

JOURNAL  
DE  
MATHÉMATIQUES

PURES ET APPLIQUÉES

FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874

PAR JOSEPH LIOUVILLE

---

SIGISMOND GUNTHER

**Résolution de l'équation indéterminée  $y^2 + ax^2 = bz$  en nombres entiers**

*Journal de mathématiques pures et appliquées 3<sup>e</sup> série*, tome 2 (1876), p. 331-341.

[http://www.numdam.org/item?id=JMPA\\_1876\\_3\\_2\\_331\\_0](http://www.numdam.org/item?id=JMPA_1876_3_2_331_0)

 gallica

NUMDAM

Article numérisé dans le cadre du programme  
Gallica de la Bibliothèque nationale de France  
<http://gallica.bnf.fr/>

et catalogué par Mathdoc  
dans le cadre du pôle associé BnF/Mathdoc  
<http://www.numdam.org/journals/JMPA>

*Résolution de l'équation indéterminée  $y^2 - ax^2 = bz$   
en nombres entiers ;*

PAR M. SIGISMOND GUNTHER,

Privat-docent à l'École Polytechnique de Munich.

La méthode ordinaire pour la résolution des équations indéterminées du second degré prend pour base le développement connu d'une expression irrationnelle  $x$  en fraction continue

$$x = \alpha_0 + \frac{1}{\alpha_1 + \frac{1}{\alpha_2 + \dots + \frac{1}{\alpha_n + \frac{1}{\alpha_1 + x}}}}$$

Mais on sait qu'il y a aussi un autre procédé qui conduit au même but, si l'on pose avec Cataldi

$$\sqrt{a^2 + n} = a + \frac{n}{2a + \frac{n}{2a + \dots}}$$

Nous proposons d'étudier les propriétés de cette forme plus simple qui s'appliquent à la solution de la congruence

(1)  $y^2 \equiv ax^2 \pmod{b}$ .

1. Considérons la fraction continue

$$K = \frac{a}{2u - \frac{a}{2u - \frac{a}{2u \dots}}}$$

et désignons par  $Q_i$  le dénominateur de la  $i^{\text{ème}}$  fraction réduite de  $K$ .  
On a la relation assez connue [\*]

$$Q_{2n} = \begin{vmatrix} 2u & \sqrt{a} & 0 & \dots & 0 & 0 & 0 \\ \sqrt{a} & 2u & \sqrt{a} & \dots & 0 & 0 & 0 \\ 0 & \sqrt{a} & 2u & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 2u & \sqrt{a} & 0 \\ 0 & 0 & 0 & \dots & \sqrt{a} & 2u & \sqrt{a} \\ 0 & 0 & 0 & \dots & 0 & \sqrt{a} & 2u_{(2n)} \end{vmatrix}$$

où l'indice du terme  $2u$  indique seulement l'ordre du déterminant.  
Additionnant à la  $q^{\text{ème}}$  série horizontale ( $q \leq n$ ) la  $(2n - q + 1)^{\text{ème}}$ , on obtient

$$Q_{2n} = \begin{vmatrix} 2u & \sqrt{a} & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & \sqrt{a} & 2u \\ \sqrt{a} & 2u & \sqrt{a} & \dots & 0 & 0 & \dots & 0 & 0 & \dots & \sqrt{a} & 2u & \sqrt{a} \\ 0 & \sqrt{a} & 2u & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 2u & \sqrt{a} & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 2u & \sqrt{a} & \dots & \sqrt{a} & 2u & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & \sqrt{a} & 2u_{(n)} + \sqrt{a} & \dots & 2u + \sqrt{a} & \sqrt{a} & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & \sqrt{a} & \dots & 2u & \sqrt{a} & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & \sqrt{a} & 2u & \dots & 0 & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 2u & \sqrt{a} & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & \sqrt{a} & 2u & \sqrt{a} \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 & 0 & \dots & 0 & \sqrt{a} & 2u_{(2n)} \end{vmatrix}$$

Si maintenant on soustrait de chaque  $q^{\text{ème}}$  colonne ( $q \leq n$ ) la

[\*] Voir, par exemple, GUNTHER, *Lehrbuch der Determinantentheorie*; Erlangen, 1875, p. 157.

$(2n - q + 1)^{i\text{ème}}$ , on trouvera, d'après le théorème de Laplace,

$$Q_{2n} = - \begin{vmatrix} 0 & 0 & 0 & \dots & 0 & \sqrt{a} & \sqrt{a}-2u \\ 0 & 0 & 0 & \dots & -\sqrt{a} & -2u & -\sqrt{a} \\ 0 & 0 & 0 & \dots & -2u & -\sqrt{a} & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & -\sqrt{a} & -2u & \dots & 0 & 0 & 0 \\ -\sqrt{a} & -2u & -\sqrt{a} & \dots & 0 & 0 & 0 \\ -2u & -\sqrt{a} & 0 & \dots & 0 & 0 & 0 \end{vmatrix} \begin{vmatrix} 0 & 0 & 0 & \dots & 0 & \sqrt{a} & 2u \\ 0 & 0 & 0 & \dots & \sqrt{a} & 2u & \sqrt{a} \\ 0 & 0 & 0 & \dots & 2u & \sqrt{a} & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \sqrt{a} & 2u & \dots & 0 & 0 & 0 \\ \sqrt{a} & 2u & \sqrt{a} & \dots & 0 & 0 & 0 \\ 2u + \sqrt{a} & \sqrt{a} & 0 & \dots & 0 & 0 & 0 \end{vmatrix}$$

et, par décomposition,

$$\begin{aligned} Q_{2n} &\doteq [(2u - \sqrt{a}) Q_{n-1} - a Q_{n-2}] [(2u + \sqrt{a}) Q_{n-1} - a Q_{n-2}] \\ &= (2u Q_{n-1} - a Q_{n-2})^2 - a Q_{n-1}^2. \end{aligned}$$

D'autre part, la loi de formation des réduites nous donne la formule

$$2u Q_{n-1} - a Q_{n-2} = Q_n,$$

et, par suite, nous obtiendrons comme résultat final

$$(2) \quad Q_n^2 - a Q_{n-1}^2 = Q_{2n}.$$

Nous avons trouvé ce théorème par la transformation des déterminants exposée ci-dessus; mais on peut aussi parvenir à cette relation au moyen du calcul algébrique; car l'identité

$$\begin{aligned} &\sqrt{u^2 - a} [(u + \sqrt{u^2 - a})^{2n+1} - (u - \sqrt{u^2 - a})^{2n+1}] \\ &= \sqrt{u^2 - a} [(u + \sqrt{u^2 - a}) (u + \sqrt{u^2 - a})^{2n} \\ &\quad - (u - \sqrt{u^2 - a}) (u - \sqrt{u^2 - a})^{2n}] \end{aligned}$$

donne immédiatement la suivante :

$$\begin{aligned} &2\sqrt{u^2 - a} [(u + \sqrt{u^2 - a})^{2n+1} - (u - \sqrt{u^2 - a})^{2n+1}] \\ &= (u + \sqrt{u^2 - a})^{2n+2} - 2a^{n+1} + (u - \sqrt{u^2 - a})^{2n+2} \\ &\quad - a [(u + \sqrt{u^2 - a})^{2n} - 2a^n + (u - \sqrt{u^2 - a})^{2n}]. \end{aligned}$$

La division par l'expression  $4(u^2 - a)$  nous conduit à l'identité

$$\frac{(u + \sqrt{u^2 - a})^{2n+1} - (u - \sqrt{u^2 - a})^{2n+1}}{2\sqrt{u^2 - a}} = \left[ \frac{(u + \sqrt{u^2 - a})^{n+1} - (u - \sqrt{u^2 - a})^{n+1}}{2\sqrt{u^2 - a}} \right]^2 - a \left[ \frac{(u + \sqrt{u^2 - a})^n - (u - \sqrt{u^2 - a})^n}{2\sqrt{u^2 - a}} \right]^2,$$

ou encore, comme on le voit aisément [\*],

$$Q_{2n} = Q_n^2 - aQ_{n-1}^2.$$

2. La comparaison de cette équation avec (1) nous montre qu'il faut poser

$$y = Q_n, \quad x = Q_{n-1}, \quad bz = Q_{2n}.$$

La valeur  $u$  jusqu'ici est inconnue, et il faudra maintenant résoudre en nombres entiers l'équation

$$(3) \quad Q_{2n} = bz.$$

Or on a, comme on a vu plus haut,

$$Q_{2n} = \frac{(u + \sqrt{u^2 - a})^{2n+1} - (u - \sqrt{u^2 - a})^{2n+1}}{2\sqrt{u^2 - a}},$$

et, par conséquent, l'équation (3) se transforme comme il suit :

$$(4) \quad \frac{(u + \sqrt{u^2 - a})^{2n+1} - (u - \sqrt{u^2 - a})^{2n+1}}{2\sqrt{u^2 - a}} = \dot{b},$$

où  $\dot{b}$  est le symbole connu introduit par Crelle pour désigner un nombre entier quelconque divisible par  $b$ . Le binôme nous conduit

---

[\*] Comparez, au besoin, la Note élémentaire qui suit l'article de M. Günther.

enfin de l'équation (4) à la forme développée

$$(5) \quad \begin{cases} \binom{2n+1}{1} u^{2n} + \binom{2n+1}{3} u^{2n-2} (u^2 - a) \\ + \binom{2n+1}{5} u^{2n-4} (u^2 - a)^2 + \dots + \binom{2n+1}{2n+1} (u^2 - a)^n = b, \\ \left[ \binom{\nu}{\omega} = \frac{\nu(\nu-1)(\nu-2)\dots(\nu-\omega+1)}{1.2.3\dots\omega} \right]. \end{cases}$$

On regardera comme inconnues, dans cette équation, les deux nombres  $u$  et  $n$ , et la discussion complète exigera la distinction de plusieurs cas séparés.

3. Soit d'abord  $a$  multiple de  $b$ , par exemple,  $a = Mb$ . Alors il suffira évidemment de faire  $u = Mbu'$  ( $u'$  arbitraire) pour satisfaire à notre condition; d'où ce théorème :

I. *Pourvu que le coefficient de  $y^2$  soit  $= M \times$  le coefficient de  $z$  (le module) et  $u'$  un nombre quelconque entier et positif, la congruence*

$$y^2 \equiv ax^2 \pmod{b}$$

*a pour solution certains dénominateurs des réduites de la fraction continue*

$$\frac{a}{2Mu'} - \frac{a}{2Mu' \dots}$$

*car on trouvera, pour l'équation*

$$y^2 - ax^2 = bz,$$

*les valeurs*

$$z = \frac{1}{b} Q_{2n}, \quad y = Q_n, \quad x = Q_{n-1}.$$

$u'$  et  $n$  représentent des nombres entiers et positifs quelconques; on a deux séries de  $\infty$  valeurs satisfaisant à notre congruence.

*Exemple.* — Soit proposée l'équation

$$y^2 - 4x^2 = 2z, \quad a = 2.2, \quad b = 1.2, \quad M = 2.$$

Si l'on pose  $u' = 3$ , il faut considérer la fraction continue

$$\frac{4}{12 - \frac{4}{12 - \dots}}$$

d'où l'on déduit les valeurs ( $n = 2$ ),

$$z = \frac{1}{2} Q_{2,2} = 9512, \quad y = Q_2 = 140, \quad x = Q_1 = 12.$$

On peut vérifier, en effet, l'identité

$$140^2 - 4 \cdot 12^2 = 2 \cdot 9512.$$

4. Tous les autres cas se ramènent à la résolution de la congruence quadratique

$$u^2 \equiv a \pmod{b}.$$

On sait que ce problème se trouve résolu dans les *Disquisitiones arithmeticae* de Gauss, et nous pouvons donc le supposer connu; nous nous contentons de résumer cette solution comme il suit.

La congruence proposée possède des racines, si l'on peut regarder  $a$  comme résidu quadratique de  $b$ . Or soit

$$b = r^m s^n t^p, \quad \dots,$$

où l'on entend par  $r, s, t, \dots$  des nombres premiers quelconques (1 et 2 inclus); alors le nombre  $a$  est toujours résidu quadratique de  $b$ , si l'on a [\*]

$$aRr, \quad aRs, \quad aRt \dots$$

Naturellement, il y a aussi des cas où la congruence ne possède pas une seule racine; si  $b$ , par exemple, est un nombre premier satisfaisant à la congruence

$$a^{\frac{b-1}{2}} \equiv -1 \pmod{b},$$

---

[\*] La notation  $aRr$  signifie, dans Gauss,  $a$  résidu quadratique de  $r$ .

il est impossible de trouver un nombre tel que

$$u^2 - a = b.$$

Mais, en général, nous supposerons qu'il existe  $k$  racines

$$u_1, u_2, u_3, \dots, u_i, \dots, u_k.$$

Nous prenons ici le mot *racine* dans le sens déterminé de Gauss; mais il est clair que chaque valeur

$$u_i \pm mb$$

satisfait également à la congruence  $u^2 \equiv a \pmod{b}$ .

5. Soit d'abord  $b$  impair  $= 2c + 1$ ; alors on voit que toute expression de la forme ( $p$  arbitraire)

$$\left[ \binom{(2p-1)(2c+1)}{\rho} \right] [\rho < (2p-1)(2c+1)]$$

est divisible par  $b$ , et l'on arrive au théorème suivant :

II. *La congruence*

$$y^2 \equiv ax^2 \pmod{2c+1}$$

peut être résolue dès qu'on connaît le dénominateur d'une réduite d'indice

$$(2p-1)(2c+1) - 1 = 2$$

de la fraction continue

$$\frac{a}{2u_i - \frac{a}{2u_i - \dots}} [u_i^2 \equiv a \pmod{2c+1}].$$

On obtiendra, en effet,

$$z = \frac{1}{b} Q_{(2p-1)(2c+1)-1}, \quad y = Q_{\frac{1}{2}[(2p-1)(2c+1)-1]}, \quad x = Q_{\frac{1}{2}[(2p-1)(2c+1)-1]}.$$



*Exemple.* — Soit proposée l'équation

$$y^2 - 4x^2 = 5z = (2 \cdot 2 + 1)z.$$

Comme  $3^2 - 4 = 5$ , on peut poser  $u_1 = 3$ , d'où l'on déduit la fraction continue

$$\frac{4}{6 - \frac{4}{6 - \dots}}$$

En posant  $p = 1$ , nous trouvons

$$z = \frac{1}{5}Q_{s-1} = \frac{1}{5}Q_1 = 176, \quad y = Q_2 = 32, \quad x = Q_1 = 6.$$

On peut vérifier, en effet, que

$$32^2 - 4 \cdot 6^2 = 5 \cdot 176.$$

6. Supposons à présent  $b$  pair. Alors il faut distinguer deux cas spéciaux, selon que l'on aura  $b$  d'une des deux formes

$$2^{2m}(2c + 1) \quad \text{ou} \quad 2^{2m+1}(2c + 1),$$

où  $m$  et  $c$  sont des nombres entiers et positifs quelconques. Le cas

$$b = 2^{2m}(2c + 1)$$

est immédiatement réductible, puisque l'équation

$$y^2 - ax^2 = bz = 2^{2m}(2c + 1)z$$

se transforme de cette manière :

$$\left(\frac{y}{2^m}\right)^2 - a\left(\frac{x}{2^m}\right)^2 = (2c + 1)z,$$

ou, si l'on introduit les inconnues nouvelles  $y'$  et  $x'$ ,

$$y'^2 - ax'^2 = (2c + 1)z.$$

*Exemple.* — Si nous avons l'équation

$$y^2 - 7x^2 = 48z = 2^4(2 \cdot 1 + 1)z,$$

nous la réduisons à la suivante :

$$y'^2 - 7x'^2 = 3z,$$

et, puisqu'on sait que 7 est une racine de la congruence

$$u^2 \equiv 7 \pmod{3},$$

on peut prendre la fraction continue

$$\frac{7}{14 - \frac{7}{14 - \dots}}$$

La substitution  $p = 2$  nous donne les solutions

$$z = \frac{1}{3} Q_8 = 378135891, \quad y' = Q_4 = 34349, \quad x' = Q_3 = 2548,$$

et nous pouvons vérifier l'identité

$$137396^2 - 7 \cdot 10192^2 = 48 \cdot 378135891.$$

L'étude du cas contraire, où

$$b = 2^{2m+1}(2c+1),$$

conduit à un résultat partiellement négatif; car, en appliquant la même méthode de transformation, nous réduisons l'équation

$$y^2 - ax^2 = bz = 2^{2m+1}(2c+1)z$$

à la forme plus simple

$$y'^2 - ax'^2 = 2(2c+1)z,$$

et l'on voit sans aucune difficulté qu'il n'est pas toujours possible de résoudre cette équation par notre méthode; car, si nous considérons la formule (5), nous trouvons que le dernier terme  $(u^2 - a)$  n'est divisible par  $b$  que dans ces deux cas :

$$\left. \begin{array}{l} a \text{ impair, } u \text{ impair} \\ a \text{ pair, } u \text{ pair} \end{array} \right\} u^2 - a = 2.$$

Dans le premier cas, il n'y a pas de solution, parce que la somme

$$\binom{2n+1}{3} u^{2n-2} (u^2 - a)^2 + \dots + \binom{2n+1}{2n+1} (u^2 - a)^n$$

est divisible par 2, mais non le premier terme  $(2n+1)u^{2n}$ , qui est toujours un nombre impair. Pour le deuxième cas, on peut se servir de la remarque suivante. Le nombre  $u_i = 2u'_i$ , comme on le suppose, est toujours pair. On fera donc

$$2n+1 = (2p-1)(2c+1), \quad [p \geq 1],$$

et l'on obtiendra

$$(2n+1)u^{2n} = (2p-1)(2c+1)2^{2n}u_i^{2n} = [2(2c+1)].$$

*Exemple.* — Si nous avons l'équation

$$y^2 - 6x^2 = 10z = 2(2 \cdot 2 + 1)z,$$

nous trouvons d'abord la racine  $u_i = 2u'_i = 2 \cdot 3$ ; prenons alors la fraction continue

$$\frac{6}{12 - \frac{6}{12 - \dots}}$$

les dénominateurs des réduites nous donnent, pour  $p = 1$ , les valeurs

$$z = \frac{1}{10}Q_1 = 1818, \quad y = Q_2 = 138, \quad x = Q_1 = 12.$$

Voici la solution complète que l'on obtient ainsi :

$$138^2 - 6 \cdot 12^2 = 18180;$$

et de plus deux autres relations équivalentes :

$$69^2 - 6 \cdot 6^2 = 4545;$$

$$23^2 - 6 \cdot 2^2 = 505.$$

Maintenant nous pouvons regarder comme finie la discussion de tous les cas possibles de la congruence proposée.

NOTE.

La valeur de  $Q_n$  et la formule fondamentale

$$Q_n = Q_n^2 - a Q_{n-1}^2$$

peuvent s'établir d'une manière élémentaire, comme il suit. Posons

$$\sqrt{u^2 - a} = v, \quad u + v = s, \quad u - v = d,$$

ce qui donne

$$2u = s + d, \quad 2v = s - d, \quad a = u^2 - v^2 = ds.$$

On trouve immédiatement

$$Q_1 = 2u = s + d = \frac{s^2 - d^2}{s - d},$$

$$Q_2 = 4u^2 - a = s^2 + 2ds + d^2 - ds = \frac{s^3 - d^3}{s - d},$$

$$Q_3 = (4u^2 - a)2u - a.2u = \frac{s^4 - d^4}{s - d}.$$

Ces valeurs font pressentir que la loi est générale, ou que l'on a

$$Q_{n-2} = \frac{s^{n-1} - d^{n-1}}{s - d}, \quad Q_{n-1} = \frac{s^n - d^n}{s - d}, \quad \dots$$

En effet, on déduit de ces relations et de la formule

$$Q_n = 2u Q_{n-1} - a Q_{n-2}$$

la valeur

$$Q_n = \frac{(s + d)(s^n - d^n) - sd(s^{n-1} - d^{n-1})}{s - d} = \frac{s^{n+1} - d^{n+1}}{s - d}.$$

Une fois ce résultat obtenu, la vérification de la formule fondamentale se fait par un calcul très-simple, identique au fond à celui qui termine le n° 1 de l'article de M. Günther.

P. MANSION.