écrit les différences des carrés à n (nommés les carrés réduits) dans une liste *(voir la figure 10)*.

On détermine maintenant les carrés réduits dont tous les facteurs premiers sont dans la base de facteurs. On pourrait utiliser la méthode des divisions successives, mais un procédé de crible est plus rapide : pour trouver quels carrés réduits sont divisibles par un nombre premier p, on détermine tous les nombres u compris entre 0 et $p - 1$ pour lesquels $(m + u)^2 - n$ est divisible par p. À partir d'une valeur trouvée pour u, on trouve d'autres valeurs en ajoutant ou en soustrayant des multiples de p à cette valeur de u.

Dans l'exemple, le crible par 2 s'applique de la façon suivante : comme $(m + 1)^2 - n$ (égal à 140) est divisible par 2, il en est de même pour $(m - 1)^2 - n$, $(m - 3)^2 - n$ et $(m + 3)^2 - n$. On divise ces nombres par 2 jusqu'à ce que l'on obtienne un nombre impair (troisième ligne de la figure 10).

Le crible par 3 fonctionne de la même manière : on constate que $m^2 - n$ et $(m + 2)^2 - n$ sont divisibles par 3. En partant de $u = 0$ et $u = 2$, on se déplace par pas de longueur 3 vers la droite et vers la gauche, et on divise tant qu'on le peut par 3 les nombres ainsi obtenus. Par la même méthode, on crible par les autres nombres premiers de la base de facteurs. Partout où il y a un 1 à la fin de la liste, on peut décomposer le carré réduit sur la base de facteurs. On détermine la décomposition à l'aide de la méthode des divisions successives.

Ici, nous avons décrit la plus simple version du crible quadratique. La technique est plus vieille que l'ordinateur : l'officier français Eugène Olivier Carissan (1880-1925) construisit une machine mécanique avec laquelle on peut effectuer le crible pour plusieurs nombres premiers à la fois *(voir la figure 1)*.

Pour décomposer un nombre de 100 chiffres, on doit encore apporter de nombreuses améliorations. La base de facteurs et l'intervalle du crible deviennent gigantesques. Pour avoir une idée de leur ordre de grandeur, examinons les paramètres de la factorisation de RSA-120, un nombre de 120 chiffres que les Laboratoires *RSA* avaient donné à factoriser. La base de facteurs contenait 245 810 éléments, et le système d'équations à résoudre 245 810 inconnues et 252 222 équations. Le calcul aurait duré environ 50 ans sur une seule machine. Pour factoriser le nombre de 129 chiffres qui ouvre l'article, c'est aussi le crible quadratique qui fut employé.

Parallélisation

En dehors de l'amélioration de l'algorithme, l'emploi simultané d'un grand nombre d'ordinateurs accélère la factorisation. On peut utiliser soit des calculateurs parallèles (mais ils sont très chers), soit des systèmes partagés, par exemple des réseaux de machines qui sont très peu utilisées pendant la nuit ou le week-end.

À Sarrebrück, nous utilisons un réseau de 250 terminaux répartis sur le campus. Le système LiPS *(Library for Parallel Systems)*, que nous avons mis au point, reconnaît automatiquement quand une machine n'est pas sollicitée par son utilisateur principal, et il lance alors, par exemple, une factorisation. Quand l'utilisateur principal veut de nouveau travailler sur sa machine, LiPS arrête le programme de factorisation et le réveille de nouveau dès que la machine est libre. LiPS expédie enfin les résultats des calculs à l'ordinateur qui les centralise.

Même sur notre système réparti, le crible quadratique demande plusieurs semaines de calculs pour la factorisation d'un nombre de 130 chiffres. Le temps de calcul est doublé chaque fois que l'on ajoute trois chiffres, car les carrés réduits que l'on crible sont à peu près de la taille de $\sqrt{n}$.

Les algorithmes plus rapides, mais reposant sur le même principe que le crible quadratique doivent obtenir des relations grâce à la décomposition de nombres plus petits (de l'ordre non plus de $\sqrt{n}$, mais de n à la puissance 1/3 ou 1/4, par exemple). Le seul algorithme clairement meilleur, sur ce point, que le crible quadratique est le crible algébrique, qui a décomposé le nombre de Fermat F_9.

Avec le crible algébrique, un ensemble d'équipes dont nous faisons partie a décomposé un nombre RSA de 130 chiffres, en avril 1996. Les spécialistes s'attendent à ce qu'un crible algébrique amélioré puisse, dans un petit nombre d'années, factoriser un nombre quelconque de 160 chiffres. Ce serait un pas important, car les nombres composés qui sont employés dans la plupart des systèmes RSA ont moins de 160 chiffres : l'utilisation de tels systèmes RSA ne serait plus sûre.

La factorisation des nombres naturels est-elle un problème difficile? Pour le moment, oui : aucun algorithme au monde ne peut retrouver les facteurs d'un produit de deux nombres premiers de 150 chiffres. De tels produits constituent donc une bonne base pour la sécurité de protocoles cryptographiques, mais pour combien de temps?

Les mathématiciens, malgré des siècles de recherche, n'ont pas encore trouvé un algorithme de factorisation réellement rapide : est-ce suffisant pour affirmer que ce problème est difficile en soi? Non : grâce au développement des ordinateurs, des algorithmes ont déjà été découverts, et rien ne laisse supposer que les progrès considérables des 20 dernières années touchent déjà à leur fin.

Johannes BUCHMANN est professeur d'informatique à l'École d'enseignement supérieur technique de Darmstadt.

Martin HELLMAN, *Les mathématiques de la cryptographie à clef révélée*, in *Pour La Science*, octobre 1979.

Carl POMERANCE, *La recherche des nombres premiers*, in *Pour La Science*, février 1983.

D.M. BRESSOUD, *Factorizations and Primality Testing*, Springer, Heidelberg, 1989.

P. RIBENBOIM, *The Book of Prime Number Records*, Springer, Heidelberg, 1989.

H. COHEN, *A Course in Computational Algebraic Number Theory*, Springer, Heidelberg, 1993.

Arjen K. LENSTRA et Hendrik W. LENSTRA, *The Development of the Number Field Sieve*, Springer Lecture Notes in Mathematics, Band 1554, Springer, Heidelberg, 1993.

Hans RIESEL, *Prime Numbers and Computer Methods for Factorization*, 2, Auflage, Birkhäuser, Basel, 1994.

Yves HELLEGOUARCH, *Fermat enfin démontré*, in *Pour La Science*, février 1996.

François MORAIN, *La machine des frères Carissan*, in *Pour La Science*, janvier 1998.

Les bibliothèques de programmes LiDIA et LiPS sont disponibles à l'adresse Internet : / / www.informatik.th-darmstadt.de / TI / Forschung

Le site Internet des laboratoires RSA a pour adresse http: / / www.rsa.com / rsalabs /

Michael J. Howell, Hoaqui

Les martingales et autres illusions

JEAN-PAUL DELAHAYE

Au casino, on peut gagner presque certainement... en risquant beaucoup!

Un de mes amis, passionné de jeux de casino, prétendait qu'il est possible de gagner à la roulette. Je lui ai dit qu'il avait tort parce qu'il est mathématiquement démontré qu'on ne pouvait gagner. Quelle ne fut pas ma surprise lorsqu'il m'a rétorqué :

«Celui qui joue jusqu'à ne plus rien avoir va tout perdre. Il y a donc une façon (au moins) de mal jouer au casino. Mais alors, il y a certainement aussi une façon de bien jouer.»

Je suis resté interloqué et je n'ai pas su lui répondre sur le coup. J'ai l'esprit de l'escalier, aussi je lui réponds ici.

RÈGLES ET PROBABILITÉS

Dans n'importe quel jeu, à chaque fois que l'on mise, il existe une probabilité p de gagner et une probabilité q de perdre sa mise. Il est certain que, soit on gagne, soit on perd! Aussi la somme $p + q$ est-elle égale à 1, et q est égal à $1 - p$. Supposons que, comme à pile ou face, celui qui gagne récupère sa mise plus une somme égale à sa mise ; quand on perd, on laisse sa mise à l'autre joueur, que nous dénommerons *la banque*. Dans les casinos, des jeux de ce type, tels le rouge et le noir à la roulette, donnent aux parieurs une chance de gagner inférieure à 1/2. Le jeu n'est alors pas équitable, et l'on soupçonne que c'est pourquoi les casinos sont des entreprises rentables. Nous verrons dans ce qui suit que la rentabilité des casinos sur le long terme est garantie par les mathématiques.

Quelle est la probabilité p des jeux qu'on vous propose? Si vous trouvez un ami qui accepte de faire la banque et que vous jouez à pile ou face avec une pièce non truquée, votre probabilité p de gain est égale à 1/2. C'est la même probabilité que si vous jouiez sur une couleur à une roulette équitable. À la *roulette simple* (dont l'invention est attribuée à Pascal et qui a été introduite à Paris en 1765), si vous jouez sur noir, vous gagnez quand l'un des 18 numéros noirs sort ; vous perdez quand l'un des 18 numéros rouges sort et quand le zéro (qui est vert) sort. Ainsi la probabilité de gain p est égale à 18/37, soit 0,4864..., car il y a 37 numéros de 0 à 36. À la *roulette française,* la règle est un peu plus compliquée, car quand le zéro sort votre mise reste *prisonnière* jusqu'à ce qu'un prochain lancement de la bille vous la fasse perdre ou récupérer (sans gain), et votre probabilité de gain p est égale à 36/73, soit 0,4931... (*voir l'explication de ce 36/73 dans l'encadré 1).* À la *roulette américaine*, il y a un zéro et un double zéro verts, tous les deux favorables à la banque, sans système de mises prisonnières. Votre probabilité de gain p est de 18/38, soit 0,4736... Il existe aussi une *roulette mexicaine,* avec un triple zéro, correspondant à un $p = 18/39 = 0,4615$, mais c'est pour les *gringos*.

Pour calculer le gain de la banque, imaginons que 100 francs sont misés sur le noir et comptabilisons ce que, en moyenne, la banque perd (c'est-à-dire paie) et gagne. Dans une proportion de p cas, elle perd 100 francs ; dans une proportion de $1 - p$ cas, elle gagne 100 francs. Aussi la banque gagne en moyenne : $100\,(1 - p) - 100\,p$ francs, soit $100\,(1 - 2p)$ francs, que l'on appelle parfois *l'espérance mathématique* de gain de la banque pour 100 francs misés. Dès que p est inférieur à 1/2, alors $1 - 2p$ est positif, et donc la banque gagne *en moyenne*.

Ce gain moyen de la banque pour 100 francs misés est de 0 franc à pile ou face (ce jeu n'est pas proposé dans les casinos!) ; de 1,36 franc à la roulette française (avec système des mises prisonnières) ; de 2,70 francs pour la roulette simple, de 5,26 francs pour la roulette américaine ; de 7,69 francs pour la mexicaine.

Est-il possible, par un comportement rusé, de contourner ce gain théorique moyen de la banque et de le retourner en sa faveur? La question est historique : l'idée d'étudier par la théorie des probabilités les meilleures façons de jouer

1. LES RÈGLES DE LA ROULETTE FRANÇAISE

Il y a 37 numéros (de 0 à 36). Une bille lancée par le croupier sur une sorte de disque (appelé cylindre) qui tourne et comporte des encoches où la bille se stabilise (sur un numéro). Les *chances simples* sont *pair* (le 0 n'est pas considéré comme pair!), *impair*, *passe* (de 19 à 36), *manque* (de 1 à 18), *rouge* (1, 3, 5, 7, 9, 12, 14, 16, 18, 19, 21, 23, 25, 27, 30, 32, 34, 36), *noir* (les autres numéros, sauf zéro, qui est vert). Si on joue une *chance simple* et qu'elle tombe, on récupère sa mise accompagnée d'un gain équivalent payé par la banque. Si elle ne tombe pas, on perd sa mise, sauf si c'est le zéro qui tombe, auquel cas la mise est *prisonnière* ; il faut alors attendre le coup suivant qui, soit permet de la récupérer (sans gain) si la chance simple choisie tombe, soit la fait perdre. Si le zéro tombe à nouveau, la mise reste prisonnière, etc.

Quand le zéro tombe, il y a symétrie entre les deux hypothèses : récupérer sa mise ou la perdre, et donc on a une chance sur deux de récupérer sa mise (sans gain) et une chance sur deux de la perdre. Donc, dans 1 cas sur 74, la partie ne compte pas (zéro, puis récupération de la mise) ; dans 1 cas sur 74, la mise est perdue (un zéro, puis perte de la mise) ; dans 18 cas sur 37, perte immédiate de la mise ; dans 18 cas sur 37, gain immédiat.

En éliminant le cas où la partie ne compte pas, la probabilité de gagner est 36/73.

Si l'on met sa mise sur un «numéro plein» et qu'il sort, on gagne 36 fois sa mise. Si on utilise autre chose que les chances simples, il n'y a pas de système de mises prisonnières, et donc la part prise par la banque est plus forte : 1/37 (au lieu de 1/73).