Dans l'exemple considéré, neuf fois n'importe quel élément de $E(5)$ est égal à O (on écrit comme d'habitude $2P$ pour $P + P$, $3P$ pour $P + P + P$, etc.).

Vérifions-le pour $P = (1, 1)$. On obtient successivement : $2P = (2, 2)$, $4P = 2 \times (2P) = (0, 2)$, $8P = 2 \times (4P) = (1, -1)$ et $9P = 8P + P = (1, -1) + (1, 1) = O$. Cet exemple montre qu'au lieu d'additionner neuf fois P, on peut employer la même astuce que pour l'exponentiation binaire : on calcule la suite $2P$, $4P$,..., 2^mP et, pour le résultat final, on additionne les puissances de deux dont on a besoin. Ainsi le temps de calcul reste raisonnable, même pour un très grand nombre à la place de 9.

Comment employer les courbes elliptiques pour trouver des diviseurs d'un nombre composé? Cherchons, par exemple, un diviseur de $n = 35$. On choisit une courbe elliptique modulo 35, c'est-à-dire deux nombres entiers a et b tels que $4a^3 + 27b^2$ ne soit pas divisible par 35 : retenons, par exemple, $a = 1$ et $b = -1$. On obtient bien une courbe elliptique, mais on ne peut pas toujours additionner ses points : dans les formules intervient un inverse modulo n, qui n'existe pas toujours, car 35 est composé. On essaie malgré tout : le calcul échoue, mais la manière dont il échoue donne l'information cherchée.

Plus précisément, on choisit un nombre entier naturel k (nous verrons comment par la suite) Pour notre exemple, prenons $k = 9$. On essaie d'additionner k fois le point $P = (2, 2)$ avec lui-même, par la méthode que nous avons considérée pour $E(5)$. On obtient $2P = (0, 22)$, $4P = (16, 19)$, $8P = (7, 13)$. Ensuite, quand on veut calculer $9P = 8P + P = (7, 13) + (2, 2)$, on doit tout d'abord évaluer λ et, pour cela, diviser par $7 - 2 = 5$ modulo 35. Cette division est impossible, car 5 n'a pas d'inverse modulo 35. On a donc finalement obtenu ce que l'on cherchait : 5 est un diviseur propre de 35! Notons que, dans le cas général, le nombre dont on ne trouve pas d'inverse n'est pas nécessairement un diviseur de n, c'est le pgcd de n et de ce nombre qui est un diviseur.

Les calculs échouent pour $k = 9$, parce que 5 est un diviseur de 35, et que 9 est le nombre d'éléments de $E(5)$. Les calculs auraient aussi échoué pour tout multiple de 9. Pour comprendre pourquoi, examinons la relation entre $E(35)$ et $E(5)$: comme on peut le vérifier sur les relations qui définissent ces courbes elliptiques, on peut «projeter» tout élément P_1 de $E(35)$ sur un élément P_2 de $E(5)$, en réduisant ses coordonnées modulo 5 ; l'élément associé à $9P_1$ est alors confondu avec $9P_2$. Faisons maintenant un raisonnement par l'absurde : si on pouvait calculer $9P_1$ dans $E(35)$, ce qui impliquerait de pouvoir calculer un λ fini, alors les coordonnées de $9P_1$ seraient finies ; en les réduisant modulo 5, on obtiendrait aussi des coordonnées finies pour $9P_2$: c'est impossible, puisque, d'après l'observation de Lagrange, $9P_2$ est l'élément neutre du groupe fini à 9 éléments $E(5)$, et que ses coordonnées sont infinies.

Comment choisir le nombre k? Si on cherche un facteur premier d'environ six chiffres, on choisit le nombre k de façon qu'il soit multiple du plus grand nombre possible de nombres de six chiffres qui n'ont pas de facteurs premiers trop gros. Alors, on a de bonnes chances pour que k soit un multiple du nombre d'éléments (nommé cardinal) de $E(p)$, que l'on ne connaît pas (p est le diviseur premier cherché). En effet, nous avons vu que le cardinal de $E(p)$ est compris entre $p - 2\sqrt{p} + 1$ et $p + 2\sqrt{p} + 1$: ce nombre est donc au plus du même ordre de grandeur que p. D'autre part, le plus souvent, il n'est pas lui-même un nombre premier, et est donc décomposable en facteurs premiers plus petits, qui, si on a de la chance, sont aussi des facteurs premiers de k. Lorsque l'on essaie de calculer k fois un élément de $E(n)$, on teste la divisibilité de n par tous ces nombres premiers d'un seul coup.

Pour trouver un nombre k approprié, on choisit un nombre B et on calcule k comme le produit de nombres premiers inférieurs à B. Par exemple, pour chercher des facteurs à au plus six chiffres, on choisit $B = 147$. On prend alors $k = 2^7 \times 3^4 \times 5^3 \times 7^2 \times 11^2 \times 13 \times 17 \times 19 \times ... \times 139$.

En général, la méthode des courbes elliptiques ne donne pas de résultat avec la première courbe elliptique choisie. On essaye plusieurs courbes, c'est-à-dire plusieurs paires de paramètres a et b. Plus B est grand, plus grand est le nombre de courbes que l'on doit essayer *(voir la figure 8)*. Ensuite, si la méthode n'a toujours pas trouvé de diviseur, on est à peu près sûr que le nombre n n'a pas de diviseur de l'ordre de grandeur que l'on s'est fixé. En effet,

NOMBRE DE CHIFFRES	6	9	12	15	18	21	24	27	30
B	147	682	2 462	8 318	28 462	62 502	162 730	395 806	945 922
NOMBRE DE COURBES	10	24	12	111	231	115	333	1 501	2 594

8. LA MÉTHODE DES COURBES ELLIPTIQUES trouve un diviseur d'un nombre n à peu près indépendamment de la taille de n. La longueur de la recherche croît avec l'ordre de grandeur du diviseur cherché. Ce tableau indique, dans la première ligne, cet ordre de grandeur en nombre de chiffres ; dans la deuxième ligne, on a indiqué le nombre B qui permet de déterminer le nombre k ; dans la troisième ligne apparaît le nombre de courbes elliptiques que l'on devra tester pour trouver un diviseur.

NOMBRE DE CHIFFRES DE n	50	60	70	80	90	100	110	120
NOMBRE D'ÉQUATIONS	3 000	4 000	7 400	15 000	30 000	51 000	120 000	245 000

9. POUR DÉTERMINER de très grands facteurs d'un nombre n, on emploie le crible quadratique. Lors de l'exécution de l'algorithme, on doit construire un système d'équations linéaires qui, selon la taille de n, peut contenir un nombre considérable d'équations.

u	−3	−2	−1	0	1	2	3
$(m+u)^2 - n$	−540	−373	−204	−33	140	315	492
CRIBLE PAR 2	−135		−51		35		123
CRIBLE PAR 3	−5		−17	−11		35	41
CRIBLE PAR 5	−1				7	7	
CRIBLE PAR 7					1	1	

10. LORS DU CRIBLE QUADRATIQUE, on choisit des nombres carrés $(m - u)^2$ proches du nombre n à décomposer (ici, $n = 7429$). Le nombre u (première ligne) numérote ces nombres carrés. On calcule la différence de chacun avec n (deuxième ligne ; $m = 86$) et on divise ces valeurs par le nombre qui constitue la base de chaque crible. Par exemple, pour $u = 1$, on divise $(m + u)^2 - n$, soit 140, par 2, puis encore par 2, puis encore par 2, pour obtenir 35 : le crible par 2 conduit à cette valeur.

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 cherchés. 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 $n = 7429$, 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 : $(87 \times 88)^2 \equiv (87^2 - 7\,429) \times (88^2 - 7\,429) \bmod 7\,429$. Donc $(87 \times 88)^2 \equiv 210^2 \bmod 7\,429$. Dans cette équation, on peut encore remplacer 87×88 par son reste dans la division par 7 429, et on obtient $227^2 \equiv 210^2 \bmod 7\,429$, 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 :

$$\lambda_1 \equiv 0 \bmod 2$$
$$\lambda_1 + \lambda_2 + \lambda_3 \equiv 0 \bmod 2$$
$$\lambda_2 + \lambda_3 \equiv 0 \bmod 2.$$

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