Méthodes Algorithmiques en Théorie des Nombres

par

Henri Cohen

Laboratoire A2X
U.M.R. 9936 C.N.R.S.
Université Bordeaux I
351 Cours de la Libération
33405 TALENCE Cedex

Ecole Jeunes Chercheurs en Algorithmique et
Calcul Formel, LaBRI, Talence, 25 mars 1999.

Plan de l'exposé :

- **1. Outils de base**
- **2. Equations et analyse diophantiennes**
- **3. Théorie algébrique des nombres**
- **4. Logiciels**

1. Outils de base

Outils standards : Bibliothèques multipréci-sion sur les entiers et sur les réels, d'algèbre linéaire, d'algèbre sur les polynômes et objets associés, d'a-nalyse numérique.

Outils pour la manipulation de réseaux :

- L'algorithme d'Hermite (HNF),
- L'algorithme de Smith (SNF),
- L'algorithme de Lenstra, Lenstra et Lovász (LLL).

Réseaux

On rappelle qu'un réseau de $\mathbb{R}^n$ est un $\mathbb{Z}$-module libre engendré par une base de $\mathbb{R}^n$.

Problèmes et réponses :

- Egalité de deux réseaux : HNF

Permet de mettre un réseau sous forme canonique.

- Quotient de deux réseaux : SNF

Permet en particulier de donner la forme canonique des groupes abéliens finis.

- Petit élément d'un réseau : LLL

Utile aussi pour trouver une base raisonnable d'un réseau.

Les algorithmes HNF et SNF sont des outils puissants et très utiles, mais seulement des outils.

L'algorithme LLL est aussi un outil, mais un outil magique, car il permet de répondre à des questions apparemment inaccessibles.

2. Equations et analyse diophantiennes

Equation diophantienne : on cherche des solutions en nombres entiers ou rationnels ou dans un corps de nombres par exemple.

Equations de degré 1

C'est typiquement une équation

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \ .$$

Apparemment sans intérêt. Réponse :

• Une solution existe si et seulement si le PGCD d des a_i divise b.

• Dans ce cas, on peut trouver des a_i en utilisant la matrice de passage donnant une HNF.

Equations de degré 1 (suite)

En fait, la matrice de passage calculée naivement va avoir des coefficients exponentiellement grands. Nécessité d'algorithmes HNF ayant de petits coefficients. Plusieurs méthodes :

• Méthodes déterministes : utilisent des réductions modulo le déterminant du réseau. Ne donne pas de très petits coefficients, mais taille polynomiale, exécution rapide.

• Méthodes heuristiques : non nécessairement probabilistes, utilisent l'algorithme LLL comme sous-algorithme. Donne de très petits coefficients, exécution plus lente.

Equations de degré 2

La plus célèbre est l'équation de Pell-Fermat : si $d > 0$ non carré est donné, résoudre en entiers

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

L'ensemble des solutions a une structure de groupe abélien grâce à la formule

$$(x^2 - dy^2)(z^2 - dt^2) = (xz + dyt)^2 - d(xt + yz)^2$$

provenant de la multiplicativité de la norme de $x + y\sqrt{d}$ dans le corps quadratique $\mathbb{Q}(\sqrt{d})$. Il est facile de trouver la structure de ce groupe, et de montrer qu'il existe une unité fondamentale $\epsilon \in \mathbb{Q}(\sqrt{d})$, $\epsilon > 1$ unique telle que toute solution soit

$$x + y\sqrt{d} = \pm\epsilon^n \quad \text{avec} \quad n \in \mathbb{Z} \ .$$

Comment trouver ϵ ?

- Recherche naive en variant y : inutile d'en parler.

- Fractions continues : en $O(d^{1/2+\epsilon})$, rapide si d n'est pas trop grand ($d < 10^{16}$ disons).

- Infrastructure de Shanks : remarquable méthode élémentaire en $O(d^{1/4+\epsilon})$, pour $d < 10^{25}$.

- Sous-exponentielle de Buchmann : la plus rapide, en temps

$$O\left(\exp\left(c\sqrt{\log d \log\log d}\right)\right)$$

pour une constante $c < 2$. Permet d'atteindre $d < 10^{60}$.

Exemples :

Pour $d = 13729$ la plus petite solution de $x^2 - dy^2 = \pm 1$ est

$$\left\{\begin{array}{lll} x & = & 2067298698698622978781414087663778 6 \\ & & \;370240523605690342866664580146794 86 \\ & & \;709342957840763527431840700555497 80, \\ y & = & 176434608758883275088400645907364 80 \\ & & \;225145559266591277103103388593278 80 \\ & & \;097286527931924281496170920222937 \end{array}\right.$$

Pour $d = (10^{31} - 4)/4$, si (x, y) est la plus petite solution on a

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

Equations de degré 3 et 4

Certaines de ces équations se ramènent à des équations de courbes elliptiques, à savoir une équation du type

$$y^2 = x^3 + ax + b \quad \text{avec} \quad 4a^3 + 27b^2 \neq 0 \ .$$

On peut se poser la question de trouver les solutions entières (qui sont en nombre fini), mais la question la plus importante est ici de trouver les solutions rationelles.

La propriété qui rend ce problème fascinant est qu'il y a encore une loi de groupe abélien, découverte par Fermat.

Equations de degré 3 et 4 (suite)

Un important théorème de Mordell affirme que ce groupe est de type fini, c'est à dire isomorphe à une partie de torsion, finie et facilement calculable, fois un groupe abélien libre $\mathbb{Z}^r$. Le calcul de $r \geq 0$ ainsi que des générateurs correspondants est algorithmiquement très difficile, et en fait procède d'une recherche exponentielle.

Le meilleur programme disponible pour calculer ce groupe est `mwrank` de J. Cremona, disponible sur le Web.

Exemple 1 : un problème de Fermat

Trouver (x, y, z) entiers plus grands ou égaux à 3 tels que $x^3 + y^3 = 9z^3$.

La loi de groupe sur la cubique $x^3 + y^3 = dz^3$ s'exprime comme suit.

$$(x_1, y_1, z_1)(x_2, y_2, z_2) = (x_3, y_3, z_3) \quad \text{où}$$

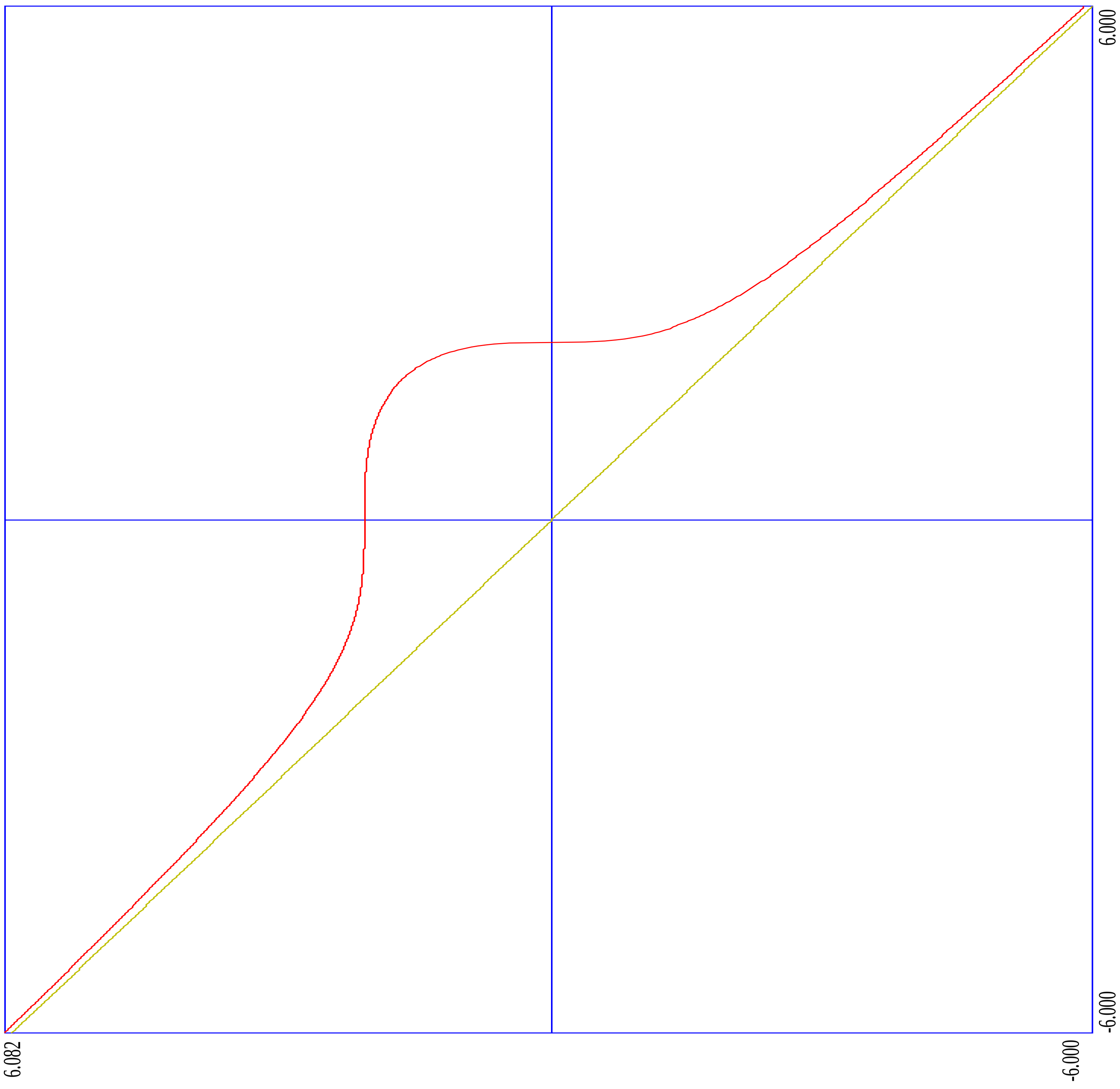
$$\begin{cases} x_3 &= dz_1z_2(y_1z_2 - y_2z_1) + x_1x_2(x_1y_2 - x_2y_1) \\ y_3 &= dz_1z_2(x_1z_2 - x_2z_1) + y_1y_2(x_2y_1 - x_1y_2) \\ z_3 &= y_1y_2(y_1z_2 - y_2z_1) + x_1x_2(x_1z_2 - x_2z_1) \end{cases}$$

si les points projectifs sont distincts, et

$$\begin{cases} x_3 &= y_1(dz_1^3 + x_1^3) \\ y_3 &= x_1(x_1^3 - 2dz_1^3) \\ z_3 &= z_1(dz_1^3 - 2x_1^3) \end{cases}$$

si les points projectifs sont confondus.

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



Exemple 1 : un problème de Fermat (suite)

Puissances successives du point $(1,2,1)$ sur $x^3+y^3=9z^3$

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

d'où la plus petite solution rationnelle à $x^3+y^3=9$ avec x et y plus grands ou égaux à 3 est $x=X/Z$, $y=Y/Z$ avec :

$$\begin{cases} X & = & 676702467503 \\ Y & = & 415280564497 \\ Z & = & 348671682660 \end{cases} .$$

Exemple 2 : le problème des nombres congruents

Date de l'antiquité et pas encore complètement résolu ! Etant donné un entier positif n, déterminer si n est la surface d'un triangle rectangle à cotés rationnels. Eventuellement, trouver ce rectangle.

Se ramène à chercher les points non triviaux sur la courbe elliptique

$$y^2 = x^3 - n^2 x = x(x-n)(x+n) \ .$$

La résolution presque complète de ce problème utilise des techniques très voisines de celles utilisées par Wiles dans sa démonstration de Fermat. Il manque seulement la démonstration d'une forme faible de la conjecture de Birch et Swinnerton-Dyer.

L'algorithmique est basée sur la méthode des points de Heegner. Exemple :

Un triangle rectangle ayant comme aire 157 est de côtés $(p/q, q/r, s/t)$ où

$$\begin{cases} p & = & 314r = 680329848782643505121 7540 \\ q & = & 411340519227716149383203 \\ r & = & 21666555693714761309610 \\ s & = & 224403517704336969924557513090674863160948472041 \\ t & = & 891233226892885958802553517896716357001648083 0 \, , \end{cases}$$

et ceci sont les plus petites valeurs possibles.

Exemples d'utilisation remarquable de LLL

Exemple 1 : $x = \sqrt{2} + \sqrt[3]{3} + \sqrt[4]{5}$ est racine de

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

Appliquant un algorithme de réduction polynomiale utilisant LLL, on trouve que

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

définit le même corps de nombres.

Exemple 2 : Identité remarquable pour $\zeta(3)$:

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

Trouvée d'abord numériquement grâce à LLL, puis démontrée. C'est le cas de nombreuses identités, y compris certaines qui ne sont pas *encore* démontrées, telles les identités sur les valeurs de fonctions zeta multiples, ou les mesures de Mahler de polynômes à plusieurs variables, bien que des progrès considérables aient été faits.

3. Théorie algébrique des nombres

Les objets mathématiques sont plus complexes. Se pose donc de manière essentielle le problème de leur représentation, de leur manipulation, et des opérations entre eux. Typiquement, on a affaire aux types suivants :

- Corps de nombres
- Eléments de corps de nombres
- Idéaux, idéaux premiers
- Bases d'entiers
- Corps résiduels, localisés
- Groupes de classes d'idéaux
- Groupes d'unités

Les outils essentiels sont toujours les mêmes : HNF, SNF et LLL, plus des algorithmes tels que la factorisation des polynômes sur $\mathbb{Z}$ ou sur un corps fini.

Toutefois il existe de nombreux algorithmes beaucoup plus compliqués : le plus important est le calcul du groupe de classes d'idéaux et le calcul du groupe des unités, combiné avec le logarithme discret correspondant, qui s'appelle le problème des idéaux principaux.

On peut désormais faire ces calculs en temps heuristiquement sous-exponentiels (comme ci-dessus), et c'est spectaculaire (travaux de Cohen-Diaz-Olivier, Pohst et al).

Petit Exemple : Si $\zeta = \exp(2i\pi/19)$, $K = \mathbb{Q}(\zeta)$ et

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

alors $\mathfrak{p} = \alpha\mathbb{Z}_K$ avec

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

C'est la solution du problème des idéaux principaux, qui est, comme LLL un algorithme magique en ce sens qu'il est impossible de trouver la solution par recherche exhaustive.

Depuis 1996, on est capable de faire de la théorie algorithmique du corps de classes de manière efficace (travaux de Cohen-Diaz-Olivier, Fieker-Pohst). Il s'agit d'une part de calculer des groupes de classes de rayon, mais surtout de calculer les extensions abéliennes correspondantes, ce qui est beaucoup plus difficile.

Ceci peut se faire avec la théorie de Kummer, pénible, lente, difficile à implanter, mais complète.

Si le corps de base est soit totalement réel, soit quadratique imaginaire, on peut aussi utiliser des méthodes analytiques telles que la multiplication complexe.

Exemple célèbre : Comme le nombre de classes de $\mathbb{Q}(\sqrt{-163})$ est égal à 1, l'invariant modulaire $j((-1+\sqrt{-163})/2)$ est un entier. Concrètement, ceci se traduit par :

$$(e^{\pi\sqrt{163}} - 744)^{1/3} =$$

$$640319.999999999999999999999999390317\ldots$$

Les progrès algorithmiques considérables sont de deux ordres :

- Réduction d'un facteur 12 du nombre de chiffres des polynômes obtenus pour les corps quadratiques imaginaires (travaux de Schertz et Cohen).
- Utilisation algorithmique des conjectures de Stark pour les corps totalement réels (travaux de Roblot).

4. Logiciels

Bien entendu, il est possible d'utiliser les logiciels de calcul formel classiques tels que Maple. Toutefois plusieurs gros inconvénients :

- Habituellement très inefficaces (facteur 100 fréquent).
- Contient peu d'algorithmes spécifiques implantés, malgré les contributions externes.
- Impossibilité d'utiliser comme bibliothèque C ou autre.
- Logiciels non libres et non modifiables.

Pour tout calcul un peu complexe, il est indispensable de se procurer ou d'utiliser (à travers le réseau `médicis` par exemple) un ou plusieurs logiciels spécialisé permettant de faire de la théorie des nombres.

Le logiciel le plus remarquable dans cette catégorie est certainement `magma` (Sidney, J. Cannon et al). Ce n'est *pas* un logiciel libre (il coûte d'ailleurs assez cher), mais il est dans un cadre académique, et son contenu et ses performances sont remarquables. Il contient les algorithmes parmi les plus performants au monde dans la plupart des domaines liés à l'algèbre et à la théorie des nombres, et possède une interface mathématique complète.

4. Logiciels (suite I)

Le logiciel `Pari/GP` (Bordeaux et Orsay, H. Cohen et K. Belabas) est complètement libre. Il permet de faire tous les calculs énumérés dans cet exposé et bien d'autres, et est l'un des logiciels les plus performants au monde dans ce domaine.

Le logiciel `Kant/Kash` (Berlin, M. Pohst et al) est concurrent de Pari, mais est d'ambition moindre car essentiellement consacré aux corps de nombres, avec une interface utilisateur sommaire. Défaut principal : le source n'est pas disponible et on ne peut pas l'utiliser comme bibliothèque. Par contre certains algorithmes sur les corps de nombres sont mieux implantés que dans Pari.

4. Logiciels (suite II)

Le logiciel LiDIA (Darmstadt, J. Buchmann et al) est destiné à devenir la référence des logiciels de théorie des nombres. Il est libre, très rapide, son source C++ est disponible et utilisable en bibliothèque. Par contre, par souci de perfection, son développement est lent, donc il ne contient pas encore autant de fonctionalités que Pari.

Il y a bien entendu beaucoup d'autres logiciels disponibles, tels que `mwrank` déja cité, et d'autres. D'autre part il y a des banques de données importantes en théorie des nombres.

Les plus importantes sont celles de Berlin (accessible uniquement à travers une liaison `TCP/IP` vers Berlin ouverte par le logiciel Kash), et celle de Bordeaux disponible simplement par `ftp` anonyme. Ces deux banques contiennnent des renseignements arithmétiques détaillés sur près d'un million de corps de nombres. De plus, celle de Bordeaux contient d'autres informations très utiles et des miroirs d'autres banques telles que des listes de courbes elliptiques.

Enfin, un peu de pub. TOUT ce que vous voulez savoir sur l'algorithmique en théorie des nombres et beaucoup plus est contenu dans mes deux livres (environ 580 pages chacun):

- A Course in Computational Algebraic Number Theory, Graduate Texts in Math **138**, third printing (1996), Springer-Verlag.

- Advanced Topics in Computational Number Theory, Graduate Texts in Math **XXX**, (1999), Springer-Verlag.

(a paraître avant l'été).