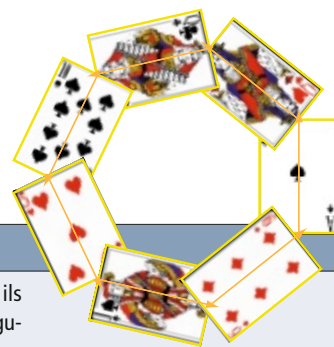




5. Une preuve mentale du théorème de Wilson

Théorème de Wilson : si p est premier, alors $(p-1)! + 1$ est divisible par p . Ce résultat était connu du mathématicien arabe Alhasen (965-1039) ; il doit son nom

On imagine un jeu de 52 cartes et on associe une direction à chaque couleur : Nord pour pique, Ouest pour trèfle, Est pour carreau, Sud pour cœur. On mélange les cartes et on en déduit une promenade aléatoire en prenant les cartes une à une et en les mettant à la suite l'une de l'autre. Comme il y a autant de Nord que de Sud et autant d'Ouest que d'Est, le parcours ramène au point de départ.

Prenons maintenant un jeu de p cartes, p étant un nombre premier. Soit l'angle $360^\circ/p$ (un p -ième d'un tour complet) qu'on dénommera angle de base. On numérote les cartes par les entiers de 0 à $p-1$. À la carte i , on associe i fois l'angle de base. Comme précédemment, quel que soit l'ordre des cartes, le parcours aléatoire qu'on en déduit ramène au point de départ. Pour le voir, on considère les p vecteurs unitaires associés à

ces p angles pris dans l'ordre : ils dessinent un grand polygone régulier à p côtés et donc leur somme est nulle. Dans un autre ordre, elle reste bien sûr nulle.

On réfléchit maintenant aux $p!$ promenades aléatoires engendrées par les différentes façons de classer les cartes. Comme le point de départ est sans importance, il n'y a que $(p-1)!$ promenades aléatoires différentes.

Certaines promenades sont peut-être invariantes par rotation, mais puisque p est premier, cela ne peut être que par la rotation de l'angle de base. Les promenades invariantes par rotation de l'angle de base sont faciles à identifier : ce sont celles qui dessinent les étoiles régulières faites en prenant p points régulièrement espacés sur une circonférence. Il y en a exactement $p-1$ (il y a deux fois moins d'étoiles, mais chacune donne deux promenades selon

la façon dont on la parcourt). Il y a donc en tout $(p-1)! - (p-1)$ promenades différentes asymétriques.

Toute rotation d'une promenade asymétrique par un multiple de l'angle de base en donne une autre. Les promenades asymétriques se regroupent donc en paquets de p (dans un paquet, toutes les promenades s'obtiennent en faisant tourner l'une d'elles par les multiples de l'angle de base). Le nombre $(p-1)! - (p-1)$ est donc divisible par p , donc $(p-1)! + 1$ aussi. CQFD.

La réciproque conduit à une caractérisation des nombres premiers. Elle se fait mentalement aussi : si $p > 4$ est composé, alors $(p-1)!$ est divisible par p (traiter le cas p carré parfait, puis p non carré), donc $(p-1)! + 1$ ne l'est pas. Pour $p = 4$, on a $(p-1)! + 1 = 7$, non divisible par 4.

à John Wilson (1741-1793) qui l'énonça en 1770 sans le démontrer, chose faite trois ans plus tard par Joseph-Louis Lagrange.

teur et vous proposent des démonstrations animées parfaitement convaincantes (voir <http://clem.mscedu/~talman/MathAnim.html> pour une collection de telles animations).

Des preuves mentales

À l'opposé des preuves sans mots, il y a les preuves sans dessins ni symbolisme mathématique, qu'on pourrait qualifier de mentales. Lors d'une promenade à pied avec un ami, vous la raconterez... et cela même en pleine nuit. Pour peu qu'il soit assez attentif, en vous écoutant, votre ami comprendra et se trouvera donc à la fin de votre exposé convaincu d'un résultat mathématique nouveau. Récemment, le mathématicien britannique Adam Goucher a proposé une preuve mentale et géométrique [ce n'est pas incompatible !] du théorème de Wilson. Ce théorème donne une caractérisation des nombres premiers comme nombres p qui divisent $(p-1)! + 1$ (voir la figure 5). Je vous recommande cette

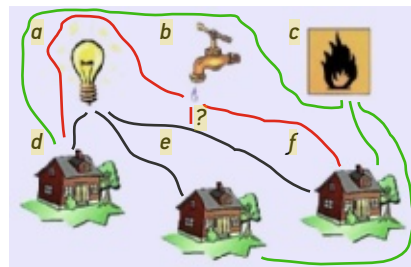
preuve pour votre prochaine excursion en montagne. Elle vous fera sentir, bien mieux que les preuves usuelles fondées sur des connaissances peu intuitives d'arithmétique modulaire, que le théorème est vrai : en un mot, elle vous fera accéder à cet état de conviction profonde qui constitue la compréhension mathématique véritable. Du fait de leur nature verbale, les preuves mentales sont en général faciles à traduire en preuves formelles.

Prouver en bougeant son corps

Les mouvements et les actions qu'on effectue soi-même sont un bon moyen de se persuader d'une vérité. Cette implication du corps dans le processus de démonstration est parfois le moyen le plus efficace d'arriver à l'état de certitude intime à propos d'un énoncé mathématique.

L'exemple du problème des trois maisons de Henry Dudeney qui doivent avoir l'eau, le

gaz et l'électricité illustre cette situation (voir ci-dessous). Il lui correspond le théorème affirmant que le graphe $K_{3,3}$ (où trois points a , b et c rejoignent chacun trois autres points d , e et f) n'est pas planaire, c'est-à-dire ne peut pas être dessiné sur un plan sans que les tracés des jonctions ne se coupent. Qui-conque essaye pendant dix minutes de résoudre le problème de Dudeney avec un papier, un crayon et une gomme, atteint cet état de certitude absolue que $K_{3,3}$ n'est pas planaire.



Le problème des trois maisons de Henry Dudeney : les tracés reliant $\{a, b, c\}$ à $\{d, e, f\}$ se coupent forcément au moins une fois.

Ces mouvements réalisés pour soi construisent une conviction privée, mais une démonstration doit être communicable. Ici, on ne peut donc pas considérer que la certitude acquise par manipulation vaut pour démonstration. Heureusement, l'énoncé que $K_{3,3}$ n'est pas planaire a des démonstrations au sens usuel... quoique utilisant de façon plus ou moins directe le théorème de Jordan et donc délicates à formaliser.

Démonstrations de physiciens

Notre connaissance instinctive ou apprise de la physique nous conduit à être certain d'énoncés pourtant purement mathématiques. Ces preuves d'énoncés mathématiques par le raisonnement physique peuvent difficilement être considérées comme de vraies preuves mathématiques et on ne sait pas ce qu'en aurait dit Thom. Cependant, elles sont fascinantes et il ne fait pas de doute qu'elles conduisent dans un état de certitude parfois aussi fort que les preuves vraiment mathématiques. La

rubrique de février 2010 qui présentait un livre de Mark Levi consacré au sujet en donnait une série d'exemples (*voir l'encadré 4 pour un autre*). Ces preuves sont délicates à analyser pour le mathématicien, car la preuve s'appuie sur des lois ou des considérations physiques qui ne sont pas permises habituellement en mathématiques. D'ailleurs, si les lois physiques ne sont pas vraies (une loi physique n'est jamais démontrée définitivement), il se pourrait que ce qu'on en a déduit de purement mathématique soit faux. L'analyse approfondie de ces preuves ferait peut-être découvrir qu'elles sont exprimables en contournant les hypothèses physiques qui y sont à l'œuvre. Le problème n'est pas très simple et il semble qu'il y ait là un beau sujet de recherche logique qui, à ma connaissance, n'a pas été traité.

La simple observation d'un programme qui affiche des images sur un écran constitue parfois une preuve entraînant une parfaite adhésion. Ce type de preuves est rarement mentionné par ceux qui réfléchissent à la nature des mathématiques

et des démonstrations. Pourtant, il existe des domaines où elles jouent un rôle central, totalement irremplaçable, et où personne n'a le moindre doute sur les énoncés mathématiques qu'il produit.

Considérons l'énoncé suivant : il existe une configuration du *Jeu de la vie* de Conway de dix cellules créant des configurations dont le nombre de cellules tend vers l'infini.

Observer le déroulement d'un programme

C'est un énoncé mathématique très simple. Il n'a été démontré qu'en 1997 par Paul Callahan, 30 ans après l'invention du jeu. En quoi consiste sa démonstration ? En la présentation d'une configuration de dix cellules (la trouvaille), suivie de l'observation de 1 000 générations successives du devenir de la configuration. Ces 1 000 générations ne peuvent pas se calculer à la main, car assez rapidement elles font intervenir un grand nombre de cellules. À partir de la génération 1 000, le calcul présente une régularité : une partie de la configuration est stable alors qu'une autre partie avance, laissant derrière elle des cellules vivantes de plus en plus nombreuses et formant un motif périodique.

La conviction que cela se poursuit est totale. En effet, d'une part, le programme a été testé un grand nombre de fois et nul ne doute qu'il calcule comme il faut (on peut aussi refaire fonctionner la configuration initiale de dix cellules avec un autre programme) ; d'autre part, la régularité de ce qu'on observe ne laisse pas de doute sur l'idée que la croissance se poursuivra indéfiniment. C'est bien l'observation du programme en train de fonctionner en continu qui crée cet état d'évidence entraînant l'adhésion dont parlait Thom et qui caractérise les preuves rigoureuses.

L'étude du *Jeu de la vie* et de bien d'autres automates cellulaires conduit à pratiquer ce type de démonstrations et essentiellement celui-là. On y prouve des théorèmes dont certains sont si peu évidents qu'on ne les a découverts qu'après plusieurs décennies

6. Les démonstrations par manipulation

Si vous réussissez à ranger la boîte de cubes, vous en tirerez sans mal une preuve descriptive du théorème géométrique affirmant que ce rangement est possible. En revanche, si, après avoir essayé durant une heure de ranger une boîte avec six pièces, vous n'avez pas réussi, vous serez persuadé que c'est impossible et n'aurez pas le moindre doute. La conviction acquise « par manipulation » que la boîte ne peut pas être rangée sera malheureusement incommunicable et ne constituera donc pas une preuve mathématique acceptable.

Le cube diabolique (A), qui date du XIX^e siècle, est, semble-t-il, le plus ancien problème de rangement du cube. Le cube de Steinhaus (B) a été inventé en 1930 et le *Half Hour Puzzle* de Coffin, inventé vers 1970 (C), se remonte après une demi-heure de réflexion... Les solutions à droite représentent les trois vues du cube (de gauche, de droite et de dessus).

