

lorsque la courbe $E(p)$ varie (c'est-à-dire lorsqu'on essaie différentes valeurs de a et b), les éléments de $E(p)$ sont assez régulièrement répartis entre $p - 2\sqrt{p} + 1$ et $p + 2\sqrt{p} + 1$: on a donc de bonnes chances (sans en être complètement sûr) que k soit un multiple du cardinal de certaines de ces courbes, ce qui permettra de découvrir le facteur p .

Le temps de calcul de cette méthode dépend donc principalement de la taille du diviseur premier recherché, et à peine de celle du nombre à factoriser. Si un nombre de 1 000 chiffres a un diviseur de 20 chiffres, on trouve celui-ci assez facilement. En revanche, le temps de calcul croît très vite avec la taille du plus petit facteur. La méthode des courbes elliptiques convient bien pour la recherche de facteurs qui ont jusqu'à 30 chiffres. À ce jour, le plus grand facteur premier trouvé par cette méthode, à 47 chiffres, fut découvert par Peter Montgomery, au Centre de mathématiques et d'informatique d'Amsterdam.

Le crible quadratique

Pour la recherche de diviseurs encore plus grands d'un nombre n , on emploie une autre méthode : l'idée est de trouver des nombres entiers naturels X et Y tels que n soit un diviseur de $X^2 - Y^2$.

En effet, si n divise $X^2 - Y^2$, il divise aussi $(X - Y)(X + Y)$. Si n n'est pas un diviseur de $X - Y$ ou de $X + Y$, alors un diviseur propre de n doit diviser $X - Y$, et un autre diviseur propre de n doit diviser $X + Y$. Ainsi le plus grand diviseur commun de n et de $X - Y$, par exemple, est plus grand que 1, et donc est l'un des diviseurs recherchés. Choisissons par exemple $n = 7\,429$, $X = 227$ et $Y = 210$. Le nombre $7\,429$ est un diviseur de $X^2 - Y^2$, puisque $X^2 - Y^2 = 7\,429$, mais il n'est pas un diviseur de $X - Y = 17$ ni un diviseur de $X + Y = 437$. Le pgcd de 17 et de $7\,429$ est 17, et c'est un diviseur propre de $7\,429$.

Comment trouve-t-on X et Y ? On établit d'abord un système d'équations linéaires ; puis on détermine X et Y à partir des solutions de ce système. Le nombre d'équations dépend de la taille du nombre à factoriser ; pour un nombre de 120 chiffres il faut à peu près 245 000 équations pour autant d'inconnues (voir la figure 9). Contrairement à la méthode des courbes elliptiques, c'est la taille du nombre à factoriser, et non la taille du facteur cherché, qui détermine le temps de calcul.

NOMBRE DE CHIFFRES DE n	50	60	70	80	90	100	110	120
TAILLE DE LA BASE DES FACTEURS PREMIERS (EN MILLIERS)	3	4	7,4	15	30	51	120	245
TAILLE DE L'INTERVALLE DE CRIBLE (EN MILLIONS)	0,2	2	5	6	8	14	16	26

11. POUR UNE VERSION améliorée du crible quadratique, dont les détails ne peuvent pas être donnés ici, on a besoin, selon la taille du nombre n à factoriser, de différentes tailles pour l'intervalle de crible (l'intervalle où l'on cherche des carrés convenables) et pour la base de facteurs (l'ensemble des facteurs premiers par lesquels doivent être divisibles les carrés réduits).

En premier lieu, on se donne une suite de carrés ayant deux propriétés : ils sont proches de n et leur différence avec n est, au signe près, un produit de petits nombres premiers. Pour $n = 7\,429$, les carrés 83^2 , 87^2 et 88^2 conviennent, car les différences sont des produits des nombres premiers 2, 3, 5 et 7 :

$$83^2 - 7\,429 = -540 = (-1) \times 2^2 \times 3^3 \times 5$$

$$87^2 - 7\,429 = 140 = 2^2 \times 5 \times 7$$

$$88^2 - 7\,429 = 315 = 3^2 \times 5 \times 7.$$

Quand on multiplie certaines de ces lignes les unes par les autres, les exposants des décompositions s'additionnent. Si la somme des exposants est paire pour chaque facteur premier, alors le produit est un carré. Par exemple, $(87^2 - 7\,429) \times (88^2 - 7\,429) = 2^2 \times 3^2 \times 5^2 \times 7^2 = (2 \times 3 \times 5 \times 7)^2 = 210^2$.

Dès lors, pour trouver X et Y , on n'a plus qu'à appliquer une fois de plus les règles des calculs de congruences. On écrit : $(87 \times 88)^2 \equiv (87^2 - 7\,429) \times (88^2 - 7\,429) \pmod{7\,429}$. Donc $(87 \times 88)^2 \equiv 210^2 \pmod{7\,429}$. Dans cette équation, on peut encore remplacer 87×88 par son reste dans la division par $7\,429$, et on obtient $227^2 \equiv 210^2 \pmod{7\,429}$, ce qui signifie que $7\,429$ est un diviseur de $227^2 - 210^2$. On peut donc prendre $X = 227$ et $Y = 210$. Ces valeurs pour X et Y fournissent le diviseur 17 de $7\,429$, comme on l'a vu précédemment.

Parmi les relations dont on dispose (elles sont très nombreuses, en général), on doit extraire celles qui se combinent en un carré de la façon décrite. À cette fin, on construit un système d'équations linéaires : à chaque relation, on associe une inconnue, qui prend la valeur 1 si la relation est employée dans la construction du carré, et 0 dans le cas contraire. Dans notre exemple, le système a trois inconnues, λ_1 , λ_2 et λ_3 . Le produit de ces relations peut être écrit ainsi :

$$((-1) \times 2^2 \times 3^3 \times 5)^{\lambda_1} \times (2^2 \times 5 \times 7)^{\lambda_2} \times (3^2 \times 5 \times 7)^{\lambda_3},$$

ou bien, en utilisant les règles de calcul de puissances :

$$(-1)^{\lambda_1} \times 2^{2\lambda_1 + 2\lambda_2} \times 3^{3\lambda_1 + 2\lambda_3} \times 5^{\lambda_1 + \lambda_2 + \lambda_3} \times 7^{\lambda_2 + \lambda_3}.$$

Comme ce produit doit être un carré, tous les exposants doivent être pairs :

$$\lambda_1 \equiv 0 \pmod{2}$$

$$\lambda_1 + \lambda_2 + \lambda_3 \equiv 0 \pmod{2}$$

$$\lambda_2 + \lambda_3 \equiv 0 \pmod{2}.$$

La première équation concerne le facteur -1 , la deuxième 5 et la troisième 7. Les exposants des facteurs 2 et 3 étant pairs dans tous les cas, ils ne nécessitent pas d'équation. On peut résoudre le système d'équations par une méthode classique d'algèbre linéaire, en prenant garde de calculer modulo 2. On obtient $\lambda_1 = 0$, $\lambda_2 = \lambda_3 = 1$, et, à partir de là, on trouve X et Y comme on l'a déjà vu.

Enfin, comment trouve-t-on les relations elles-mêmes ? On utilise un procédé de crible, auquel l'algorithme du « crible quadratique » doit son nom : on cherche des carrés de nombres dont la différence avec n se décompose en petits facteurs premiers.

On fixe d'abord les nombres premiers qui peuvent intervenir dans les relations. Dans l'exemple considéré précédemment, on a pris 2, 3, 5 et 7. Pour traiter le signe, on ajoute le nombre -1 . L'ensemble de ces nombres premiers forme ce que l'on appelle la base des facteurs.

Ensuite on calcule des carrés de nombres qui sont proches de n . Pour cela, on prend le plus grand nombre entier m inférieur à $\sqrt{n}$. Dans l'exemple, il s'agit de $m = 86$. Les carrés de nombres au voisinage de n sont alors $(m-3)^2 = 83^2$, $(m-2)^2 = 84^2$, $(m-1)^2 = 85^2$, $m^2 = 86^2$, $(m+1)^2 = 87^2$, $(m+2)^2 = 88^2$, ..., et en général tous les $(m+u)^2$, où u est un nombre entier positif ou négatif petit par rapport à m .

Enfin on se fixe l'intervalle de crible, c'est-à-dire le domaine des nombres u avec lesquels on veut travailler. On