5. LES JEUX DE CARTES COMME ARMES DE GUERRE ET LES NOMBRES PREMIERS ILLÉGAUX

Le matériel de cryptographie est assimilé dans certains pays à une arme de guerre et, à ce titre, sévèrement contrôlé. Les systèmes trop puissants, car utilisant des clefs longues, empêchant les approches exhaustives, sont par exemple interdits à l'exportation par les lois fédérales des États-Unis. Pour prendre en compte l'existence du système cryptographique de Schneier qui n'utilise comme matériel qu'un jeu de 54 cartes et dont les clefs dépassent les longueurs autorisées, les douaniers américains confisqueront-ils tous les jeux de 54 cartes que les voyageurs emportent dans leurs bagages?

Ce n'est pas le seul cas où la cryptographie met les lois en difficulté, conduisant à des situations plus ou moins ridicules. Récemment, l'algorithme de cryptage des DVD (le DVD *Movie encryption scheme* : DeCSS) a été reconstitué par des spécialistes qui ont analysé des puces et des logiciels chargés du décryptage (cet exemple montre que vouloir cacher un algorithme est une mauvaise idée).

En janvier 2000, le juge Lewis Kaplan, de New York, a décidé d'interdire la diffusion du programme de décryptage des DVD qui avait été publié sur internet. Cette interdiction est apparue en contradiction avec le principe exprimé par le premier amendement de la constitution américaine qui garantit la liberté d'expression. Le juge a donc été amené à préciser dans un jugement complémentaire que les codes sources (les programmes d'ordinateurs que l'ordinateur comprend et fait fonctionner) ne rentraient pas dans le champ du premier amendement et pouvaient être interdits.

La difficulté est qu'entre le langage parlé courant (qui ne peut être soumis à restriction) et le langage symbolique codé d'un programme toutes sortes d'intermédiaires sont possibles. On peut, par exemple, prendre le texte interdit du programme de décryptage des DVD et en faire une description lettre par lettre du type : "la première lettre du texte est un A, puis vient un =, etc." Ce texte, qui n'est pas un programme source, ne peut pas être interdit, alors que pourtant, il permet de reconstituer le programme source interdit.

Pour montrer l'absurdité des arrêts pris par le juge Kaplan une série de textes et d'images décrivant de manière indirecte le programme interdit ont été réalisés et placés sur internet. Plusieurs dizaines de ces documents sont disponibles librement à l'adresse internet suivante : www.cs.cmu.edu/~dst/DeCSS/Gallery/

En particulier, on y propose un nombre premier qui, quand on le traduit en base de numération 16, correspond à une version comprimée du programme interdit par le juge Kaplan. Connaître ce nombre premier c'est donc à peu de chose près connaître le programme interdit.

Si le juge Kaplan réussit à faire prévaloir son point de vue le nombre premier est donc illégal et interdit de publication. La rédaction de *Pour la Science,* choquée qu'un nombre premier puisse être interdit de publication, a décidé de passer outre en offrant à ses lecteurs ce magnifique nombre premier que l'on pourra consulter sur le site de *Pour la Science* : www.pourlascience.com

Pour plus de détails voir :
www.utm.edu/research/primes//curios/48565...29443.html

Une fois passées toutes les lettres de la phrase convenue, le paquet de 54 cartes sera dans un ordre qui sera celui qu'on utilisera pour produire (par l'utilisation répétée des opérations 1, 2, 3, 4, et 5) un flux de clefs.

Avec un tel procédé, après s'être rencontré une seule fois pour convenir de la façon de choisir la phrase clef du jour Alice et Bernard peuvent échanger indéfiniment des messages qui seront inviolables, même pour les plus puissants systèmes informatiques d'aujourd'hui et des décennies à venir.

ATTAQUES?

L'idée de Schneier suscite un certain intérêt et depuis que l'algorithme a été publié (il y a quelques mois) des attaques contre ce système ont été lancées. Bien que bâti par un des meilleurs cryptologue mondial, à partir de principes dont les spécialistes sont convaincus de l'efficacité, seule la résistance à des attaques nombreuses et répétées attestera de l'inviolabilité de *Solitaire* de Schneier.

Un premier travail a consisté à écrire un programme qui peut essayer 10^6 clefs par seconde et conduit à établir des statistiques. C'est ainsi que Paul Crowley a découvert que dans les suites pseudo-aléatoires engendrées par *Solitaire* un léger biais statistique était décelable : la probabilité que deux lettres consécutives dans un flux de clefs soient identiques au lieu d'être égale à 1/26 est de 1/22,5. Ce léger biais ne remet pas en cause la robustesse de *Solitaire*, mais si d'autres propriétés plus fines du flux de clefs sont découvertes il se pourrait que Schneier doive modifier son système.

D'autres chercheurs ont dès à présent proposé d'autres méthodes analogues ne demandant qu'un jeu de cartes pour le calcul et c'est peut-être bien tout un domaine nouveau de recherche qui vient de naître : la crypto-carto-ludico-graphie.

Paul CROWLEY, *Problems with Bruce Schneier's «Solitaire»* (Une attaque du Solitaire de Schneier) : www.cluefactory.org.uk/paul/solitaire/

David KAHN, *The Codebreakers*, 2e éditions, Scribner, New York, 1996. Traduction de la première édition : *La Guerre des codes secrets,* Interéditions, 1980.

Simon SINGH, *Histoire des codes secrets,* J.-C. Lattès, Paris, 1999.

Bruce SCHNEIER, *The Solitaire Encryption Algorithm*,1999. www.counterpane.com/solitaire.html

Bruce SCHNEIER, *Secret and Lies*, John Wiley and Sons, Inc., New York, 2000.

J. SAVARD, *Fun With Playing Cards* (un autre système de cryptographie à base de jeu de cartes) http://home.ecn.ab.ca/~jsavard/crypto/pp0105.htm

Neal STEPHENSON, *Cryptonomicon I. Le code enigma*, Payot-SF, 2000. Site internet consacré au roman de N. Stephenson. www.cryptonomicon.com

Leïla Belkon

Les sauts champions

IAN STEWART

Les sauts entre des nombres premiers consécutifs se livrent à une compétition de fréquences.

Quoi de plus banal que la suite des entiers naturels 1, 2, 3, 4...? Pourtant, cette suite est à l'origine d'un concept très déroutant, celui des nombres premiers 2, 3, 5, 7, 11... La structure de la suite des entiers naturels est évidente : quel que soit l'entier que vous choisissez, déterminer le suivant est trivial, il suffit d'ajouter 1. Il en va tout autrement pour les nombres premiers. Pourtant, le passage des nombres entiers aux nombres premiers est aisé : il suffit de prendre ceux sans diviseur autre qu'eux-mêmes ou 1.

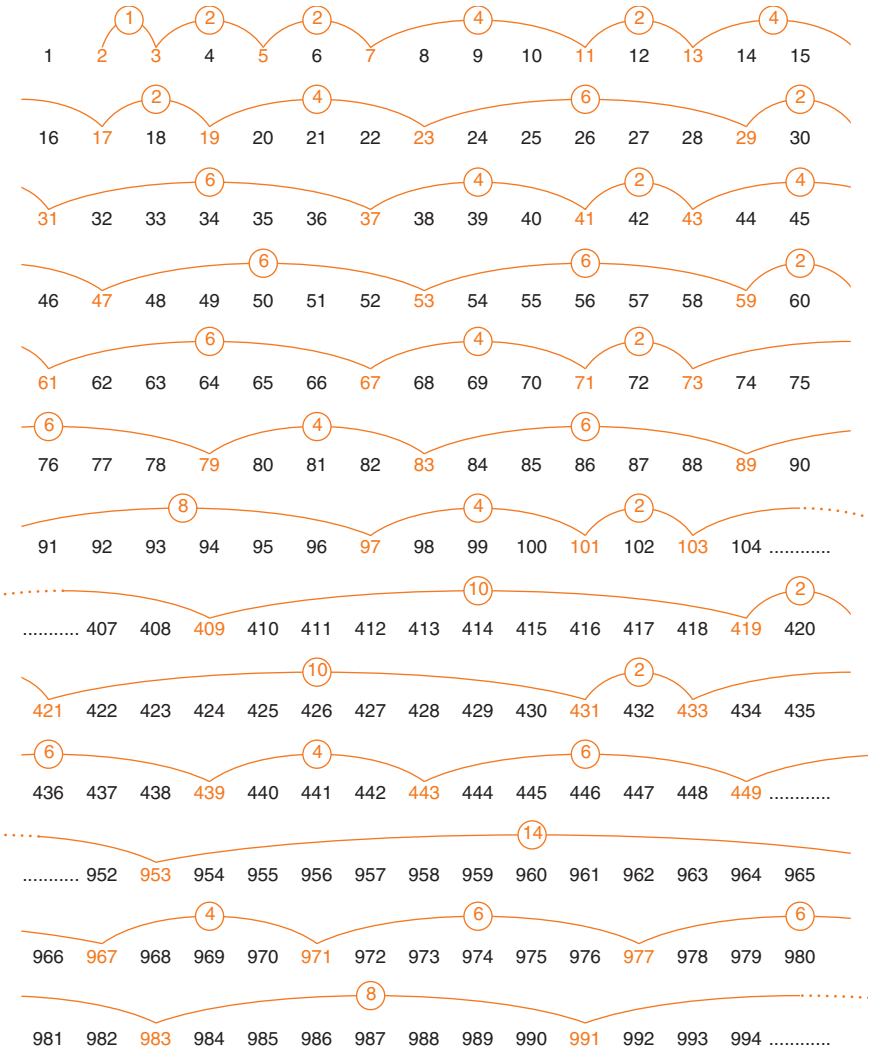
Nous connaissons nombre de propriétés des nombres premiers, notamment certaines formules puissantes qui donnent de bonnes approximations lorsque les réponses exactes sont inaccessibles. Par exemple, le *Théorème de répartition* indique que le nombre de nombres premiers inférieurs à x est approximativement $x/\ln x$ lorsque x est assez grand ($\ln$ est le logarithme népérien de x). Ainsi, nous savons qu'il y a environ $4{,}3.10^{27}$ nombres premiers qui ont moins de 100 chiffres, mais leur nombre exact est inconnu.

Récemment, Andrew Odlyzko, des Laboratoires *AT&T*, Michael Rubinstein, de l'Université du Texas, et Marek Wolf, de l'Université de Breslau, en Pologne, se sont intéressés aux intervalles, ou sauts, entre deux nombres premiers consécutifs. Dans un article publié dans *Experimental Mathematics* (vol. 8, n° 2, 1999), ils ont traité du problème suivant : parmi les nombres premiers successifs inférieurs à x, quel est le saut le plus fréquent? Cette question a été posée à la fin des années 1970 par Harry Nelson, du Laboratoire Lawrence Livermore. Plus tard, John Horton Conway, de l'Université Princeton, a utilisé l'expression de «sauts champions» pour nommer ces intervalles les plus fréquents.

Les nombres premiers jusqu'à 50 sont 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 et 47. La suite de sauts est donc 1, 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2 et 4. Le nombre 1 n'apparaît qu'une seule fois, car les nombres premiers autres que 2 sont impairs. Les autres sauts sont donc pairs : 2 apparaît six fois, 4 cinq fois et 6 deux fois. Ainsi, pour x égal à 50, le saut le plus fréquent est 2, qui est le saut champion.

Pour certaines valeurs de x, le titre de sauts champions a plusieurs gagnants. Pour x = *5*, les sauts sont 1 et 2, chacun apparaissant une fois. Pour x supérieur, le seul saut champion est 2 tant que x est inférieur à 101, pour lequel 2 et 4 sont champions *ex aequo (voir la figure 1)*. Jusqu'à $x = 179$ pour qui 2, 4 et 6 partagent le titre, les champions sont soit 2, soit 4, soit les deux. Ensuite, 4 s'incline et 2 règne sans partage jusqu'à $x = 379$ pour qui 2 et 6 dominent. Pour x supérieur à 389, le champion est souvent 6, qui parfois partage son titre avec 2 ou 4 ou les deux. De 491 à 541, 4 est champion. Au-delà de 947, l'unique champion est 6 : grâce à un ordinateur, on sait que cela reste vrai au moins jusqu'à $x = 1\,012$.

Est-il raisonnable de conclure qu'excepté pour des petits nombres pour qui



Les dessins sont de Bryan Christie

1. Les sauts les plus fréquents entre des nombres premiers successifs inférieurs à $x = 1\,000$ sont, selon x, les nombres 2, 4 ou 6. Toutefois, personne ne connaît les «sauts champions» pour de longues suites de nombres entiers.

1, 2 et 4 se disputent, 6 est l'unique saut champion pour des nombres très grands. Toutefois, une propriété vérifiée pour des milliards d'entiers peut ne plus l'être pour d'autres. La surprise est là !

Les mathématiciens ont proposé un argument convaincant selon lequel, aux environs de $x = 1{,}7427 \times 10^{35}$, le titre de champion passe de 6 à 30. Ce titre échoirait à 210 pour x supérieur à 10^{425}.

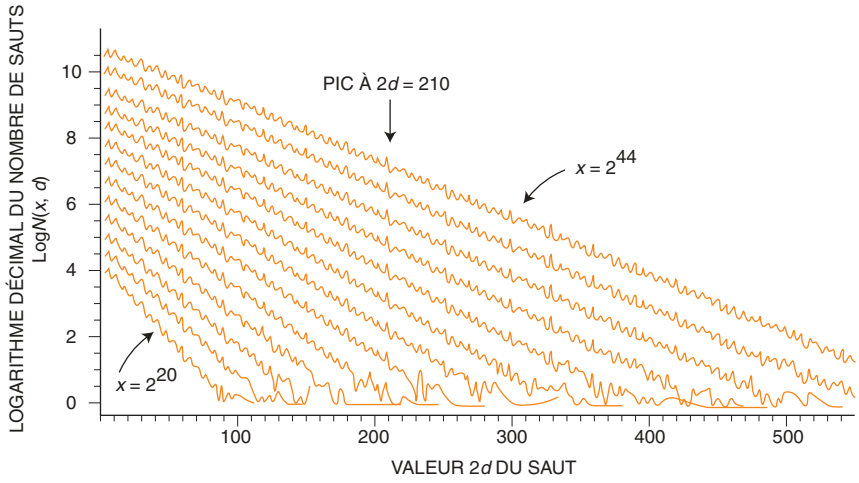
LA CONJECTURE DES NOMBRES PRIMORIELS

À l'exception de 4, les factorisations des champions conjecturés s'inscrivent dans une élégante structure : $2 = 2$, $6 = 2 \times 3$, $30 = 2 \times 3 \times 5$, $210 = 2 \times 3 \times 5 \times 7$. Chacun d'eux est obtenu par la multiplication des premiers nombres premiers consécutifs. Ces nombres sont dits primoriels – un mot valise entre *premier* et *factoriel* – et les suivants sont 2 310, 30 030 et 510 510. Dans leur article, A. Odlyzko et ses coauteurs proposent la conjecture des sauts champions : ce sont 4 et les nombres primoriels.

Comment sont-ils parvenus à cette hypothèse ? Un examen de la suite des nombres premiers révèle que, parfois, deux d'entre eux sont des entiers impairs consécutifs, tels, par exemple, 5 et 7, 11 et 13, 17 et 19… La *Conjecture des nombres premiers jumeaux* énonce qu'il y a une infinité de tels couples. Elle est fondée sur la distribution aléatoire des nombres premiers au sein des nombres entiers impairs, avec une probabilité issue du *Théorème de répartition*. Cette hypothèse semble un non-sens – un entier est premier ou non, sans qu'il soit question de probabilité –, cependant, dans ce problème, il s'agit d'un non-sens raisonnable : la probabilité d'avoir un ensemble fini de nombres premiers jumeaux est nulle.

Trois nombres impairs consécutifs peuvent-ils être premiers ? Il n'y a qu'un seul exemple (3, 5, 7), car dans trois nombres impairs consécutifs, l'un d'entre eux est un multiple de trois. S'il est premier, c'est donc 3. Un tel argument ne s'applique pas aux triplets p, $p + 2$, $p + 6$ ou p, $p + 4$, $p + 6$ qui sont fréquents. Par exemple, 11, 13, 17 ou 41, 43, 47 sont du premier type et 7, 11, 13 ou 37, 41, 43 du second.

Dans les années 1920, les mathématiciens britanniques Godfrey Hardy et John Littlewood ont analysé les structures de ce type avec un grand nombre de nombres premiers. Avec un calcul de probabilités similaire à celui des nombres premiers jumeaux, ils ont établi une formule précise pour le nombre de suites de nombres premiers dotés d'une structure donnée de sauts. Cette formule est complexe, aussi ne la donnerais-je pas ici ; vous la trouverez dans l'article cité précédemment.



2. Ce diagramme indique en fonction de x la fréquence des écarts entre deux nombres premiers consécutifs. Pour la première courbe, on a étudié les nombres premiers inférieurs à 2^{20}, puis on a calculé le nombre de fois où l'écart entre deux nombres premiers consécutifs était 2, puis 4, puis 6… Les courbes suivantes sont construites de la même façon pour $x = 2^{22}$, $x = 2^{24}$ jusqu'à $x = 2^{44}$. À mesure que x croît, un pic apparaît pour un écart $2d$ égal à 210. Il est conjecturé que ce pic finit par dépasser l'ordonnée du point de départ, c'est-à-dire que pour une certaine valeur (élevée) de x, l'écart le plus fréquent est 210.

Du travail de Hardy et Littlewood, A. Odlyzko et ses collègues ont déduit une formule pour $N(x, d)$, le nombre de sauts de valeur $2d$ entre des nombres premiers consécutifs inférieurs à x (nous préférons $2d$ à d pour signifier que les sauts sont pairs). Cette formule n'est estimée valide que lorsque $2d$ est grand et x bien plus grand encore. La figure 2 montre comment $\log N(x, d)$ varie selon $2d$ pour 13 valeurs de x de 2^{20} à 2^{44} (log désigne le logarithme en base 10). Chaque graphe est approximativement linéaire avec un très grand nombre de pics. L'un d'eux est particulièrement marqué, à $2d = 210$, le saut champion conjecturé pour x très grand (il serait encore plus marqué s'il n'était pas «écrasé» par le logarithme). Ce type de résultat indique que la formule de $N(x, d)$ est proche de la réalité.

Quand $2d$ s'approche de la valeur du saut champion, $N(x, d)$ est nécessairement très grand. La meilleure situation qui s'accorde avec cette idée est lorsque $2d$ a de nombreux facteurs premiers distincts. De plus, $2d$ doit être aussi petit que possible, aussi, les choix les plus plausibles pour $2d$ sont-ils les primoriels. Le saut champion 4 est vraisemblablement une exception. Par ailleurs, il apparaît à des tailles pour lesquelles la formule $N(x, d)$ n'est pas une bonne approximation. La formule donne le résultat lorsqu'un primoriel donné prend le dessus sur le précédent comme nouveau saut champion.

Que reste-t-il à faire pour les mathématiciens ? Prouver la conjecture des sauts champions, bien sûr – ou la réfuter. Si vous n'envisagez ni l'un ni l'autre, essayez de trouver d'autres propriétés des sauts champions entre des nombres premiers successifs. Par exemple, quel est le saut le moins fréquent entre les nombres premiers consécutifs inférieurs à x ? Quel saut apparaît le plus proche du nombre moyen de fois ? Pour ce que j'en sais, ces questions restent ouvertes, et ce, même pour de petites valeurs de x.

Réactions

Dans mon récent article *Paradoxes perdus et retrouvés* (voir *Pour la science*, août 2000), j'indiquais que le paradoxe du contrôle surprise résulte d'une interprétation déraisonnable du mot surprise et, qu'en définitive, ce n'est pas un paradoxe du tout.

Plusieurs lecteurs ont attiré mon attention sur un article intitulé *Surprise maximization* dans *American Mathematical Monthly* (vol. 107, n° 6, juin-juillet 2000). Les auteurs définissent une mesure de la surprise et examinent quelle stratégie doit adopter le professeur pour maximaliser la surprise des étudiants. Leur conclusion est que pour choisir le jour de la semaine, il doit utiliser une distribution de probabilité qui reste quasi constante au début de la semaine pour croître rapidement sur la fin. Selon cette stratégie, il choisira plus souvent le vendredi.

La poussée d'Archimède

ROLAND LEHOUCQ • JEAN-MICHEL COURTY

Formulée il y a plus de 2 200 ans, la loi d'Archimède est simple, mais ses applications sont souvent plus subtiles qu'il n'y paraît.

Hiéron, roi de Syracuse (–265 à –215), soupçonna un jour son orfèvre de l'avoir volé. L'artisan avait-il remplacé par de l'argent une partie de l'or fourni pour fabriquer la couronne du roi? Hiéron demanda à son ami Archimède de vérifier quelle proportion d'argent contenait l'ornement royal. Le grand géomètre chercha à évaluer le volume de la couronne et sa densité. Toutefois, la forme compliquée de la couronne interdisait tout calcul simple. La légende veut qu'Archimède prit un bain pour réfléchir, et qu'il remarqua que la baignoire débordait quand il y entrait. Il comprit alors que l'immersion d'un corps déplace une quantité d'eau équivalente à son volume. Il se serait alors élancé nu dans la rue en criant *Euréka!*

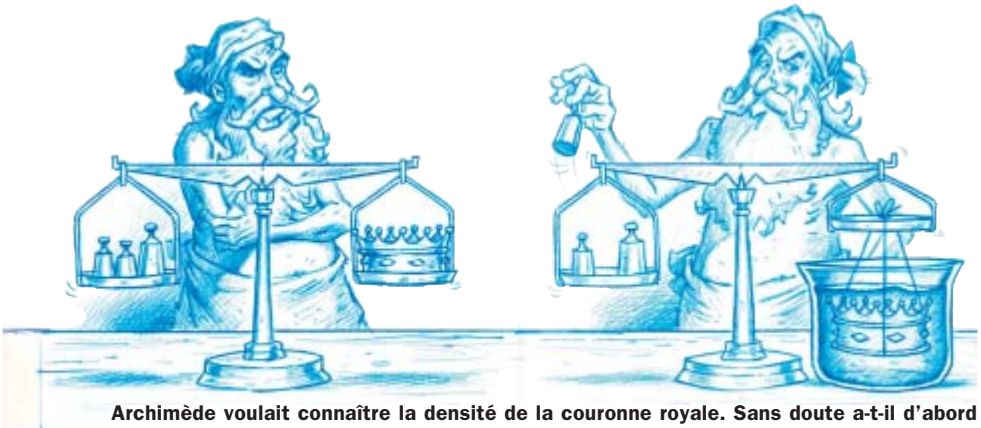
Archimède formula ainsi ce qu'il avait observé : tout corps plongé dans un liquide subit une poussée verticale dirigée vers le haut et égale au poids du volume de liquide déplacé. Hiéron serait satisfait! Pour déterminer la densité de la couronne par rapport à celle de l'eau, il lui suffisait de mesurer la diminution de son poids apparent dans l'eau. Imaginons les mesures qu'Archimède réalisa pour satisfaire le roi. Sans doute commença-t-il par peser la couronne en la suspendant sous le plateau d'une balance. Puis, il répéta l'opération en immergeant la couronne dans l'eau. Pour rétablir l'équilibre, Archimède dut retirer des poids du plateau opposé à celui qui soutenait la couronne. Il calcula ensuite la densité du métal en faisant le rapport entre le poids de la couronne du roi et le poids retiré du plateau. Archimède répéta ensuite cette opération avec un lingot d'or, afin de comparer la densité de la couronne à celle de l'or pur.

ARCHIMÈDE ET LA PRESSION

Pourquoi la poussée d'Archimède est-elle toujours dirigée vers le haut et égale au poids du volume du liquide déplacé? Quand la pression qui règne dans un fluide est uniforme, la résultante des forces qui s'exercent à la surface d'un volume de forme quelconque est nulle. En revanche, au sein d'un fluide placé à la surface de la Terre, la pression n'est pas uniforme, mais croît avec la profondeur à cause de la gravité. Dans les océans, par exemple, la pression augmente de l'équivalent d'une fois la pression atmosphérique tous les dix mètres (quelque 10^5 pascals). La force d'Archimède est verticale, car elle résulte de la différence entre les pressions qui règnent à des altitudes variées au sein du fluide. Examinons le cas d'un tube cylindrique immergé en position verticale. Un tel tube est symétrique : les forces de pression qui agissent sur la partie verticale de sa surface se compensent exactement : dans chaque plan horizontal, la résultante des forces qui s'exercent sur le corps immergé est nulle. En revanche, la pression que subit le tube sur sa face inférieure est plus grande que celle qui s'exerce sur sa face supérieure. Dirigée vers le haut, la résultante des forces de pression – la poussée d'Archimède – est la même que celle que le fluide exercerait sur une «colonne d'eau» occupant le même volume. Une telle colonne d'eau est en équilibre, puisqu'elle est immergée dans… de l'eau. Son poids contrebalance exactement la poussée d'Archimède : cette dernière est égale au poids de la colonne d'eau, c'est-à-dire au «poids du volume du liquide déplacé». On généralise ce raisonnement à des objets de formes quelconques.

Valable au sein des liquides, la loi d'Archimède s'applique à n'importe quel gaz soumis à l'attraction gravitationnelle terrestre. Ainsi, comme dans l'eau, la pression atmosphérique diminue dans l'air, avec l'altitude, mais beaucoup plus lentement. Un objet placé dans l'air subit aussi une poussée d'Archimède, car il déplace un volume d'air. Celle-ci est environ 1 000 fois inférieure à celle qui règne dans l'eau, car l'air est 1 000 fois moins dense que l'eau. C'est pourquoi en dehors de l'étude des aérostats et autres montgolfières, il est courant de négliger la force d'Archimède exercée par l'air.

Un objet dont la poussée d'Archimède compense le poids semble être en impesanteur. Dans la mer, il flotte entre deux eaux. Ce type d'équilibre est utilisé, par exemple, pour entraîner les astronautes aux manœuvres dans l'espace. On les immerge avec leur scaphandre dans une piscine, de sorte que la force Archimède les maintient en suspension.Toutefois, contrairement à la pesanteur, la force d'Archimède n'agit pas sur l'oreille interne, qui contrôle l'équilibre. Les astronautes



Dessins de Bruno Vacaro

Archimède voulait connaître la densité de la couronne royale. Sans doute a-t-il d'abord pesé la couronne *(à gauche)*. Puis, il a plongé la couronne dans de l'eau *(à droite)*. L'eau exerce une force dirigée vers le haut qui déséquilibre la balance. Pour la redresser, on doit enlever un poids égal à celui du volume d'eau déplacé : ici le volume *v* de la couronne, multiplié par la masse volumique de l'eau, égale à un gramme par centimètre cube (soit $\rho_{eau} v$). Or le poids total de la couronne est égal à son volume *v*, multiplié par la masse volumique de l'alliage dont elle est faite (soit $\rho_{alliage} v$). Le rapport de ces deux résultats donne le rapport des deux masses volumiques, c'est-à-dire la densité de l'alliage.