PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 89, Number 2, October 1983

SUMS OF THREE INTEGER SQUARES IN COMPLEX QUADRATIC FIELDS

DENNIS R. ESTES AND J. S. HSIA[1]

ABSTRACT. We classify all complex quadratic number fields that have all their algebraic integers expressible as a sum of three integer squares. These fields are $F = \mathbf{Q}(\sqrt{-D})$, D a positive square-free integer congruent to 3 (mod 8) and such that D does not admit a positive proper factorization $D \equiv d_1 d_2$ that satisfies simultaneously: $d_1 \equiv 5, 7 \pmod 8$ and $(d_2/d_1) = 1$.

We consider the following problem: *Which complex quadratic number fields* $F = \mathbf{Q}(\sqrt{-D})$, *$D$ square-free, have all their algebraic integers expressible as a sum of three integer squares?*

The fact that *all* the algebraic integers in F must be representable as a sum of 3 integer squares forces some necessary conditions on D. Firstly, -1 must be so expressible implies that -1 is a sum of two squares in F. This is because the minimal number ("Stufe") of representing -1 as a sum of squares in any formally nonreal field is well known to be always a 2-power. On the other hand, those number fields with Stufe ≤ 2 are known, already to Hasse in [**2**], to be classified by the property that all the local degrees are even at all the primes lying over $2\mathbf{Z}$. In the present situation this means $D \not\equiv 7 \pmod 8$. Secondly, since every sum of squares is congruent to a perfect square mod 2, we see that if $2\mathbf{Z}$ were ramified in F then there are algebraic integers which are incongruent to a square mod 2. Therefore, the discriminant of F must be an odd integer. These conditions then force $2\mathbf{Z}$ to be inert in F, i.e., $D \equiv 3 \pmod 8$, which we shall assume henceforth.

Presently, the following partial results are known. Every integer in F may be expressible as a sum of 3 integer squares when any of the following conditions is fulfilled:

(i) the class number h_F of F is odd [**3**, p. 532];
(ii) $h_F = 2 \times$ (odd integer) [**1**];
(iii) $D = q_1 q_2 q_3$ where q_i are primes congruent to 3 (mod 4) and $(q_i q_j / q_k) = -1$ for $\{i, j, k\} = \{1, 2, 3\}$ [**1**];
(iv) $X^2 + 2Y^2 = D$ is solvable in $\mathbf{Z}$ [**6**, p. 7].

In terms of factorizations of D, the classical theorems of Gauss and Rédei-Reichardt imply respectively that (i) is equivalent to D being a prime and (ii) to $D = pq$ where p, q are primes and $(p/q) = -1$. As for (iv) it is well known that the only odd square-free positive integers (and hence D) which can be represented by the binary form $X^2 + 2Y^2$ are those whose prime factors are either congruent to 1 or to 3 (mod 8).

Received by the editors October 15, 1982.
1980 *Mathematics Subject Classification.* Primary 10C02, 10C05.
Key words and phrases. Exceptional integer, genus, χ-invariant, Artin symbol.
[1]Research partially supported by NSF Grant MCS 80-02985 and MCS 82-02065.

0002-9939/83 $1.00 + $.25 per page

In fact, it was shown in [1] that in the first three cases above every algebraic integer in F is representable by *every* quadratic form in the genus of $X^2+Y^2+X^2$.

On the negative side, however, one knows not every integer is a sum of 3 integer squares for certain fields whose ideal class groups are either the Klein 4-group or the cyclic group of order four. See [1].

We shall give a complete answer to our problem, which is the following

THEOREM. *Every algebraic integer in* $F = \mathbf{Q}(\sqrt{-D})$, D *a positive square-free integer, can be expressed as a sum of three integer 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*: (1) $d_1 \equiv 5, 7 \pmod 8$ *and* (2) $(d_2/d_1) = 1$.

We may extract the following immediate corollary which is more explicit when the Sylow 2-subgroup $C_F(2)$ of the ideal class group C_F is cyclic.

COROLLARY. *Let* F *be as in the theorem with* $D \equiv 3 \pmod 8$. *Suppose* $C_F(2)$ *is cyclic. Then, every integer in* F *is a sum of three integer squares if and only if* D *satisfies any of the three conditions*: (a) D *is a prime;* (b) $D = pq$, p, q *primes,* $(p/q) = -1$; *and* (c) $D = pq$, p, q *primes,* $(p/q) = 1$, *and* $p \equiv 1 \pmod 8$, $q \equiv 3 \pmod 8$.

We now see that all the previously known results are recaptured. Results (i) and (ii) are covered by the corollary. As for (iv), since the only prime factors of D are those congruent to either 1 or 3 (mod 8), no such proper factorizations as required by the theorem are possible. To see result (iii), suppose $q_1 \equiv q_2 \equiv 7 \pmod 8$. Then d_1 can be either $q_1, q_2, q_1 q_3$, or $q_2 q_3$ so that violating condition (2) of the Theorem forces result (iii).

Next, we observe that since -1 is a sum of 2 squares in F the quadratic space associated to the form $I_3 = X^2 + Y^2 + Z^2$ must be isotropic, and therefore, the theoretical machinery derived in [1] may be applied. In particular, we can extract the following special cases of the theorems in [1, §§1, 2] for the genus of I_3 over $F = \mathbf{Q}(\sqrt{-D})$.

FACT I. *A nonzero integer* c *of* F *is an exceptional integer for the genus of* I_3 *(i.e.,* c *is representable by some, but not by every form in the genus) if and only if*:

(I.1) $-c$ *is a nonsquare in* F;

(I.2) $-c$ *is a square in* F_2;

(I.3) $F(\sqrt{-c})/F$ *is unramified*;

(I.4) *writing* $(c) = (\mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_t^{a_t})^2$, $a_j > 0$, *then at each* j *the Artin symbol*

$$\left(\frac{F(\sqrt{-c})/F}{\mathfrak{p}_j}\right) = 1.$$

FACT II. *A nonzero integer* c *of* F *is an exceptional integer for* I_3 *(i.e., some form in the genus of* I_3, *but not* I_3 *itself, represents* c*) if and only if*:

(II.1) $-c$ *is a nonsquare in* F;

(II.2) *every prime dividing* $(2c)$ *splits in* $F(\sqrt{-c})$;

(II.3) $F(\sqrt{-c})/F$ *is unramified*;

(II.4) *if* $\chi(I_3) = \tilde{A} C_F^2$ *then* $\tilde{A}$ *is not a norm from* $F(\sqrt{-c})$.

Here $\tilde{A}$ denotes the ideal class of A. For the definition of the χ-invariant, see [**4**, p. 329]. For our purpose here, it suffices to know that $\chi(I_3) = \tilde{A}C_F^2$ where A is the coefficient ideal of any isotropic vector.

REMARK. Fact II solves the finer problem of whether *a particular* algebraic integer c in F is or is not a sum of 3 integer squares. This can be exploited to pinpoint explicitly an integer which is not a sum of 3 integer squares. For example, take the cyclic Sylow 2-subgroup case where $D = pq$, p, q primes, $(p/q) = 1$, $p \equiv 5 \pmod 8$ and $q \equiv 7 \pmod 8$. One checks that $c = q$ is an exception for I_3.

PROOF OF THEOREM. View the form I_3 as a free ternary lattice with orthonormal basis $\{e_1, e_2, e_3\}$. If v is an isotropic vector with $v = a_1e_1 + a_2e_2 + a_3e_3$, then the coefficient ideal A of v in I_3 is given by

$$(a_1^{-1}) \cap (a_2^{-1}) \cap (a_3^{-1}) = (a_1) + (a_2) + (a_3).$$

See [**5**, p. 212]. Let R denote the ring of algebraic integers in F. Then, $\sum_{i=1}^3 a_iR$ is generated by any two of the a_i. To see this, we localize and assume R is a discrete valuation ring. Put $aR = \sum_{i=1}^3 a_iR$ and $a_i = at_i$. We may assume that not all a_i are zero so that one of t_i is a unit. But, $\sum t_i^2 = 0$. So, at least two of the t_i must be units which proves the claim.

Suppose $r, s, t, w \in \mathbf{Z}$ satisfy the equation $Dr^2 = s^2 + t^2 + w^2$. Then,

$$(s^2 + t^2)^2 + (sw + tr\sqrt{-D})^2 + (tw - sr\sqrt{-D})^2 = 0$$

gives rise to an isotropic vector. Hence, $\chi(I_3) = \tilde{A}C_F^2$ where $A = (s^2 + t^2)R + (sw + tr\sqrt{-D})R$.

Consider the binary quadratic form $f(X, Y) = -2X^2 + 2XY + ((D-1)/2)Y^2$. Since $D \equiv 3 \pmod 8$, this form is primitive. Hence, it represents an odd prime p prime to any fixed integer of our choice (see e.g. Dickson's History, Vol. I, p. 417). We take p prime to D. As $2p = 2f(x, y) = -(2x - y)^2 + Dy^2 = -1 + 3 \pmod 8$, $p \equiv 1 \pmod 4$. Set $2p = s^2 + t^2$, $2x - y = w$ and $y = r$. Then, $Dr^2 = s^2 + t^2 + w^2 = 2p + w^2$ and $\chi(I_3) = \tilde{A}C_F^2$, where

$$A = pR + \left(\frac{sw + tr\sqrt{-D}}{2}\right)R.$$

Now,

$$\begin{aligned} N_{F/\mathbf{Q}}(A) &= \left(pR + \left(\frac{sw + tr\sqrt{-D}}{2}\right)R\right)\left(pR + \left(\frac{sw - tr\sqrt{-D}}{2}\right)R\right) \\ &= p\left(pR + swR + \left(\frac{w^2 + t^2}{2}\right)R + \left(\frac{sw + tr\sqrt{-D}}{2}\right)R\right) = pR \end{aligned}$$

since $pR + swR + ((w^2 + t^2)/2)R = R$. We conclude, therefore, that A is a prime ideal of norm $p\mathbf{Z}$.

Suppose c is an exceptional integer for I_3, then it is surely exceptional for the genus of I_3. Set $(c) = B^2$ as in (I.4). Then $\tilde{B}$ contains an ambiguous ideal E. Write $B = bE$ and $E^2 = (d_1)$, where $d_1 | D$ and $c = ud_1b^2$ for some unit in R. We may assume clearly that $D > 3$. Hence, $u = \pm 1$. Replacing d_1 by $-d_1$, if needed, we may suppose that $c = d_1b^2$. By (I.1), $d_1 \neq -1$, D and $d_1 \equiv 3 \pmod 4$ by (I.2). Since

$F(\sqrt{-c}) = F(\sqrt{-d_1}) = F(\sqrt{d_2})$, $d_1 d_2 = D$, condition (I.4) implies that

$$\left(\frac{F(\sqrt{d_2})/F}{E}\right) = \left(\frac{d_2}{|d_1|}\right) = 1.$$

Next, condition (II.4)

$$\left(\frac{F\sqrt{-c})/F}{A}\right) = \left(\frac{-d_1}{p}\right) = \left(\frac{-2}{|d_1|}\right) = -1.$$

Conversely, assume there is a factorization $D = d_1 d_2$ satisfying $d_1 \equiv 3 \pmod 4$, $d_1 \neq -1$, D, $(d_2/|d_1|) = 1$ and $(-2/|d_1|) = -1$. Set $(d_1) = E^2$ and choose a prime ideal P in E and write $P = bE$ and $c = d_1 b^2$. Then $(c) = P^2$. Clearly, $-c$ is a nonsquare in F. Since $d_1 \equiv 3 \pmod 4$, $-c$ is a square in F_2. Condition (II.3) is a consequence of the equalities $F(\sqrt{-c}) = F(\sqrt{-d_1}) = F(\sqrt{d_2})$. Hence,

$$\left(\frac{F(\sqrt{-c})/F}{P}\right) = \left(\frac{F(\sqrt{d_2})/F}{E}\right) = \left(\frac{d_2}{|d_1|}\right) = 1.$$

So, we see (II.2) is satisfied. Finally, we note that $(-2/|d_1|) = -1$ implies condition (II.4) is also met. This proves c is an exceptional integer for I_3.

Recapturing, we have proved that I_3 has an exceptional integer if and only if D admits a factorization $D = d_1 d_2$ where (i) $d_1 \equiv 3 \pmod 4$, (ii) $d_1 \neq -1$, D, (iii) $(d_2/|d_1|) = 1$ and (iv) $(-2/|d_1|) = -1$. If we require the factorization of D to be positive proper then we get exactly the conditions as stated in our Theorem.

References

1. D. R. Estes and J. S. Hsia, *Exceptional integers of some ternary quadratic forms*, Adv. in Math. **45** (1982), 310–318.
2. H. Hasse, *Darstellbarkeit von Zahlen durch quadratische Formen in einem beliebigen algebraischen Zahlkorper*, J. Reine Angew. Math. **153** (1924), 113–130.
3. J. S. Hsia, *Representations by integral quadratic forms over algebraic number fields*, Queen's Papers in Pure and Appl. Math. **46** (1977), 528–537.
4. ———, *On the classification of unimodular quadratic forms*, J. Number Theory **12** (1980), 327–333.
5. O. T. O'Meara, *Introduction to quadratic forms*, Grundlehren der Math. Wiss., Springer-Verlag, New York, 1963.
6. P. Revoy, *Sur les sommes de carrés dans un anneau*, Ann. Sci. Univ. Besançon Math. (3) **11** (1979), 3–8.

Department of Mathematics, University of Southern California, Los Angeles, California 90089-1113

Department of Mathematics, Ohio State University, Columbus, Ohio 43210