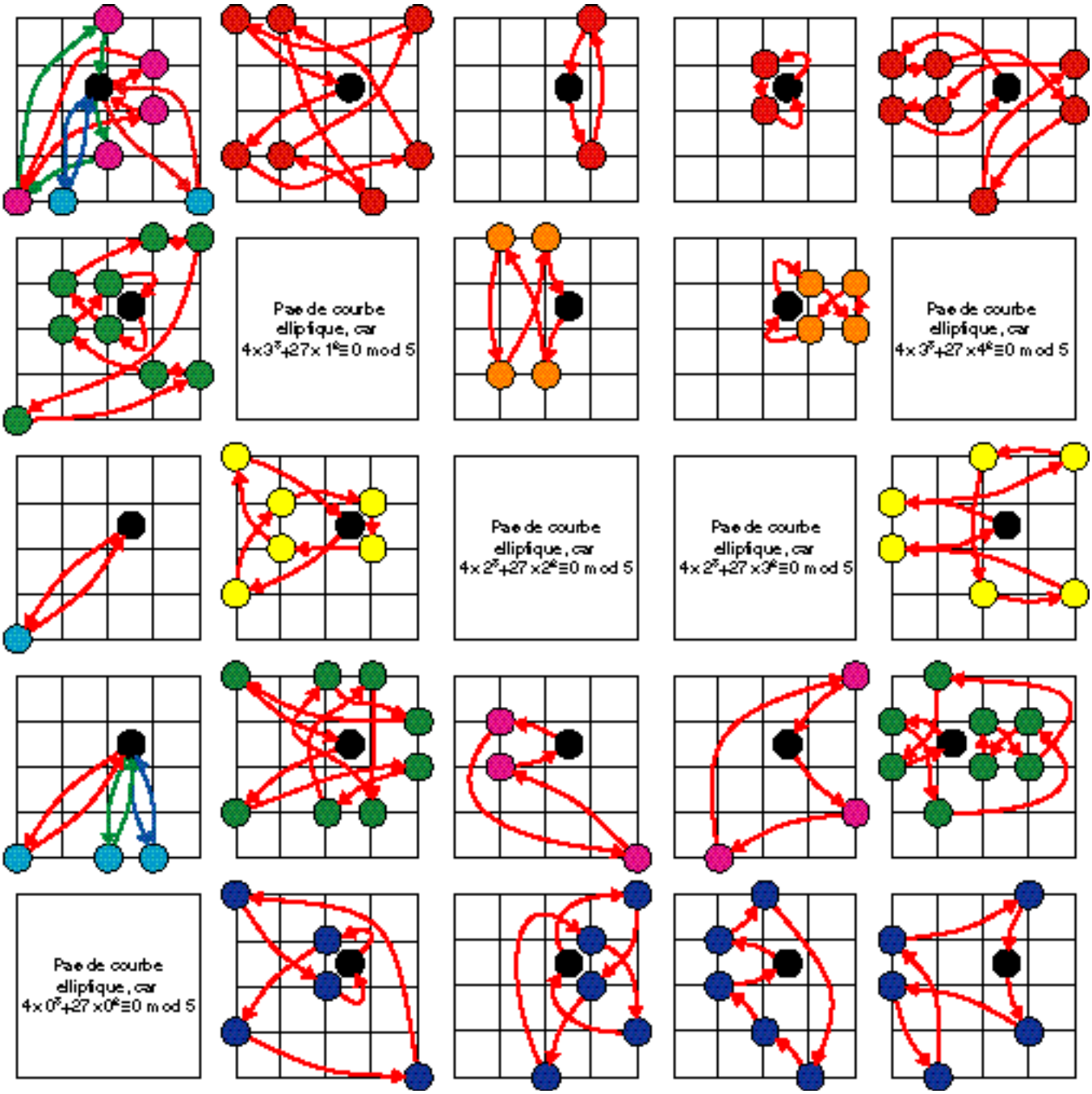
calculer les coordonnées (x_3, y_3) du point $P_3 = P_1 + P_2$, on applique les formules indiquées précédemment, mais avec les règles de la congruence, et l'on obtient $x_3 = 3$ et $y_3 = 2$. Effectivement, (3, 2) est un point de la courbe.

L'ensemble *E(p)* des points des courbe elliptique modulo *p* n'a qu'un nombre fini d'éléments, compris entre $p - 2\sqrt{p} + 1$ et $p + 2\sqrt{p} + 1$. En essayant tous les couples de nombres possibles, on trouve que la courbe elliptique *E*(5), pour $a = 1$ et $b = 4$, est constituée des neuf éléments (3,3), (3,2), (0,3), (0,2), (1,4), (1,1), (2,3), (2,2) et O *(voir la figure 7)*.

La méthode de factorisation par les courbes elliptiques repose sur une observation du mathématicien français Joseph Louis Lagrange (1736-1813) : quand on additionne un élément d'un groupe fini à lui-même autant de fois qu'il y a d'éléments dans le groupe, on obtient l'élément neutre.



7. LES COURBES ELLIPTIQUES *E(p)*, pour $p = 5$. Chaque case correspond à un couple de paramètres *(a,b)* ; la coordonnée *a* croît de bas en haut, et *b* de gauche à droite, chacune variant de 0 à 4. Dans chaque case, les coordonnées croissent également de 0 à 4 : chaque élément du groupe est représenté par un disque de couleur à la position correspondante. L'élément neutre O *(cercle noir)* est indiqué au milieu de la case, bien que ses coordonnées soient infinies. Par exemple, le groupe pour $a = 0$ et $b = 1$ est représenté par la deuxième case en partant de la gauche dans la ligne inférieure : il contient les éléments (0,1), (0,4), (2,2), (2,3), (4,0) et O. Dans chaque groupe, une flèche rouge relie O à un autre élément *x*. Les multiples de celui-ci (*x*, *x* + *x*, *x* + *x* + *x*, etc.) sont reliés par une chaîne de flèches rouges qui finit de nouveau sur O : c'est ce que l'on nomme un cycle. Certains groupes contiennent plus d'un cycle (marqués par des couleurs différentes). La couleur de chaque cercle désigne le nombre d'éléments du cycle auquel il appartient. Sur cet exemple très simple, on voit que, pour un couple *(a,b)* choisi au hasard, la probabilité qu'il soit inutilisable (parce qu'il n'y a pas de courbe elliptique) ou improductif (parce qu'un groupe présentant la même structure à déjà été trouvé) est faible.

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	118	21	24	27	30
B	147	682	2462	8 318	28 462	62 502	162 730	395 806	945 922
NOMBRE DE COURBES	10	24	12	111	231	445	883	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 $(m+u)^2 - n$	−3 −540	−2 −373	−1 −204	0 −33	1 140	2 315	3 492
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.