## ALGORITHMES REMARQUABLES EN THÉORIE DES NOMBRES

Henri Cohen

Le but de cet article est de donner un certain nombre d'exemples de problèmes et d'algorithmes remarquables en théorie des nombres. Ils auront tous un point commun : les solutions numériques les plus petites aux différents problèmes seront très grandes (des dizaines de chiffres), ce qui rend ces problèmes impossible à attaquer avec des méthodes naïves.

### 1. L'équation de Pell-Fermat

Le problème général que l'on se pose est la détermination des points à coordonnées entières sur une conique donnée par une équation à coefficients entiers. Ceci peut se résoudre complètement, mais nous considérerons un cas particulier fort important, la détermination des solutions entières de l'équation

$$x^2 - dy^2 = \pm 1 \ ,$$

où $d$ est un nombre entier non nul fixé. Si $d < 0$ ou si $d$ est un carré, c'est trivial. Nous supposerons donc $d > 0$ non carré.

Deux problèmes distincts peuvent alors se poser. Le premier est de trouver au moins *une* solution non triviale (i.e. avec $y \neq 0$). Le deuxième est de trouver *toutes* les solutions.

Une remarque intéressante peut être faite immédiatement : puisque

$$(x_1^2 - dy_1^2)(x_2^2 - dy_2^2) = (x_1x_2 + dy_1y_2)^2 - d(x_1y_2 + x_2y_1)^2$$

et

$$1/(x^2 - dy^2) = (x/(x^2 - dy^2))^2 - d(y/(x^2 - dy^2))^2$$

on voit que l'ensemble des solutions de notre équation est un *groupe* multiplicatif (abélien), d'élément neutre $(x, y) = (1, 0)$. Ceci permet une remarque, en apparence banale, mais très importante : il est très facile de construire de nouvelles solutions à partir d'anciennes, puisqu'il suffit de les multiplier entre elles. Un exemple éclairera cette situation. Pour $d = 6$, on constate aisément que $(x, y) = (5, 2)$ convient. Utilisant la loi de groupe ci-dessus, on calcule que $(5, 2)^2 = (49, 20)$, et donc $(x, y) = (49, 20)$ est une autre solution.

En fait, un résultat très ancien donne la structure du groupe des solutions :

**Théorème 1.** *Soit $d > 0$ un entier qui ne soit pas un carré. Le groupe des solutions de l'équation $x^2 - dy^2 = \pm 1$ est isomorphe à $\{\pm 1\} \times \mathbb{Z}$. En d'autres termes, si $(x, y)$ est la solution avec $x > 1$ le plus petit possible, toute autre solution est de la forme $\pm(x, y)^k$ pour $k \in \mathbb{Z}$.*

Cet important théorème ne donne malheureusement pas de manière de trouver la plus petite solution, ou même une solution.

Une première réponse satisfaisante à ce problème a été trouvée depuis également fort longtemps : l'utilisation du développement en fraction continue de $\sqrt{d}$. Il n'est pas difficile de montrer que cette fraction continue conduit à une solution de notre équation, et un peu plus difficile de montrer que c'est effectivement la plus petite solution non triviale.

Pour donner un exemple frappant, prenons $d = 13729$, ce qui n'est quand même pas très grand. On montre que la plus petite solution est

$$\begin{aligned}(x,y) = (&20672986986986229787814140876637786370240523605690342866645\backslash\\ &80146794867093429578407635274318407005554978 0,\\ &17643460875888327508840064590736480225145559266591277 1\backslash\\ &0310338859327880097286527931924281496170920222937)\end{aligned}$$

donc $x$ et $y$ sont des nombres de plus de 100 chiffres. Il est bien évident qu'il est absolument hors de question d'avoir trouvé cette solution (et encore moins d'autres qui sont bien plus grandes) sans une méthode particulièrement efficace. Incidemment, le temps pris pour trouver ce résultat sur un ordinateur moderne est inférieur à 20 millisecondes.

Pour satisfaisante qu'elle soit, cette méthode n'est pas suffisante pour des exemples plus grands. En effet, le temps d'exécution de l'algorithme utilisant les fractions continues est de l'ordre de $\sqrt{d}$, ce qui est négligeable quand $d$ est aussi petit que ci-dessus, mais devient prohibitif dès que $d$ a quelques dizaines de chiffres. Dans ce cas d'ailleurs, les solutions de notre équation ne peuvent pas être écrites directement (le nombre de chiffre dépasse rapidement le nombre de particules dans l'univers), et on doit donc, soit les représenter grâce à un codage astucieux (ce qui est possible), soit par leur logarithme.

Il a fallu attendre l'époque moderne pour que de véritables progrès soient faits sur le sujet. Tout d'abord, vers 1970, D. Shanks découvre que l'on peut circuler sur le développement en fraction continue de $\sqrt{d}$ (qui est périodique) en faisant des "grands sauts", et pas seulement pas à pas. Cette technique, qui a depuis été employée dans bien d'autres domaines (méthode des pas de bébé-pas de géant) permet de réduire le temps d'exécution à $O(d^{1/4})$ environ, ce qui est un progrès remarquable. Enfin, en 1989 J. Buchmann a l'idée d'utiliser des "bases de facteurs" dans ce domaine, idée déja utilisée dans bien d'autres contextes tels que la factorisation des nombres entiers. La première implantation machine de cette idée a été réalisée par F. Diaz y Diaz, M. Olivier et moi-même en 1990 et est disponible dans le logiciel Pari. C'est ainsi que par exemple pour $d = (10^{31} - 4)/4$, on trouve en quelques dizaines de minutes que si $(x, y)$ est la plus petite solution,

$$\ln x = 266159847242543.5473497806775605521...$$

(en fait à plusieurs centaines de décimales si on le désire). Ceci montre que $x$ a plus de $10^{14}$ chiffres décimaux.

Comme dernier exemple de ce type de problème, mentionnons le problème des troupeaux du soleil d'Archimdède.

Ce célèbre problème, énoncé par archimède sous forme d'un épigramme, s'écrit mathématiquement comme suit. Trouver des entiers positifs $A$, $B$, $C$, $D$, $a$, $b$, $c$, $d$, $m$, $n$ tels que

$$\begin{cases} A & = (1/2 + 1/3)B + D \\ B & = (1/4 + 1/5)C + D \\ C & = (1/6 + 1/7)A + D \\ a & = (1/3 + 1/4)(B + b) \\ b & = (1/4 + 1/5)(C + c) \\ c & = (1/5 + 1/6)(D + d) \\ d & = (1/6 + 1/7)(A + a) \\ A + B & = m^2 \\ C + D & = n(n + 1)/2 \end{cases} .$$

La solution des 7 premières équations est immédiate, et il est remarquable que la solution (unique a multiple entier près) a bien tous ses coefficients positifs. Il reste ensuite à satisfaire aux deux dernières conditions. Il n'est pas difficile de voir que l'on se ramène à l'équation

$$x^2 - 410286423278424y^2 = \pm 1 \ .$$

L'algorithme des fractions continues (modifié ici pour tenir compte du fait que le nombre 410286423278424 est divisible par $4657^2$), montre que la plus petite solution a 206554 chiffres décimaux. Comme ceci doit être la taille d'un troupeau, il semble qu'Archimède se soit moqué de la tête de ses contemporains.

## 2. L'équation $x^3 + y^3 = d$

J'ai déja dit que la recherche des solutions entières d'équations du second degré est essentiellement résolue, aussi bien en théorie qu'en pratique. Passons maintenant au degré 3. Ici la théorie aussi bien que la pratique sont beaucoup moins complètes, mais beaucoup plus passionnantes, et abondent en résultats et en conjectures : c'est la théorie des courbes elliptiques. Vous savez certainement que le dernier théorème de Fermat (qui n'est *pas* une équation de degré 3) a été résolu par Wiles en utilisant de manière fondamentale la théorie des courbes elliptiques.

Il est hors de question pour moi d'aborder cette théorie, mais je conseille vivement aux auditeurs interessés de consulter les livres qui abondent sur le sujet (voir par exemple [Sil1], [Sil2], [Sil-Tat], [Coh]). Je vais toutefois traiter deux exemples très différents.

Le premier exemple, dû à Fermat est le suivant : trouver *une* solution entière $(x, y, z)$ à l'équation $x^3 + y^3 = 9z^3$ avec $x$, $y$ et $z$ strictement positifs, autre que la solution banale (mais pas si triviale que ça) $(x, y) = (2, 1, 1)$ (et bien entendu sa symétrique $(1, 2, 1)$). En autorisant des signes quelconques à $x$, $y$ et $z$, ce que nous ferons pour notre étude, les solutions vraiment triviales sont $(1, -1, 0)$ et $(-1, 1, 0)$. Noter que, si l'on écarte les solutions triviales, il revient au même de chercher les solutions (positives ou non) à notre équation ou bien les solutions en nombres *rationnels* de l'équation $x^3 + y^3 = 9$.

La solution, tout à fait inattendue si l'on n'a jamais vu ce problème, est que la technique employée dans le cas de l'équation de Pell-Fermat marche aussi ici : il existe encore une fois une loi de groupe sur l'ensemble des solutions. Pour voir celà (et trouver explicitement la loi), considérons la courbe projective $X^3 + Y^3 = 9Z^3$, et deux points $(x_1, y_1, z_1)$ et $(x_2, y_2, z_2)$ à coordonnées rationnelles, non nécessairement distincts (rappelons qu'en coordonnées projectives, on identifie $(x, y, z)$ avec $(ax, ay, az)$ pour tout $a$ non nul).

La droite passant par ces deux points (la tangente à la courbe s'ils sont confondus) recoupe la courbe en un troisième point puisqu'on a affaire à une équation aux abcisses du troisième degré. De plus, cette équation sera à coefficients rationnels, d'où on déduit aisément que les coordonnées du troisième point d'intersection seront rationnelles, et donneront donc une nouvelle solution à notre équation. En fait, ce n'est pas tout à fait ce troisième point que l'on prend pour définir la loi de groupe, mais son symétrique par rapport à l'axe de symétrie $X = Y$ de la courbe.

Tous calculs faits, la loi de groupe s'exprime de la manière suivante :

$$(x_1, y_1, z_1)(x_2, y_2, z_2) = (x_3, y_3, z_3)$$

où

$$\left\{\begin{array}{lcl} x_3 & = & dz_1z_2(y_1z_2 - y_2z_1) + x_1x_2(x_1y_2 - x_2y_1) \\ y_3 & = & dz_1z_2(x_1z_2 - x_2z_1) + y_1y_2(x_2y_1 - x_1y_2) \\ z_3 & = & y_1y_2(y_1z_2 - y_2z_1) + x_1x_2(x_1z_2 - x_2z_1) \end{array}\right.$$

si les points sont distincts, et

$$\left\{\begin{array}{lcl} x_3 & = & y_1(dz_1^3 + x_1^3) \\ y_3 & = & x_1(x_1^3 - 2dz_1^3) \\ z_3 & = & z_1(dz_1^3 - 2x_1^3) \end{array}\right.$$

si les points sont confondus.

Il n'est *pas du tout* évident est que ceci définisse une loi de groupe (abélien). La commutativité est évidente, le point à l'infini (correspondant aux solutions triviales $\pm(1, -1, 0)$ ci-dessus, c'est à dire au point projectif $(1, -1, 0)$) est l'élément neutre, et l'opposé de $(x, y, z)$ est $(y, x, z)$. Par contre l'associativité est un peu embêtante à démontrer. En fait, on le montre élégamment dans le contexte tout à fait général des courbes elliptiques en utilisant la théorie des diviseurs.

En utilisant cette loi, il est maintenant aisé, comme dans le cas de l'équation de Pell-Fermat, de contruire de nouvelles solutions à notre équation, en calculant les puissances successives du point non trivial $(x, y, z) = (1, 2, 1)$. On obtient :

$$\left\{\begin{array}{ll} (1,2,1)^2 & = (20, -17, 7) \\ (1,2,1)^3 & = (-271, 919, 438) \\ (1,2,1)^4 & = (188479, -36520, 90391) \\ (1,2,1)^5 & = (-152542262, 169748279, 53023559) \\ (1,2,1)^6 & = (676702467503, 415280564497, 348671682660) \end{array}\right. .$$

(Noter que l'on a normalisé les coordonnées projectives $(x, y, z)$ pour avoir $(x, y, z) = 1$ et $z \geq 0$.)

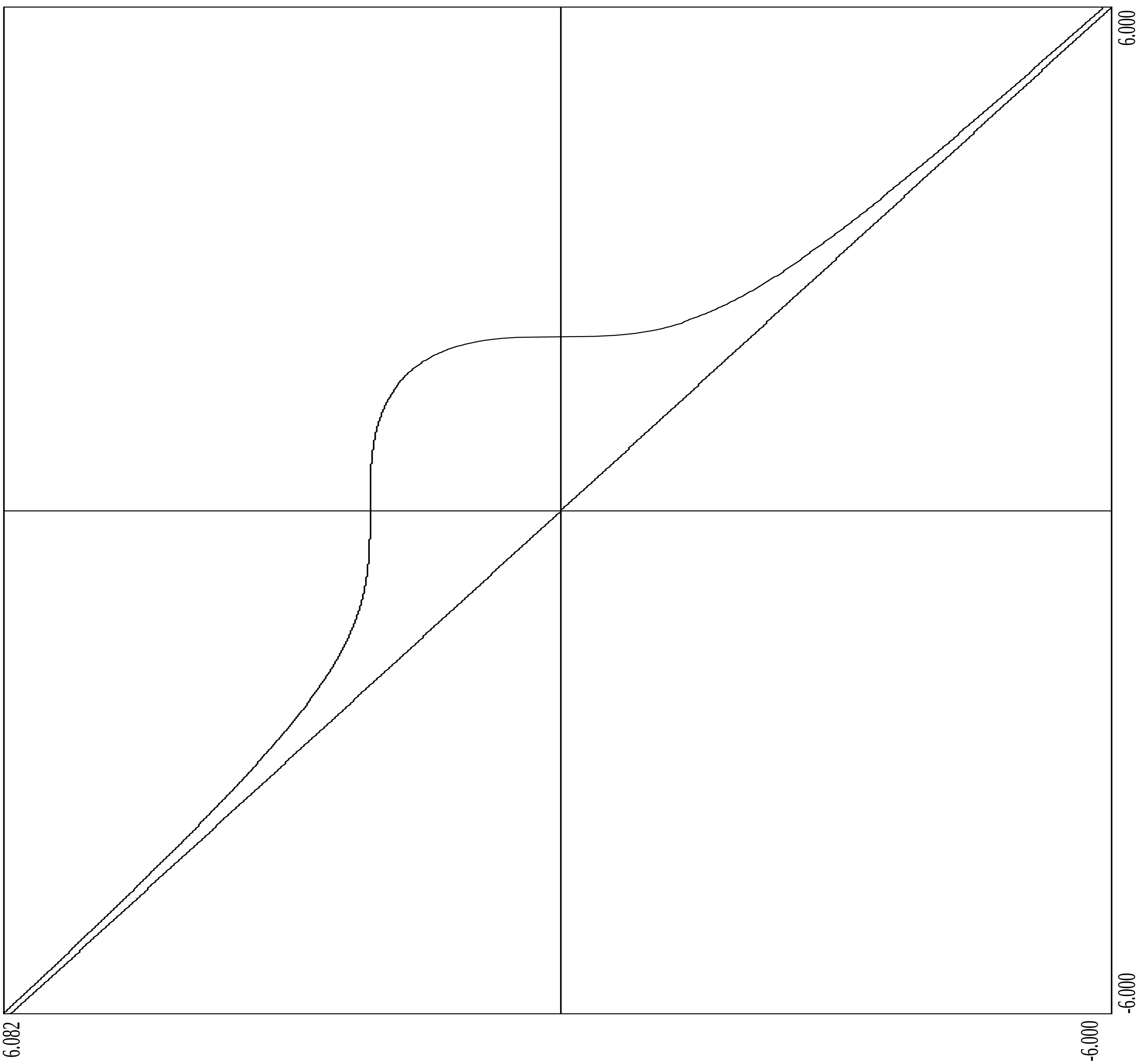
Puisque nous devons avoir des coordonnées positives, on voit que la plus petite solution qui convient est la puissance sixième, et donc

$$\left\{\begin{array}{lcl} x & = & 676702467503 \\ y & = & 415280564497 \\ z & = & 348671682660 \end{array}\right. .$$

Le lecteur vérifiera qu'on a bien $x^3 + y^3 = 9z^3$, ce qui donne donc bien une solution à notre problème. Noter que la solution a 12 chiffres, et donc il y aurait eu de l'ordre de $10^{24}$ essais à faire pour trouver la solution par une recherche bête, ce qui est évidemment impossible.

Nous n'avons bien entendu pas prouvé qu'il n'y a pas de plus petite solution. En fait, dans ce cas il n'est pas trop difficile de montrer que le groupe des points projectifs à coefficients rationnels sur notre courbe est isomorphe à $\mathbb{Z}$, et qu'un générateur est justement le point $(1, 2, 1)$. Donc nous avons (à échange près de $x$ et $y$) trouvé la solution à notre problème. D'une manière générale, un très important théorème de Mordell affirme que le groupe des points rationnels sur une courbe elliptique est un groupe abélien de type fini, c'est à dire qu'il possède une partie de torsion finie (ici elle est triviale) et que le reste est un groupe abélien libre ayant un nombre fini de générateurs $r$, appelé le *rang* de la courbe. Ici, le rang est égal à 1. Le calcul du rang est très difficile en général, et à l'heure actuelle quasiment impossible sauf dans les petits cas, si l'on ne suppose pas un certain nombre de conjectures sur les courbes elliptiques. Le programme le plus performant effectuant le calcul du rang est dû à J. Cremona et s'appelle mwrank (MW=Mordell-Weil), et disponible sur tout bon serveur.

La courbe $x^3 + y^3 = 9$ avec son asymptote



## 3. Le problème des nombres congruents

Pour ce paragraphe, je réfère à l'excellent livre de Koblitz [Kob] qui est consacré pratiquement exclusivement à ce sujet.

Dans le premier exemple ci-dessus, nous avons été énormément aidés par le fait que nous connaissions déja une solution non-triviale de notre équation, à savoir $(1, 2, 1)$. Mais que se passe-t-il si l'on n'en connait pas ? C'est analogue à l'équation de Pell-Fermat (et tout autre problème où on a un groupe) : si l'on connait une solution, on peut toujours l'élever à une puissance et obtenir d'autres solutions. Par contre, si l'on ne connait pas à l'avance de solutions, il faut employer des techniques plus savantes, telles que les fractions continues, les pas de géants de Shanks ou les bases de facteurs utilisées par Buchmann.

Comme illustration frappante de ces considérations, nous allons examiner un deuxième problème où interviennent des équations cubiques, i.e. des courbes elliptiques. Il s'agit d'un très vieux problème, dû aux anciens grecs, appelé problème des nombres congruents. Le problème est le suivant : étant donné un entier positif $n$, déterminer si $n$ est l'aire d'un triangle rectangle à cotés rationnels, et si oui, trouver un tel triangle. Si $n$ est l'aire d'un tel triangle, on dira que $n$ est *congruent*, et *non congruent* dans le cas contraire.

Par exemple, puisque $3^2 + 4^2 = 5^2$, le triangle de cotés $(3, 4, 5)$ est rectangle et son aire est $3 \cdot 4/2 = 6$, donc 6 est un nombre congruent. Un peu moins évident est le fait que le nombre 5 est congruent, car c'est l'aire du triangle rectangle de cotés $(3/2, 20/3, 41/6)$. Par contre, on peut montrer (c'est nettement moins facile) que les nombres 1, 2 et 3 sont non congruents. Noter qu'il est inutile de considérer le nombre 4, et plus généralement les entiers divisibles par un carré supérieur à 1, puisque si $n$ est congruent, $nk^2$ est trivialement congruent (faire une homothétie de rapport $k$ sur le triangle) et réciproquement.

Le rapport avec les équations cubiques est le suivant. Soit $(a, b, c)$ un triangle rectangle d'aire $n$ (où $c$ est l'hypothénuse), et posons

$$x = a(c + a)/2, \quad y = a^2(c + a)/2 \ .$$

On vérifie aisément que

$$y^2 = x^3 - n^2x \ .$$

Réciproquement, il n'est pas difficile de montrer que si $(x, y)$ est un point à coordonnées rationnelles sur cette courbe avec $y \neq 0$, alors, quite à multiplier (pour la loi de groupe sur la courbe) le point $(x, y)$ par l'un des trois points triviaux $(u, 0)$ pour $u = 0$ ou $u = \pm n$, et éventuellement de changer $y$ en $-y$ (ce qui signifie ici inverser pour la loi de groupe), il existe un triangle rectangle $(a, b, c)$ d'aire $n$ tel que $x' = a(a + c)/2$, $y' = a^2(c + a)/2$. Nous sommes donc ramenés à la détermination des points à coordonnées rationnelles sur la courbe ci-dessus.

La raison pour laquelle nous sommes obligés de faire toutes ces contorsions est que $a$ et $b$ jouent des roles symétriques, et la seule relation importante étant $a^2 + b^2 = c^2$, $a$, $b$ et $c$ n'ont un sens qu'au signe près (le fait qu'ils soient positifs est de nature géométrique), donc en fait la donnée du triangle $(a, b, c)$ fournit en fait huit points sur la courbe, à savoir les points quatre points

$$(\varepsilon_1 a(c + \varepsilon_1 a)/2, \varepsilon_2 a^2(x + \varepsilon_1 a)) \quad (\text{où } \varepsilon_1 = \pm 1 \text{ et } \varepsilon_2 = \pm 1)$$

et les quatre points analogues obtenus en remplaçant $a$ par $b$, Comme dans le cas de l'équation $x^3 + y^3 = 9$, la courbe $y^2 = x^3 - n^2 x$ est une courbe elliptique, en d'autres termes il existe une loi de groupe tout à fait explicite sur cette courbe (considérée comme d'habitude comme courbe projective, c'est à dire avec en plus le point à l'infini $(x, y, z) = (0, 1, 0)$). Je laisse au lecteur le soin d'écrire la loi d'addition (en coordonnées projectives) explicitement comme nous l'avons fait ci-dessus.

Le problème est que nous n'avons maintenant plus de point avec lequel démarrer. Plus exactement si, on a bien les points $(x, y) = (0, 0)$, $(n, 0)$, $(-n, 0)$ ainsi que le point à l'infini, mais on vérifie immédiatement que ces quatre points forment un groupe isomorphe à $(\mathbb{Z}/2\mathbb{Z})^2$, et donc qu'on ne peut pas construire d'autres points à partir d'eux. Il n'est d'ailleurs pas trop difficile de montrer que ces points sont exactement l'ensemble des points d'ordre fini à coordonnées rationnelles sur la courbe.

Que faire alors ? Rappelons de plus que nous avons deux problèmes distincts à résoudre : savoir s'il y a des points (autres que les 4 points triviaux), et les trouver. Pour résoudre ces problèmes, on peut essayer de s'inspirer de l'équation de Pell-Fermat.

Tou d'abord, comment savait-on à l'avance que l'équation de Pell-Fermat avait effectivement une solution ? Cela provient de la considération des *corps quadratiques* $\mathbb{Q}(\sqrt{d})$ dont on peut montrer que pour $d > 0$ non carré, le groupe des *unités* (c'est à dire les solutions de notre équation de Pell-Fermat) est un groupe abélien de rang égal à 1 (c'est le Théorème 1). Il est à noter que pour les corps quadratiques ce résultat est facile, mais que pour les corps de nombres (corps obtenus en adjoignant à $\mathbb{Q}$ un nombre fini de racines de polynômes à coefficients rationnels) plus généraux, on a une formule donnant ce rang $r$, mais que ce résultat, dû à Dirichlet, est difficile.

L'analogue pour les courbes elliptiques est le suivant. Le groupe des unités est remplacé par le groupe des points rationnels, et le rang du groupe des unités par le rang de la courbe. Malheureusement, dans le cas des courbes elliptiques, on n'a pas de théorème analogue au théorème de Dirichlet donnant une formule pour $r$. Toutefois, on a une très importante *conjecture* donnant ce rang, appelée conjecture de Birch et Swinnerton-Dyer. C'est probablement l'une des conjectures les plus importantes de toute la théorie des nombres, et à mon avis la plus élégante. Cette conjecture affirme (en gros) que $r$ n'est rien d'autre que l'ordre du zéro en $s = 1$ d'une certaine fonction analytique que l'on peut construire à partir de notre courbe elliptique.

Malgré les nombreux efforts de célèbres mathématiciens (dont Wiles par exemple), cette conjecture n'a pu être démontrée que dans des cas très particuliers.

En tous cas, pour un $n$ fixé pas trop grand, on peut maintenant répondre à la question de savoir si $n$ est congruent ou non. C'est ainsi que vers les années 1980 on a construit des tables de nombres congruents jusqu'à 1000 ou 2000.

Se pose alors la question suivante : en admettant la conjecture ci-dessus (d'ailleurs une forme très faible suffit), peut-on trouver un critère simple pour déterminer si $n$ est congruent ou non ? La réponse a été donnée en 1981 par Tunnell, grâce à l'utilisation de ce qu'on appelle les formes modulaires de poids demi-entier (spécifiquement de poids $3/2$). Le nombre $n$ impair (respectivement pair), supposé sans facteur carré plus grand que 1, est congruent si et seulement s'il y autant de solutions *entières* (c'est à dire dans $\mathbb{Z}$) de l'équation $x^2 + 2y^2 + 8z^2 = n$ (respectivement $x^2 + 4y^2 + 8z^2 = n/2$) avec $z$ impair que de solutions avec $z$ pair.

Noter qu'il est extrêmement facile pour un $n$ donné de compter ce nombre de solutions, et nous avons donc répondu au premier problème de manière tout à fait satisfaisante, du moins en supposant une forme faible de la conjecture de Birch et Swinnerton-Dyer.

(Sans cette conjecture, l'implication $n$ congruent entraine qu'il y a autant de solutions est toujours vraie.) Par exemple pour $n = 1$, il n'y a que $(x, y, z) = (\pm 1, 0, 0)$ donc 2 solutions avec $z$ pair et 0 avec $z$ impair, donc 1 est non congruent. Par contre, pour $n = 5$, il n'y a pas du tout de solution, donc 5 est congruent.

Un examen des tables montre immédiatement que tout nombre sans facteur carré congru à 5, 6 ou 7 modulo 8 est congruent, ce qui résulte effectivement trivialement du critère de Tunnell, car, comme dans le cas de $n = 5$, la considération du critère modulo 8 montre qu'il n'y a pas du tout de solutions. Ceci peut se démontrer sans la conjecture de Birch et Swinnerton-Dyer. Dans les autres classes de congruence (c'est à dire les nombres congrus à 1, 2 ou 3 modulo 8), les nombres congruents sont beaucoup plus rares. Par exemple, en utilisant le critère de Tunnell, on montre aisément que les seuls nombres congruents (sans facteurs carrés) congrus à 1, 2 ou 3 modulo 8 et inférieurs à 5000 sont 65, 138, 330, 602, 1178, 3122, 3882.

Le deuxième problème, à savoir de trouver explicitement un triangle rectangle d'aire $n$, ou de manière équivalente un point à coordonnées rationnelles sur notre courbe $y^2 = x^3 - n^2 x$ est beaucoup plus difficile. Reprenons à nouveau notre analogie avec l'équation de Pell-Fermat. Dans ce cas, l'algorithme fondamental que nous avons introduit est celui des fractions continues (les algorithmes de Shanks et de Buchmann n'en sont en fait que des améliorations). Y a-t-il quelque chose d'analogue ici ? Tout d'abord, même dans le cas des corps de nombres, l'algorithme des fractions continues et ses généralisations ne fonctionne que quand le rang du groupe des unités est égal à 1. C'est le cas justement des corps $\mathbb{Q}(\sqrt{d})$ avec $d > 0$ non carré. Il faut penser à cela en termes géométriques : si le rang est $r$, on doit explorer un tore de dimension $r$. Quand $r = 1$, c'est simplement un cercle, et il suffit donc de tourner en rond (une fois) pour résoudre le problème, alors que pour $r \geq 2$ ce qu'il faut faire n'est pas du tout évident.

Et effectivement, je le dis dès à présent, quand le rang de notre courbe elliptique est strictement supérieur à 1, on ne sait essentiellement rien faire à part une recherche systématique plus ou moins guidée (je ne peux évidemment pas donner de détails, mais c'est l'objet de recherches très actives, par exemple de J. Silverman et J. Cremona).

Par contre quand le rang est 1, on peut espérer trouver quelque chose. On peut se raccrocher à une analogie supplémentaire dont je n'ai pas encore parlé. Dans le cas de l'équation de Pell-Fermat (i.e. des unités du corps quadratique $\mathbb{Q}(\sqrt{d})$), si $(x, y)$ est la plus petite solution non triviale avec $x$ et $y$ positifs, on appelle *régulateur* du corps la quantité $\ln(x + y\sqrt{d})$. Ce régulateur a un analogue impeccable sur les courbes elliptiques (qu'on appelle d'ailleurs également le régulateur), et qui, pour une courbe de rang 1, est ce qu'on appelle la *hauteur canonique* du générateur de la partie sans torsion du groupe des points rationnels de notre courbe. Cette hauteur peut etre calculée par des moyens tout à faits algorithmiques, mais il suffit de dire que si $(x, y, z)$ est un point projectif sur notre courbe, normalisé de telle manière que $x$, $y$ et $z$ soient des entiers premiers entre eux dans leur ensemble, alors la hauteur de $(x, y, z)$ est voisine de $\ln(\max(|x|, |y|, |z|))$.

De manière analogue à la formule

$$\ln((x + y\sqrt{d})^n) = n \ln(x + y\sqrt{d})$$

qui suggère que le régulateur dans $\mathbb{Q}(\sqrt{d})$ est en fait une forme linéaire, on peut montrer que, si $h$ désigne la hauteur sur une courbe elliptique on a

$$h((x, y, z)^n) = n^2 h(x, y, z) \quad ,$$

où bien entendu $(x,y,z)^n$ désigne la puissance $n$-ième du point $(x,y,z)$ sur la courbe elliptique, et ce qui suggère que $h$ est une forme quadratique, ce qui est le cas.

Raisonnant à nouveau par analogie, supposons que l'on sache par une certaine méthode calculer le régulateur $R$ de $\mathbb{Q}(\sqrt{d})$. Il est facile de voir que l'on peut en déduire la solution de notre équation de Pell-Fermat (du moins si celle-ci n'est pas trop grande). En effet, on aura $x+y\sqrt{d}=e^R$, et puisque $x^2-dy^2=\pm 1$, on aura aussi $x-y\sqrt{d}=\pm e^{-R}$, d'où on en déduit $x$ et $y$ par élimination (un seul des deux signes donnera $x$ et $y$ proche d'entiers). Maintenant, comment peut-on calculer $R$ (sans utiliser de fractions continues) ? Dans le cas des corps de nombres, on peut aussi définir une fonction analytique dont l'ordre du zéro (cette fois-ci en $s=0$) est égal au rang $r$, mais ceci n'est pas conjectural mais un théorème dû à Dedekind. Le coefficient de $s^r$ est proportionnel (à un facteur rationnel que je ne veux pas préciser) à notre régulateur $R$, et ceci donne donc un moyen *analytique* de calculer $R$, bien entendu assez peu efficace.

On peut espérer qu'une méthode analogue pourrait marcher pour les courbes elliptiques de rang exactement égal à 1 (et satisfaisant une propriété technique supplémentaire, conjecturalement toujours vraie, et en tous cas vraie pour nos courbes $y^2=x^3-n^2x$). C'est effectivement le cas, mais avec d'assez grosses modifications. C'est ce qu'on appelle la méthode des points de Heegner. Avec un langage informatique suffisamment puissant tel que GP ce n'est pas difficile à mettre en œuvre, et un programme de quelques lignes suffit.

Dans le cas de l'équation de Pell, nous avons donné un exemple ($d=13729$) ou la plus petite solution était très grande. Il en va bien entendu de même ici. Pour donner un exemple célèbre, calculé pour la première fois par D. Zagier, grâce au critère de Tunnell on montre que $n=157$ est un nombre congruent (il n'y a pas de solutions à $x^2+2y^2+8z^2=157$), et un triangle rectangle ayant comme aire 157 est de côtés $(p/q,q/r,s/t)$ où

$$\begin{cases} p &= 314r = 6803298487826435051217540 \\ q &= 411340519227716149383203 \\ r &= 21666555693714761309610 \\ s &= 224403517704336969924557513090674863160948472041 \\ t &= 8912332268928859588025535178967163570016480830\ , \end{cases}$$

et ceci sont les plus petites valeurs possibles.

## 4. L'algorithme LLL

L'un des algorithmes les plus remarquables découvert ces vingt dernières années est l'algorithme LLL, du nom de ses inventeurs, H. Lenstra, A. Lenstra et L. Lovász. Cet algorithme a de nombreuses applications dans des domaines fort éloignés de la théorie des nombres, tels que la programmation linéaire, et il a même des applications en physique.

Nous allons examiner l'une de ses applications en théorie des nombres. Le problème que l'on cherche à résoudre est le suivant. Soient $\alpha_1,\ldots,\alpha_n$ un ensemble de $n$ nombres complexes. Ces nombres sont-ils linéairement dépendants sur $\mathbb{Z}$, c'est à dire existe-t-il des entiers $x_1,\ldots,x_n$ tels que $\sum_{1\le i\le n} x_i\alpha_i=0$, et si oui, les calculer. Le cas particulier $\alpha_i=\theta^{i-1}$ de ce problème est important, puisqu'il consiste à demander si $\theta$ est un nombre algébrique de degré inférieur ou égal à $n-1$.

Posé de cette manière, le problème n'a pas beaucoup de sens. En effet, un nombre complexe n'est donné en général que par une approximation rationelle, et donc tout ensemble de nombres complexes est linéairement dépendant sur $\mathbb{Z}$, et même de dimension 1.

Par contre, si l'on exige que les coefficients $x_i$ soit relativement petits par rapport à la précision des $\alpha_i$, on peut donner un sens précis au problème, bien que ce soit délicat.

Le cas particulier $n = 2$ est connu depuis plusieurs siècles. Pour voir si $\alpha$ et $\beta$ sont linéairement dépendants sur $\mathbb{Z}$, on calcule le développement en fraction continue de $\alpha/\beta$. Si l'un des quotients partiels obtenu est très grand, le nombre rationnel obtenu en arrêtant la fraction continue juste avant ce grand quotient partiel est une excellente approximation de $\alpha/\beta$, et on peut alors regarder s'il convient par rapport à la précision souhaitée.

Pour $n \geq 3$ le problème est beaucoup plus difficile, et l'algorithme LLL a fourni une réponse très satisfaisante vers 1980. Cet algorithme possède les propriété suivantes : il peut trouver un vecteur relativement petit dans un réseau, et ceci en temps polynomial (donc assez rapidement). On construit alors un réseau lié à nos nombres $\alpha_i$, et on applique LLL pour trouver les $x_i$.

Donnons trois exemples d'application. Dans un premier exemple, considérons un nombre dont on sait à l'avance qu'il est algébrique car il est somme ou produit de nombres algébriques, mais dont on ne connait pas le polynôme minimal. L'algorithme LLL va essayer de trouver un tel polynôme.

Choisissons tout d'abord $x = \sqrt{2} + \sqrt{3} + \sqrt[3]{3}$, qui est clairement un nombre algébrique de degré $2 \cdot 2 \cdot 3 = 12$. Appliquant LLL, on trouve en 1 seconde que $x$ est racine de l'équation

$$x^{12} - 30x^{10} - 12x^9 + 303x^8 - 1006x^6 - 1656x^5 + 1113x^4 + 5172x^3 + 2940x^2 + 144x - 8648 = 0 \ .$$

Noter qu'avec notre implémentation, ceci a pu être trouvé quand $x$ a été calculé à 60 décimales, mais pas à 50 décimales. Vu la taille et le nombre de coefficients, il est clair qu'il est illusoire de chercher une telle équation de manière brutale, alors que grâce à LLL on peut la trouver en 1 seconde.

Maintenant choisissons $x = \sqrt{2} + \sqrt[3]{3} + \sqrt[4]{5}$. Ce nombre est algébrique de degré 24. Ici, nous devons calculer avec 250 décimales, et en moins de trois minutes on trouve que $x$ est solution de l'équation

$$\begin{aligned}x^{24} &- 24x^{22} - 24x^{21} + 234x^{20} + 288x^{19} - 1388x^{18} - 1944x^{17} + 9927x^{16} \\ &- 57960x^{15} - 38928x^{14} + 445824x^{13} + 2162x^{12} - 1070568x^{11} - 2510400x^{10} \\ &- 1856328x^9 + 7229025x^8 + 8106696x^7 + 14935732x^6 - 10731960x^5 \\ &- 31538628x^4 - 12201072x^3 - 2666976x^2 + 54232416x - 30291344 = 0 \ .\end{aligned}$$

Bien entendu il existe des méthodes purement algébriques et plus rapides pour obtenir cette équation, mais je souhaitais illustrer la puissance de l'algorithme même dans ces grandes dimensions.

Comme exemple voisin, l'algorithme LLL peut également être utilisé pour chercher des équations plus simples pour un corps de nombres. C'est l'algorithme Polred de F. Diaz y Diaz et moi-même. Appliqué au corps de nombres de degré 24 ci-dessus, on trouve qu'il peut également être défini grâce à l'équation

$$x^{24} - 342x^{18} + 20574x^{12} - 395118x^6 + 6561 = 0$$

qui est bien entendu nettement plus simple.

Comme deuxième exemple, je citerai la recherche explicite des *conjugués galoisiens* d'un nombre. Il est inutile de connaître la théorie de Galois pour comprendre cet exemple. Prenons par exemple $a = \sqrt{2} + \sqrt{3} + \sqrt{5}$. En utilisant la méthode ci-dessus on montre immédiatement que $a$ est racine de l'équation

$$x^8 - 40x^6 + 352x^4 - 960x^2 + 576 = 0 \ .$$

Bien entendu, tous les nombres de la forme $\pm\sqrt{2} \pm \sqrt{3} \pm \sqrt{5}$ seront également racines de cette équation puisqu'il est impossible de distinguer algébriquement entre deux racines carrées d'un entier. On démontre d'autre part sans difficulté que cette équation définit un corps de nombres *galoisien*, c'est à dire que toutes les racines de ce polynôme sont en fait exprimables comme polynômes d'une seule racine. Par exemple, si on pose $b = \sqrt{2} - \sqrt{3} + \sqrt{5}$, alors $b$ est un polynôme en $a$. Par une application de l'algorithme LLL voisine de celle vu ci-dessus, en moins d'une seconde on montre que

$$b = (1/48)a^7 - (37/48)a^5 + (61/12)a^3 - (13/2)a$$

(ceci est rigoureux, pas seulement une égalité numérique). Dans des exemples à peine plus compliqués, les coefficients seraient beaucoup plus gros et pourtant trouvés sans peine par LLL.

Un troisième type d'application importante de la recherche de relation linéaires entre nombres complexes est la recherche expérimentale *d'identités analytiques*. Par exemple, posons

$$S_k = \sum_{n=1}^{\infty} \frac{(-1)^{n-1}}{n^k \binom{2n}{n}^5} \ .$$

Ces séries convergent rapidement, et il est donc facile d'en calculer des centaines de décimales si on le désire. Une application de l'algorithme LLL à $\alpha_1 = \zeta(3)$, $\alpha_i = S_{i+1}$ pour $i = 2$, 3 et 4 montre que numériquement on a

$$2\zeta(3) - 205S_3 + 160S_4 - 32S_5 = 0 \ .$$

Pour découvrir expérimentalement cette formule, il suffit de 28 décimales. Une fois découverte expérimentalement de cette manière, on la vérifie à plusieurs centaines de décimales (elle est toujours vraie!), puis bien sûr, on s'attaque à la démonstration (due dans ce cas à Amdeberhan et Zeilberger [Amd-Zei]). On a donc effectivement l'identité

$$\zeta(3) = \frac{1}{2} \sum_{n=1}^{\infty} \frac{(-1)^{n-1}(205n^2 - 160n + 32)}{n^5 \binom{2n}{n}^5} \ .$$

On voit que LLL est un outil puissant qui sert aussi bien dans le cas où on sait à l'avance qu'il y a une relation à trouver (cas des nombres algébriques ci-dessus) que dans le cas où on ne sait pas s'il en existe et qu'on veut expérimenter.

## 5. Le problème des idéaux principaux

Le dernier problème que nous allons aborder est le problème dit des idéaux principaux. Soit $K$ un corps de nombres, c'est à dire un corps qui est une extension finie de $\mathbb{Q}$. Les éléments de $K$ sont tous des nombres algébriques, et parmi ceux-ci il y a les *entiers* algébriques, c'est à dire ceux qui sont racines d'une équation polynomiale à coefficients entiers et *unitaire*. L'ensemble de ces nombres est noté $\mathbb{Z}_K$, et on démontre que c'est un anneau. Le problème algorithmique, qui a de nombeuses applications, est le suivant. Soit $I$ un idéal de $\mathbb{Z}_K$. Déterminer si oui ou non $I$ est un idéal principal (c'est à dire de la forme $\alpha\mathbb{Z}_K$ pour un $\alpha \in I$), et si c'est le cas, déterminer $\alpha$.

Une solution satisfaisante à ce problème n'a vraiment été apportée que depuis 4 ans, grâce aux travaux de F. Diaz y Diaz, M. Olivier et moi-même, et aux travaux concurrents de l'équipe de M. Pohst à Berlin. L'algorithme est complexe et son implémentation a nécessité de longs mois d'efforts. C'est en quelque sorte une généralisation de la méthode de Shanks pour l'équation de Pell. Je ne peux même pas esquisser la technique, sauf pour expliquer que, comme on l'a déja signalé, nous devons maintenant circuler sur un tore de dimension $r$, ce qui n'est pas facile, mais peut se faire.

Je me contente de donner un exemple. Posons $\zeta = exp(2i\pi/19)$, une racine primitive 19-ième de l'unité, et $K = \mathbb{Q}(\zeta)$. On montre aisément que $K$ est un corps de nombres de degré 18, et que $\mathbb{Z}_K = \mathbb{Z}[\zeta]$, l'ensemble des polynômes en $\zeta$ à coefficients entiers. Il n'est pas non plus difficile de montrer que $\mathbb{Z}_K$ est un anneau principal, c'est à dire que *tout* idéal est principal. Mais c'est une autre paire de manches de trouver des générateurs. Considérons par exemple l'idéal

$$\mathfrak{p} = 229\mathbb{Z}_K + (\zeta + 11)\mathbb{Z}_K \ .$$

On montre immédiatement que $\mathfrak{p}$ est un idéal premier et que le cardinal de $\mathbb{Z}_K/\mathfrak{p}$ est égal à 229. Puisque c'est un idéal, il doit être principal, et donc il doit exister $\alpha$ tel que $\mathfrak{p} = \alpha\mathbb{Z}_K$.

Le programme mentionné ci-dessus nous dit en moins de 2 secondes, qu'un $\alpha$ possible est

$$\begin{aligned}\alpha = \zeta^{17} - 4\zeta^{16} - \zeta^{15} + 2\zeta^{14} - 3\zeta^{13} - 2\zeta^{12} + 2\zeta^{11} - 2\zeta^{10} - 3\zeta^{9} \\ + 2\zeta^{8} - \zeta^{7} - 4\zeta^{6} + 2\zeta^{5} - 4\zeta^{3} + \zeta^{2} + \zeta - 4 \ .\end{aligned}$$

A nouveau, vu qu'il y avait 18 coefficients à trouver en valeur absolue inférieurs ou égaux à 4, il aurait fallu de l'ordre de $9^{18}$ essais pour trouver cet élément de manière brutale, ce qui est évidemment impossible. Noter que je n'affirme pas ici qu'il n'existe pas d'éléments plus “simples”. D'ailleurs, en utilisant le même programme, une recherche assez brutale mais d'une minute seulement montre qu'une autre valeur beaucoup plus simple de $\alpha$ est

$$\alpha = \zeta^{15} - \zeta^{12} - 1 \ .$$

En fait, le problème des idéaux principaux est une généralisation à un degré quelconque de l'équation de Pell-Fermat où on autorise le membre de droite a être quelconque, et pas seulement égal à $\pm 1$.

## Bibliographie

[Amd-Zei] T. Amdeberhan et D. Zeilberger, *Hypergeometric series acceleration via the WZ method*, Electronic J. of Combinatorics (to appear).

[Coh] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Math. **138**, Springer, 1993, third corrected printing, 1996.

[Kob] N. Koblitz, *Introduction to elliptic curves and modular forms*, Graduate Texts in Math. **97**, Springer, 1984, Second edition, 1992.

[Sil1] J. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Math. **106**, Springer, 1986.

[Sil2] J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Math. **151**, Springer, 1994.

[Sil-Tat] J. Silverman and J. Tate, *Rational points on elliptic curves*, Undergraduate Texts in Math., Springer, 1992.