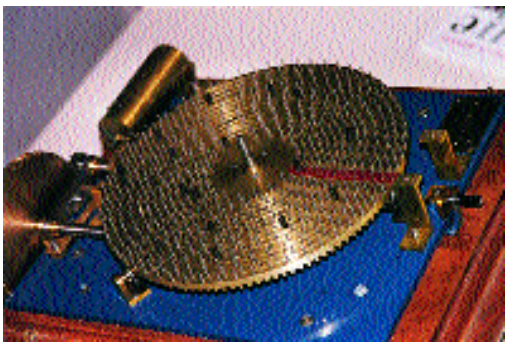

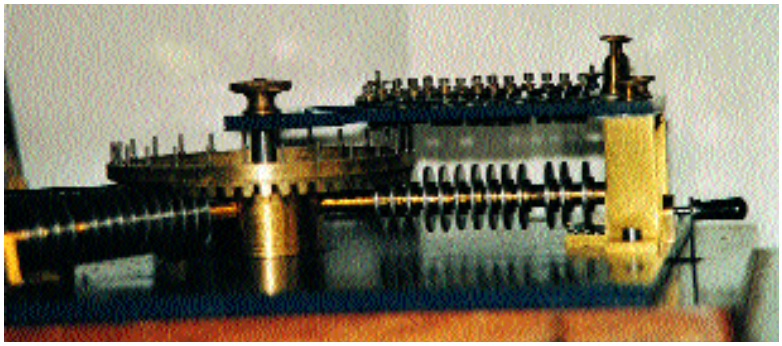

2. TOUTES LES COURONNES de la «machine à congruences» ont une position zéro (visible en rouge sur la photographie de gauche, où l'on a enlevé la barrette métallique). Les couronnes ne roulent pas seulement sur la roue dentée commune, mais aussi sur des disques, dont les axes, fixés à l'axe de la roue 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 ≡ 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.