BULL. AUSTRAL. MATH. SOC. 11R18, 11E25, 11R33
VOL. 68 (2003) [101–106]

SUMS OF THREE INTEGRAL SQUARES IN CYCLOTOMIC FIELDS

CHUN-GANG JI

Let m be an odd positive integer greater than 2 and f the smallest positive integer such that $2^f \equiv 1 \pmod{m}$. It is proved that every algebraic integer in the cyclotomic field $\mathbb{Q}(\zeta_m)$ can be expressed as a sum of three integral squares if and only if f is even.

1. INTRODUCTION

Let K be an algebraic number field of degree n with exactly r real conjugates $K^{(1)}, \dots, K^{(r)}$, in particular, the field K is totally real in the case $r = n$. A number α in K is called totally positive, $\alpha \gg 0$, whenever the r conjugates $\alpha^{(1)}, \dots, \alpha^{(r)}$ are all positive. Siegel had proved the following two theorems in [**5**]

THEOREM A. *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 number field $\mathbb{Q}(\sqrt{5})$.*

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

These two results are from different aspects of quadratic forms theory: Theorem A deals with definite forms, and theorem B with indefinite forms. While the proof of theorem A was elegant, albeit surprisingly elementary, Siegel resorted to a generalisation of the circle method to show that five integral squares applies for theorem B, and expressed his belief that perhaps four may be possible. Using the modern powerful machinery of spinor genus, theorem B is easily reducible to a local question. In fact, the conjectured value of four integral squares quickly falls out.

THEOREM B*. *If K is not totally real, then all totally positive algebraic integers are sums of four integral squares in K when and only when the discriminant of K is odd.*

In (A), over $\mathbb{Q}$ it is well-known that all positive integer v are sums of four squares (Lagrange) and that such a v is a sum of three squares if and only if $v \neq 4^a(8b+7)$

Received 19th December, 2002
This work was partially supported by the grant #10201013 from NNSF of China. The author was indebted to Professor Fei Xu for his encouragement.

(Legendre). Maass later showed via function-theoretic means that actually three squares works for $\mathbb{Q}(\sqrt{5})$, see [3].

In (B), which formally non-real K has all its integers expressible as sums of three integral squares in K?

Using some results from the algebraic K-theory of integral quadratic forms and the theory of spinor genus of quadratic forms, Estes and Hsia [1, 2] gave a complete answer to this problem when K is an imaginary quadratic number field, which is stated in the following.

THEOREM C. *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 factorisation $D = d_1 d_2$ (that is, $d_i > 1$) which satisfies the conditions:*

(1) $d_1 \equiv 5, 7 \pmod 8$ *and*
(2) $(d_2/d_1) = 1$.

Let m be a positive integer greater than 2 and $K = \mathbb{Q}(\zeta_m)$ a cyclotomic field. If $m \equiv 2 \pmod 4$ then $K = \mathbb{Q}(\zeta_{m/2})$. If $m \equiv 0 \pmod 4$ then it is easy to show that ζ_m is not expressible as a sum of integral squares in K. If m is odd, then by the above discussion we know that every algebraic integer in K can be expressed as a sum of four integral squares. Which cyclotomic field K has all its algebraic integers expressible as sums of three integral squares? In this paper, we shall give a complete answer to this problem, in the following theorem.

THEOREM. *Let m be an odd positive integer greater than 2 and let the order of 2 modulo m be f (that is, f is the smallest positive integer such that $2^f \equiv 1 \pmod m$). Then every algebraic integer in $K = \mathbb{Q}(\zeta_m)$ can be expressed as a sum of three integral squares if and only if f is even.*

COROLLARY 1. *Let $p \equiv 3 \pmod 4$ be a prime. Then every algebraic integer in $\mathbb{Q}(\sqrt{-p})$ can be expressed as a sum of three integral squares if and only if $p \equiv 3 \pmod 8$.*

COROLLARY 2. *Let $p \equiv 3 \pmod 8$ be a prime. Then $x^2 - py^2 = -2$ is solvable in integers.*

2. Some Lemmas

LEMMA 1. *Let p be an odd prime. If the order of 2 modulo p is even, then -1 can be represented as a sum of two integral squares in $K = \mathbb{Q}(\zeta_p)$.*

PROOF: Let $f = 2n$, $n \geq 1$, be the order of 2 modulo p. Then we have

$$2^{2n} = 2^f \equiv 1 \pmod p, \quad \text{and} \quad 2^n \equiv -1 \pmod p.$$

From

$$\left(1+\zeta_p^2\right)\left(1+\zeta_p^{2^2}\right)\left(1+\zeta_p^{2^3}\right)\dots\left(1+\zeta_p^{2^n}\right)=\frac{1-\zeta_p^{2^{n+1}}}{1-\zeta_p^2}=\frac{1-\zeta_p^{-2}}{1-\zeta_p^2}=\frac{-1}{\zeta_p^2},$$

we have

$$-1=\zeta_p^2\left(1+\zeta_p^2\right)\left(1+\zeta_p^{2^2}\right)\dots\left(1+\zeta_p^{2^n}\right). \tag{1}$$

Then the result follows from (1) and the following identity

$$\left(a^2+b^2\right)\left(c^2+d^2\right)=(ac+bd)^2+(ad-bc)^2. \tag{2}$$

□

Lemma 2. *Let $m \geq 3$ be an odd positive integer. If -1 can be expressed as a sum of two integral squares in $K = \mathbb{Q}(\zeta_m)$, then every algebraic integer can be expressed as a sum of three integral squares in K.*

Proof: By Siegel's theorem B*, we know that every $\alpha \in \mathbb{Z}[\zeta_m]$, the ring of integers of K, is expressible as a sum of four integral squares in K. Write

$$-\alpha=\beta_1^2+\beta_2^2+\beta_3^2+\beta_4^2, \quad \beta_i \in \mathbb{Z}[\zeta_m].$$

Then there exists a $\gamma \in \mathbb{Z}[\zeta_m]$ such that

$$\alpha+(\beta_1+\beta_2+\beta_3+\beta_4+1)^2=(\gamma+1)^2-\gamma^2.$$

So there exist $x, y, z \in \mathbb{Z}[\zeta_m]$ such that

$$\alpha=x^2-\left(y^2+z^2\right).$$

Because -1 can be expressed as a sum of two integral squares in K and using (2) we can obtain the result. □

Lemma 3. *Let $m \geq 3$ be an odd positive integer and $K = \mathbb{Q}(\zeta_m)$. Then $s(K)$ (the stufe of K, that is to say, the smallest number of squares necessary to represent -1 in K) is equal to 2 or to 4 depending on whether the order of 2 modulo m is even or odd.*

Proof: See [4]. □

https://doi.org/10.1017/S000497270003745X Published online by Cambridge University Press

3. Proof of Theorem

If the order of 2 modulo m is odd, then by Lemma 3 the stufe $s(K) = 4$. So -1 can not be expressed as a sum of three integral squares in K.

Next we consider the order of 2 modulo m is even. According to lemma 2, we shall only show that -1 can be expressed as a sum of two integral squares in $\mathbb{Z}[\zeta_m]$. Let

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_t^{\alpha_t},$$

where the p_j are distinct odd primes. Then K is the composite of the fields $K_j = \mathbb{Q}\left(\zeta_{p_j{}^{\alpha_j}}\right)$, $j = 1, 2, \dots, t$. If the order of 2 modulo $p_j^{\alpha_j}$ is odd, that is, the residue class degree above 2 in K_j is odd, then the residue class degree above 2 in K is odd. Thus we may assume that $m = p^\alpha$, p is an odd prime, and the order of 2 modulo p^α is even. We must prove that the order of 2 modulo p is even. We know that

$$\mathbb{Q} \subset \mathbb{Q}(\zeta_p) \subset \mathbb{Q}(\zeta_{p^\alpha}).$$

Suppose the order of 2 modulo p were odd. Then the residue class degree above 2 in $\mathbb{Q}(\zeta_p)$ is odd. Using $\left[\mathbb{Q}(\zeta_{p^\alpha}) : \mathbb{Q}(\zeta_p)\right] = p^{\alpha - 1}$ is odd, we get the residue class degree above 2 in $\mathbb{Q}(\zeta_{p^\alpha})$ is odd, that is, the order of 2 modulo p^α is odd, this contradicts the assumption. By lemmas 1 and 2, the proof of theorem is finished.

4. Proof of Corollary 1

If $p \equiv 7 \pmod 8$, then 2 splits completely in $\mathbb{Q}(\sqrt{-p})$ and $\left[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\sqrt{-p})\right] = (p-1)/2$ is odd. So the order of 2 modulo p is odd. Hence by lemma 3, $s\big(\mathbb{Q}(\zeta_p)\big) = 4$. So -1 can not be expressed as a sum of three integral squares in $\mathbb{Q}(\sqrt{-p})$.

In the following, we consider the case $p \equiv 3 \pmod 8$. In this case the residue class degree above 2 in $\mathbb{Q}(\sqrt{-p})$ is 2. By

$$\mathbb{Q} \subset \mathbb{Q}\big(\sqrt{-p}\big) \subset \mathbb{Q}(\zeta_p),$$

we obtain the order of 2 modulo p is even. So there exist $x, y \in \mathbb{Z}[\zeta_p]$ such that

$$-1 = x^2 + y^2. \tag{3}$$

Let $G = \mathrm{Gal}\big(\mathbb{Q}(\zeta_p)/\mathbb{Q}(\sqrt{-p})\big)$. So that $|G| = (p-1)/2$ is odd. From (3) we have

$$\prod_{\sigma \in G} (-1)^\sigma = \prod_{\sigma \in G} \left(x^2 + y^2\right)^\sigma, \quad \text{that is,}$$

$$-1 = \prod_{\sigma \in G} \left(x^\sigma + \sqrt{-1}y^\sigma\right)\left(x^\sigma - \sqrt{-1}y^\sigma\right). \tag{4}$$

Now let

$$\prod_{\sigma\in G}\left(x^{\sigma}+\sqrt{-1}y^{\sigma}\right)=U+\sqrt{-1}V,$$

where U, V are algebraic integers in $\mathbb{Q}(\zeta_p, \sqrt{-1})$. Then for $\tau \in G$, we have

$$\tau(U+\sqrt{-1})=\tau\prod_{\sigma\in G}\left(x^{\sigma}+\sqrt{-1}y^{\sigma}\right)=\prod_{\sigma\in G}\left(x^{\tau\sigma}+\sqrt{-1}y^{\tau\sigma}\right)=U+\sqrt{-1}V,$$

since σ runs through G, so does $\tau\sigma$. It follows that $U+\sqrt{-1}V$ is an algebraic integer in $\mathbb{Q}(\zeta_p, \sqrt{-1})$, that is, that U, V are algebraic integers in $\mathbb{Q}(\sqrt{-p})$. Hence

$$\prod_{\sigma\in G}\left(x^{\sigma}-\sqrt{-1}y^{\sigma}\right)=U-\sqrt{-1}V.$$

Now (4) gives

$$-1=\left(U+\sqrt{-1}V\right)\left(U-\sqrt{-1}\right)=U^2+V^2, \tag{5}$$

where U, V are algebraic integers in $\mathbb{Q}(\sqrt{-p})$. By theorem B* and using a similar method of proof to Lemma 2, we finish the proof of the Corollary.

5. Proof of Corollary 2

Since $p \equiv 3 \pmod 8$, from (5) we have $a, b, c, d \in \mathbb{Z}$ such that

$$-1=\left(\frac{a+b\sqrt{-p}}{2}\right)^2+\left(\frac{c+d\sqrt{-p}}{2}\right)^2 \tag{6}$$

and

$$a \equiv b \pmod 2, \quad c \equiv d \pmod 2. \tag{7}$$

Let

$$s=b^2+d^2. \tag{8}$$

Then by (6) we have

$$sp-4=a^2+c^2, \tag{9}$$

$$0=ab+cd. \tag{10}$$

From (8), (9) and (10), we have

$$(sp-4)s=\left(a^2+c^2\right)\left(b^2+d^2\right)-(ab+cd)^2=(ad-bc)^2. \tag{11}$$

From (7) and (10) we have $a \equiv b \equiv c \equiv d \pmod 2$. If $a \equiv b \equiv c \equiv d \equiv 0 \pmod 2$, then by (8) we have $(s, sp-4)=4$. From (11) we get

$$s=4n^2, \quad sp-4=4m^2, \quad \left((m,n)=1, ad-bc=4mn\right),$$

so $m^2-n^2p=-1$, which contradicts with $p \equiv 3 \pmod 8$. Hence $a \equiv b \equiv c \equiv d \equiv 1 \pmod 2$, furthermore $(s, sp-4)=2$. Again from (11) we get

$$s=2x^2, \quad sp-4=2y^2, \quad \left((x,y)=1, ad-bc=2xy\right),$$

that is, $x^2-py^2=-2$ is solvable in integers.

https://doi.org/10.1017/S000497270003745X Published online by Cambridge University Press

References

[1] D.R. Estes and J.S. Hsia, 'Exceptional integers of some ternary quadratic forms', *Adv. Math.* **45** (1982), 310–318.

[2] D.R. Estes and J.S. Hsia, 'Sums of three integer squares in complex quadratic fields', *Proc. Amer. Math. Soc.* **89** (1983), 211-214.

[3] H. Maass, 'Über die Darstellung total positiver Zahlen des Köpers $R(\sqrt{5})$ als Summe von drei Quadraten', *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 185–191.

[4] 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.

[5] C.L. Siegel, 'Sums of mth powers of algebraic integers', *Ann. of Math.* **46** (1945), 313-339.

Department of Mathematics
Nanjing Normal University
Nanjing 210097
China
and
Institute of Mathematics
AMSS, Chinese Academy of Sciences
Beijing 100080
China
e-mail: cgji@amss.ac.cn