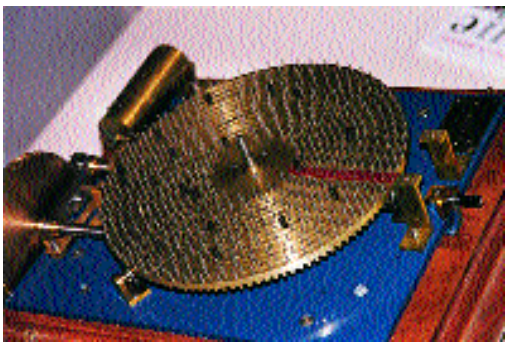

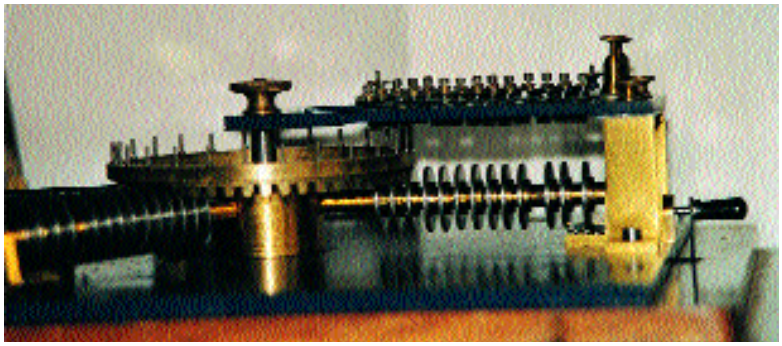

2. TOUTES LES COURONNES de la «machine à congruences» ont une position zéro (visible en rouge sur la photographie de gauche, où l'on a enlevé la barrette métallique). Les couronnes ne roulent pas seulement sur la roue dentée commune, mais aussi sur des disques, dont les axes, fixés à l'axe de la roue dentée, font des angles de 120 degrés les uns avec les autres *(à droite)*. Seules les pointes portant un capuchon produisent le contact dans la barrette métallique.

F_5, égal 4 294 967 297, était égal au produit de 641 par 6 700 417 : F_5 n'est donc pas un nombre premier (on dit que c'est un nombre composé). Puis, 150 ans plus tard, en 1880, F_6 fut factorisé et, encore 90 ans plus tard, en 1970, les deux facteurs premiers de F_7 ont été obtenus. Le nombre F_8 a été décomposé en 1980, et le nombre F_9 en 1990.

Cette histoire des nombres de Fermat montre combien la factorisation est difficile : les mathématiciens mirent 240 ans pour factoriser le nombre de Fermat F_7, à 39 chiffres, et, même équipés d'ordinateurs ils ont mis 20 ans à décomposer le nombre F_9, de 155 chiffres.

En revanche, il savaient que F_7, F_8 et F_9 n'étaient pas premiers bien avant de connaître leurs facteurs : on peut déterminer, grâce à un test spécial, si un nombre est composé, sans calculer ses facteurs. On s'assure ainsi que la factorisation est possible, avant de l'entreprendre.

Un test simple de primalité

Comment détermine-t-on qu'un nombre est premier? On peut utiliser le test de Fermat, c'est-à-dire examiner si n est un diviseur de $2^{n-1}-1$: Fermat a prouvé que tout nombre premier n (sauf 2) est diviseur de 2^{2n-1}. Par exemple, 3, qui est premier, est un diviseur de $2^{3-1}-1$, soit 3. Inversement, si n n'est pas un diviseur de $2^{n-1}-1$, n n'est pas premier. Par exemple, le nombre 6 n'est pas un diviseur de $2^{6-1}-1$, soit 31 ; il n'est pas premier.

Examinons un exemple plus compliqué, afin d'apprécier l'utilité du test de Fermat : le nombre 58 483 est-il premier? On pourrait commencer par calculer $2^{58\,482}-1$, puis chercher si le résultat est un multiple de 58 483, mais un calcul direct serait extrêmement long, car le nombre $2^{58\,482}-1$ s'écrit avec 17 604 chiffres. On utilise plutôt l'arithmétique des congruences *(voir l'encadré de la page 91)*, pour obtenir un algorithme efficace, fondé sur l'idée suivante : vérifier que 58 483 est un diviseur de $2^{58\,482}-1$ revient à chercher si le reste de la division de $2^{58\,482}$ par 58 483 est 1.

Pour calculer ce reste, on effectue une «exponentiation binaire». On commence par écrire 58 483 comme une somme de puissances de 2 : $58\,482 = 2^{15}+2^{14}+2^{13}+2^{10}+2^6+2^5+2^4+2$. Puis on utilise cette décomposition pour écrire le nombre $2^{58\,482}$ comme un produit de puissances de 2 : $2^{2^1}\times 2^{2^4}\times 2^{2^5}\times 2^{2^6}\times 2^{2^{10}}\times 2^{2^{13}}\times 2^{2^{14}}\times 2^{2^{15}}$. Ensuite on calcule successivement les restes des divisions par 58 483 de 2^{2^0}, 2^{2^1}, 2^{2^2}, 2^{2^3}... jusqu'à $2^{2^{15}}$. Le reste de la division de $2^{2^{i+1}}$ par 58 483, pour n'importe quel nombre entier i, s'obtient simplement à partir du reste précédent (celui de la division de 2^{2^i} par 58 483) : on l'élève au carré, on divise ce carré par 58 483, et on prend le reste de cette division *(voir la figure 3)*. Ainsi, de proche en proche, on détermine le reste par 58 483 de la division pour chacune des puissances qui interviennent dans le développement binaire de 58 482. On multiplie enfin tous ces restes, mais en ne gardant, après chaque multiplication, que le reste de la division par 58 483. De cette façon, les résultats intermédiaires restent de taille raisonnable. On détermine ainsi que le reste de la division de $2^{58\,482}$ par 58 483 est égal à celui du produit $4\times 7\,053\times 34\,259\times 42\,237\times 34\,763\times 53\,664\times 5010\times 10\,893$: il est égal à 11 669. Pour simplifier l'expression des résultats, les mathématiciens écrivent : $2^{58\,482}\equiv 11\,669 \bmod 58\,483$. Le signe $\equiv$ se lit «congru à» ; il indique que les expressions à sa gauche et à sa droite ont le même reste dans la division par le nombre indiqué après l'abréviation mod, laquelle se lit «modulo».

Le système RSA

Le protocole de cryptographie RSA se fonde sur le résultat suivant :

Soit p et q deux nombres premiers. On pose $n = pq$. Si e est un nombre entier premier avec $(p-1)(q-1)$, alors il existe un nombre entier d positif, tel que, pour tout A, $A^{ed} - A$ soit divisible par n.

(X et Y sont dits premiers entre eux si leur seul diviseur commun est 1).

Le protocole est le suivant :

Alice choisit p, q, e (p et q premiers, et e premier avec $(p-1)(q-1)$.

Alice calcule $n = pq$ et d, ce qui est facile.

Alice rend publics n et e (par exemple en les publiant dans un annuaire).

Robert, qui veut communiquer une information secrète à Alice, transforme son information en un nombre entier A inférieur à n (ou en plusieurs nombres si nécessaire) avec un codage connu de tous.

Robert calcule le reste B de la division de A^e par n, envoie B à Alice par un canal qui n'a pas besoin d'être protégé (par exemple en publiant B dans un journal).

Alice, pour décoder B, va calculer B^d ; comme les restes de la division de B^d et de A^{ed} par n sont égaux à A, elle connaîtra A et donc le message de Robert.

Sécurité du système RSA

La sécurité de ce codage à clé publique repose sur la difficulté du calcul des facteurs de n : quiconque les connaît peut facilement calculer d et déchiffrer les messages envoyés par Robert à Alice.

L'application du test de Fermat, finalement, indique que le nombre 58 483 n'est pas premier, puisque le résultat n'est pas 1. Ce procédé est relativement rapide, mais il ne fournit pas la décomposition en facteurs premiers de 58 483.

La méthode des divisions successives

Quand on sait qu'un nombre n n'est pas premier, comment peut-on le factoriser? On cherche une décomposition en diviseurs propres, c'est-à-dire qui ne sont égaux ni à 1 ni à n (les nombres 1 et n sont nommés diviseurs triviaux de n) ; par exemple, 3 est un diviseur propre de 12. Puis on examine si ces diviseurs sont des nombres premiers. S'ils ne le sont pas, on les décompose à leur tour, jusqu'à ce que tous les diviseurs soient premiers.

Par exemple, $12 = 3 \times 4$. Le nombre 3 est premier, mais 4 est composé et peut être factorisé : $4 = 2 \times 2$. La décomposition complète de 12 s'écrit donc $12 = 2 \times 2 \times 3$. Ainsi, dans un algorithme de factorisation, la recherche d'un facteur propre d'un nombre composé est une opération fondamentale.

La méthode la plus simple est celle des divisions successives : on divise n par tous les nombres premiers 2, 3, 5, 7, 11, 13, 17, etc. (préalablement stockés dans une table), jusqu'à ce qu'une division tombe juste. Dans le cas de n = 58 483, on observe que le 51e nombre premier, 233, est un diviseur ($58\,483 = 233 \times 251$). On doit donc effectuer 51 divisions avec reste pour trouver ce facteur, ce qui reste possible, mais quand le plus petit facteur premier p de n devient grand, les divisions nécessaires sont de plus en plus nombreuses *(voir la figure 4)*, et la table des nombres premiers nécessaires aux calculs est de plus en plus grande. La factorisation par divisions successives ne convient que pour la recherche de petits facteurs ; pour des facteurs plus grands, une méthode fondamentalement différente s'impose.

Les courbes elliptiques

En 1985, Hendrik Lenstra a trouvé un algorithme de factorisation qui utilise des courbes elliptiques. Ces objets mathématiques, qui ont notamment été employés par le mathématicien britannique Andrew Wiles dans sa démonstration de la conjecture de Fermat, sont également utilisés dans des protocoles cryptographiques.

Dans la méthode des courbes elliptiques comme dans le test de Fermat, on effectue un calcul qui réussit si n est un nombre premier et qui échoue quand n est composé (ce que l'on sait, par exemple, grâce à un test de Fermat préliminaire) : au cours des calculs, on doit à plusieurs reprises extraire le plus grand diviseur commun (pgcd) de n et d'autres nombres, et le calcul ne se poursuit que si le pgcd est égal à 1, c'est-à-dire si les deux nombres sont premiers entre eux. Dans le cas contraire, ce pgcd est un diviseur de n, et même un diviseur propre si on a de la chance : l'objectif est alors atteint.

Du hasard intervient dans cette méthode, car on a le choix entre un grand nombre de courbes elliptiques pour mener les calculs *(voir la figure 7)*. On en choisit une au hasard. Si elle ne fournit pas de diviseur, on essaie la sui-

i	0	1	2	3	4	5	6	7
RESTE	2	4	16	256	7 053	34 259	42 237	57 220
i	8	9	10	11	12	13	14	15
RESTE	16 128	38 483	34 763	31 340	44 631	53 664	5 010	10 838

3. LES RESTES DES DIVISIONS de 2^{2^i} par 58 483 pour i compris entre 0 et 15. Pour trouver ces valeurs, il n'est pas nécessaire de calculer les nombres 2^{2^i} (qui peuvent être très grands) : on utilise les restes précédemment calculés.

S	10^3	10^6	10^9	10^{12}	10^{15}	10^{18}
NOMBRES PREMIERS INFÉRIEURS OU ÉGAUX À S	167	78 497	$1,8 \times 10^7$	$3,6 \times 10^{10}$	$2,8 \times 10^{13}$	$2,4 \times 10^{16}$

4. LE NOMBRE de nombres premiers inférieurs à 10^3, 10^6, etc. est aussi le nombre de divisions qui sont nécessaires, dans la méthode des divisions successives, pour obtenir un facteur premier de chaque taille respective.

Congruences et calcul du plus grand diviseur commun (pgcd)

Les mathématiciens ont étendu les opérations courantes aux restes de divisions des nombres entiers. Par exemple, quand on divise 7 par 3, le quotient est 2 et le reste 1, car $7 = 2 \times 3 + 1$. Pour les nombres négatifs, le calcul est analogue. Le quotient de –7 par 3 est –3 et le reste est 2, car $3 \times (-3) + 2 = -7$. Lors de la division de a par n, le reste est un des nombres $0, 1, 2, \ldots, n-1$. On le note $R(a,n)$.

Le plus grand diviseur commun (pgcd) de deux nombres entiers naturels a_1 et a_2 est obtenu par l'algorithme d'Euclide. On calcule la suite $a_3 = R(a_1, a_2)$, $a_4 = R(a_2, a_3)$, etc. Après un certain nombre de divisions, le reste est 0. Le pgcd de a_1 et a_2 est le dernier reste non nul. Par exemple, le pgcd de $a_1 = 631$ et de $a_2 = 405$ est obtenu de la façon suivante :

631/405 = 1 reste 226
405/226 = 1 reste 179
226/179 = 1 reste 47
179/47 = 3 reste 38
47/38 = 1 reste 9
38/9 = 4 reste 2
9/2 = 4 reste 1
2/1 = 2 reste 0.

Le dernier reste non nul est 1, donc le pgcd de 405 et de 631 est 1. Les deux nombres sont premiers entre eux. Lorsque deux nombres entiers a et b donnent le même reste dans la division par un entier naturel n, on dit qu'ils sont congrus modulo n et on écrit $a \equiv b \bmod n$. Par exemple, $10 \equiv 4 \bmod 3$, car 10 et 4 donnent le reste 1quand on les divise par 3. On démontre facilement que $a \equiv b \bmod n$ si n est un diviseur de $b - a$: le nombre $10 - 4 = 6$ est divisible par 3.

Quand on calcule le reste, pour une expression compliquée qui inclut des additions, des soustractions ou des produits, on peut remplacer tous les résultats intermédiaires par leur reste. Par exemple, si l'on veut calculer le reste de $14 \times (12 + 7)^8$ dans la division par 8, on remplace 14 par 6 (le reste de la division de 14 par 8) et 12 par 4, et l'on a : $14 \times (12 + 7)^8 \equiv 6 \times (4 + 7)^8 \bmod 8$. Ensuite, on obtient $6 \times (4 + 7)^8 \equiv 6 \times 3^8 \equiv 6 \times (3^2)^4 \equiv 6 \times (1^4) \equiv 6 \bmod 8$. On aurait aussi pu calculer $14 \times (12 + 7)^8 = 237\,769\,882\,574$, puis diviser le résultat par 8 et prendre le reste. Avec la première méthode, les résultats intermédiaires ne dépassent jamais 7, ce qui rend les calculs beaucoup plus rapides.