At this point it may be appropriate to recall also the following known (see [2]) fact:

(c) For $n \geqslant 1$, $S_n = H_n(i)$ where $H_n(\tau) = \sum_{m=1}^{\infty} c_n(m) e^{2\pi i m\tau}$ with $c_n(m) = 2\big(1+(1+(-1)^n)\pi m/n\big)\sigma_{-(2n+1)}(m)$ (for n odd, $H_n(\tau) = 2F(\tau)$).

If we define, more generally, $H_n(\tau;\chi) = \sum_{m=1}^{\infty} \chi(m) c_n^*(m) e^{2\pi i m\tau/k}$ with $c_n^*(m) = 2\big(1+(1+(-1)^{n+\delta})\pi m/kn\big)\sigma_{-(2n+1)}(m)$, where $\chi(m)$ is a real, primitive (non-principal!) congruence character modulo $k>1$ and $\delta = (1-\chi(-1))/2$, then $H_n(i,\chi)\pi^{-(2n+1)}$ belongs to the quadratic field generated by $\sqrt{k}$ over the rationals. This result apparently cannot be extended in any obvious way to $\chi(m)$ a principal character.

Neither of these remarks seems to have any direct bearing upon the rationality or transcendency of $\pi^{-(2n+1)}\zeta(2n+1)$.

Bibliography

[1] E. Grosswald, *Die Werte der Riemannschen Zetafunktion an ungeraden Argumentstellen*, Nachrichten der Akad. Wiss. Göttingen (1970), pp. 9–13.

[2] — *Remarks concerning the values of the Riemann zeta function at integral odd arguments* (to appear Journ. Number Theory 4 (1972)).

[3] G. H. Hardy, *A formula of Ramanujan*, Journ. London Math. Soc. 3 (1928), pp. 238–240; Collected Papers IV, pp. 537–539.

[4] S. Ramanujan, *Notebooks*, Facsimile edition in 2 volumes by The Tata Institute of Fundamental Research, Bombay 1957.

[5] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Oxford 1951.

[6] G. N. Watson, *Theorems stated by Ramanujan (II)*, Journ. London Math. Soc. 3 (1928), pp. 216–225.

[7] A. Weil, *Sur une formule classique*, Journ. Math. Soc. Japan 20 (1968), pp. 400–402.

DEPARTMENT OF MATHEMATICS
TEMPLE UNIVERSITY
Philadelphia, Pennsylvania

Received on 23. 11. 1970 (123)

ACTA ARITHMETICA
XXI (1972)

Sur la résolubilité de l'équation $x^2+y^2+z^2 = 0$ dans un corps quadratique

par

TRYGVE NAGELL (Uppsala)

§ 1. Méthode non-constructive

1. Introduction. Pour que l'équation

$$x^2+y^2+z^2 = 0 \tag{1}$$

soit résoluble en nombres x, y, z d'un corps algébrique K (hors le cas $x = y = z = 0$) il faut évidemment que K soit totalement imaginaire ($=$ t. im.). Pour reconnaître si cette équation est résoluble ou non il est naturel d'appliquer le résultat suivant:

LEMME 1. *Soit donné le corps algebrique K t. im. Pour que l'équation* (1) *soit résoluble en nombres entiers x, y, z du corps K (le cas $x = y = z = 0$ étant exclu) il faut et il suffit que la congruence*

$$\xi^2+\eta^2+\zeta^2 \equiv 0 \pmod{\mathfrak{j}}$$

soit résoluble en entiers ξ, η, ζ de K pour tous les idéaux de K, tel qu'on ait $(\xi, \eta, \zeta, \mathfrak{j}) = 1$.

Ce résultat est, bien entendu, un cas particulier d'un théorème de Hilbert sur les formes quadratiques; voir [2](1). Il est évident qu'on peut, dans ce lemme, remplacer l'idéal $\mathfrak{j}$ par l'idéal (N) où N parcourt tous les nombres naturels.

Or, si N est *impair* il est bien connu que la congruence

$$x^2+y^2+z^2 \equiv 0 \pmod{N}$$

est toujours résoluble dans le corps rationnel de manière qu'on ait $(x, y, z, N) = 1$; voir p. ex. [4], p. 192. Donc, on peut remplacer le Lemme 1 par le

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

LEMME 2. *Soit K un corps algébrique t. im. Pour que l'équation* (1) *soit résoluble en nombres entiers x, y, z de K (le cas $x = y = z = 0$ étant exclu) il faut et il suffit que la congruence*

$$\xi^2+\eta^2+\zeta^2 \equiv 0 \pmod{2^m} \tag{2}$$

soit résoluble en entiers ξ, η, ζ de K pour toutes les valeurs entières de m, tel qu'on ait $(\xi, \eta, \zeta, 2) = 1$.

Lorsque l'équation (1) est résoluble dans le corps K, il y a une infinité de solutions. Quand on connaît une solution de (1) on aura toutes les autres par la méthode de sécante; voir p. ex. [4], p. 216.

2. Nous nous proposons d'étudier la résolubilité de l'équation (1) dans le corps quadratique imaginaire engendré par le nombre $\sqrt{-\Delta}$, où Δ est un nombre naturel, qui n'est divisible par aucun carré > 1. Dans le corps $K(\sqrt{-\Delta})$ nous avons les règles suivantes: Si $\Delta \equiv -1 \pmod 8$ l'idéal (2) est le produit de deux idéaux premiers distincts. Si $\Delta \equiv 3 \pmod 8$ l'idéal (2) est un idéal premier. Si $\Delta \equiv 1$ ou $\equiv 2 \pmod 4$ l'idéal (2) est le carré d'un idéal premier.

Dans la suite K signifie le corps $K(\sqrt{-\Delta})$. Il faut distinguer plusieurs cas suivant le reste de Δ modulo 8:

Premier cas: $\Delta \equiv -1 \pmod 8$; deuxième cas: $\Delta \equiv 3 \pmod 8$;
troisième cas: $\Delta \equiv 5 \pmod 8$; quatrième cas: $\Delta \equiv 1 \pmod 8$;
cinquième cas: $\Delta \equiv 2 \pmod 8$; sixième cas: $\Delta \equiv -2 \pmod 8$.

Nous allons montrer que la congruence (2) est toujours résoluble sauf dans le premier cas.

Nous avons besoin du fait élémentaire suivant (voir p. ex. [4], Theorem 72):

LEMME 3. *Si $a \equiv 1 \pmod 8$ la congruence*

$$x^2 \equiv a \pmod{2^m}$$

est résoluble en nombres entiers (rationnels) pour toutes les valeurs de m.

3. Premier cas. Dans ce cas nous avons $(2) = \mathfrak{p}\mathfrak{p}_1$, où $\mathfrak{p}$ et $\mathfrak{p}_1$ sont des idéaux premiers distincts du corps K. Pour tout nombre entier du corps on a

$$\xi^2 \equiv \xi \pmod{\mathfrak{p}}.$$

Si ξ n'est pas divisible par $\mathfrak{p}$, il s'ensuit que $\xi \equiv 1 \pmod{\mathfrak{p}}$ et même $\xi \equiv -1 \pmod{\mathfrak{p}}$, donc

$$\xi^2 \equiv 1 \pmod{\mathfrak{p}^2}. \tag{3}$$

Supposons qu'on ait la relation

$$x^2+y^2+z^2 = 0 \tag{4}$$

en nombres entiers du corps. Nous pouvons supposer que deux des nombres x, y, z soient indivisibles par $\mathfrak{p}$. En effet, soit x divisible par $\mathfrak{p}^m$ et non par $\mathfrak{p}^{m+1}$, soit y divisible par $\mathfrak{p}^n$ et non par $\mathfrak{p}^{n+1}$, et soit z divisible par $\mathfrak{p}^s$ et non par $\mathfrak{p}^{s+1}$. Supposons de plus que

$$1 \leqslant m \leqslant n \leqslant s.$$

Alors, il faut évidemment que $m = n$. Si x_1 est le nombre conjugué à x nous aurons en multipliant (4) par x_1^2 la relation

$$(xx_1)^2+(yx_1)^2+(zx_1)^2 = 0,$$

où $xx_1 = 2^m u$ et $yx_1 = 2^m v$, u et v étant des nombres entiers dans K non divisibles par $\mathfrak{p}$. Donc, $w = zx_1 \cdot 2^{-m}$ est un entier, et l'équation (4) sera remplacée par

$$u^2+v^2+w^2 = 0. \tag{5}$$

En vertu de (3) nous aurons $u^2 \equiv v^2 \equiv 1 \pmod{\mathfrak{p}^2}$. Ainsi l'équation (5) entraînera $w^2 \equiv -2 \pmod{\mathfrak{p}^2}$ ce qui est impossible. Donc, la congruence (2) n'a pas de solutions pour $m \geqslant 2$. Par conséquent, nous avons obtenu le résultat:

L'équation (1) *est impossible dans le corps K si $\Delta \equiv -1 \pmod 8$.*

4. Deuxième cas. Dans ce cas la congruence

$$\xi^2+\eta^2+\zeta^2 \equiv 0 \pmod 8$$

est satisfaite par

$$\xi = 1, \quad \eta = \tfrac{1}{2}(u+\sqrt{-\Delta}), \quad \zeta = \tfrac{1}{2}(u-\sqrt{-\Delta}),$$

où u est un entier rationnel $\equiv 1 \pmod 8$ si $\Delta \equiv 3 \pmod{16}$, et $\equiv 3 \pmod 8$ si $\Delta \equiv 11 \pmod{16}$. On a donc

$$u^2 \equiv \Delta - 2 \pmod{16}.$$

D'après le Lemme 3 il existe alors un nombre entier rationnel u_1 tel que

$$u_1^2 \equiv \Delta - 2 \pmod{2^{m+1}}$$

pour toute valeur donnée de m. Par conséquent on a la relation

$$1+[\tfrac{1}{2}(u_1+\sqrt{-\Delta})]^2+[\tfrac{1}{2}(u_1-\sqrt{-\Delta})]^2 \equiv 0 \pmod{2^m}.$$

Cela nous le résultat:

L'équation (1) *set résoluble dans le corps K si $\Delta \equiv 3 \pmod 8$.*

5. Troisième cas. Dans ce cas la congruence

$$\xi^2+\eta^2+\zeta^2 \equiv 0 \pmod 8$$

est satisfaite par

$$\xi = u, \quad \eta = 2, \quad \zeta = \sqrt{-\Delta},$$

où u est un entier rationnel impair. Donc

$$u^2 \equiv \Delta - 4 \equiv 1 \pmod 8.$$

Alors, vu que la congruence

$$u^2 \equiv \Delta - 4 \pmod{2^m}$$

est résoluble pour toute valeur de m (Lemme 3), on aura le résultat:

L'équation (1) *est résoluble dans le corps* $\boldsymbol{K}$ *si* $\Delta \equiv 5 \pmod 8$.

6. Quatrième cas. Dans ce cas la congruence

$$\xi^2 + \eta^2 + \zeta^2 \equiv 0 \pmod 8$$

est satisfaite par

$$\xi = u, \quad \eta = 0, \quad \zeta = \sqrt{-\Delta},$$

où u est un entier rationnel impair. Donc

$$u^2 \equiv \Delta \equiv 1 \pmod 8.$$

Alors, vu que la congruence

$$u^2 \equiv \Delta \pmod{2^m}$$

est résoluble pour toute valeur de m (Lemme 3), on aura le résultat:

L'équation (1) *est résoluble dans le corps* $\boldsymbol{K}$ *si* $\Delta \equiv 1 \pmod 8$.

7. Cinquième cas. Dans ce cas la congruence

$$\xi^2 + \eta^2 + \zeta^2 \equiv 0 \pmod 8$$

est satisfaite par

$$\xi = u, \quad \eta = 1, \quad \zeta = \sqrt{-\Delta},$$

où u est un entier rationnel impair. Donc

$$u^2 \equiv \Delta - 1 \equiv 1 \pmod 8.$$

Alors, vu que la congruence

$$u^2 \equiv \Delta - 1 \pmod{2^m}$$

est résoluble pour toute valeur de m (Lemme 3), on aura le résultat:

L'équation (1) *est résoluble dans le corps* $\boldsymbol{K}$ *si* $\Delta \equiv 2 \pmod 8$.

8. Sixième cas. Dans ce cas la congruence

$$\xi^2 + \eta^2 + \zeta^2 \equiv 0 \pmod 8$$

est satisfaite par

$$\xi = 2u + \sqrt{-\Delta}, \quad \eta = u - 2\sqrt{-\Delta}, \quad \zeta = 1,$$

où u est un entier rationnel impair. Donc

$$5u^2 \equiv 5\Delta - 1 \equiv 5 \pmod 8.$$

Alors, vu que la congruence

$$5u^2 \equiv 5\Delta - 1 \pmod{2^m}$$

est résoluble pour toute valeur de m (Lemme 3), on obtiendra le résultat:

L'équation (1) *est résoluble dans le corps* $\boldsymbol{K}$ *si* $\Delta \equiv -2 \pmod 8$.

9. En résumant les résultats des numéros 3–8 nous pouvons énoncer le

THÉORÈME. *L'équation* (1) *est résoluble dans tous les corps quadratiques imaginaires engendrés par le nombre* $\sqrt{-\Delta}$, *sauf dans le cas où* $\Delta \equiv -1 \pmod 8$.

A l'aide de ce théorème on peut évidemment obtenir des résultats sur la résolubilité de l'équation (1) dans certains corps cyclotomiques, dans des corps biquadratiques du premier rang etc.

Il faut observer que la méthode employée dans ce paragraphe n'est pas constructive, c'est-à-dire elle ne donne aucun algorithme pour déterminer effectivement une solution lorsque l'équation (1) est résoluble. Cela est une conséquence de la non-constructivité de la méthode de Hilbert dans son mémoire cité au commencement.

§ 2. Méthode constructive

10. Introduction. Le but de ce paragraphe-ci est de montrer que le résultat du § 1 peut être obtenu par une méthode constructive, essentiellement différente de celle appliquée aux pages précédentes.

Des méthodes constructives dans le cas du corps $\boldsymbol{K}(\sqrt{-\Delta})$ ont déjà été employées lorsque $\Delta = 1$ et $= 3$ (voir Skolem [5]) et lorsque $\Delta = 1, 2, 3, 7$ et 11 (voir Hemer [1]). Les méthodes de Skolem et de Hemer sont applicables seulement pour les corps euclidéens.

Dans le cas d'un Δ quelconque nous allons montrer comment on peut ramener le problème de résoudre l'équation

$$x^2 + y^2 + z^2 = 0 \tag{6}$$

en nombres d'un corps quadratique, au problème de résoudre en nombres rationnels l'équation de Legendre

$$aX^2 + bY^2 + cZ^2 = 0,$$

où a, b et c sont des nombres rationnels qui n'ont pas tous le même signe. Il y a des résolutions constructives de ce dernier problème; voir p. ex. [4], no. 61 et aussi [3], Theorem 5, p. 47. De cette manière nous aurons aussi une méthode constructive pour résoudre l'équation (6).

11. Comme dans le § 1 nous supposons donné le corps $K(\sqrt{-\Delta})$ engendré par le nombre $\sqrt{-\Delta}$, où Δ est un nombre naturel qui n'est divisible par aucun carré > 1. Pour les faits sur les corps quadratiques nous renvoyons au numéro 2. Dans le numéro 3 nous avons déjà montré, sans appliquer le théorème de Hilbert, que l'équation (6) est impossible dans le corps lorsque $\Delta \equiv -1 \pmod 8$.

Dans la suite nous distinguons les quatre cas suivants:

Premier cas: $\Delta \equiv 1 \pmod 4$; deuxième cas: $\Delta \equiv 2 \pmod 8$; troisième cas: $\Delta \equiv -2 \pmod 8$; quatrième cas: $\Delta \equiv 3 \pmod 8$.

On voit sans difficulté que l'équation (6) peut être supposée d'avoir la forme

$$w^2+(u+v\sqrt{-\Delta})^2+(u_1-v_1\sqrt{-\Delta})^2 = 0,$$

où w, u, v, u_1 et v_1 sont des nombres entiers rationnels. Il en résulte les deux équations

$$w^2+u^2+u_1^2-\Delta v^2-\Delta v_1^2 = 0$$

et

$$uv = u_1v_1.$$

En éliminant u de ces relations on aura

$$(v^2+v_1^2)(\Delta v^2-u_1^2) = (vw)^2.$$

Supposons maintenant qu'on ait

$$v = Az, \quad v_1 = Az_1, \quad (z, z_1) = 1,$$

A étant le plus grand commun diviseur de v et v_1. Il en résulte

$$A^2(z^2+z_1^2)(\Delta A^2z^2-u_1^2) = (zw)^2. \tag{7}$$

Vu que $uz = u_1z_1$, on voit que u_1 est divisible par z. Alors, en posant $u_1 = Bz$, nous aurons de (7) la relation

$$(z^2+z_1^2)(\Delta A^2-B^2) = \left(\frac{w}{A}\right)^2 = w_1^2, \tag{8}$$

où w_1 est un nombre entier rationnel. Dans les trois premiers cas nous choisissons z et z_1 tels que

$$z^2+z_1^2 = p$$

soit un nombre premier $\equiv 1 \pmod 4$. Alors w_1 est divisible par p. Si nous posons $w_1 = pC$, l'équation (8) peut s'écrire

$$pC^2+B^2-\Delta A^2 = 0. \tag{9}$$

Maintenant il faut choisir le nombre premier p de façon que l'équation (9) soit résoluble en nombres entiers rationnels A, B et C. Pour cela il faut le nombre $-p$ soit un reste quadratique modulo Δ. Donc, nous choisissons p tel que $-p$ soit un reste quadratique modulo chacun des diviseurs premiers impairs q de Δ. En vertu du théorème de Dirichlet sur les nombres premiers dans les progressions arithmétiques, l'existence d'une infinité de tels nombres premiers p est assurée. Un nombre premier p satisfaisant aux propriétés exigées peut être trouvé par essai.

Nous avons alors pour tous les nombres premiers q:

$$\left(\frac{-p}{q}\right) = +1, \quad \text{d'où} \quad \left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(q-1)}.$$

Si $q \equiv 1 \pmod 4$, q est un reste quadratique modulo p. Si $q \equiv -1 \pmod 4$, q est un non-reste quadratique modulo p.

12. Premier cas: $\Delta \equiv 1 \pmod 4$. Si h signifie le nombre des q qui sont $\equiv -1 \pmod 4$ nous aurons

$$\Delta = \prod q \equiv (-1)^h \pmod 4.$$

Vu que $\Delta \equiv 1 \pmod 4$ il faut donc que h soit pair. Nous avons de plus

$$\left(\frac{\Delta}{p}\right) = \prod\left(\frac{q}{p}\right) = (-1)^h = +1.$$

Cela signifie que Δ est un reste quadratique modulo p. Par conséquent, toutes les conditions sont satisfaites pour que l'équation (9) soit résoluble. Donc, l'équation (6) est aussi résoluble pour $\Delta \equiv 1 \pmod 4$. Vu qu'on peut trouver une solution de (9), cela est aussi possible pour l'équation (6).

13. Deuxième cas: $\Delta \equiv 2 \pmod 8$. Dans ce cas le nombre premier p sera choisi $\equiv 1 \pmod 8$. Si h signifie le nombre des q qui sont $\equiv -1 \pmod 4$ nous aurons

$$\tfrac{1}{2}\Delta = \prod q \equiv (-1)^h \pmod 4.$$

Donc h est pair, et nous aurons de plus

$$\left(\frac{\Delta}{p}\right) = \left(\frac{\frac{1}{2}\Delta}{p}\right) = \prod\left(\frac{q}{p}\right) = (-1)^h = +1,$$

c'est-a-dire que Δ est un reste quadratique modulo p. Ainsi toutes les conditions pour la résolubilité de (9) sont remplies. Donc, l'équation (6) est aussi résoluble pour $\Delta \equiv 2 \pmod 4$. Vu qu'on peut trouver une solution de (9), on peut aussi déterminer une solution de l'équation (6).

14. Troisième cas: $\Delta \equiv -2 \pmod 8$. Dans ce cas le nombre premier p sera choisi $\equiv 5 \pmod 8$. Si h signifie le nombre des q qui sont $\equiv -1 \pmod 4$ nous aurons

$$\tfrac{1}{2}\Delta = \prod q \equiv (-1)^h \pmod 4.$$

Donc h est impair, et nous aurons de plus

$$\left(\frac{\Delta}{p}\right) = -\left(\frac{\frac{1}{2}\Delta}{p}\right) = -\prod\left(\frac{q}{p}\right) = -(-1)^h = +1$$

c'est-à-dire que Δ est un reste quadratique modulo p. Alors, tout-à-fait comme dans les deux cas précédents on obtiendra le résultat: L'équation (6) est résoluble pour $\Delta \equiv -2 \pmod 8$, et l'on peut toujours trouver une solution de celle-ci.

15. Quatrième cas: $\Delta \equiv 3 \pmod 8$. Dans ce cas nous choisissons z et z_1 tels qu'on ait

$$z^2 + z_1^2 = 2p,$$

où p est un nombre premier $\equiv 1 \pmod 4$.

Alors w_1 dans (8) est divisible par $2p$. Si nous posons $w_1 = 2pC$, l'équation (8) peut s'écrire

$$2pC^2 + B^2 - \Delta A^2 = 0. \tag{10}$$

Maintenant nous choisissons p de façon que $-2p$ soit un reste quadratique modulo Δ. Pour cela il faut et il suffit que $-2p$ soit un reste quadratique modulo chacun des diviseurs premiers q de Δ. D'après le théorème de Dirichlet sur les progressions arithmétiques, l'existence d'une infinité de tels nombres premiers p est assurée.

Nous supposons ensuite que a des nombres premiers q soient $\equiv 1 \pmod 8$, que b de ces nombres soient $\equiv -1 \pmod 8$, que c de ces nombres soient $\equiv 5 \pmod 8$ et que d de ces nombres soient $\equiv 3 \pmod 8$.

Si $q \equiv 1$ ou $\equiv 3 \pmod 8$ on a évidemment $(q/p) = +1$; si $q \equiv -1$ ou $\equiv 5 \pmod 8$ on a $(q/p) = -1$. Alors on aura

$$\Delta = \prod q \equiv (-1)^b \cdot 5^c \cdot 3^d \equiv (-1)^{b+c} \cdot 3^{c+d} \pmod 8.$$

Il en résulte, vu que $\Delta \equiv 3 \pmod 8$, que $b+c$ est pair et $c+d$ impair. Nous aurons ensuite

$$\left(\frac{\Delta}{p}\right) = \prod\left(\frac{q}{p}\right) = (-1)^b \cdot (-1)^c = (-1)^{b+c} = +1.$$

Donc Δ est un reste quadratique modulo p. Ainsi toutes les conditions pour la résolubilité de l'équation (10) sont satisfaites. Par conséquent, l'équation (6) est aussi résoluble pour $\Delta \equiv 3 \pmod 8$. Vu qu'on peut trouver une solution de (10), on peut aussi trouver une solution de l'équation (6).

16. Ainsi nous avons montré qu'il existe dans le cas de l'équation (6) une méthode constructive pour déterminer les solutions lorsque celle-ci est résoluble dans un corps quadratique. Il est évident qu'une méthode analogue et constructive peut être développée pour résoudre dans un corps quadratique l'équation plus générale $ax^2 + by^2 + cz^2 = 0$, où a, b et c sont des nombres rationnels. Cela est possible même dans le cas d'un corps réel, lorsque les coefficients a, b, c n'ont pas le même signe.

Travaux cités

[1] O. Hemer, *On the solvability of the Diophantine equation* $ax^2 + by^2 + cz^2 = 0$ *in imaginary Euclidean quadratic fields*, Arkiv för Matematik, 2 (1952).

[2] D. Hilbert, *Über die Theorie des relativquadratischen Zahlkörpers*, Math. Annalen, 51 (1899).

[3] L. J. Mordell, *Diophantine Equations*, London and New York 1969.

[4] T. Nagell, *Introduction to Number Theory*, New York 1951.

[5] Th. Skolem, *Über die Lösung der unbestimmten Gleichung* $ax^2 + by^2 + cz^2 = 0$ *in einigen einfachen Rationalitätsbereichen*, Norsk Matematisk Tidsskrift 10 (1928).

Reçu le 27. 11. 1970 (124)