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, $4 \times 5 = 8$.

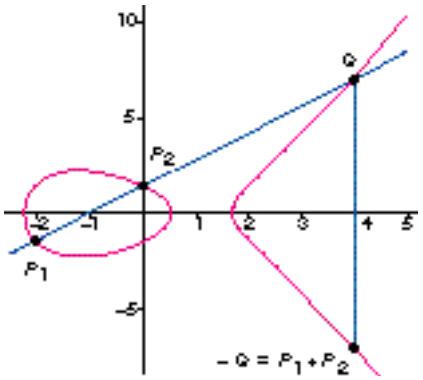
La division pose des problèmes particuliers. Une division est analogue à une multiplication par l'inverse, et l'inverse de x est l'élément y qui vérifie $xy = 1$. Par exemple, pour $n = 12$, l'inverse de 5 est 5, car $5 \times 5 = 25$ et $25 \equiv 1 \bmod 12$. En revanche, 4 n'a pas d'inverse car $4y$ 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 $y^2 \equiv x^3 + ax + b \bmod p$. 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 $p = 5$; $a \equiv 1 \bmod 5$; $b \equiv 4 \bmod 5$), 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 : $y^2 = x^3 + ax + b$.