ACTA ARITHMETICA
XVII (1971)

Sur la solubilité en nombres entiers des équations du second degré à deux indéterminées

par

TRYGVE NAGELL (Uppsala)

§ 1. Introduction. Résultats antérieurs

1. Pour certains ensembles d'équations diophantiennes à deux indéterminées il existe des résultats du type suivant: Parmi les équations appartenant au même ensemble il y a au plus une seule équation qui est résoluble en nombres entiers rationnels. Quelquefois il y a exactement deux équations résolubles.

Il y a de tels résultats sur des ensembles d'équations quadratiques; voir [5](1) et [6]. Pour des résultats analogues sur les équations cubiques, biquadratiques et même de degré > 4 voir [7], [3], [4] et [1]. Dans [8], § 4, j'ai donné un aperçu de tous ces résultats.

2. Dans les travaux [5] et [6] j'ai établi le résultat suivant:

THÉORÈME 1. *Soit donné le nombre naturel $D \geqslant 2$ qui n'est divisible par aucun carré > 1. De plus, soient A et B des nombres naturels variables tels que $AB = D$ et $1 \leqslant A < B$. Pour toutes les valeurs permises de A et B nous considérons l'ensemble des équations*

$$Ax^2 - By^2 = E, \tag{1}$$

où $E = \pm 1$ et ± 2 pour D impair et $E = \pm 1$ pour D pair.

Alors, abstraction faite de l'équation

$$x^2 - Dy^2 = 1, \tag{2}$$

il y a dans cet ensemble exactement une et une seule équation qui est résoluble en nombres naturels x et y.

Cette équation résoluble, distincte de l'équation (2), sera appelée *l'équation singulière* de l'ensemble. Dans ce qui suivra nous la désignerons par

$$A^*x^2 - B^*y^2 = E^*, \tag{3}$$

où $A^*B^* = D$, $1 \leqslant A^* < B^*$ et $E^* = \pm 1$ ou ± 2.

(1) Les numéros figurant entre crochets renvoient à la bibliographie placée à la fin de ce mémoire.

Lorsque D est impair le nombre E^* peut prendre toutes les quatre valeurs possibles, ainsi qu'on le voit des exemples suivants;

$$D = 3, \qquad x^2 - 3y^2 = -2;$$

$$D = 5, \qquad x^2 - 5y^2 = -1;$$

$$D = 7, \qquad x^2 - 7y^2 = +2;$$

$$D = 33, \qquad 3x^2 - 11y^2 = +1.$$

Pour D pair, on a les exemples suivants:

$$D = 6, \qquad 2x^2 - 3y^2 = -1;$$

$$D = 14, \qquad 2x^2 - 7y^2 = +1.$$

Nous désignons l'ensemble défini dans le Théorème 1 par le symbole $[D, A, B; E]$. Si D est le produit de r nombres premiers, le nombre d'équations dans cet ensemble est $= 2^{r+1}$ ou $= 2^r$ suivant que D est impair ou pair.

Un résultat analogue est donné par le

THÉORÈME 2. *Soit donné le nombre naturel* $D \equiv 5 \pmod 8$ *qui n'est divisible par aucun carré* > 1. *De plus, soient* A *et* B *des nombres naturels variables tels que* $AB = D$ *et* $1 \leqslant A < B$. *Supposons que l'équation*

$$x^2 - Dy^2 = 4 \tag{4}$$

soit résoluble en nombres naturels impairs x *et* y. *Pour toutes les valeurs permises de* A *et* B *nous considérons l'ensemble des équations*

$$Ax^2 - By^2 = \pm 4. \tag{5}$$

Alors, abstraction faite de l'équation (4), *il y a dans l'ensemble* (5) *exactement une et une seule équation qui est résoluble en nombres naturels impairs* x *et* y.

Si D est le produit de r nombres premiers, le nombre d'équations dans l'ensemble de ce théorème est $= 2^r$.

On peut se demander s'il est possible de généraliser le Théorème 1 et établir un résultat analogue pour un ensemble d'équations

$$Ax^2 - By^2 = EN,$$

où A, B, D et E ont les mêmes significations que dans le Théorème 1, et où N est un nombre naturel impair > 1.

Nous désignons l'ensemble ainsi défini par le symbole $[D, A, B; EN]$.

Dans le paragraphe suivant nous allons traiter le cas où N est un nombre premier impair, qui ne divise pas D.

§ 2. Les ensembles $[D, A, B; Ep]$

3. Soient D, A, B et E des nombres définis comme dans le Théorème 1, et soit p un number premier fixe $\geqslant 3$ qui ne divise pas D. Cela étant, nous considérons l'ensemble $[D, A, B; Ep]$ constitué de toutes les équations permises de la forme

$$Ax^2 - By^2 = Ep.$$

Parmi ces équations nous distinguons deux catégories: La *première catégorie* avec $E = \pm 1$; la *seconde catégorie* avec $E = \pm 2$.

Supposons maintenant qu'il existe deux équations résolubles appartenant à la même catégorie, savoir

$$Ax^2 - By^2 = Ep \tag{6}$$

et

$$A_1x_1^2 - B_1y_1^2 = E_1p. \tag{7}$$

Alors on a $AB = A_1B_1 = D, 1 \leqslant A < B, 1 \leqslant A_1 < B_1$ et $|E| = |E_1|$. Les nombres Ax/y et A_1x_1/y_1 sont des solutions de la congruence

$$z^2 \equiv D \pmod p.$$

Les signes de ces nombres peuvent évidemment être choisis de façon qu'on ait

$$A_1x_1y \equiv Axy_1 \pmod p. \tag{8}$$

On doit observer que p ne divise pas le produit xyx_1y_1.

Considérons maintenant le produit

$$[(Ax)^2 - Dy^2][(A_1x_1)^2 - Dy_1^2] = EE_1AA_1p^2.$$

Il peut s'écrire

$$(AA_1xx_1 - Dyy_1)^2 - D(A_1yx_1 - Axy_1)^2 = EE_1AA_1p^2. \tag{9}$$

Supposons ensuite que

$$(A, A_1) = A_2, \qquad A = A_2A_3, \; A_1 = A_2A_4,$$

où A_2, A_3 et A_4 sont des nombres naturels, premiers entre eux deux à deux. Alors on obtient de (9) la relation

$$A_3A_4U^2 - \frac{D}{A_3A_4}V^2 = \pm 1 = \frac{|EE_1|}{EE_1}, \tag{10}$$

où les quantités

$$U = \frac{1}{Ep}\left[A_2xx_1 - \frac{D}{AA_4}yy_1\right] \tag{11}$$

et

$$V = \frac{1}{Ep}[A_3xy_1 - A_4x_1y] \tag{12}$$

sont des nombres entiers en vertu de la congruence (8) et en vertu du fait que pour $|E| = |E_1| = 2$ tous les nombres $D, A, A_1, A_2, A_3, A_4, x, y, x_1$ et y_1 sont impairs.

Pour l'équation (10) il existe deux possibilités: Ou elle coïncide avec l'équation $x^2 - Dy^2 = 1$, ou elle coïncide avec l'équation singulière (3) de l'ensemble $[D, A, B; E]$. Vu que dans (10) le terme à droite est ± 1, le dernier cas se présente seulement lorsque $E^* = \pm 1$; la possibilité $E^* = \pm 2$ est donc exclue dans le présent cas.

Il y aura donc deux possibilités à examiner. Nous allons d'abord montrer que le cas où l'équation (10) coïncide avec l'équation $x^2 - Dy^2 = 1$ ne peut exister.

4. Premier cas. L'équation (10) coïncide avec l'équation $U^2 - DV^2 = 1$. Si on prend le signe inférieur dans (10) il faut que $D = A_3 A_4$. Donc

$$BB_1 = \frac{D^2}{A_2^2 A_3 A_4} = \frac{D}{A_2^2},$$

ce qui entraîne $A_2 = 1$ et par suite $BB_1 = D$, d'où $B = A_1$ et $B_1 = A$. Or, cela est impossible vu que $1 \leqslant A < B$ et $1 \leqslant A_1 < B_1$.

Prenons ensuite le signe supérieur dans (10). Alors il faut que $A_3 A_4 = 1$. Donc $A_3 = A_4 = 1$ et $A = A_1$ et par suite $B = B_1$. Cela entraîne que $E_1 = -E$.

Donc, l'équation (7) aura la forme

$$Ax_1^2 - By_1^2 = -Ep.$$

Cependant, cela entraîne que le terme à droite dans (10) soit égal à -1. Or, nous venons de montrer qu'on ne peut pas avoir le signe inférieur dans (10).

Second cas. L'équation (10) coïncide avec l'équation singulière (3) de l'ensemble $[D, A, B; E]$, savoir

$$A^* U^2 - B^* V^2 = E^*. \tag{13}$$

Ici on a $A^* B^* = D$. En supprimant la condition $1 \leqslant A^* < B^*$ nous pouvons supposer que $E^* = +1$. Le cas $A^* = 1, B^* = D$, que nous venons de traiter, peut être exclu. Sans rien perdre de la généralité nous pouvons supposer que $A \geqslant A_1$.

Si on prend le signe supérieur dans (10) il faut que

$$A^* = A_3 A_4 \quad \text{et} \quad B^* = \frac{D}{A_3 A_4} = \frac{AB}{A_3 A_4}.$$

Il en résulte, vu que $(A_3, A_4) = 1$,

$$(A, A^*) = (A_2 A_3, A_3 A_4) = A_3$$

et de plus

$$\frac{B^*}{(B, B^*)} = A_2 \frac{B}{A_4 (B, B^*)}.$$

On en conclut que

$$B = A_4 (B, B^*) \quad \text{et} \quad B_1 = \frac{D}{A_1} = \frac{AB}{A_2 A_4} = A_3 (B, B^*).$$

Par conséquent on aura

$$B_1 = (A, A^*)(B, B^*), \tag{14}$$

$$A_1 = \frac{D}{(A, A^*)(B, B^*)}. \tag{15}$$

Il faut contrôler qu'on a $A_1 < B_1$. En effet, il résulte en vertu de la condition $A \geqslant A_1$ que $A_3 \geqslant A_4$. Des formules (14) et (15) on obtient

$$\frac{A_1}{B_1} = \frac{D}{(A, A^*)^2 (B, B^*)^2},$$

d'où, vu que

$$(A, A^*) = A_3 \quad \text{et} \quad (B, B^*) = \frac{B}{A_4},$$

$$\frac{A_1}{B_1} = \frac{A}{B} \left(\frac{A_4}{A_3} \right)^2 < 1.$$

Si on prend le signe inférieur dans (10) on aura au lieu des formules (14) et (15) les relations

$$B_1 = (A, B^*)(B, A^*), \tag{16}$$

$$A_1 = \frac{D}{(A, B^*)(B, A^*)}. \tag{17}$$

Donc, A_1 et B_1 sont univoquement déterminés lorsque A et B sont données, par les formules (14) et (15) si $E = E_1$ et par les formules (16) et (17) si $E = -E_1$. A^* et B^* sont univoquement déterminés lorsque D est donné.

Il résulte du raisonnement précédent qu'une troisième équation résoluble de la même catégorie ne peut pas exister.

S'il y a une équation résoluble dans l'ensemble, il y en a une seconde équation résoluble dans la même catégorie lorsque l'équation (13) est résoluble. En effet, lorsque les nombres $A, B, E, x, y, A^*, B^*, U$ et V sont connus et si $E = E_1$, on peut d'abord déterminer A_1 et B_1 à l'aide

de formules (14) et (15) et puis x_1 et y_1 à l'aide des formules (11) et (12), qui prennent alors la forme

$$EUp = (A, A^*)xx_1 - (B, B^*)yy_1,$$

$$EVp = \frac{A}{(A, A^*)}xy_1 - \frac{B}{(B, B^*)}x_1y.$$

Il en résulte

$$x_1 = \frac{A}{(A, A^*)}Ux + (B, B^*)Vy, \tag{18}$$

$$y_1 = \frac{B}{(B, B^*)}Uy + (A, A^*)Vx, \tag{18'}$$

ce qui montre que x_1 et y_1 sont des nombres entiers.

Dans le cas de $E_1 = -E$ il faut appliquer les formules (16) et (17) pour déterminer A_1 et B_1. Pour obtenir les valeurs de x_1 et y_1 dans ce cas on aura seulement d'échanger A et B, ainsi que U et V, dans les formules (18) et (18').

Il est évident que la possibilité $A = A_1, B = B_1$ ne peut se présenter que pour $E_1 = -E$.

5. Supposons maintenant que les deux équations suivantes de catégories différentes soient résolubles à la fois:

$$Ax^2 - By^2 = Ep = \pm 2p, \tag{19}$$

$$A_1x_1^2 - B_1y_1^2 = E_1p = \pm p. \tag{20}$$

Alors tous les nombres D, A, B, A_1 et B_1 sont impairs. La congruence (8) pour les nombres x, y, x_1 et y_1 est toujours satisfaite.

En appliquant la même méthode que dans le numéro 3 sur le produit

$$[(Ax)^2 - Dy^2][(A_1x_1)^2 - Dy_1^2]$$

nous aurons une équation analogue à (10), de la forme

$$A^*U^2 - B^*V^2 = EE_1 = \pm 2,$$

où $A^*B^* = D$, et où U et V sont des nombres entiers. Cette équation est nécessairement l'équation singulière dans l'ensemble $[D, A, B; E]$.

Nous venons de voir tout à l'heure que pour l'existence de deux équations de la même catégorie une condition nécessaire est que l'équation singulière de l'ensemble $[D, A, B; E]$ soit de la forme

$$A^*U^2 - B^*V^2 = \pm 1.$$

On en conclut: S'il existe deux équations résolubles de catégories différentes, ces équations sont les seules résolubles dans l'ensemble $[D, A, B; Ep]$.

Par conséquent, nous avons établi le

THÉORÈME 3. *Dans l'ensemble* $[D, A, B; Ep]$ *il y a exactement deux équations résolubles, s'il y en a une. Il y a les quatre possibilités suivantes*: 1° *Il n'y a aucune équation résoluble*; 2° *Deux équations de la première catégorie sont résolubles*; 3° *Deux équations de la seconde catégorie sont résolubles*; 4° *Une seule équation de chacune des deux catégories est résoluble.*

On peut d'ailleurs établir ce résultat à l'aide de la théorie des formes binaires quadratiques. Cependant la présente méthode est evidemment plus simple.

Pour déterminer les équations résolubles dans un ensemble donné on peut p.ex. appliquer la méthode que j'ai devéloppée dans mon livre [9], Chapter VI, no. 58.

Notons le résultat suivant:

Soit donné le nombre naturel D qui est le produit de nombres premiers différents. Alors il existe une infinité de nombres premiers p, tels que l'ensemble $[D, A, B; Ep]$ *contienne deux équations résolubles.*

On le vérifie à l'aide d'un théorème de Weber; voir [10].

6. Nous allons donner quelques exemples numériques pour illustrer les quatre cas dans le Théorème 3. Il est toujours question de l'ensemble $[D, A, B; Ep]$.

Premier cas. Si le nombre D n'est pas un résidue quadratique modulo p, il n'y a aucune équation résoluble dans l'ensemble.

Deuxième cas. Pour $D = 5$ et $p = 11$ les équations résolubles sont

$$x^2 - 5y^2 = 11 \ (x = 4, y = 1) \quad \text{et} \quad x^2 - 5y^2 = -11 \ (x = 3, y = 2).$$

L'équation singulière est

$$x^2 - 5y^2 = -1 \quad (x = 2, y = 1).$$

Pour $D = 78$ et $p = 11$ les équations résolubles sont

$$6x^2 - 13y^2 = 11 \ (x = 2, y = 1) \quad \text{et} \quad 2x^2 - 39y^2 = 11 \ (x = 31, y = 7).$$

L'équation singulière est

$$3x^2 - 26y^2 = 1 \quad (x = 3, y = 1).$$

Pour $D = 6$ et $p = 29$ les équations résolubles sont

$$2x^2 - 3y^2 = 29 \ (x = 4, y = 1) \quad \text{et} \quad x^2 - 6y^2 = -29 \ (x = 5, y = 3).$$

L'équation singulière est

$$2x^2 - 3y^2 = -1 \quad (x = y = 1).$$

Troisième cas. Pour $D = 55$ et $p = 3$ les équations résolubles sont

$$5x^2-11y^2 = -6 \ (x = y = 1) \quad \text{et} \quad x^2-55y^2 = -6 \ (x = 7, y = 1).$$

L'équation singulière est

$$5x^2-11y^2 = 1 \quad (x = 3, y = 2).$$

Quatrième cas. Pour $D = 15$ et $p = 17$ les équations résolubles sont

$$x^2-15y^2 = 34 \ (x = 7, y = 1) \quad \text{et} \quad 3x^2-5y^2 = -17 \ (x = 1, y = 2).$$

L'équation singulière est

$$3x^2-5y^2 = -2 \quad (x = y = 1).$$

Pour $D = 23$ et $p = 13$ les équations résolubles sont

$$x^2-23y^2 = 13 \ (x = 6, y = 1) \quad \text{et} \quad x^2-23y^2 = 26 \ (x = 7, y = 1).$$

L'équation singulière est

$$x^2-23y^2 = 2 \quad (x = 5, y = 1).$$

Finissons par un exemple où le nombre de facteurs premiers de D est relativement grand. Soit D égal au produit de dix nombres premiers différents impairs. Alors l'ensemble $[D, A, B; Ep]$, où p est un nombre premier impair qui ne divise pas D, contient 2048 équations, dont au plus deux sont résolubles.

§ 3. Le cas général d'un ensemble $[D, A, B; EN]$

7. Il est évident que notre méthode pour établir le Théorème 3 peut servir à démontrer un théorème analogue sur les ensembles plus généraux $[D, A, B; EN]$, où N est un nombre naturel composé. Pour simplifier, nous nous bornons au cas dans lequel N est le produit de s nombres premiers impairs distincts. Les nombres D, A, B et E seront définis comme plus haut. Nous supposons que $(D, N) = 1$.

Cela étant, on obtiendra aisément le

THÉORÈME 4. *Supposons que les nombres D, A, B, E et N satisfassent aux conditions indiquées ci-dessus. Alors, le nombre d'équations résolubles dans l'ensemble $[D, A, B; EN]$ est au plus égal à 2^s.*

En effet, pour la démonstration on aura seulement à remplacer partout dans les paragraphes précédents le nombre p par N. Parmi les équations appartenant à l'ensemble $[D, A, B; EN]$ nous distinguons,

comme ci-dessus, deux catégories: La *première catégorie* avec $E = \pm 1$; la *seconde catégorie* avec $E = \pm 2$.

Supposons maintenant qu'il existe deux équations résolubles appartenant à la même catégorie, savoir

$$Ax^2-By^2 = EN \tag{21}$$

et

$$A_1x_1^2-B_1y_1^2 = E_1N. \tag{22}$$

Alors on a $AB = A_1B_1 = D$, $1 \leqslant A < B$, $1 \leqslant A_1 < B_1$, $|E| = |E_1|$ et $(D, N) = 1$. Les nombres Ax/y et A_1x_1/y_1 sont des solutions de la congruence

$$z^2 \equiv D \pmod N. \tag{23}$$

Nous supposons que ces nombres appartiennent à la même classe de congruences modulo N. Donc

$$A_1x_1y \equiv Axy_1 \pmod N. \tag{24}$$

Il est bien connu que le nombre de solutions incongrues de la congruence (23) est égal à 2^s; voir p.ex. [2], p. 47. Alors, la condition donnée par (24) entraîne qu'il y aura au plus 2^{s-1} possibilités pour la paire (21) et (22), abstraction faite de la classification d'après les catégories.

Le même raisonnement s'appliquera à la paire d'équations

$$Ax^2-By^2 = EN = \pm 2N,$$

$$A_1x_1^2-B_1y_1^2 = E_1N = \pm N,$$

qui remplaçera la paire (19) et (20).

Par ailleurs, la démonstration se poursuivra entièrement comme dans le cas de l'ensemble $[D, A, B; Ep]$.

Cependant, il faut observer que le Théorème 4 est illusoire lorsque le nombre s des facteurs premiers de N surpasse le nombre r, éventuellement $r+1$, des facteurs premiers de D.

En utilisant la théorie des idéaux dans le corps quadratique engendré par $\sqrt{D}$ on pourrait obtenir un résultat plus précis.

Remarque 1. Il est évident que le Théorème 3 reste encore vrai si on y remplace le nombre premier p par une puissance de p. Il faut cependant ajouter la condition que p ne divise aucun des produits xy des inconnues.

Remarque 2. Nous avons aussi établi le résultat suivant relatif aux formes définites

$$Ax^2+By^2 = Ep. \tag{25}$$

Soient A, B, D, E et p définis comme au Théorème 3, et soit $A < B$. Si m désigne le nombre d'équations résolubles en nombres entiers x et y parmi les equations (25) on a ou $m = 0$ ou $m = 1$.

Dans le cas exceptionnel

$$x^2+y^2 = Ep,$$

où $p \equiv 1 \pmod 4$ on a évidemment $m = 2$.

Index Bibliographique

[1] A. af Ekenstam, *Contributions to the theory of the Diophantine equation* $Ax^n - By^n = C$, Dissertation, Uppsala 1959.

[2] E. Landau, *Vorlesungen über Zahlentheorie*, Bd. 1, Leipzig 1927.

[3] W. Ljunggren, *Einige Eigenschaften der Einheiten reeller quadratischen und rein-biquadratischer Zahlkörper*, Vidensk. Akad. Skrifter, Matem.-naturv. klasse, nr. 12, Oslo 1936.

[4] — *Solution complète de quelques équations du sixième degré à deux indéterminées*, Archiv for matem. o. naturv., Bd. 48, Nr. 7, Oslo 1946.

[5] T. Nagell, *Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns*, Nova Acta Reg. Soc. Scient. Upsaliensis, Ser. IV, Vol. 16, No. 2, Uppsala 1955.

[6] — *On a special class of Diophantine equations of the second degree*, Arkiv för matem., Bd. 3, Nr. 2, Stockholm 1954.

[7] — *Solution complète de quelques équations cubiques à deux indéterminées*, Journ. de mathém., 9e sér., t. 4, Paris 1925.

[8] — *Remarques sur une classe d'équations indéterminées*, Arkiv för matem., Bd. 8, Nr., Stockholm 1970.

[9] — *Introduction to Number Theory*, New York 1951.

[10] H. Weber, *Beweis des Satzes, dass jede eigentlich primitive quadratische Form unendlich viele Primzahlen darzustellen fähig ist*, Math. Annalen 20 (1882).

Reçu le 14. 12. 1969

ACTA ARITHMETICA
XVIII (1971)

Representations of real numbers by series of reciprocals of odd integers

by

A. Oppenheim (Legon, Ghana)

Harold Davenport in memoriam

1. It is well-known that a real number x between 0 and 1 can be expanded into a series of reciprocals of integers (a "sorites" of Sylvester) originally found by Lambert (see Perron [2]) as follows:

$$x = x_1 = \frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \dots \tag{1.1}$$

where the positive integers a_i are given in succession uniquely by the algorithm

$$a_i = 1 + [1/x_i], \quad x_{i+1} = x_i - \frac{1}{a_i}, \quad 0 < x_{i+1} < x_i, \quad \dots \tag{1.2}$$

The process is unending: the integers a_i satisfy the inequalities

$$a_i \geqslant 2, \quad a_{i+1} \geqslant a_i^2 - a_i + 1 \quad (i \geqslant 1). \tag{1.3}$$

A convergent series (1.1) in which the integers a_i satisfy (1.3) is necessarily the Sylvester expansion of its sum. For rational x equality must occur eventually in (1.3), i.e. for all $i > i_0$, $a_{i+1} = a_i^2 - a_i + 1$. The converse is trivially true.

I have taken the algorithm so that the process is non-ending. If we take $1/a_i \leqslant x_i < 1/(a_i - 1)$, the process ends for rational x; for irrational numbers the two processes naturally yield the same series.

Variations of (1.1) exist in which signs can be attached to the terms in accordance with prescribed rules (and appropriate changes in (1.3)).

2. Engel (anticipated by Lambert: see Perron [2]) obtained another kind of series for x in $(0, 1)$:

$$x = \frac{1}{c_1} + \frac{1}{c_1 c_2} + \frac{1}{c_1 c_2 c_3} + \dots, \tag{2.1}$$