Available online at www.sciencedirect.com

ScienceDirect

C. R. Acad. Sci. Paris, Ser. I 344 (2007) 413–416

COMPTES RENDUS MATHEMATIQUE

http://france.elsevier.com/direct/CRASS1/

Number Theory

Sums of integral squares in cyclotomic fields ☆

Chun-Gang Ji [a,b], Da-Sheng Wei [c]

[a] *Department of Mathematics, Nanjing University, Nanjing 210093, P.R. China*
[b] *Department of Mathematics, Nanjing Normal University, Nanjing 210097, P.R. China*
[c] *Department of Mathematics, The University of Science and Technology of China, Hefei 230026, P.R. China*

Received 19 September 2006; accepted after revision 7 February 2007

Available online 21 March 2007

Presented by Jean-Pierre Serre

Abstract

Let $K_n = \mathbb{Q}(\zeta_n)$ be the n-th cyclotomic field with $n \not\equiv 2 \pmod 4$. Let $O_n = \mathbb{Z}[\zeta_n]$ be the ring of integers of K_n and S_n the set of all elements $\alpha \in O_n$ which are sums of squares in O_n. Let g_n be the smallest positive integer m such that every element in S_n is a sum of m squares in O_n. In this Note, we show that $g_n = 3$ unless n is odd and the order of 2 in $(\mathbb{Z}/n\mathbb{Z})^*$ is odd, in which case $g_n = 4$. ***To cite this article: C.-G. Ji, D.-S. Wei, C. R. Acad. Sci. Paris, Ser. I 344 (2007).***

Résumé

Sommes de carrés dans les anneaux d'entiers de corps cyclotomiques. Soit K_n le n-ième corps cyclotomique, avec $n \not\equiv 2 \pmod 4$, $n > 1$. Soit O_n l'anneau des entiers de K_n et soit S_n le sous-ensemble de O_n formé des éléments qui sont sommes de carrés. Soit g_n le plus petit entier $m > 0$ tel que tout élément de S_n soit somme de m carrés d'éléments de O_n. Nous montrons que : $g_n = 3$ si n est divisible par 4 ; $g_n = 3$ (resp. $g_n = 4$) si n est impair et si l'ordre de 2 dans le groupe multiplicatif $(\mathbb{Z}/n\mathbb{Z})^*$ est pair (resp. impair). ***Pour citer cet article : C.-G. Ji, D.-S. Wei, C. R. Acad. Sci. Paris, Ser. I 344 (2007).***

1. Introduction

It is well known that all positive integers are sums of four integral squares, first proved by Lagrange. What happens for other number fields? Let K be an algebraic number field of degree n with exactly r_1 real embeddings $\sigma_1, \sigma_2, \ldots, \sigma_{r_1}$ and r_2 pairs of complex embeddings $\sigma_{r_1+1}, \bar{\sigma}_{r_1+1}, \ldots, \sigma_{r_1+r_2}, \bar{\sigma}_{r_1+r_2}$. The field K is totally real in the case $r_1 = n$. A number α in K is called totally positive whenever the r_1 conjugates $\sigma_1(\alpha), \ldots, \sigma_{r_1}(\alpha)$ are all positive. In 1902, Hilbert conjectured that every totally positive α in K is a sum of four squares in K. The first published proof of this was given by Siegel [10] in 1921. F. Götzky [3] proved the following surprising theorem:

☆ This work was partially supported by the Grant No. 10171046 and 10201013 from NNSF of China and Jiangsu planned projects for postdoctoral research funds.

E-mail addresses: cgji@njnu.edu.cn (C.-G. Ji), dshwei@ustc.edu.cn (D.-S. Wei).

1631-073X/$ – see front matter
doi:10.1016/j.crma.2007.02.003

Theorem 1. *The field $K = \mathbb{Q}(\sqrt{5})$ is the only real quadratic field in which every totally positive integer is the sum of four integral squares in K.*

Götzky's result was improved by H. Maass [7], who proved that

Theorem 2. *Let $K = \mathbb{Q}(\sqrt{5})$. Then every totally positive integer in K is the sum of three integral squares in K.*

Continuing this line of investigation, Siegel [11] proved the following startling results.

Theorem 3. *Let K be totally real and suppose that all totally positive algebraic integers are sums of integral squares in K; then K is either the rational number field $\mathbb{Q}$ or the real quadratic field $\mathbb{Q}(\sqrt{5})$.*

Theorem 4. *If K is not totally real, then all totally positive algebraic integers are sums of integral squares in K if and only if the discriminant of K is odd.*

Hsia [4, page 531] obtained the following result:

Corollary. *Let F be a totally imaginary number field, R the ring of integers in F. Assume that the absolute discriminant of F is an odd integer. Then we have*:

(i) *Every integer of R is representable as a sum of four integer squares*;
(ii) *Every integer of R is representable as a sum of three integer squares provided the class number of F is odd, and moreover, the residue degree $f(\mathfrak{p}/2)$ at dyadic primes of F are even* (*e.g.* $F = \mathbb{Q}(\sqrt{-p})$ *with prime* $p \equiv 3 \pmod 8$).

In Theorem 4, when K is an imaginary quadratic field, using some results from algebraic K-theory of integral quadratic forms and the theory of spinor genus of quadratic forms, Estes and Hsia [1,2] proved that

Theorem 5. *Every algebraic integer in $K = \mathbb{Q}(\sqrt{-D})$, D a positive square free integer, can be expressed as a sum of three integral squares when and only when $D \equiv 3 \pmod 8$ and D does not admit a positive proper factorization $D = d_1 d_2$ (i.e., $d_i > 1$) which satisfies the conditions*: (a) $d_1 \equiv 5, 7 \pmod 8$ *and* (b) *the Jacobi symbol* (d_2/d_1) *is* 1.

In [6], we determined all algebraic integers as sums of three integral squares over all imaginary quadratic fields. In [9], Qin gave a criterion for the sum of two squares over a quadratic number fields.

Let $K_n = \mathbb{Q}(\zeta_n)$ be the n-th cyclotomic field where ζ_n is a primitive n-th root of unity. Let $O_n = \mathbb{Z}[\zeta_n]$ be the ring of integers of K_n. If $n \equiv 2 \pmod 4$ then $K_n = \mathbb{Q}(\zeta_{n/2}) = K_{n/2}$. Hence in this note we assume that $n \not\equiv 2 \pmod 4$. Let S_n be the set of all elements $\alpha \in O_n$ which are sums of squares in O_n and set

$$g_n = \min\{m\colon \text{ any element in } S_n \text{ is a sum of } m \text{ integral squares}\}.$$

How to determine S_n and g_n? It is easy to see that $-1 \in S_n$ and S_n is a subring of O_n. In particular, $S_n = O_n$ if n is odd. In [5], we proved that every algebraic integer in O_n is a sum of three integral squares if and only if n is odd and the order of 2 in $(\mathbb{Z}/n\mathbb{Z})^*$ is even. In this note, we shall prove that:

Theorem 6. *Let $n > 2$ be an integer with $n \not\equiv 2 \pmod 4$. Then* (1) $g_n = 3$ *if* $n \equiv 0 \pmod 4$; (2) $g_n = 3$ (*resp.* $g_n = 4$) *if n is odd and the order of 2 in $(\mathbb{Z}/n\mathbb{Z})^*$ is even* (*resp. odd*).

2. Some lemmas

For any cyclotomic field K_n, there are exactly $\phi(n)/2$ pairs of complex embeddings of K_n, i.e., K_n is totally imaginary. So every element of K_n is totally positive. Let $n = p_1^{t_1} \cdots p_s^{t_s}$, where $p_1, \ldots, p_s$ are different primes. Then we have $O_n = O_{p_1^{t_1}} \cdots O_{p_s^{t_s}}$.

Lemma 1. *Let $n > 2$ be an integer with $n \not\equiv 2 \pmod 4$. Then* (1) *If n is odd, then $S_n = O_n$*; (2) *If $n = 2^m r$ with $m \geqslant 2$ and r is odd, then $\alpha \in S_n$ if and only if*

$$\alpha = a_0 + a_1\zeta_{2^m} + \cdots + a_{t-1}\zeta_{2^m}^{t-1} \in O_r[\zeta_{2^m}]$$

such that $t = \phi(2^m)$ and $a_{2k-1} \in 2O_r$ for $1 \leqslant k \leqslant t/2$.

Proof. (1) If n is odd, then the discriminant of K_n is odd. So by Theorem 4 we have $S_n = O_n$. (2) Let $z = \zeta_{2^m}$ and $\beta = \sum_{j=0}^{t-1} b_j z^j$, where $b_j \in O_r$. Then $\beta^2 = \sum_{j=0}^{t-1} c_j z^j \in O_r[z]$ such that $c_j \in 2O_r$ for $2 \nmid j$. So if $\alpha \in S_n$, then $\alpha = \sum_{j=0}^{t-1} a_j z^j \in O_r[z]$ such that $a_j \in 2O_r$ for $2 \nmid j$. Conversely, since $O_r = S_r$, the a_k are sums of integral squares, and it is enough to prove that z^{2j} and $2z^{2j+1}$ belong to S_n for all j, which reduces to $2z \in S_n$. But $2z = (1+z)^2 + (-1) + (-z^2)$ and the result follows since -1 belongs to the subring S_n. □

Let $s(K)$ be the Stufe of the number field K, that is to say, the smallest number of squares necessary to represent -1 in K.

Lemma 2. *Let $K = \mathbb{Q}(\zeta_m)$, where $m \geqslant 3$ is odd. Then $s(K)$ is equal to 2 or to 4 depending on whether the order of 2 modulo m is even or odd.*

Proof. See [8]. □

3. Proof of Theorem 6

Case A. Suppose that $n \equiv 0 \pmod 4$, we have $i = \sqrt{-1} \in K_n$. So if $\alpha \in S_n$ then $-\alpha \in S_n$. Hence there exist $\beta_1, \ldots, \beta_l \in O_n$ such that $-\alpha = \beta_1^2 + \cdots + \beta_l^2$. So there exists a $\gamma \in O_n$ such that

$$\alpha + (\beta_1 + \cdots + \beta_l + 1)^2 = (\gamma + 1)^2 - \gamma^2.$$

Hence

$$\alpha = (\gamma + 1)^2 - \gamma^2 - (\beta_1 + \cdots + \beta_l + 1)^2 = (\gamma + 1)^2 + (i\gamma)^2 + \big(i(\beta_1 + \cdots + \beta_l + 1)\big)^2.$$

Now we obtain that every $\alpha \in S_n$ is a sum of three integral squares in K_n. Next we shall find an element in S_n which is not a sum of two integral squares in K_n. Suppose $n = 2^m r$ with $m \geqslant 2$ and r is odd. Let $\alpha = 2(1 - \zeta_{2^m})$.By Lemma 1, $\alpha \in S_n$. Suppose that α is a sum of two integral squares in K_n. Let $\alpha = 2(1 - \zeta_{2^m}) = \beta^2 + \gamma^2 = (\beta + \gamma i)(\beta - \gamma i)$, where $\beta, \gamma \in O_n$. Let $x = \beta + \gamma i$, $y = \beta - \gamma i$. Then $x, y \in O_n$ and $x = 2\beta - y$. Let $\mathfrak{p}$ be a prime ideal of O_n lying over 2, and let $v_{\mathfrak{p}}(.)$ be a valuation determined by $\mathfrak{p}$ such that $v_{\mathfrak{p}}(1 - \zeta_{2^m}) = 1$. Then $v_{\mathfrak{p}}(2) = 2^{m-1}$.

(a) If $v_{\mathfrak{p}}(y) < 2^{m-1}$, then $v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(y)$. So $v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y) = 2v_{\mathfrak{p}}(y)$ is even. But $v_{\mathfrak{p}}(2(1 - \zeta_{2^m})) = 2^{m-1} + 1$ is odd. A contradiction.
(b) If $v_{\mathfrak{p}}(y) \geqslant 2^{m-1}$, then $v_{\mathfrak{p}}(x) \geqslant 2^{m-1}$. Hence $v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y) \geqslant 2^m$. But $v_{\mathfrak{p}}(2(1 - \zeta_{2^m})) = 2^{m-1} + 1 < 2^m$. A contradiction.

So $g_n = 3$ for $n \equiv 0 \pmod 4$.

Case B. Suppose that $n > 1$ is odd and the order of 2 in $(\mathbb{Z}/n\mathbb{Z})^*$ is even. Then there exists an odd prime p such that $p|n$ and the order of 2 in $(\mathbb{Z}/p\mathbb{Z})^*$ is even. Let $f = 2a$ be the order of 2 modulo p. Then we have $2^{2a} = 2^f \equiv 1 \pmod p$ and $2^a \equiv -1 \pmod p$. From

$$(1 + \zeta_p^2)(1 + \zeta_p^{2^2}) \cdots (1 + \zeta_p^{2^a}) = -1/\zeta_p^2,$$

we have

$$-1 = \zeta_p^2(1 + \zeta_p^2)(1 + \zeta_p^{2^2}) \cdots (1 + \zeta_p^{2^a}) = \alpha^2 + \beta^2,$$

where $\alpha, \beta \in \mathbb{Z}[\zeta_p]$. In the following, we shall prove that every $\gamma \in S_n$ is a sum of three integral squares in O_n. Let $\gamma \in S_n$. Then $-\gamma \in S_n$. Hence we have $-\gamma = \beta_1^2 + \cdots + \beta_l^2$, $\beta_i \in O_n$. Then there exists a $\delta \in O_n$ such that

$$\gamma + (\beta_1 + \cdots + \beta_l + 1)^2 = (\delta + 1)^2 - \delta^2.$$

So there exist $x, y, z \in O_n$ such that $\gamma = x^2 - (y^2 + z^2)$, using $-1 = \alpha^2 + \beta^2$, we have

$$\gamma = x^2 + (\alpha y + \beta z)^2 + (\alpha z - \beta y)^2.$$

Now it remains to prove that there exists an element in S_n which is not a sum of two integral squares in O_n. Let $K = K_n$, $O = O_n$ and $L = K(\sqrt{-1}) = \mathbb{Q}(\zeta_{4n})$. Then $[L : K] = 2$. Let $\mathfrak{p}$ be a prime ideal over 2 in K and $\mathfrak{q}$ a prime ideal over $\mathfrak{p}$ in L. Then $\mathfrak{p}$ is totally ramified in L. Let $L_\mathfrak{q}$ and $(K)_\mathfrak{p}$ denote the completions of L and K at $\mathfrak{q}$ and $\mathfrak{p}$ respectively. By local class field theory, we have $(K)_\mathfrak{p}^*/N(L_\mathfrak{q}^*) \cong Gal(L_\mathfrak{q}/(K)_\mathfrak{p})$. Hence $[(K)_\mathfrak{p}^* : NL_\mathfrak{q}^*] = 2$. Suppose that every element in S_n is a sum of two integral squares and let $a/b \in K$, $a, b \in O$. Then $ab \in O = S_n$ (Lemma 1) is a sum of two squares and so is a/b. Hence every element in K is a sum of two squares in K. But O is dense in $O_\mathfrak{p}$. Let $a = \lim a_k$ in $O_\mathfrak{p}$ with a_k in O. By assumption, each $a_k = b_k^2 + c_k^2$ is a sum of two squares. By compactness of $O_\mathfrak{p}$, we can assume that b_k and c_k converge. In particular, a is a sum of two squares in $O_\mathfrak{p}$. This implies that each element in $(K)_\mathfrak{p}$ is a sum of two squares, a contradiction. Hence $g_n = 3$.

Case C. Suppose that $n > 1$ is odd and the order of 2 in $(\mathbb{Z}/n\mathbb{Z})^*$ is odd. By the Corollary of Hsia [4], we have $g_n \leqslant 4$. On the other hand by Lemma 2, we have $g_n \geqslant 4$. So $g_n = 4$. This completes the proof of Theorem 6. □

Acknowledgements

This work arose from a series lectures given by Prof. Yuan Wang on the circle method in Morningside Center of Mathematics. The authors would like to thank the Center for its support. We are indebted to Professor Fei Xu for his encouragement.

References

[1] D.R. Estes, J.S. Hsia, Exceptional integers of some ternary quadratic forms, Adv. in Math. 45 (1982) 310–318.
[2] D.R. Estes, J.S. Hsia, Sums of three integer squares in complex quadratic fields, Proc. Amer. Math. Soc. 89 (1983) 211–214.
[3] F. Götzky, Über eine zahlentheoretische Anwendung von Modulfunktionen einer Veränderlichen, Math. Ann. 100 (1928) 411–437.
[4] J.S. Hsia, Representations by integral quadratic forms over algebraic number fields, in: Conference on Quadratic Forms—1976, in: Queen's Papers in Pure and Appl. Math., vol. 46, 1977, pp. 528–537.
[5] C.-G. Ji, Sums of three integral squares in cyclotomic fields, Bull. Austral. Math. Soc. 68 (2003) 101–106.
[6] C.-G. Ji, Y.-H. Wang, F. Xu, Sums of three squares over imaginary quadratic fields, Forum Math. 18 (2006) 585–601.
[7] H. Maass, Über die Darstellung total positiver Zahlen des Körpers $R(\sqrt{5})$ als Summe von drei Quadraten, Abh. Math. Sem. Hansischen Univ. 14 (1941) 185–191.
[8] C. Moser, Représentation de -1 par une somme de carrés dans certains corps locaux et globaux, et dans certains anneaux d'entiers algébriques, C. R. Acad. Sci. Paris Ser. A-B 271 (1970) A1200–A1203.
[9] H. Qin, The sum of two squares in a quadratic field, Comm. Algebra 25 (1997) 177–184.
[10] C.L. Siegel, Darstellung total positiver Zahlen durch Quadrate, Math. Z. 11 (1921) 246–275.
[11] C.L. Siegel, Sums of mth powers of algebraic integers, Ann. of Math. 46 (1945) 313–339.