ARKIV FÖR MATEMATIK Band 7 nr 17

1.67 03 1 Communiqué le 8 Février 1967

Sur quelques propriétés arithmétiques des formes binaires à coefficients entiers

Par TRYGVE NAGELL

§ 1. Remarques sur la représentabilité d'un nombre entier donné par une forme binaire

1. Lemmes. Dans ce travail polynome (forme) signifie un polynome (forme) à coefficients entiers rationnels.

Il est facile d'établir les résultats suivants :

Lemme 1. *Soit $f(x)$ un polynome (non constant) dont tous les zéros sont simples, et soit p un nombre premier tel que la congruence*

$$f(x) \equiv 0 \pmod{p}$$

soit résoluble. Alors, si p ne divise pas le discriminant de $f(x)$, on peut trouver une infinité de nombres entiers x_0 (positifs et négatifs) tels que le nombre $f(x_0)$ soit divisible par p et non par p^2.

Lemme 2. *Soient $f(x)$ et $g(x)$ des polynomes tels que l'équation $f(x)g(x)=0$ n'ait aucune racine double. Soit x_0 un nombre entier tel que chacun des nombres $f(x_0)$ et $g(x_0)$ soit divisible par le nombre premier p. Alors, le résultant $R(f(x), g(x))$ est divisible par p.*

On trouvera une démonstration du lemme 1 dans Nagell [1][1], p. 346.

Démonstration du lemme 2. En vertu des conditions on a les identités

$$f(x) = (x - x_0)\, f_1(x) + p f_2(x),$$
$$g(x) = (x - x_0)\, g_1(x) + p g_2(x),$$

où $f_1(x)$, $f_2(x)$, $g_1(x)$ et $g_2(x)$ sont des polynomes. On en conclut

$$R(f(x) - p f_2(x), g(x) - p g_2(x)) = 0. \tag{1}$$

Vu que le résultant de deux polynomes est une fonction (entière) symétrique à coefficients entiers des coefficients de ces polynomes, on aura, en considérant l'équation (1) modulo p,

$$R(f(x), g(x)) \equiv 0 \pmod{p},$$

et le lemme 2 se trouve démontré.

A l'aide de ces lemmes on peut établir le

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

Lemme 3. *Soit $F(x)$ un polynome ayant la propriété suivante : Pour toute valeur entière de x le nombre entier $F(x)$ est une m-ième puissance, m étant un nombre naturel $\geqslant 2$. Alors, le polynome $F(x)$ est la m-ième puissance d'un polynome.*

Démonstration. Il est évident que $F(x)$ peut s'écrire sous la forme

$$F(x) = c[f_1(x)]^{n_1}\,[f_2(x)]^{n_2} \ldots [f_r(x)]^{n_r}, \tag{2}$$

où c est un nombre entier différent de zéro, où $f_1(x)$, $f_2(x)$, ..., $f_r(x)$ sont des polynomes irréductibles distincts, et où les exposants $n_1, n_2, \ldots, n_r$ sont des nombres naturels. Alors tous les résultants

$$R_{i,j} = R(f_i(x), f_j(x)),$$

$i \neq j$, sont différents de zéro. Désignons par D_i le discriminant du polynome $f_i(x)$, $1 \leqslant i \leqslant r$.

Soit p un nombre premier qui ne divise aucun des nombres c, D_i, $R_{i,j}$, et supposons que la congruence

$$f_k(x) \equiv 0 \pmod{p}$$

est résoluble pour une certaine valeur de k. Alors, d'après le lemme 1, il existe une valeur entière de x, soit x_0, telle que $f_k(x_0)$ soit divisible par p et non par p^2. D'après le lemme 2 il est clair que aucun des nombres $f_i(x_0)$, pour $i \neq k$, n'est divisible par p. Donc, il résulte de la relation (2) que $F(x)$ est divisible par p^{n_k} et non par p^{n_k+1}. On en conclut que n_k est divisible par m. Par conséquent, tous les exposants n_i, pour $1 \leqslant i \leqslant r$, sont divisibles par m. Cela entraîne que le nombre c est une m-ième puissance, et le lemme 3 se trouve ainsi démontré.

Remarque. Dans l'énoncé du lemme 3 on peut évidemment remplacer la condition « Pour toute valeur entière de x », par la condition « Pour toute valeur entière de x surpassant une limite donnée ».

Nous avons aussi besoin du résultat suivant:

Lemme 4. *Soit p un nombre premier et soit A un nombre naturel qui n'est pas la p-ième puissance d'un nombre naturel. Alors, il existe une infinité de nombres premiers q tels que la congruence*

$$x^p \equiv A \pmod{q}$$

ne soit pas résoluble. La densité de ces nombres premiers est positive.

Cette proposition est un corollaire d'un résultat établi par Hilbert: voir Hilbert [2], Satz 152.

D'ailleurs, le lemme 4 est contenu dans la proposition plus générale que voici:

Lemme 5. *Soit $f(x)$ un polynome irréductible d'un degré $\geqslant 2$. Alors, il y a une infinité de nombres premiers q tels que la congruence*

$$f(x) \equiv 0 \pmod{q}$$

ne soit pas résoluble. La densité de ces nombres premiers est positive.

Ce résultat est une conséquence des lois de densité de Frobenius–Tchebotareff. En effet, ces lois permettent de conclure qu'il y a une infinité de nombres premiers, de densité positive, qui ne sont divisibles par aucun idéal premier du premier degré dans les corps algébriques engendrés par l'équation $f(x) = 0$. Voir Hasse [3], §§ 23–24.

2. Formes binaires qui ne représentent pas un nombre entier donné. Nous désignerons par le symbole $((a_0, a_1, \ldots, a_n))$ la forme binaire de degré $n(\geqslant 2)$

$$F(x, y) = a_0 x^n + a_1 x^{n-1} y + \ldots + a_n y^n,$$

où les coefficients $a_0, a_1, \ldots, a_n$ sont entiers. Si la forme est définite a_0 et a_n sont supposés positifs. Supposons que la forme est irréductible dans le domaine rationnel, et soit $\mathbf{K}$ un corps du n-ième degré engendré par l'équation

$$a_0 x^n + a_1 x^{n-1} + \ldots + a_n = 0.$$

Nous dirons alors que la forme $F(x, y)$ est construite sur $\mathbf{K}$.

Dans un travail qui vient de paraître nous avons etudié les représentations de l'unité par une forme biquadratique du premier rang. Nous avons, entre autres, montré qu'il existe au plus 8 représentations de l'unité si les corps engendrés par la forme admet un souscorps quadratique; voir Nagell [4].

Dans d'autres travaux nous avons traité la question analogue pour les formes cubiques binaires de discriminant négatif. Ces formes admettent au plus 3 représentations de l'unité, exception faite des trois classes de formes représentées par $((1, 1, 0, -1))$, $((1, 0, 1, -1))$ et $((1, 1, 1, -1))$ qui admettent exactement 5, 4 et 4 représentations respectivement: voir Nagell [5], [6] et [7].

D'autre part on peut montrer l'existence de formes binaires qui ne peuvent pas représenter l'unité. En effet, nous allons établir le

Théorème 1. *Soit* $\mathbf{K}$ *un corps algébrique du n-ième degré,* $n \geqslant 3$, *et soit c un nombre entier rationnel quelconque* $\neq 0$. *Alors, il existe une infinité de classes de formes binaires du n-ième degré construites sur le corps* $\mathbf{K}$, *qui ne peuvent pas représenter le nombre c.*

Démonstration. Soit

$$F(x, y) = x^n + a_1 x^{n-1} y + \ldots + a_n y^n$$

une forme construite sur $\mathbf{K}$. Supposons d'abord que c n'est pas de la forme d^p, d nombre entier et p nombre premier divisant n. D'après le lemme 4 il existe une infinité de nombres premiers q tels que c ne soit pas un reste p-ième modulo q. Alors, il est évident que la forme $F(x, qz)$ ne peut pas représenter le nombre c.

Supposons ensuite que $c = d^p$, d nombre entier et p nombre premier divisant n. Par la transformation

$$x = eu + fqv, \; y = gu + hqv,$$

où e, f, g, h et q sont des nombres entiers tels que $eh - fg \neq 0$, la forme $F(x, y)$ sera transformée dans la forme

$$G(u, v) = F(e, g)\, u^n + b_1 q u^{n-1} v + \ldots + b_n q^n v^n,$$

où les coefficients $b_1, \ldots, b_n$ sont entiers. D'après le lemme 3 il est évident qu'on peut choisir les nombres e et g tels que $F(e, g)$ ne soit pas une p-ième puissance. Alors,

d'après le lemme 4 il existe une infinité de nombres premiers q tels que $F(e, g)$ ne soit pas un reste p-ième modulo q. Donc, la forme $G(u, v)$ ne peut pas représenter le nombre $c = d^p$, et le théorème 1 se trouve démontré.

Le résultat suivant est une conséquence immédiate du lemme 5.

Théorème 2. *Soit $F(x, y)$ une forme binaire irréductible, ayant le diviseur fixe maximal δ. Alors, il existe une infinité de nombres entiers, premiers entre eux deux à deux, qui ne peuvent pas être représentés par la forme $F(x, y)/\delta$.*

Ce théorème est, bien entendu, aussi vrai pour une forme réductible qui n'est pas le produit de formes linéaires à coefficients rationnels.

§ 2. Remarques sur les formes binaires biquadratiques du premier rang

3. Sur le nombre de représentations d'un nombre entier dans quelques cas particuliers. Dans un mémoire publié récemment nous avons étudié les représentations de l'unité par des formes du type en question; voir [4]. Dans ce qui suivra nous allons continuer les recherches commencées dans ce mémoire; les notions seront les mêmes. Nous allons étudier l'équation biquadratique

$$N(x - \theta y) = a, \tag{3}$$

où θ est un nombre entier du quatrième degré qui engendre le corps $\mathbf{K}(\theta)$ *imprimitif* et du premier rang; ici N signifie la norme dans $\mathbf{K}(\theta)$; a est un nombre naturel > 1. Nous désignons par $\tau(a)$ le nombre d'idéaux principaux de norme a. Nous allons montrer comment on peut, dans certains cas, trouver une limite supérieure, relativement basse du nombre de solutions de l'équation (3) en nombres entiers rationnels x et y, premiers entre eux, $y \neq 0$. Nous dirons que $x - \theta y$, $(x, y) = 1$, est une solution de (3) lorsque x et y satisfont à cette équation. Deux solutions $x - \theta y$ et $x_1 - \theta y_1$ dont le quotient est une unité, seront appelées *solutions associées*. Si $x - \theta y$ est une solution, $-x + \theta y$ l'est aussi.

Il faut distinguer les cas d'après la classe du corps $\mathbf{K}(\theta)$; pour la définition des classes, des unités fondamentales etc. voir [4], p. 483.

Les classes 5 et 7

Dans les corps de ces classes on a $\eta = \varepsilon$. Supposons qu'il existe deux solutions associées de (3). Donc

$$x - \theta y = \pm \varepsilon^n (x_1 - \theta y_1),$$

où n est un nombre entier rationnel. Vu que ε est réel et que θ est imaginaire on en conclut

$$x = \pm \varepsilon^n x_1 \quad \text{et} \quad y = \pm \varepsilon^n y_1.$$

Or cela entraine $n = 0$, $x = \pm x_1$ et $y = \pm y_1$.

Conclusion: Le nombre de solutions de (3) est au plus égal à $2\tau(a)$.

La classe 8

Dans les corps de cette classe on a $\eta=\sqrt{-\varepsilon}$. Nous considérons seulement le cas particulier de $\theta=\sqrt{-\varepsilon}$.

Supposons qu'il existe deux solutions associées de l'équation

$$N(x-\sqrt{-\varepsilon}\,y)=a. \tag{4}$$

Alors nous aurons la relation

$$x-\sqrt{-\varepsilon}\,y=\pm(\sqrt{-\varepsilon})^n\cdot(x_1-\sqrt{-\varepsilon}\,y_1),$$

où n est un nombre entier rationnel. Il suffit de prendre le signe supérieur. Si n est pair on aura comme dans le cas précédent $x=\pm x_1$, $y=\pm y_1$.

Si n est impair $=2m+1$ on aura

$$x=(-\varepsilon)^{m+1}\cdot y_1 \quad \text{et} \quad -y=(-\varepsilon)^m x_1,$$

ce qui est évidemment impossible si $y_1\neq 0$.

Conclusion: Le nombre de solutions de (4) est au plus égal à $2\tau(a)$.

La classe 9

Dans les corps de cette classe on a $\eta=\varepsilon i$. Nous nous limitons au cas particulier de $\theta=\varepsilon i$. Supposons qu'il existe deux solutions associées de l'équation

$$N(x-\varepsilon i y)=a. \tag{5}$$

Alors nous aurons la relation

$$x-\varepsilon i y=\pm(\varepsilon i)^n(x_1-\varepsilon i y_1),$$

où n est un nombre entier rationnel. Il suffit de prendre le signe supérieur. Si n est pair on aura comme tout à l'heure $x=x_1$, $y=y_1$.

Si n est impair $=2m+1$ il faut qu'on ait

$$x=-(-\varepsilon^2)^{m+1}y_1, \quad -y=(-\varepsilon^2)^m x_1.$$

Or, cela entraîne que $m=0$ et $y_1=0$.

Conclusion: Le nombre de solutions de (5) est au plus égal à $2\tau(a)$.

La classe 6

Dans ce cas il n'y a qu'un seul corps dans la classe. Ce corps est engendré par le nombre $\xi=e^{2\pi i/5}$. On a $\eta=\varepsilon=\frac{1}{2}(1+\sqrt{5})$ et $\xi^2=\varepsilon^{-1}\xi-1$. Nous considérons seulement le cas $\theta=\xi$. Supposons qu'il existe deux solutions associées de l'équation

$$N(x-\xi y)=a. \tag{6}$$

Alors nous obtenons la relation

$$x-\xi y=\pm\xi^h\varepsilon^n(x_1-\xi y_1),$$

où n est un nombre entier rationnel, et où h a une des valeurs $0, \pm 1, \pm 2$. Il suffit de prendre le signe supérieur. Si $h = 0$ on aura comme plus haut $x = x_1$, $y = y_1$.

1) Dans le cas $h = 1$ nous obtenons

$$x - \xi y = x_1\xi\varepsilon^n - y_1\xi^2\varepsilon^n = x_1\xi\varepsilon^n - y_1\xi\varepsilon^{n-1} + y_1\varepsilon^n.$$

On en conclut $\qquad x = y_1\varepsilon^n \quad \text{et} \quad -y = x_1\varepsilon^n - y_1\varepsilon^{n-1},$

ce qui est évidemment impossible si $y_1 \neq 0$.

Si $h = -1$ on retombera sur le même cas en échangeant x et x_1, y et y_1 et n et $-n$.

2) Dans le cas $h = 2$ nous obtenons

$$\begin{aligned} x - \xi y &= (\xi\varepsilon^{-1} - 1)(x_1 - \xi y_1)\varepsilon^n \\ &= \xi\varepsilon^{n-1}x_1 - \varepsilon^n x_1 - \xi^2\varepsilon^{n-1}y_1 + \xi\varepsilon^n y_1 \\ &= \xi\varepsilon^{n-1}x_1 - \varepsilon^n x_1 - \xi\varepsilon^{n-2}y_1 + \varepsilon^{n-1}y_1 + \xi\varepsilon^n y_1. \end{aligned}$$

Cela entraîne $\qquad x = -\varepsilon^n x_1 + \varepsilon^{n-1}y_1,$

$$-y = \varepsilon^{n-1}x_1 - \varepsilon^{n-2}y_1 + \varepsilon^n y_1,$$

et par suite $\qquad x - \varepsilon y = y_1\varepsilon^{n+1}.$

D'une manière analogue on obtient

$$x + y = -x_1\varepsilon^{n-1},$$

ce qui entraîne $n = -1$, et par conséquent

$$x - \varepsilon y = y_1.$$

Il faut donc que $y = 0$, ~~valeur que nous avons exclue~~.

Si $h = -2$ on retombe sur le même cas en échangeant x et x_1, y et y_1, et n et $-n$.

Conclusion: Le nombre de solutions de (6) est au plus égal à $2\tau(a)$.

Nous allons revenir prochainement sur l'équation plus générale $N(x - \theta y) = a$, où θ est un entier quelconque générateur du corps.

Nous profitons de l'occasion pour aviser les fautes d'impression suivantes au travail [8]: Dans la ligne 9, p. 161, il faut lire b_1 au lieu de $b_1 - a_2$. Dans la ligne 18, p. 165, il faut ajouter: et $\neq 0$. Dans la ligne 11, p. 168, il faut lire $t\theta$, $t\theta^2$ au lieu de $r\theta$, $r\theta^2$. Dans la ligne 2, p. 177, il faut lire *est* au lieu de *et*.

Il ne serait pas difficile de généraliser les résultats obtenus dans ce chapitre; mais nous nous arrêtons ici.

4. Sur les formes ayant exactement quatre représentations de l'unité. Dans le mémoire [4] nous avons établi le résultat suivant (Théorème 11, p. 509–511):

Soit **K** *un corps quelconque appartenant à une classe qui est différente des deux classes 5 et 7. Alors, il y a une infinité de classes de formes construites sur* **K** *pour lesquelles on a* $M = 4$.

Ici M signifie le nombre de représentations de l'unité par la forme biquadratique. Pour la démonstration de ce théorème il est naturel de considérer la forme

$$N(x - yE),$$

où E est supposée d'être une unité du quatrième degré dans le corps **K**. Il faut cependant observer qu'il y a dans certains corps des anneaux entiers dans lesquels toutes les unités (irrationnelles) sont du second degré. De la manière suivante nous allons simplifier la démonstration de l'existence dans tous les corps en question d'une infinité d'anneaux entiers dans lesquels il y a des unités du quatrième degré. Il suffit de considérer les classes de corps 8, 9, 10, 11, 12, 13 et 14.

Dans la classe 8 on peut prendre

$$E = (\sqrt{-\varepsilon})^{2n+1}.$$

Dans la classe 9 on peut prendre

$$E = i\varepsilon^n.$$

Dans la classe 10 on peut prendre

$$E = (\sqrt{i\varepsilon})^{2n+1}.$$

Dans la classe 11 on peut prendre

$$E = \varrho\varepsilon^n,$$

où ϱ est une racine de l'équation $\varrho^2 + \varrho + 1 = 0$.

Dans la classe 12 on peut prendre

$$E = (\sqrt{-\varepsilon})^{2n+1}.$$

Dans la classe 13 on peut prendre

$$E = \xi\varepsilon^n,$$

où ξ est une racine de l'équation $\xi^4 + 1 = 0$.

Dans la classe 14 enfin on peut prendre

$$E = (\sqrt{i\varepsilon})^{2n+1}.$$

Ici n signifie un nombre naturel; ε signifie l'unité fondamentale dans le sous-corps quadratique réel. Il est évident que E sera toujours du quatrième degré. En faisant accroître le nombre n on aura des unités E dont les discriminants $D(E)$ ne peuvent prendre une valeur donnée qu'un nombre fini de fois. Cela est une conséquence du Théorème 21 de notre mémoire [8]. On aura ainsi, dans tous les corps, une infinité d'anneaux $R(E)$ et de formes $N(x - yE)$ jouissant de la propriété demandée.

Institut de mathématiques, Université, Uppsala, Suède

INDEX BIBLIOGRAPHIQUE

1. NAGELL, T., Généralisation d'un théorème de Tchebycheff, *Journ. de mathém.* 8. série, t. IV, Paris, 1921.
2. HILBERT, D., Die Theorie der algebraischen Zahlkörper, *Jahresber. d. Deutschen Mathem. Vereinigung*, Bd. 4, Berlin 1898.
3. HASSE, H., Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper, Teil II: Reziprozitätsgesetze, *Jahresber. d. Deutschen Mathem. Vereinigung*. Bd. 36, Berlin 1930.

4. NAGELL, T., Sur les représentations de l'unité par les formes binaires biquadratiques du premier rang, *Arkiv för matematik*, Bd. 5, nr. 33, Stockholm 1965.
5. —— Darstellung ganzer Zahlen durch binäre kubische Formen mit negativer Diskriminante, *Mathem. Zeitschrift*, Bd. 28, Berlin 1928.
6. —— Solution complète de quelques équations cubiques à deux indéterminées, *Journ. de mathem. 9.* série, t. IV, Paris 1925.
7. —— Zahlentheoretische Notizen VII. Zur Theorie der binären kubischen Formen mit negativer Diskriminante, *Norsk Matem. Forenings Skrifter*, Ser. 1, Nr. 17, Oslo 1927.
8. —— Contributions à la théorie des modules et des anneaux algébriques, *Arkiv för matematik*, Bd. 6, nr. 9, Stockholm 1965.

Tryckt den 2 oktober 1967

Uppsala 1967. Almqvist & Wiksells Boktryckeri AB