QUATERNIONS AND SUMS OF FOUR SQUARES

LILY SILVERSTEIN

1. Abstract

This paper will prove the theorem that every positive integer can be written as the sum of four squares. First, it will build a definition of Hamilton's quaternions, which comprise a four-dimensional vector space that extends the complex numbers. Just as the norm of a complex number is a sum of two squares, the norm of a quaternion is a sum of four squares, and so every number that can be the norm of a quaternion can be written as a sum of four squares. A subset of these can be written as a sum of four integral squares. The proof will show that this subset of norms is closed under multiplication and that it contains all the positive prime integers. Thus every positive integer will be expressible both as the norm of a rational quaternion and as a sum of four squares.

2. Introduction to Quaternions

Much as the complex plane is constructed by adjoining the real numbers with a new element, $i = \sqrt{-1}$, the ring of quaternions is constructed by adjoining the real numbers with three new elements, creating a four-dimensional vector space.

We denote the ring of quaternions $\mathbb{H}$ after Sir William Hamilton, who discovered them in 1843.

These new basis vectors are denoted j, k, l, with $j^2 = k^2 = l^2 = -1$, so each is a square root of -1. Nonetheless, they are distinct elements, with the following relations:

Date: 12/1/09.

$$ij = k \quad ji = -k$$
$$jk = i \quad kj = -i$$
$$ki = j \quad ik = -j$$

Thus every element α of the quaternions is expressed as a linear combination of these basis vectors: $\alpha = a + bi + cj + dk$. The set $\mathbb{H} = \{a + bi + cj + dk \,|\, a, b, c, d \in \mathbb{Q}\}$ is known as the rational quaternions.

Another way to regard the rational quaternions is as a subset of $M_2(\mathbb{C})$, the 2 x 2 matrices with complex entries. Here, we can define i, j, and k so that they are more clearly distinct:

$$i = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix} \quad j = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \quad k = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$$

If we let $1 = I_2 \in M_2(\mathbb{C})$, we can see more naturally that the above defined relationships among the basis elements hold true, and that i, j, k are all indeed distinct square roots of -1. The matrix definitions of the elements of $\mathbb{H}$ also make it easier to see that multiplication of elements is associative and distributive (since matrix multiplication is associative and distributive). Knowing these properties hold, we can find a product formula for $(a+bi+cj+dk)(a'+b'i+c'j+d'k)$ by expanding and distributing tediously. Like terms are combined, keeping in mind that the rational numbers of the center of $\mathbb{H}$; that is, rational numbers will commute with all elements of $\mathbb{H}$, i.e. $\frac{3}{5}j = j\frac{3}{5}$, and so like terms can be further combined.. This tedious multiplication yields a new element of the form $a + bi + cj + dk$, showing that $\mathbb{H}$ is closed under multiplication. Closure of addition follows immediately from the definition of addition as component-wise. Thus $\mathbb{H}$ is a ring.

3. Conjugate, Norm, and Inverse

For $\alpha \in \mathbb{H}$ we will define the conjugate $\bar{\alpha}$ and the norm $N(\alpha)$ as follows:

$$\bar{\alpha} = a - bi - cj - dk$$
$$N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2$$

From the definition of $N(\alpha)$ it is clear that $N(\alpha)$ is a rational number, and as such $N(\alpha)$ will commute with any quaternion. Further, it is clear that $N(\alpha) = N(\bar{\alpha})$.

We use these definitions to demonstrate an inverse for every nonzero quaternion. Let $\alpha \neq 0$. We claim that $N(\alpha)^{-1}\bar{\alpha}$ is a multiplicative inverse:

$$\begin{aligned}\alpha(N(\alpha)^{-1}\bar{\alpha}) &= (\alpha N(\alpha)^{-1})\bar{\alpha} \\ &= (N(\alpha)^{-1}\alpha)\bar{\alpha} \\ &= N(\alpha)^{-1}N(\alpha) \\ &= 1\end{aligned}$$

and

$$\begin{aligned}(N(\alpha)^{-1}\bar{\alpha})\alpha &= N(\alpha)^{-1}(\bar{\alpha}\alpha) \\ &= N(\alpha)^{-1}N(\bar{\alpha}) \\ &= N(\alpha)^{-1}N(\alpha) \\ &= 1\end{aligned}$$

Since every nonzero element $\alpha \in \mathbb{H}$ has an inverse in $\mathbb{H}$, the ring of quaternions is a division ring. It is not a field, since multiplication is not commutative (easily seen from $ij = -ji$, for instance). $\mathbb{H}$ was the first known example of a noncommutative division ring, or strictly skew field[**?**].

4. Integral Quaternions

We define a subring of $\mathbb{H}$ which we will call the ring of integral quaternions:

$$\mathbf{D} = \{a + bi + cj + dk \mid 2a, 2b, 2c, 2d \text{ are integers of the same parity}\}$$

If $\alpha \in \mathbf{D}$, then $N(\alpha)$ is an integer, by the following argument:

$4N(\alpha) = (2a)^2 + (2b)^2 + (2c)^2 + (2d)^2 \in \mathbb{Z}$, since we assumed $2a, 2b, 2c, 2d$ were all integers.

We also assumed $2a \equiv 2b \equiv 2c \equiv 2d \pmod 2$. Thus $(2a)^2 \equiv (2b)^2 \equiv (2c)^2 \equiv (2d)^2 \pmod 4$. Thus $4N(\alpha) \equiv 0 \pmod 4$, so $N(\alpha)$ is an integer.

Calling $\mathbf{E}$ the set of all norms of integral quaternions, we see that $\mathbf{E} \subseteq \mathbb{Z}$.

5. Norms of Integral Quaternions are Sums of Four Squares

Now we will prove that $n \in \mathbf{E} \iff n$ can be written as the sum of four squares.

$\implies$ Assume $n \in \mathbf{E}$; then $n = N(\alpha)$ for $\alpha \in \mathbf{D}$. Then

$$4n = (2a)^2 + (2b)^2 + (2c)^2 + (2d)^2$$

where $2a, 2b, 2c, 2d$ are all integers. So write:

$$4n = x^2 + y^2 + z^2 + w^2$$

Using a parity argument, since this sum is even, it must be that x, y, z, w are all odd, all even, or two odd and two even. At the very least we can say the latter, so assume $x \equiv y \pmod 2$ and $z \equiv w \pmod 2$. Then

$$2n = \left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2$$

Since x, y and z, w have the same parity, $2n$ is again a sum of four integral squares.

Now we have $2n = x'^2 + y'^2 + z'^2 + w'^2$ for some new integers x', y', z', w', so we can make the same parity argument and write n itself as a sum of four integral squares.

$\impliedby$ If $n = a^2 + b^2 + c^2 + d^2 = N(\alpha)$, then $\alpha = \pm a \pm b \pm c \pm d$ where $a, b, c, d \in \mathbb{Z}$, so $\alpha \in \mathbf{D}$, so $n \in \mathbf{E}$.

6. All Positive Integers are Sums of Four Squares

We will take it for granted that $\mathbf{E}$ is closed under multiplication, since $\mathbf{D}$ is closed under multiplication and $N(\alpha_1)N(\alpha_2) = N(\alpha_1\alpha_2)$ (see [**?**] for details).

Now all we need to show is that all the primes belong to $\mathbf{E}$ and it will follow that all positive integers belong to this set, and thus all positive integers are expressible as the sum of four squares.

Let p be an odd prime. There is a lemma that we can find x, y such that $1+x^2+y^2 \equiv 0 \pmod{p}$. (Proof: Let $\{r_1, r_2, \ldots, r_{(p-1)/2}\}$ be the quadratic residues of p. Together with $r_0 = 0$, form the two subsets $\{r_0, r_1, \ldots, r_{(p-1)/2}\}$ and $\{-1-r_0, -1-r_1, \ldots, -1-r_{(p-1)/2}$. Each has $(p-1)/2+1$ elements, so $r_j = -1 - r_i$ for some i, j. Let $x^2 \equiv r_j \pmod{p}$ and $y^2 \equiv r_i \pmod{p}$. Then $1 + x^2 + y^2 \equiv 0 \pmod{p}$.)

Write $p \,|\, 1 + x^2 + y^2$. If we let $\gamma = 1 + xi + yj \in \mathbf{D}$, then $p \,|\, \gamma\bar{\gamma}$ in $\mathbf{D}$. If p were prime in $\mathbf{D}$, it would have to divide either γ or $\bar{\gamma}$ since it divides their product. But neither $\frac{\gamma}{p} = \frac{1}{p} + \frac{x}{p}i + \frac{y}{p}j$ nor $\frac{\bar{\gamma}}{p} = \frac{1}{p} - \frac{x}{p}i - \frac{y}{p}j$ is integral, so p divides neither and is not prime in $\mathbf{D}$.

Thus, we can write $p = \alpha\beta$ for two non-units α and β. We already knew that $N(p) = p^2$; now we can say that $N(p) = N(\alpha)N(\beta) = p^2$. Since neither α nor β is a unit, $N(\alpha) > 1$ and $N(\beta) > 1$. Thus $N(\alpha) = N(\beta) = p$. Since p is the norm of an integral quaternion, it is the sum of four squares.

All odd primes thus belong to $\mathbf{E}$, since $2 = 1^2 + 1^2 + 0^2 + 0^2$ also does, we get every positive integer as the sum of four primes.

7. Problems

(1) Find an isomorphism that takes an arbitrary quaternion $a + bi + cj + dk$ to a 2 x 2 matrix (hint: find each entry of the matrix in terms of a, b, c, and d).

(2) Prove that $N(\alpha_1\alpha_2) = N(\alpha_1)N(\alpha_2)$.

References

[1] Bolker, Ethan. *Elementary Number Theory: An Algebraic Approach*, Dover, 1969. pp 127-138

[2] Fraleigh, John. *A First Course in Abstract Algebra, Seventh Ed.*, Addison-Wesley, 2002. pp 224-226

[3] Goodman, Roe and Nolan Wallach. *Symmetry, Representations, and Invariants*. Springer, 2009. pp 8-10