ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 13, Number 1, Winter 1983

SUMS OF THREE AND FOUR INTEGER SQUARES

GARY R. GREENFIELD

The classical problem of determining which positive integers can be expressed as the sum of four integer squares was first solved in 1770 by Lagrange, while a solution to the companion problem of determining which positive integers can be expressed as the sum of three integer squares seems to have been known as early as the time of Gauss. The purpose of this note is to give brief, but elegant, proofs of these well known results. More specifically, by determining up to isomorphism the subfields of the division ring of rational quaternions and relying on certain properties of the ring's (reduced) norm and trace, we are able to solve the three square problem. From this we obtain the four square result as a simple corollary.

For the most part, our approach is of an elementary nature. But, unlike that of say [3] or [4], not completely so, since at a certain stage of the development we must rely on facts concerning the division ring of rational quaternions which are to be more properly found in the theory of finite dimensional central simple algebras and algebraic number theory. Thus, upon completion, it is our hope that the interested reader will delve more deeply into these fascinating subjects by consulting the references provided.

Fix a positive integer n. To determine whether n is the sum of three integer squares it is necessary first to reduce to the problem of determining when the square-free part of n is the sum of three rational squares. To facilitate this reduction we introduce some notation.

In three dimensional Eucludean space E^3, we say a point $\mathbf{p} = (p_1, p_2, p_3)$ is *rational* (respectively *integral*) if each coordinate p_i is rational (respectively integral). For a rational point $\mathbf{p}$, there is a smallest positive integer d_p such that $d_p\mathbf{p}$ is integral (d_p is merely the least common multiple of the denominators of the p_i when expressed as fractions in lowest terms) and, evidently, $d_p = 1$ if and only if $\mathbf{p}$ is integral. Let $S(n)$ be the sphere of radius $\sqrt{n}$ in E^3 centered at the origin. We have $S(n) = \{\mathbf{p} \in E^3: p_1^2 + p_2^2 + p_3^2 = n\}$. Clearly, n is the sum of three rational (respectively integer) squares if and only if $S(n)$ contains a rational (respectively integral) point.

Received by the editors on February 6, 1981.

LEMMA 1. *The positive integer n is the sum of three integer squares if and only if it is the sum of three rational squares.*

PROOF. It suffices to show that if $S(n)$ contains a rational point, then it contains an integral point. Suppose not. Then among all rational points of $S(n)$ select one, say $\mathbf{x}$, with d_x minimal. Let $\mathbf{y} \in E^3$ be an integral point chosen such that $|x_i - y_i| \leqq 1/2$ for all i. Set $\mathbf{z} = \mathbf{x} - \mathbf{y}$ and $d = d_x |\mathbf{z}|^2$. Since $|\mathbf{z}|^2 = |\mathbf{x} - \mathbf{y}|^2 \leqq (1/2)^2 + (1/2)^2 + (1/2)^2 = 3/4$ and $\mathbf{x} \neq \mathbf{y}$, we have

$$(*) \qquad 0 < |\mathbf{z}|^2 < 1$$

and therefore,

$$(**) \qquad 0 < d < d_x.$$

In addition,

$$\begin{aligned} d &= d_x|\mathbf{z}|^2 \\ &= d_x(\mathbf{x} - \mathbf{y})\cdot(\mathbf{x} - \mathbf{y}) \\ &= d_x(|\mathbf{x}|^2 - 2(\mathbf{x}\cdot\mathbf{y}) + |\mathbf{y}|^2) \\ &= d_x|\mathbf{x}|^2 - 2(d_x\mathbf{x})\cdot\mathbf{y} + d_x|\mathbf{y}|^2 \end{aligned}$$

and by examining this last expression we easily conclude that d is an integer.

Let L be the line in E^3 through $\mathbf{x}$ and $\mathbf{y}$. If L is tangent to $S(n)$, the Pythagorean Theorem yields $|\mathbf{x}|^2 + |\mathbf{z}|^2 = |\mathbf{y}|^2$ which forces $|\mathbf{z}|^2$ to be an integer, contradicting (*) above. Thus L intersects $S(n)$ in another point $\mathbf{x}'$. By virtue of the vector equation for L, we may write $\mathbf{x}' = \mathbf{x} + \lambda\mathbf{z}$ for some nonzero real number λ. Using $\mathbf{x}'\cdot\mathbf{x}' = (\mathbf{x} + \lambda\,\mathbf{z})\cdot(\mathbf{x} + \lambda\,\mathbf{z})$ to solve for λ, we find $\lambda = -2(\mathbf{x}\cdot\mathbf{z})/|\mathbf{z}|^2$ so λ is fact rational, whence $\mathbf{x}'$ is a rational point of $S(n)$. Now, the calculation

$$\begin{aligned} d\mathbf{x}' &= d_x|\mathbf{z}|^2(\mathbf{x} + \lambda\mathbf{z}) \\ &= d_x|\mathbf{z}|^2\mathbf{x} - 2d_x(\mathbf{x}\cdot\mathbf{z})\mathbf{z} \\ &= |\mathbf{z}|^2\, d_x\mathbf{x} - 2d_x(\mathbf{x}\cdot\mathbf{z})\mathbf{x} + 2d_x(\mathbf{x}\cdot\mathbf{z})\,\mathbf{y} \\ &= (|\mathbf{x}|^2 - 2(\mathbf{x}\cdot\mathbf{y}) + |\mathbf{y}|^2)d_x\mathbf{x} - 2d_x\,|\mathbf{x}|^2\,\mathbf{x} \\ &\quad + 2d_x(\mathbf{x}\cdot\mathbf{y})\mathbf{x} + 2d_x(\mathbf{x}\cdot\mathbf{z})\,\mathbf{y} \\ &= (|\mathbf{y}|^2 - |\mathbf{x}|^2)(d_x\mathbf{x}) + (2d_x\,|\mathbf{x}|^2 - 2(d_x\mathbf{x})\cdot\mathbf{y})\mathbf{y} \end{aligned}$$

shows $d\mathbf{x}'$ is an integral point of E^3. Thus, by definition, $d_{x'} \leqq d$ and combining with (**) we get $d_{x'} < d_x$ which contradicts the choice of $\mathbf{x}$. This completes the proof of the lemma.

LEMMA 2. *Let $n = s^2m$ where s, m are positive integers and m is square*

free. Then n is the sum of three rational squares if and only if m is the sum of three rational squares.

PROOF. This is routine, and left to the reader.

Let K be a Pythagorean field and denote by U_K the division ring of ordinary quaternions over K. Recall that $U_K = \{x_0 + x_1 i + x_2 j + x_3 k: x_i \in K\}$ is a four-dimensional vector space over K with basis $\{1, i, j, k\}$ and that multiplication in U_K is determined by extending linearly the multiplication defined on basis elements as follows: $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$, and $i^2 = j^2 = k^2 = -1$. The element $u = x_0 + x_1 i + x_2 j + x_3 k \in U_K$ has *conjugate* $\bar{u} = x_0 - x_1 i - x_2 j - x_3 k$, *(reduced) norm* $N(u) = u\bar{u} = x_0^2 + x_1^2 + x_2^2 + x_3^2$, and *(reduced) trace* $T(u) = u + \bar{u} = 2x_0$. Moreover, direct calculation shows that for u, $v \in U_K$, $\overline{uv} = \bar{v}\bar{u}$, $\overline{u + v} = \bar{u} + \bar{v}$, and $\bar{\bar{u}} = u$. Of primary importance to us are the special properties that the subfields of U_K possess.

LEMMA 3. *Let L be a field with $K \subsetneq L \subsetneq U_K$. Let $u \in U_K \backslash K$.*
(i) *The minimal polynomial for u is $x^2 - T(u)\,x + N(u)$.*
(ii) *The field $K(u)$ is quadratic over K.*
(iii) *If $v \in L \backslash K$, then $L = K(v)$.*
(iv) *L is a maximal subfield of U_K.*

PROOF. Multiplying the identity $u - T(u) + \bar{u} = 0$ by u gives $u^2 - T(u)\,u + N(u) = 0$. Since $u \notin K$, the monic polynomial $x^2 - T(u)\,x + N(u)$ which u satisfies must be its minimal polynomial. This proves (i). Statement (ii) follows directly from (i). By the Primitive Element Theorem $L = K(w)$ for some $w \in L \backslash K$. But v, $w \in U_K \backslash K$ so both $K(v)$ and $K(w)$ are quadratic over K. Since $K(v) \subseteq L$, $L = K(v)$ and (iii) is proved. We have seen that proper subfields of U_K are quadratic, so indeed they must be maximal, as stated in (iv).

REMARK. If $u \in U_K \backslash K$, then $K(u)$ is Galois over K, with Galois group generated, say, by the automorphism σ. Since $\bar{u} = T(u) - u \in \{a + bu: a, b \in K\} = K(u)$ and $\bar{u}^2 - T(u)\bar{u} + N(u) = \bar{u}^2 - T(\bar{u})\bar{u} + N(\bar{u}) = 0$, we must have $\sigma(u) = \bar{u}$. Therefore $N(u) = u\sigma(u)$, $T(u) = u + \sigma(u)$ and we see N and T are just the ordinary norm and trace of the element u calculated from the field $K(u)$ to K.

We say a field extension L of K is a *splitting field* for U_K if $U_K \otimes_K L \cong M_2(L)$, the ring of 2×2 matrices over L. By invoking a rather deep structure theorem [1, Theorem 27, p. 61] it follows that a field extension L of K with $[L: K] = 2$ is isomorphic to a (maximal) subfield of U_K if and only if it is a splitting field for U_K. This fact will play an important role in the sequel.

Before leaving our general setting, a final remark is in order. U_K has

the structure of a *cyclic crossed product* (see [1] or [7]) as follows. Let τ be the generating automorphism of the Galois extension $K(i)$ over K. Denote by $(K(i)/K, \tau, -1)$ the left $K(i)$-module $\{c + dj: c, d \in K(i)\}$ with multiplication defined according to the relations $j^2 = -1$ and $jd = \tau(d)j$. Then $U_K = (K(i)/K, \tau, -1)$.

Let Q be the field of rational numbers and consider U_Q, the familiar division ring of rational quaternions. A quick glance at the reduced norm formula makes it readily apparent that in U_Q, $N(u)$ is a positive rational number for all $u \neq 0$. The following two lemmas make precise the relationship between U_Q and the three square problem.

LEMMA 4. *Let $m > 1$ be a square free integer. Then m is the sum of three rational squares if and only if there exists $u \in U_Q$ such that $N(u) = m$ and $T(u) = 0$.*

PROOF. If m is the sum of three rational squares, say $m = x_1^2 + x_2^2 + x_3^2$, simply take $u = x_1 i + x_2 j + x_3 k$. Conversely an element $u = x_0 + x_1 i + x_2 j + x_3 k$ satisfying $N(u) = m$ and $T(u) = 0$ has $x_0 = 0$ so $m = x_1^2 + x_2^2 + x_3^2$, as desired.

LEMMA 5. *Let $m > 1$ be a square free integer. Then m is the sum of three rational squares if and only if there exists $u \in U_Q \backslash Q$ such that the fields $Q(u)$ and $Q(\sqrt{-m})$ are isomorphic.*

PROOF. Assume m is the sum of three rational squares. By the previous lemma, we are guaranteed the existence of an element $u \in U_Q$ with $T(u) = 0$ and $N(u) = m$. If $u \in Q$, then $N(u) = u^2$ so m is a square, a contradiction. Thus $u \in U_Q \backslash Q$ and by Lemma 3 u has minimal polynomial $x^2 - T(u)x + N(u) = x^2 + m$ whence the field $Q(u)$ is isomorphic to $Q(\sqrt{-m})$. For the converse, suppose we are given $u \in U_Q$ such that $Q(u) \cong Q(\sqrt{-m})$. Then we may choose $v \in Q(u)$ such that $v^2 = -m$. Clearly, $v \notin Q$, $Q(v) = Q(u)$, and v has minimal polynomial $x^2 + m$. Comparing with the minimal polynomial expression found in Lemma 3, we conclude $T(v) = 0$ and $N(v) = m$. By the previous lemma, m is the sum of three rational squares.

Of course, up to isomorphism, representatives for fields quadratic over Q are given by the fields $Q(\sqrt{d})$ where $d \neq 0, 1$ ranges over the square free integers. The objective now is clear: we want to determine which fields of this type are isomorphic to subfields of U_Q. By a previous remark, this is equivalent to determining which fields of this type are splitting fields for U_Q. Though this may seem to be a formidable obstacle, with the aid of Hasse invariants it will become almost effortless.

We shall not attempt to give a full treatment of Hasse invariants here (excellent sources are [2] and [7]). For the moment, it is enough to say that the Hasse invariants of U_Q are fractions modulo one which are

assigned to the primes (inequivalent valuations) of Q subject to certain arithmetic restrictions. To compute these Hasse invariants we must rely on the construction of U_Q as a cyclic crossed product. Let ∞ denote the infinite prime of Q, and let R be the field of real numbers.

LEMMA 6. *The Hasse invariants of U_Q are given by*

$$\operatorname{inv}_p U_Q \equiv \begin{cases} 1/2 & \text{modulo one, if } p = 2 \text{ or } \infty \\ 0 & \text{modulo one, otherwise.} \end{cases}$$

PROOF. By definition, $\operatorname{inv}_\infty U_Q \equiv 1/2$ modulo one, as $U_Q \otimes_Q Q_\infty \cong U_Q \otimes_Q R \cong U_R$. If $p \neq 2$ is a finite prime of Q, then p is unramified from Q to $Q(i)$ [**5**, Theorem 9.1, p. 39], so the cyclic crossed product $(Q(i)/Q, \tau, -1)$ has $\operatorname{inv}_p U_Q \equiv 0$ modulo one [**1**, Theorem 14, p. 75, and Theorem 19, p. 141]. Finally, Hasse's Sum Theorem ensures $\operatorname{inv}_p U_Q \equiv 1/2$ modulo one, for $p = 2$.

To determine when $L = Q(\sqrt{d})$ with $d \neq 0, 1$ square free is a splitting field for U_Q, we must determine when $U_Q \otimes_Q L \cong M_2(L)$. Fortunately, Hasse invariants are defined for tensor products of U_Q with finite extensions of Q and, more importantly, they will distinguish matrix rings according to the criterion that the invariants of the tensor product be identically zero. With this in mind we prove the following lemma.

LEMMA 7. *Let $d \neq 0, 1$ be a square free integer. Then $Q(\sqrt{d})$ is a splitting field for U_Q if and only if $d < 0$ and $d \not\equiv 1 \pmod 8$.*

PROOF. Let ∞_1, ∞_2 be the primes of $Q(\sqrt{d})$ extending the prime ∞ of Q. If $d < 0$, these primes are complex, while if $d > 0$, these primes are real. Thus, by definition,

$$\operatorname{inv}_\infty U_Q \otimes_Q Q(\sqrt{d}) \equiv \begin{cases} 1/2 & \text{modulo one, if } d > 0 \\ 0 & \text{modulo one, if } d < 0. \end{cases}$$

This shows the condition $d < 0$ is necessary. Moreover, when $d < 0$, $Q(\sqrt{d})$ will be a splitting field for U_Q unless the prime $p = 2$ of Q splits completely in $Q(\sqrt{d})$. This occurs [**8**, Theorem 6, 2–1] if and only if $d \equiv 1 \pmod 8$. Our proof is complete.

We can now give our main result. It is a solution to the three square problem obtained by blending the prepared ingredients.

THEOREM 8. *Let n be a positive integer. Write $n = s^2 m$ where s, m are positive integers and m is square free. Then n is the sum of three integer squares if and only if $m \not\equiv -1 \pmod 8$.*

PROOF. If $m = 1$, this is obvious, so assume $m > 1$. By Lemmas 1 and

2 it suffices to show m is the sum of three rational squares if and only if $m \not\equiv -1 \pmod 8$. By Lemma 5 and a remark on splitting fields, m is the sum of three rational squares if and only $Q(\sqrt{-m})$ is a splitting field for U_Q; and by the previous lemma this occurs if and only if $-m \not\equiv 1 \pmod 8$ or, equivalently, $m \not\equiv -1 \pmod 8$.

A version of the three square result more amenable to computations, and frequently given (see [3] or [6]) is the following corollary.

COROLLARY 9. *Let n be a positive integer. Write $n = 4^a\ell$ where $4 \nmid \ell$. Then n is the sum of three integer squares if and only if $\ell \not\equiv 7 \pmod 8$.*

PROOF. If we write $n = s^2m$ as in our theorem and say $s = 2^bq$ where q is odd, then evidently $q^2m = \ell$. An examination of cases shows $q^2 \equiv 1 \pmod 8$, whence $m \equiv \ell \pmod 8$. Therefore n is the sum of three integer squares if and only if $\ell \not\equiv -1 \pmod 8$ or, equivalently, $\ell \not\equiv 7 \pmod 8$.

A special case of the theorem is highlighted for use in solving the four square problem.

COROLLARY 10. *If $m \equiv 7 \pmod 8$ is a square free positive integer, then $m - 1$ is the sum of three integer squares.*

PROOF. Let $m - 1 = 4^e\ell$, where $4 \nmid \ell$. Since $m \equiv 7 \pmod 8$, $m - 1 \equiv 6 \pmod 8$, so $e = 0$. Thus $\ell = m - 1 \equiv 6 \pmod 8$, and by Corollary 9, the result follows.

Our final result is at hand. Though it is really a corollary to the three square result, for historical reasons we will list it as a theorem.

THEOREM 11. *Every positive integer is the sum of four integer squares.*

PROOF. Let $n = 4^e\ell$ where $4 \nmid \ell$ is a positive integer. By Corollary 9 we need only consider the case where $\ell \equiv 7 \pmod 8$. Then the previous corollary shows $\ell - 1$ is the sum of three integer squares, say $\ell - 1 = x_1^2 + x_2^2 + x_3^2$, whence $n = (2^ex_1)^2 + (2^ex_2)^2 + (2^ex_3)^2 + (2^e)^2$ and the proof is complete.

REFERENCES

1. A. Albert, *Structure of Algebras*, American Math. Society, New York, 1939.
2. M. Deuring, *Algebra*, Springer-Verlag, New York/Berlin, 1968.
3. L. Dickson, *Modern Elementary Theory of Numbers*, The University of Chicago Press, Chicago, 1960.
4. I. Herstein, *Topics in Algebra*, 2nd Ed., Xerox Publishing Company, Lexington, MA, 1975.
5. J. Janusz, *Algebraic Number Fields*, Academic Press, New York, 1973.
6. E. Landau, *Elementare Zahlentheorie*, Chelsea, New York, 1945.

7. I. Reiner, *Maximal Orders*, Academic Press, New York, 1975.
8. E. Weiss, *Algebraic Number Theory*, Chelsea, New York, 1963.

MATHEMATICAL SCIENCES DEPARTMENT, UNIVERSITY OF RICHMOND, RICHMOND, VA 23173