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 /