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	7 063	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	10 836

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.

vante. H. Lenstra a démontré que, pour tout nombre composé n, il existe des courbes elliptiques qui fournissent un diviseur.

Comme pour la méthode par divisions successives, le temps nécessaire pour trouver un diviseur par la méthode des courbes elliptiques dépend de la taille de ce diviseur. Cependant, cette méthode identifie en un temps raisonnable les facteurs ayant jusqu'à 30 chiffres *(voir la figure 5)*.

Qu'est-ce qu'une courbe elliptique? C'est un ensemble de points d'un plan, dont les coordonnées x et y vérifient l'équation $y^2 = x^3 + ax + b$. Les paramètres a et b sont des nombres entiers choisis de telle sorte que $4a^3 + 27b^2$ soit différent de 0 *(voir la figure 6)*. Malgré leur nom, les courbes elliptiques n'ont qu'un rapport très éloigné avec les ellipses. Elles sont parfois composées de plusieurs branches.

Les courbes elliptiques sont des ensembles intéressants, car on peut définir une opération d'addition de leurs points : à deux points P_1 et P_2 d'une courbe elliptique, une construction géométrique simple associe un troisième point de la courbe, qui est nommé $P_1 + P_2$. L'opération ainsi définie a des propriétés analogues à l'addition des nombres entiers : elle est associative (le point $(P + Q) + R$ est confondu avec $P + (Q + R)$), commutative (le point $P + Q$ est le même que le point $Q + P$), elle admet un élément neutre (c'est-à-dire un point qui, ajouté à un point quelconque, ne change pas ce dernier) et chaque point a un opposé (ou inverse, tel que la somme du point et de son opposé soit égale à l'élément neutre).

L'inverse $-P$ d'un point P de la courbe est le symétrique de P par rapport à l'axe des abscisses. En général, on trouve la somme $P_1 + P_2$ de deux points P_1 et P_2 en traçant la droite qui passe par ces deux points : elle coupe la courbe en un troisième point Q, dont le symétrique $-Q$ par rapport à l'axe des abscisses est la somme cherchée, $P_1 + P_2$ *(voir la figure 6)*.

Quand P_1 et P_2 sont confondus, on obtient le point $P_1 + P_2$, ou $2P_1$, en remplaçant la droite P_1P_2 par la tangente à la courbe elliptique au point P_1. Enfin, quand P_1 est égal à $-P_2$, la droite passant par P_1 et P_2 ne coupe pas la courbe en un autre point ; on imagine alors que la droite coupe la courbe à l'infini. Pour cette raison, on ajoute aux points de la courbe un point que l'on se représente à l'infini et que l'on nomme O ; on pose $P_1 - P_1 = O$. Le point O est le zéro (l'élément neutre) de l'addition des courbes elliptiques.

L'addition de deux points peut aussi se définir algébriquement. Si P_1 et P_2 sont deux points de la courbe elliptique de coordonnées (x_1, y_1) et (x_2, y_2), alors : $-P_1 = (x_1, -y_1)$, $P_1 + P_2 = O$, si $P_1 = -P_2$; $P_1 + P_2 = P_2$, si $P_1 = O$; $P_1 + P_2 = P_1$, si $P_2 = O$; dans les autres cas, on détermine la somme $P_1 + P_2$ en calculant d'abord un nombre λ par les formules : $\lambda = (y_1 - y_2) / (x_1 - x_2)$, si P_1 est différent de P_2, et $\lambda = (3x_1^2 + a) / 2y_1$, si P_1 est égal à P_2. On détermine finalement les coordonnées (x_3, y_3) du point $P_3 = P_1 + P_2$ par : $x_3 = -x_1 - x_2 + \lambda^2$, et $y_3 = y_1 + \lambda(x_1 - x_3)$.

Notons que, lorsque P_1 est égal à $-P_2$, on pourrait étendre, d'une certaine façon, le calcul de λ : en toute rigueur, il est impossible, car la division par zéro n'est pas définie, mais on peut aussi admettre que l'élément neutre O possède des coordonnées infinies.

On peut utiliser ces formules sans chercher à se représenter x et y comme les coordonnées d'un point du plan. Cette abstraction devient utile quand les coordonnées des points considérés ne sont pas des nombres réels : tant qu'on peut additionner, soustraire, multiplier ou diviser ces coordonnées, on conserve les propriétés des courbes elliptiques. Nous avons notamment vu, à propos des congruences, que l'on peut additionner, soustraire et multiplier des restes de divisions. Plus précisément, le reste de la division d'un nombre entier par un nombre naturel n peut prendre les valeurs 0, 1, 2, ..., $n-1$. On calcule avec ces restes comme on le fait avec des nombres entiers, mais, quand le résultat d'un calcul sort de l'intervalle compris entre 0 et $n-1$, on le divise par n et on conserve le reste de cette division. Par exemple, dans l'ensemble des nombres modulo 12, $10 + 5 = 3$; $1 - 2 = 11$ (on utilise couramment ce calcul : 5 heures après 10 heures, il est 3 heures, et deux heures avant 1 heure, il est 11 heures). On multiplie de même : par exemple, $4 \times 5 = 8$.

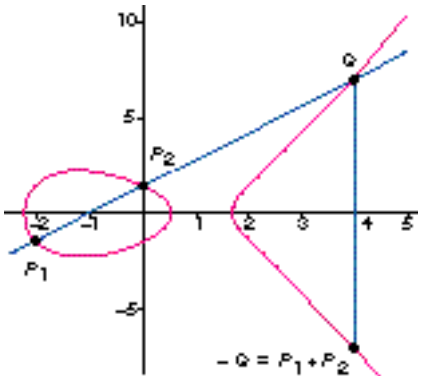
La division pose des problèmes particuliers. Une division est analogue à une multiplication par l'inverse, et l'inverse de x est l'élément y qui vérifie $xy = 1$. Par exemple, pour $n = 12$, l'inverse de 5 est 5, car $5 \times 5 = 25$ et $25 \equiv 1 \mod 12$. En revanche, 4 n'a pas d'inverse car $4y$ a plusieurs solutions, 3, 6 ou 9, modulo 12. On ne divise simplement que si n est un nombre premier. On calcule l'inverse grâce à la série d'opérations de l'algorithme classique de la division.

Avec cet ensemble de restes muni de ces opérations de bases, on définit également une courbe elliptique. Le cas le plus simple est celui où le module (le nombre par rapport auquel on prend le reste) est un nombre premier p. Les paramètres a et b de la courbe doivent être des nombres compris entre 0 et $p - 1$ tels que $4a^3 + 27b^2$ ne soit pas congru à 0 modulo p. La courbe est constituée du point O et des points associés aux couples (x, y) de nombres compris entre 0 et $p - 1$ qui vérifient la congruence $y^2 \equiv x^3 + ax + b \mod p$. Les formules pour l'addition restent inchangées, mais on remplace tous les nombres qui se présentent par le reste de leur division par p.

Par exemple, pour $p = 5$, $a = 1$ et $b = -1$ (cette écriture est une simplification de $p = 5$; $a \equiv 1 \mod 5$; $b \equiv 4 \mod 5$), les points P_1 et P_2 de coordonnées respectives $P_1 = (1, 1)$ et $P_2 = (2, 2)$ sont des points de la courbe elliptique. Pour

NOMBRE DE CHIFFRES	TEMPS DE CALCUL
6	6 secondes
9	20 secondes
12	2,5 minutes
15	16 minutes
18	95 minutes
21	7,2 heures
24	39,5 heures
27	140 heures
30	574 heures

5. TEMPS DE FACTORISATION, par la méthode des courbes elliptiques exécutée, sur un ordinateur puissant : à gauche, on lit le nombre de chiffres des nombres à factoriser et, à droite, le temps moyen nécessaire pour trouver un facteur ayant ce nombre de chiffres.



6. LA COURBE ELLIPTIQUE *(en rouge)* pour les paramètres $a = -4$ et $b = 2$. Les points P_1 et P2, de coordonnées respectives $(-2, -\sqrt{2})$ et $(0, \sqrt{2})$ sont sur la courbe elliptique, car ils vérifient son équation : $y^2 = x^3 + ax + b$.