Sums of Four Squares

Ryan C. Daileda

Trinity University

Number Theory

Introduction

We have completely classified the natural numbers that can be written as sums of two or three squares.

What about sums of four squares?

It turns out that the quadratic form

$$Q(X, Y, Z, W) = X^2 + Y^2 + Z^2 + W^2$$

is *universal*, i.e. it represents *every* natural number.

This is Lagrange's four squares theorem, which we will prove today.

Sums of Four Squares

The representability of integers as sums of four squares relies on the following lemma.

Lemma 1 (Euler)

If $m, n \in \mathbb{N}$ are both sums of four squares, then so is mn.

Rather than simply cite a mysterious identity, let's put this result in context.

We define the *Hamiltonian quaternions* to be the 4-dimensional real vector space

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}.$$

Quaternions can be added together coordinate-wise, and multiplied together by appealing to the rules

$$i^2 = j^2 = k^2 = ijk = -1.$$

These give us

$$\begin{aligned} ij &= -(ij)k^2 = -(ijk)k = k, \;\; jk = -i^2jk = -i(ijk) = i, \\ ki &= -ki(j^2) = -k(ij)j = -k^2j = j, \\ ji &= -j(k^2)i = -(jk)(ki) = -ij, \\ kj &= -k(i^2)j = -(ki)(ij) = -jk, \\ ik &= -i(j^2)k = -(ij)(jk) = -ki, \end{aligned}$$

so that i, j and k are *anti-commutative*.

Remarks

- The relationships $ij = k$, $jk = i$, $ki = j$, $ij = -ji$, $kj = -jk$ and $ik = -ik$ are precisely the relationships satisfied by the unit vectors i, j and k in $\mathbb{R}^3$ under the cross product!

- The map

$$a + bi + cj + dk \mapsto \begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

  embeds $\mathbb{H}$ into the ring $\mathrm{M}_{4\times 4}(\mathbb{R})$.

  This yields a concrete representation of $\mathbb{H}$ as a ring of real 4×4 matrices.

Norms of Quaternions

Given $z \in \mathbb{H}$, write $z = a + \mathbf{v}$, where $\mathbf{v} = xi + yj + zk \in \mathbb{R}^3$.

Suppose $w = b + \mathbf{u} \in \mathbb{H}$. Then it is not hard to show that

$$zw = (ab - \mathbf{u} \cdot \mathbf{v}) + a\mathbf{u} + b\mathbf{v} + \mathbf{v} \times \mathbf{u},$$

the final product being the cross product in $\mathbb{R}^3$.

In particular

$$\begin{aligned} N(z) &= (a + \mathbf{v})(a - \mathbf{v}) = (a^2 + \mathbf{v} \cdot \mathbf{v}) + a\mathbf{v} - a\mathbf{v} - \mathbf{v} \times \mathbf{v} \\ &= a^2 + |\mathbf{v}|^2 = a^2 + x^2 + y^2 + z^2. \end{aligned}$$

Given $z = a + \mathbf{v} \in \mathbb{H}$, define $z^* = a - \mathbf{v}$.

Then $N(z) = zz^*$.

Write $z = a + \mathbf{v}$ and $w = b + \mathbf{u}$. Then

$$\begin{aligned} w^*z^* = (b - \mathbf{u})(a - \mathbf{v}) &= (ab - \mathbf{u} \cdot \mathbf{v}) - a\mathbf{u} - b\mathbf{v} + \mathbf{u} \times \mathbf{v} \\ &= (ab - \mathbf{u} \cdot \mathbf{v}) - a\mathbf{u} - b\mathbf{v} - \mathbf{v} \times \mathbf{u} \\ &= ((a + \mathbf{v})(b + \mathbf{u}))^* = (zw)^*. \end{aligned}$$

Hence

$$\begin{aligned} N(zw) = (zw)(zw)^* &= (zw)(w^*z^*) \\ &= zN(w)z^* = zz^*N(w) = N(z)N(w), \end{aligned}$$

since $N(w) \in \mathbb{R}$ commutes with all of $\mathbb{H}$.

Quaternions and Euler's Lemma

Because $N(a+bi+cj+dk) = a^2+b^2+c^2+d^2$, we obtain:

Lemma 2 (Euler)

If $m, n \in \mathbb{N}$ can be written as the sum of four squares, then so can mn.

Explicitly, if $m = a_1^2+a_2^2+a_3^2+a_4^2 = N(\underbrace{a_1+a_2i+a_3j+a_4k}_{z})$and

$n = b_1^2+b_2^2+b_3^2+b_4^2 = N(\underbrace{b_1+b_2i+b_3j+b_4k}_{w})$, then

$$\begin{aligned} mn = N(z)N(w) = N(zw) &= (a_1b_1-a_2b_2-a_3b_3-a_4b_4)^2 \\ &+ (a_1b_2+a_2b_1+a_3b_4-a_4b_3)^2 + (a_1b_3-a_2b_4+a_3b_1+a_4b_2)^2 \\ &+ (a_1b_4+a_2b_3-a_3b_2+a_4b_1)^2. \end{aligned}$$

Sums of Squares in $\mathbb{Z}/p\mathbb{Z}$

We now need another lemma.

Lemma 3

Let p be a prime. For all $a \in \mathbb{Z}$, there exist $x, y \in \mathbb{Z}$ so that

$$x^2 + y^2 \equiv a \pmod{p}.$$

Proof. If $a \equiv 0 \pmod{p}$ or $\left(\dfrac{a}{p}\right) = 1$, we are finished.

So we may assume that $\left(\dfrac{a}{p}\right) = -1$.

Suppose, for the sake of contradiction, that $x^2 + y^2 \equiv a \pmod{p}$ has no solution.

Suppose $\left(\dfrac{b}{p}\right) = -1$. Then $\left(\dfrac{ab}{p}\right) = (-1)(-1) = 1$,so that $ab \equiv z^2 \pmod{p}$, for some $z \in \mathbb{Z}$.

If $x^2 + y^2 \equiv b \pmod{p}$, then $(ax)^2 + (ay)^2 \equiv a^2 b \equiv z^2 a \pmod{p}$.

Multiplying by $z^{-2} \pmod{p}$, we obtain $(axz^{-1})^2 + (ayz^{-1})^2 \equiv a \pmod{p}$, contrary to our assumption on a.

We conclude that if $\left(\dfrac{b}{p}\right) = -1$, then $x^2 + y^2 \equiv b \pmod{p}$ has no solution.

This means that $x^2 + y^2 \equiv z^2 \pmod{p}$ for all integers x and y.

This shows that the set of squares in $\mathbb{Z}/p\mathbb{Z}$ is closed under addition.

Thus

$$a \equiv \underbrace{1^2 + 1^2 + \cdots + 1^2}_{a \text{ times}} \equiv z^2 \pmod{p},$$

which is a contradiction.

Therefore $x^2 + y^2 \equiv a \pmod{p}$ must have a solution when $\left(\frac{a}{p}\right) = -1$, which completes the proof. □

Remark. Lemma 3 still holds (with essentially the same proof) if we replace $\mathbb{Z}/p\mathbb{Z}$ by any *finite field*.

Now let p be an odd prime. Taking $a = -1$ in Lemma 3, we obtain $x, y \in \mathbb{Z}$ so that

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}.$$

We can assume $0 \le x, y \le p - 1$. Replacing x and y by $p - x$ and $p - y$, if necessary, we can arrange it so that $x, y < p/2$.

We then have

$$0 < kp = x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{2} + 1 < p^2,$$

which implies that $k < p$.

Thus:

Lemma 4

Let p be an odd prime. Then there exists a positive integer $k < p$ so that kp is the sum of four squares.

Proof. Indeed, our work above shows that

$$kp = x^2 + y^2 + 1^2 + 0^2.$$

□

We are now ready to establish the next important result.

Theorem 1

Every prime can be expressed as the sum of four squares (some of which may be 0).

Proof

Let p be a prime. Since $2 = 1^2 + 1^2 + 0^2 + 0^2$, we may assume p is odd.

According to Lemma 4, there is a positive $k < p$ so that kp is the sum of four squares.

The Well Ordering Principle implies that there is a least such k. We claim that, in fact, $k = 1$.

Write $kp = x^2 + y^2 + z^2 + w^2$ and assume that $k > 1$.

If k is even we obtain $0 \equiv x^2 + y^2 + z^2 + w^2 \equiv x + y + z + w \pmod 2$, by Fermat's theorem.

It follows that among x, y, z, w, an even number of them must be odd.

This implies that we can reorder x, y, z and w so that

$$x \equiv y \pmod{2} \quad \text{and} \quad z \equiv w \pmod{2}.$$

Then

$$\frac{x+y}{2}, \frac{x-y}{2}, \frac{z+w}{2}, \frac{z-w}{2}$$

are all integers, and

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

which contradicts the minimality of k.

Therefore we must have that k is odd and at least 3.

Choose $a, b, c, d \in \mathbb{Z}$ so that

$$a \equiv x \pmod{k}, b \equiv y \pmod{k}, c \equiv z \pmod{k}, d \equiv w \pmod{k},$$

with $|a|, |b|, |c|, |d| < k/2$.

Then

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{k},$$

so that $a^2 + b^2 + c^2 + d^2 = nk$ for some $n \geq 0$.

Note that

$$0 \leq nk = a^2 + b^2 + c^2 + d^2 < 4\left(\frac{k}{2}\right)^2 = k^2 \;\; \Rightarrow \;\; n < k.$$

If $n = 0$, then $a = b = c = d = 0$, and $x \equiv y \equiv z \equiv w \equiv 0 \pmod{k}$, which implies

$$k^2 | x^2 + y^2 + z^2 + w^2 = kp \ \Rightarrow \ k|p \ \Rightarrow \ k = 1,$$

since $k < p$. But $k > 1$ so this cannot be.

We conlclude that $0 < n < k$.

Thus

$$\begin{aligned} k^2np = (nk)(kp) &= (a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) \\ &= r^2 + s^2 + t^2 + u^2, \end{aligned}$$

where r, s, t, u are as described above.

Specifically,

$$\begin{aligned} r &= ax + by + cz + dw, \\ s &= ay - bx - cw + dz, \\ t &= az + bw - cx - dy, \\ u &= aw - bz + cy - dx. \end{aligned}$$

Here we have replaced b, c, d with $-b, -c, -d$, which is permissible since each of these quantities is squared.

Notice that

$$\begin{aligned} r &\equiv a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod{k}, \\ s &\equiv ab - ab - cd + cd \equiv 0 \pmod{k}, \\ t &\equiv ac + bd - ac - bd \equiv 0 \pmod{k}, \\ u &\equiv ad - bc + bc - ad \equiv 0 \pmod{k}. \end{aligned}$$

Thus we can divide our earlier equality by k^2 to obtain

$$np = \left(\frac{r}{k}\right)^2 + \left(\frac{s}{k}\right)^2 + \left(\frac{t}{k}\right)^2 + \left(\frac{u}{k}\right)^2,$$

with $0 < n < k$.

This contradicts the minimality of k, and the proof is complete. □

Remark. The proof we have given is nonconstructive: it guarantees the existence of a representation as a sum of four squares, but gives no indication of how to actually find it.

Lagrange's Four Squares Theorem

As a corollary we now deduce:

Theorem 2 (Lagrange)

Every natural number can be written as the sum of four squares (some of which may be 0).

Proof. Let $n \in \mathbb{N}$. Since $1 = 1^2 + 0^2 + 0^2 + 0^2$, we may assume $n > 1$.

Then n is a product of primes, each of which can be written as the sum of four squares, by the preceding theorem.

By Euler's lemma (and a quick induction) this implies that n is a sum of four squares.

□

Example

Because Euler's lemma *is* constructive, the proof of Lagrange's theorem is also constructive, up to expressing each prime as a sum of four squares.

Consider the integer $564 = 2^2 \cdot 3 \cdot 47$.

We have

$$3 = 1^2 + 1^2 + 1^2 + 0^2, \;\; 47 = 6^2 + 3^2 + 1^2 + 1^2.$$

Let $z = 1 + i + j$ and $w = 6 + 3i + j + k$. Then

$$\begin{aligned} zw &= (6 - 3 - 1) + (3 + 6 + 1)i + (1 + 6 + -1)j + (1 + 1 - 3)k \\ &= 2 + 10i + 6j - k. \end{aligned}$$

Thus

$$\begin{aligned}564 &= 2^2 \cdot 3 \cdot 47 = 2^2 N(z)N(w)\\ &= 2^2 N(zw) = 2^2(2^2 + 10^2 + 6^2 + 1^2)\\ &= \boxed{4^2 + 20^2 + 12^2 + 2^2}.\end{aligned}$$

Remarks.

Given $k \geq 2$, *Waring's problem* asks for the least $g(k)$ so that every natural number can be expressed as the sum of $g(k)$ kth powers.

Our work on sums of squares proves that $g(2) = 4$.

It is known that $g(3) = 9$, $g(4) = 19$, $g(5) = 37$, and that

$$g(k) = [(3/2)^k] + 2^k - 2$$

for $k \geq 6$, with at most finitely many exceptions.