entier n . La sécurité du protocole d'échange de clefs dépend de la simplicité de l'opération à réaliser (comme calculer g^a modulo p) et de la difficulté à inverser cette opération (comme trouver a en ne connaissant que g et g^a modulo p) : c'est le problème du *logarithme discret*.

La loi de groupe sur une courbe elliptique modulo p satisfait pleinement aux exigences du problème du logarithme discret. Cette intarissable source de recherches mathématiques fondamentales, malgré son caractère purement abstrait en apparence, rejoint ainsi la réalité pratique.