L'algorithme de Cornacchia

Abderrahmane Nitaj

We give in a simple way a new proof of the validity of Cornacchia's algorithm. This algorithm consists of finding all primitive solutions (x, y) (if any) of the diophantine equation $ax^2 + by^2 = m$, where a, b and m are positive coprime integers. Our proof is based on some properties of the rational continued fractions.

1. Introduction

Soient a, b et m des entiers strictement positifs, premiers entre eux deux à deux et tels que $m > a + b$. On considère l'équation:

$$ax^2 + by^2 = m, \tag{1}$$

en entiers $x \neq 0$ et $y > 0$. Une solution (x, y) de l'équation (1) vérifiant $(x, y) = 1$ sera appelée *solution primitive*. Puisque a, b et m sont premiers entre eux deux à deux, toute solution primitive vérifie: $(ax, by) = (x, m) = (y, m) = 1$. Si $a = b = 1$, on exige de plus que $|x| > y > 0$. On considère de même la congruence:

$$t^2 \equiv -ba^{-1} \pmod{m}, \tag{2}$$

avec $0 < t < m$.

Dans cet article, nous donnons une nouvelle démonstration de l'algorithme de Cornacchia, qui date de 1908 (voir [1]) et qui permet de déterminer les solutions primitives de l'équation (1). Cette démonstration se distingue particulièrement par sa simplicité de celles qui ont été données récemment dans [2] et [4]. Voici une description de l'algorithme de Cornacchia.

Algorithme 1. (Cornacchia)

- Résoudre la congruence (2);
- Pour chaque solution t avec $m/2 < t < m$, appliquer l'algorithme d'Euclide à t et m;
  - Déterminer le premier reste $r < \sqrt{m/a}$;
  - Si $\sqrt{(m - ar^2)/b}$ est entier, alors $\left(r, \sqrt{(m - ar^2)/b}\right)$ est une solution de (1).

Nous verrons dans la partie 4 que toute solution obtenue par cet algorithme est primitive.

Notre démonstration de la validité de l'algorithme de Cornacchia se base sur l'utilisation de certaines propriétés du développement des nombres réels en fractions continues. Nous résumons ces outils dans la section 2. Dans la section 3, nous décrivons la résolution de l'équation (1), dans la section 4 nous donnons la nouvelle démonstration de l'algorithme de Cornacchia et dans la section 5, nous donnons une nouvelle version de cet algorithme, illustré par un exemple.

2. Les fractions continues

La fraction continue d'un nombre réel $\xi \neq 0$ s'obtient de la façon suivante. On écrit:

$$\xi = a_0 + \frac{1}{\xi_1},$$

où $a_0 = \lfloor \xi \rfloor$ est la partie entière de ξ. On recommence ensuite en remplaçant dans l'expression ci-dessus ξ par ξ_1, ce qui donne un entier a_1 et un réel ξ_2. Par ce procédé, on obtient les formules de récurrence:

$$\xi_i = a_i + \frac{1}{\xi_{i+1}}, \qquad i \geq 0,$$

avec $\xi_0 = \xi$ et $a_i = \lfloor \xi_i \rfloor$. On a alors l'expression:

$$\xi = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}},$$

et on écrit tout simplement $\xi = [a_0, a_1, a_2, a_3, \ldots]$, qu'on appelle développement de ξ en fraction continue. Si ξ est rationnel, son développement en fraction continue est fini. En adoptant la convention que le dernier terme, s'il existe, est strictement supérieur à 1, alors le développement en fraction continue de tout réel est unique. Pour $i \geq 0$, les *réduites* u_i/v_i de ξ sont obtenues en prenant $(u_i, v_i) = 1$ et

$$\frac{u_i}{v_i} = [a_0, \ldots, a_i].$$

Si on convient que $u_{-2} = 0, v_{-2} = 1, u_{-1} = 1, v_{-1} = 0$, alors on a les relations de récurrence, valables pour tout $i \geq 0$:

$$u_i = a_i u_{i-1} + u_{i-2},$$
$$v_i = a_i v_{i-1} + v_{i-2}.$$

Parmi les propriétés des fractions continues, nous aurons besoin des résultats suivants:

Théorème 1. **([3], p. 10)** *Soit ξ un nombre réel non nul. Soient u_n/v_n et u_{n+1}/v_{n+1} deux réduites consécutives de ξ. Pour tout couple (a,b) d'entiers, si $0 < b < v_{n+1}$, alors $|b\xi - a| \geq |v_n\xi - u_n|$.*

Théorème 2. **([3], p. 11)** *Soit ξ un nombre réel. Si la fraction irréductible a/b avec $b \geq 1$ vérifie:*

$$\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2},$$

alors a/b est une réduite de la fraction continue de ξ.

Théorème 3. **([3], p. 8, 9)** *Soit ξ un nombre réel non nul et soient u_i/v_i, $i \geq -2$ ses réduites (si ξ est rationnel, le nombre s de ses réduites est fini). Alors*

$$0 < v_0 \leq v_1 < v_2 < \cdots,$$

et pour tout $i \geq 1$ ($i \leq s$ si ξ est rationnel):

$$|v_i\xi - u_i| > |v_{i+1}\xi - u_{i+1}|.$$

3. Résolution de l'équation (1)

La résolution de l'équation (1) en entiers x et y est basée sur le théorème suivant.

Théorème 4. *Soit (x,y) une solution de l'équation (1) vérifiant $x \neq 0$, $y > 0$ et $(x,y) = 1$. Alors il existe une solution t de (2) et une réduite u/v de t/m telles que $x = tv - mu$ et $y = v$.*

Preuve. Soit (x,y) une solution de l'équation (1) avec $(x,y) = 1$. Alors $(y,m) = 1$ et on peut définir t par $t \equiv xy^{-1} \pmod m$ et $0 < t < m$. Ainsi t est une solution de la congruence (2) et il existe un entier u tel que $x = ty - mu$. L'hypothèse $a+b < m$ implique $|x|y \neq 1$ et donc $0 < 2|x|y < x^2 + y^2 \leq ax^2 + by^2 = m$. Alors:

$$\left|\frac{u}{y} - \frac{t}{m}\right| = \frac{|x|}{my} < \frac{1}{2y^2}.$$

Le théorème 2 montre alors que u/y est une réduite de t/m. ■

Le théorème 4 montre comment déterminer certaines solutions de l'équation (1) en résolvant la congruence (2) et en calculant les réduites des différents rationnels t/m. La proposition suivante montre que toutes les solutions obtenues de cette façon sont primitives.

Proposition 1. *Soit t une solution de la congruence (2). Si (x,y) est une solution de (1) vérifiant $x \equiv ty \pmod m$, alors (x,y) est primitive.*

Preuve. Si t est une solution de la congruence (2), alors il existe un entier q tel que $at^2 + b = mq$. Si x et y vérifient $x \equiv ty \pmod{m}$, alors il existe un entier u tel que $x = ty - mu$, et donc $ax^2 + by^2 = m\left(qy^2 - 2atuy + mau^2\right)$. Si (x, y) vérifie $ax^2 + by^2 = m$, alors

$$qy^2 - 2atuy + mau^2 = (qy - 2atu)y + mau^2 = 1$$

et donc $(m, y) = 1$, ce qui montre que (x, y) est primitive. ∎

La proposition suivante montre qu'une solution t de la congruence (2) donne au plus une solution primitive pour l'équation (1), et donc que le nombre de solutions primitives de cette équation est au plus égal au nombre de solutions de la congruence (2).

Proposition 2. *Soit t une solution de la congruence* (2)*. Si (x, y) et (x', y') sont deux solutions primitives de l'équation* (1) *vérifiant $x \equiv ty \pmod{m}$ et $x' \equiv ty' \pmod{m}$, alors $x = x'$ et $y = y'$.*

Preuve. Des congruences $x \equiv ty \pmod{m}$ et $x' \equiv ty' \pmod{m}$, on tire:

$$axx' + byy' \equiv (at^2 + b)yy' \equiv 0 \pmod{m},$$

et donc $axx' + byy' = mq_1$ où q_1 est entier. On a aussi $xy' - yx' \equiv 0 \pmod{m}$ et donc $xy' - yx' = mq_2$ où q_2 est entier. Des égalités $ax^2 + by^2 = m$ et $ax'^2 + by'^2 = m$, on tire:

$$(axx' + byy')^2 + ab(xy' - yx')^2 = m^2,$$

ce qui donne:

$$q_1^2 + abq_2^2 = 1. \tag{3}$$

Supposons d'abord que $a = b = 1$. Les solutions vérifient par hypothèse $0 < y < |x|$ et $0 < y' < |x'|$. Si dans (3) on a $q_1 = 0$, alors $xx' + yy' = 0$ et donc puisque $(x, y) = 1$ et $(x', y') = 1$, alors $x = \pm y'$ et $y = \mp x'$. L'inégalité $0 < y < |x|$ donne $0 < |x'| < y'$ ce qui est impossible. Alors on a $q_2 = 0$ dans (3), d'où $x/y = x'/y'$, ce qui donne $x = x'$ et $y = y'$.

Supposons maintenant que $ab > 1$. La relation (3) implique alors que $q_2 = 0$, et comme ci-dessus, on a $x = x'$ et $y = y'$. ∎

4. L'algorithme de Cornacchia

Nous dirons qu'une solution t de la congruence (2) *produit* une solution (x, y) pour l'équation (1) s'il existe une réduite u/v de t/m telle que $x = tv - mu$ et $y = v$. Nous donnons dans cette partie la démonstration de l'algorithme de Cornacchia. Contrairement au théorème 4, cet algorithme ne permet de déterminer que les solutions positives de l'équation (1). D'autre part, l'algorithme de Cornacchia ne considère que les solutions t de la congruence (2) vérifiant $m/2 < t < m$. En fait, nous avons la proposition suivante.

Proposition 3. *Soit t une solution de la congruence* (2) *avec $0 < t < m/2$. Si (x, y) est une solution de de* (1) *produite par t, alors $(-x, y)$ est une solution de* (1) *produite par $m - t$.*

Preuve. Développons t/m en fraction continue, $t/m = [a_0, a_1, a_2, \ldots, a_s]$ avec $a_s \geq 2$, $a_0 = \lfloor t/m \rfloor = 0$ et $a_1 = \lfloor m/t \rfloor \geq 2$. Alors ([3], p. 15)

$$(m-t)/m = 1 - t/m = [0, 1, a_1 - 1, a_2, a_3, \ldots, a_s].$$

Soient u_i/v_i et u'_i/v'_i, $i \geq -2$ les réduites de t/m et $(m-t)/m$ respectivement. On montre facilement par récurrence que pour tout $1 \leq i \leq s$, $u'_i = v_{i-1} - u_{i-1}$ et $v'_i = v_{i-1}$. Si (x, y) est une solution produite par t, alors $x = ty - mu$ où u/y est une réduite de t/m. Alors $(y-u)/y$ est une réduite de $(m-t)/m$ et

$$(m-t)y - m(y-u) = -(ty - mu) = -x$$

et donc $(-x, y)$ est une solution produite par $m - t$. ■

Maintenant, on peut se limiter aux solutions t de la congruence (2) vérifiant $m/2 < t < m$. Nous allons établir le lien entre la suite des restes considérés dans l'algorithme 1 et la suite des entiers $x = tv - mu$, où u/v est une réduite de t/m, considérés dans le théorème 4.

Soit t une solution de la congruence (2) avec $m/2 < t < m$. La suite des restes considérés dans l'algorithme 1 est obtenue en appliquant l'algorithme d'Euclide à t et m. On définit les suites (a_i) et (r_i) par:

$$\begin{aligned}
t &= a_0 m + r_0, \\
m &= a_1 r_0 + r_1, \\
r_{i-1} &= a_{i+1} r_i + r_{i+1}, \quad (i = 1, \ldots, s-1).
\end{aligned}$$

Nous avons en particulier $a_0 = 0$, $a_1 = 1$, $r_0 = t$, $r_s = 0$, et pour tout $1 \leq i \leq s$, $a_i \geq 1$ et $r_i < r_{i-1}$. La fraction continue de t/m est (voir [5], p. 325):

$$t/m = [0, 1, a_2, \ldots, a_s].$$

Proposition 4. *Soient u_i/v_i, $(-2 \leq i \leq s)$ les réduites de t/m. Pour tout $0 \leq i \leq s$, $x_i = tv_i - mu_i = (-1)^i r_i$.*

Preuve. Pour $i = 0$ on a $x_0 = tv_0 - mu_0 = t = r_0$. Pour $i = 1$, on a $x_1 = tv_1 - mu_1 = t - m = -r_1$. Supposons que l'égalité ait lieu jusqu'au rang i. Alors:

$$\begin{aligned}
tv_{i+1} - mu_{i+1} &= t(a_{i+1}v_i + v_{i-1}) - m(a_{i+1}u_i + u_{i-1}) \\
&= a_{i+1}(tv_i - mu_i) + tv_{i-1} - mu_{i-1} \\
&= (-1)^i a_{i+1} r_i + (-1)^{i-1} r_{i-1} \\
&= (-1)^{i+1}(r_{i-1} - a_{i+1} r_i) \\
&= (-1)^{i+1} r_{i+1}.
\end{aligned}$$

Ceci montre donc la proposition. ■

La proposition ci-dessus montre que les solutions obtenues par l'algorithme de Cornacchia sont primitives. Nous donnons maintenant la démonstration de cet algorithme.

Théorème 5. *Soit t une solution de la congruence (2) avec $m/2 < t < m$. Soient u_i/v_i, $i \geq -2$ les réduites de t/m, $x_i = tv_i - mu_i$ et $y_i = v_i$. Si t produit une solution (x_k, y_k) pour l'équation (1), alors k est le plus petit entier $i \geq 0$ tel que $|x_i| < \sqrt{m/a}$.*

Preuve. Si une solution t de la congruence (2) produit une solution (x_k, y_k) pour l'équation (1), d'après le théorème 4, elle est de la forme $x_k = tv_k - mu_k$, $y_k = v_k$ où u_k/v_k est une réduite de t/m, avec $k \geq 0$. Puisque $ax_k^2 + by_k^2 = m$ et $x_k y_k \neq 0$, alors:

$$|x_k| < \sqrt{m/a} \qquad \text{et} \qquad y_k < \sqrt{m/b}.$$

Soit $i_0 \geq 0$ le plus petit entier tel que $|x_{i_0}| < \sqrt{m/a}$. Si $i_0 < k$, alors (théorème 3) $y_{i_0} \leq y_k < \sqrt{m/b}$ et donc $ax_{i_0}^2 + by_{i_0}^2 < 2m$. D'autre part,

$$0 < ax_{i_0}^2 + by_{i_0}^2 = a(tv_{i_0} - mu_{i_0})^2 + bv_{i_0}^2 \equiv 0 \pmod{m},$$

alors $ax_{i_0}^2 + by_{i_0}^2 = m$ et donc (x_{i_0}, y_{i_0}) est aussi une solution de l'équation (1) produite par t, ce qui contredit la proposition 1. ■

5. Nouvelle version de l'algorithme et exemple

Nous donnons maintenant un algorithme basé sur l'utilisation des fractions continues pour déterminer toutes les solutions primitives de l'équation (1). Si on connait la factorisation de m, plusieurs méthodes permettent de résoudre la congruence (2) (voir [2] et [5]).

Algorithme 2. $(ax^2 + by^2 = m)$

Entrée: $a > 0$, $b > 0$, $m > a + b$, premiers entre eux deux à deux.

Initialisation: Déterminer les solutions t_j, $j = 1, \ldots, n_0$ de $t^2 \equiv -ba^{-1} \pmod{m}$ telles que $m/2 < t_j < m$;

$j := 0$;
Tant que $j \leq n_0 - 1$ **répéter**
    $j := j + 1$;
    $y_{-1} := 0$;
    $i := -1$;
    Tant que $y_i < \sqrt{m/b}$ **répéter**
        $i := i + 1$;
        Calculer la réduite $\dfrac{u_i}{y_i}$ de $\dfrac{t_j}{m}$;
        $x_i := t_j y_i - mu_i$;
        Si $|x_i| < \sqrt{m/a}$ **et** $y_i < \sqrt{m/b}$**alors** écrire x_i et y_i.

Exemple. Pour illustrer l'algorithme 2, nous avons traité l'exemple suivant avec l'aide de Maple. Soient $a = 317$, $b = 15$ et

$$m = 19387588709124669472 28 = 2^2 \cdot 239 \cdot 55286879 \cdot 36681225047.$$

La première étape de l'algorithme 2 consiste à résoudre la congruence $at^2+b \equiv 0 \pmod{m}$, avec $m/2 < t < m$. On trouve les valeurs suivantes:

$$\begin{aligned} t_1 &= 1540268285466516237559, & t_2 &= 1624103215407503974869, \\ t_3 &= 1352352495007639360927, & t_4 &= 1812019005866380851501, \\ t_5 &= 1096119300502319569341, & t_6 &= 1555785811361061059915, \\ t_7 &= 1284035090961196445973, & t_8 &= 1367870020902184183283. \end{aligned}$$

La deuxième étape consiste à déterminer pour chaque t_j, $1 \leq j \leq 8$, l'unique réduite (s'il en existe) u/y de t_j/m qui vérifie les inégalités $y < \sqrt{m/b}$ et $|t_j y - mu| < \sqrt{m/a}$. La table ci-dessus résume cette recherche.

t_j	u	y	x
t_1	−	−	−
t_2	−	−	−
t_3	−	−	−
t_4	−	−	−
t_5	−	−	−
t_6	9082110491	11317767621	−234156733
t_7	7520168509	11354668973	123452677
t_8	−	−	−

Ainsi les seules solutions primitives sont les huit couples

$$(x, y) = (\pm 234156733, \pm 11317767621), (\pm 123452677, \pm 11354668973).$$

Remarque. On peut obtenir toutes les solutions de l'équations (1) (y compris les solutions non primitives) en résolvant les différentes équations $ax_d^2 + by_d^2 = m/d^2$ où d^2 décrit l'ensemble des diviseurs carrés de m. Les solutions de (1) sont alors de la forme (dx_d, dy_d).

Références

[1] G. Cornacchia, *Su di un metodo per la risoluzione in numeri interi dell' equazione* $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$, Giornale di Matematiche di Battaglini **46** (1908), 33−90.

[2] K. Hardy, J. B. Muskat, and K. S. Williams, *A deterministic algorithm for solving* $n = fu^2 + gv^2$ *in coprime integers* u *and* v, Math. Comp. **55** (1990), 327 − 343.

[3] S. Lang, *Introduction to Diophantine Approximations,* Addison-Wesley Publishing Compagny, Reading, Massachusetts, 1966

[4] F. Morain, *Courbes elliptiques et tests de primalité,* Thèse (1990), Université de Lyon 1.

[5] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory of Numbers*, John Wiley and Sons, (New York) 1991.

Département de Mathématiques
Université de Caen, 14032, Caen Cedex France
(e-mail nitaj@math.unicaen.fr)