

# Classifying Quaternion Identities

THEODORE EHRENBORG

I SHOULD THANK PROFESSOR LEEP, PROFESSOR SARNAK, AND  
GIVING ME TIME.

September 1, 2019

## Abstract

This number theory project investigates identities found by multiplying together quaternions in  $\mathbb{L}[x, y, z, w]$ , the Lipschitz quaternions  $\mathbb{L}$  adjoined with the indeterminates  $x, y, z, w$ . Recall that quaternions are 4-dimensional complex numbers. These identities provide solutions to  $\sum_{j=1}^p \tau_j^2 = (\sum_{i=1}^m x_i^2)^n$ . We present a rigorous definition that captures the intuitive notion of when two such identities are equivalent. This definition implies that the true structure of this problem involves the group action of the direct product  $\mathfrak{S}_4^\pm \times \mathfrak{S}_4^\pm$ . Using two complementary methods, we compute the number of equivalence classes for  $n = 1, 2, 3, 4$ , where  $n$  is the number of quaternion factors. We move to the case concerning products of complex numbers, namely  $\mathbb{Z}[i][x, y]$ . Using the fact that the Gaussian integers are commutative under multiplication, we characterize these equivalence classes, thus also providing an enumeration. This enumeration quickly gives a proof that the total number of solutions in  $\mathbb{Z}[x, y]$  to  $a^2 + b^2 = (x^2 + y^2)^n$  is  $4n + 4$ . Assuming that all identities when  $p = m = 4$  are a product of quaternions, we prove that the total number of solutions in  $\mathbb{Z}[x, y, z, w]$  to  $a^2 + b^2 + c^2 + d^2 = (x^2 + y^2 + z^2 + w^2)^n$  is no more than  $8 \sum_{i=0}^n 47^i$ . Experimental data for  $n = 0, 1, 2, 3$  suggests that this expression is exact.

## Todo list

■ I should thank Professor Leep, Professor Sarnak, and LAA at HCHS for giving me  
time. . . . . 1

## 1 Introduction

The author's previous work in [2] focused on characterizing the integer solutions to  $a^2 + b^2 + c^2 + d^2 = e^2$ . This paper explores the polynomial solutions in  $\mathbb{Z}[x, y, z, w]$  to  $a^2 + b^2 + c^2 + d^2 = e^n$ , where  $e = x^2 + y^2 + z^2 + w^2$ .

In [2] the author characterized integer solutions by viewing  $a^2 + b^2 + c^2 + d^2 = e^2$  as a product of two quaternions. This gave rise to polynomial solutions to  $a^2 + b^2 + c^2 + d^2 = e^2$  with  $e = x^2 + y^2 + z^2 + w^2$ . The paper found that an upper bound for the number of such solutions is 57. This paper seeks to improve that bound, as well as to investigate the cases when  $n > 2$ .

Recall that the *complex numbers*  $\mathbb{C}$  are a two-dimensional field extension of  $\mathbb{R}$ . Complex numbers take the form  $x + iy$ , where  $i$  is defined to be the square root of  $-1$  and  $x, y \in \mathbb{R}$ . Addition is component-wise, and multiplication follows from the distributive property and the fact that  $i^2 = -1$ . The *conjugate* of a complex number  $z = x + iy$  is  $\bar{z} = x - iy$ , and the *norm* is  $N(z) = z\bar{z} = x^2 + y^2$ .

The *Gaussian integers*  $\mathbb{Z}[i]$  are a subring of  $\mathbb{C}$ :

$$\mathbb{Z}[i] = \{x + iy : x, y \in \mathbb{Z}\}.$$

Recall that the *quaternions*  $\mathcal{Q}$  are a four-dimensional division ring extension of  $\mathbb{R}$ . Quaternions were first discovered by Sir William Rowan Hamilton; see [3]. Quaternions take the form  $x + iy + jz + kw$ , with  $x, y, z, w \in \mathbb{R}$ , and the linearly independent elements  $i, j, k$  satisfy the relations:

$$\begin{aligned} i^2 &= j^2 = k^2 = -1, \\ ij &= -ji = k, \\ jk &= -kj = i, \\ ki &= -ik = j. \end{aligned}$$

Addition is component-wise, and multiplication, which is in general not commutative, follows from the distributive property and the preceding relations. The *conjugate* of a quaternion  $\alpha = x + iy + jz + kw$  is  $\bar{\alpha} = x - iy - jz - kw$ , and the *norm* is  $N(\alpha) = \alpha\bar{\alpha} = x^2 + y^2 + z^2 + w^2$ .

The *Lipschitz quaternions*  $\mathbb{L}$  are a subring of the quaternions  $\mathcal{Q}$ :

$$\mathbb{L} = \{x + iy + jz + kw \in \mathcal{Q} : x, y, z, w \in \mathbb{Z}\}.$$

In the remainder of this paper  $x, y, z, w$  will usually refer to indeterminates.

The following groups are an essential part of Definition 1.2 and Definition 2.1.

**Definition 1.1.** The *symmetric group*  $\mathfrak{S}_n$  is the set of all permutations  $\pi = \pi_1\pi_2 \cdots \pi_n$  of the  $n$  element set  $\{1, 2, \dots, n\}$ , where  $\pi(i) = \pi_i$ . The *signed symmetric group*  $\mathfrak{S}_n^\pm$  is the set of all permutations  $\sigma = \sigma_1\sigma_2 \cdots \sigma_n$  of the set  $\{\pm 1, \pm 2, \dots, \pm n\}$  such that  $|\sigma| = |\sigma_1| \cdots |\sigma_n| \in \mathfrak{S}_n$  and  $\sigma(-i) = -\sigma(i)$ .

For a signed permutation  $\pi \in \mathfrak{S}_m^\pm$ , let  $\pi$  act on a polynomial in the  $m$  variables  $x_1, x_2, \dots, x_m$  by sending  $x_j$  to

$$\pi(x_j) = \begin{cases} x_{\pi_j} & \text{if } \pi_j > 0 \\ -x_{-\pi_j} & \text{if } \pi_j < 0 \end{cases}$$

**Definition 1.2.** Fix  $p, m \in \mathbb{N}$ . Let  $\tau = (\tau_1, \tau_2, \dots, \tau_p)$  be a tuple of length  $p$  where  $\tau_i \in \mathbb{Z}[x_1, x_2, \dots, x_m]$  for  $i = 1, \dots, p$ . We define an equivalence relation, denoted by  $\simeq$ , on  $p$ -tuples  $\tau$  by taking the transitive closure of the following three relations:

- $(\tau_1, \dots, \tau_p) \simeq (\tau'_1, \dots, \tau'_p)$  if there exists a signed permutation  $\pi \in \mathfrak{S}_m^\pm$  acting on the  $m$  variables such that  $\pi(\tau_i) = \tau'_i$ , where  $i = 1, \dots, p$ .
- $(\tau_1, \dots, \tau_p) \simeq (\tau'_1, \dots, \tau'_p)$  if there exists a permutation  $\sigma \in \mathfrak{S}_p$  such that  $\tau_{\sigma(i)} = \tau'_i$ , where  $i = 1, \dots, p$ .
- $(\tau_1, \dots, \tau_p) \simeq (\pm\tau_1, \dots, \pm\tau_p)$

**Example 1.3.** Definition 1.2 implies that the following is true:

$$\begin{aligned} (xz, y^2, yz) &\simeq ((-y)(-x), z^2, z(-x)) \\ &\simeq ((-y)(-x), z(-x), z^2) \\ &\simeq (-(-y)(-x), z(-x), -z^2) \end{aligned}$$

We are interested in counting the number of equivalence classes of the set of all tuples  $\tau = (\tau_1, \dots, \tau_p)$ , where

$$\sum_{j=1}^p \tau_j^2 = \left( \sum_{i=1}^m x_i^2 \right)^n \quad (1.1)$$

This problem is most easily attacked when we view  $(\sum_{i=1}^m x_i^2)^n$  as the norm of a product of complex numbers or quaternions. Thus we will focus on the cases where  $p = m = 2$  and where  $p = m = 4$ . The general problem can also be viewed as finding the disjoint orbits of various tuples, where the group action is  $\mathfrak{S}_p^\pm \times \mathfrak{S}_m^\pm$ .

**Example 1.4.** Consider the case where  $p = m = 2$  and  $n = 2$ . The following two identities are representatives from the two different equivalence classes in this case. These identities were generated by a product of complex numbers.

Identity I:

$$(x + iy)(x + iy) = (x^2 - y^2) + i(2xy).$$

Taking norms gives the identity

$$(x^2 - y^2)^2 + (2xy)^2 = (x^2 + y^2)^2. \quad (1.2)$$

Identity II:

$$(x + iy)(x - iy) = (x^2 + y^2) + i(0).$$

Taking norms gives the identity

$$(x^2 + y^2)^2 + (0)^2 = (x^2 + y^2)^2. \quad (1.3)$$

*Remark 1.5.* Equation (1.2) dates back to Euclid; see [5].

**Example 1.6.** The following two identities are representatives from the two different equivalence classes in the case where  $p = m = 2$  and  $n = 3$ . These identities were generated by a product of complex numbers.

Identity III:

$$(x + iy)(x + iy)(x + iy) = x(x^2 - 3y^2) + iy(3x^2 - y^2).$$

Taking norms gives the identity

$$(x(x^2 - 3y^2))^2 + (y(3x^2 - y^2))^2 = (x^2 + y^2)^3. \quad (1.4)$$

Identity IV:

$$(x + iy)(x + iy)(x - iy) = x(x^2 + y^2) + i(y(x^2 + y^2)).$$

Taking norms gives the identity

$$(x(x^2 + y^2))^2 + (y(x^2 + y^2))^2 = (x^2 + y^2)^3. \quad (1.5)$$

## 2 The case where $p = m = 2$

In the case where  $p = m = 2$ , Definition 1.2 has an alternate form.

**Definition 2.1.** Let  $h(z), h'(z) \in \mathbb{Z}[i][x, y]$ , where  $z = x + iy$ . Let  $M$  be the following set of mappings:

$$M = \{z \mapsto uz : u \in \{\pm 1, \pm i\}\} \cup \{z \mapsto u\bar{z} : u \in \{\pm 1, \pm i\}\}.$$

We say  $h(z)$  is equivalent to  $h'(z)$ , denoted  $h(z) \simeq h'(z)$ , when there exist mappings  $\varphi, \varphi' \in M$  such that  $\varphi(h(\varphi'(z))) = h'(z)$ .

**Lemma 2.2.** *The relation  $\simeq$  is an equivalence relation.*

*Proof.* The relation  $\simeq$  satisfies the three conditions of an equivalence relation:

1. Reflexive Property: If we choose  $\mu$  and  $\mu'$  to be the identity map  $z \mapsto z$ , then  $h(z) \simeq h(z)$ .
2. Symmetric Property: Let  $h(z) \simeq h'(z)$ , that is, there exist mappings  $\mu, \mu' \in M$  such that  $\mu(h(\mu'(z))) = h'(z)$ . The set  $M$  is isomorphic to the signed symmetric group  $\mathfrak{S}_2^\pm$ , so every mapping in  $M$  has an inverse in  $M$ . As  $\mu^{-1}(h'((\mu')^{-1}(z))) = h(z)$ , we have  $h'(z) \simeq h(z)$ .

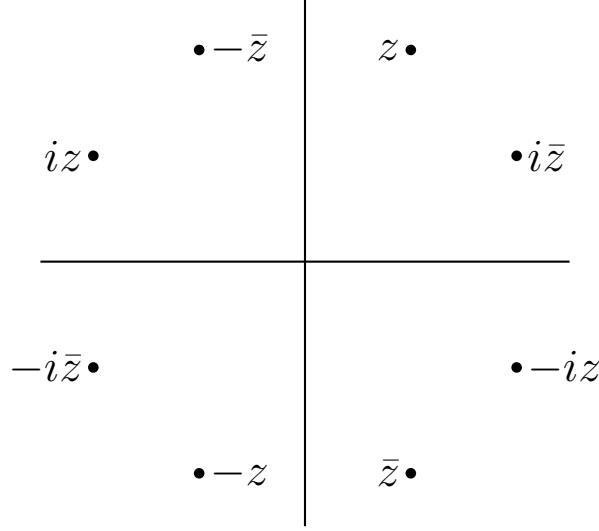


Figure 1: The set  $M$  in Definition 2.1 is isomorphic to the signed symmetric group  $\mathfrak{S}_2^\pm$ .

3. Transitive Property: Let  $a(z) \simeq b(z)$  and  $b(z) \simeq c(z)$ . By the Symmetric Property, we have  $c(z) \simeq b(z)$ . Thus there exist mappings  $\mu, \mu', \nu, \nu' \in M$  such that  $\mu(a(\mu'(z))) = b(z)$  and  $\nu(c(\nu'(z))) = b(z)$ . As a result we obtain

$$\mu(a(\mu'(z))) = \nu(c(\nu'(z))).$$

Thus we have

$$a(z) = \mu^{-1}(\nu(c((\mu')^{-1}(\nu'(z)))).$$

This means that  $c(z) \simeq a(z)$  or  $a(z) \simeq c(z)$ . □

Recall that given  $a(x, y), b(x, y) \in \mathbb{Z}[x, y]$ , we can find  $h(z) \in \mathbb{Z}[i][x, y]$  such that  $z = x + iy$  and  $h(z) = a(x, y) + i \cdot b(x, y)$ . The converse is also true.

**Lemma 2.3.** *Let  $h(z) \simeq h'(z)$ , where  $h(z), h'(z) \in \mathbb{Z}[i][x, y]$  and  $z = x + iy$ . Suppose  $(x^2 + y^2)^u \mid h(z)$ , where  $u \in \mathbb{N}$ . Then  $(x^2 + y^2)^u \mid h'(z)$  also holds.*

*Proof.* Let  $h(z) = (x^2 + y^2)^u p(z)$ , where  $p(z) \in \mathbb{Z}[i][x, y]$ . Whatever mappings we apply to  $h$  and  $z$  to obtain  $h'(z)$ , we also apply to the factors of  $h(z)$ . No mapping will remove the factor of  $(x^2 + y^2)^u$ . □

**Corollary 2.4.** *Let  $h(z), h'(z) \in \mathbb{Z}[i][x, y]$  with  $z = x + iy$ . Suppose  $h(z) \simeq h'(z)$ . Then for all  $u \in \mathbb{N} \cup \{0\}$ , the following two conditions are equivalent:*

- i.  $(x^2 + y^2)^u \mid h(z)$ ,
- ii.  $(x^2 + y^2)^u \mid h'(z)$ .

**Theorem 2.5.** *Consider the set of all 2-tuples  $\tau = (\tau_1, \tau_2)$  where  $\tau_1^2 + \tau_2^2 = (x_1^2 + x_2^2)^n$ . The number of equivalence classes within this set is exactly  $\lfloor n/2 \rfloor + 1$ . Moreover, each equivalence class contains a tuple of the form  $(\operatorname{Re}(\beta), \operatorname{Im}(\beta))$ , where  $\beta = (x + iy)^j(x - iy)^{n-j}$ , with  $j$  being one of  $0, 1, \dots, \lfloor n/2 \rfloor$ .*

*Proof.* Suppose

$$(x^2 + y^2)^n = a(x, y)^2 + b(x, y)^2,$$

where  $a(x, y), b(x, y) \in \mathbb{Z}[x, y]$ . Both sides of the equation can be factored, leading to

$$(x + iy)^n(x - iy)^n = (a(x, y) + i \cdot b(x, y))(a(x, y) - i \cdot b(x, y)).$$

Since  $\mathbb{Z}[i][x, y]$  is a unique factorization domain, we can factor this as

$$a(x, y) + i \cdot b(x, y) = c \cdot (x + iy)^j(x - iy)^k$$

and

$$a(x, y) - i \cdot b(x, y) = d \cdot (x + iy)^r(x - iy)^s,$$

where  $j, k, r, s \in \mathbb{N} \cup \{0\}$  and  $c \cdot d = 1$  with  $c, d \in \{\pm 1, \pm i\}$ . We know  $j + r = n$  and  $k + s = n$ , as well as (by taking norms)  $j + k = n$  and  $r + s = n$ . Thus  $k = r$  and  $j = s$ .

Clearly the relation  $a(x, y) + i \cdot b(x, y) \simeq a(x, y) - i \cdot b(x, y)$  holds. Since

$$a(x, y) + i \cdot b(x, y) = c \cdot (x + iy)^j(x - iy)^{n-j}$$

and

$$a(x, y) - i \cdot b(x, y) = d \cdot (x + iy)^{n-j}(x - iy)^j,$$

each equivalence class contains a representative with  $j \leq n - j$ . As  $2j \leq n$ , we have  $j \leq n/2$ , so  $j$  is one of  $0, 1, \dots, \lfloor n/2 \rfloor$ . This shows that there are at most  $\lfloor n/2 \rfloor + 1$  equivalence classes. Now we show that there are at least that many.

Consider  $(x + iy)^u(x - iy)^{n-u}$  and  $(x + iy)^v(x - iy)^{n-v}$ , where  $u \neq v$  and  $u, v \leq \lfloor n/2 \rfloor$ . We have

$$\begin{aligned} (x + iy)^u(x - iy)^{n-u} &= (x^2 + y^2)^u(x - iy)^{n-2u}, \\ (x + iy)^v(x - iy)^{n-v} &= (x^2 + y^2)^v(x - iy)^{n-2v}. \end{aligned}$$

Without loss of generality, we may assume  $u > v$ . Since  $\mathbb{Z}[i][x, y]$  is a unique factorization domain,  $(x^2 + y^2) \nmid (x - iy)^e$  for  $e \in \mathbb{N} \cup \{0\}$ . Thus  $(x^2 + y^2)^u \mid (x + iy)^u(x - iy)^{n-u}$  but  $(x^2 + y^2)^u \nmid (x + iy)^v(x - iy)^{n-v}$ .

By Corollary 2.4,  $(x + iy)^u(x - iy)^{n-u} \not\sim (x + iy)^v(x - iy)^{n-v}$ , so the  $\lfloor n/2 \rfloor + 1$  representatives arise from distinct equivalence classes. Thus there are  $\lfloor n/2 \rfloor + 1$  equivalence classes, one each for  $u = 0, 1, \dots, \lfloor n/2 \rfloor$ .  $\square$

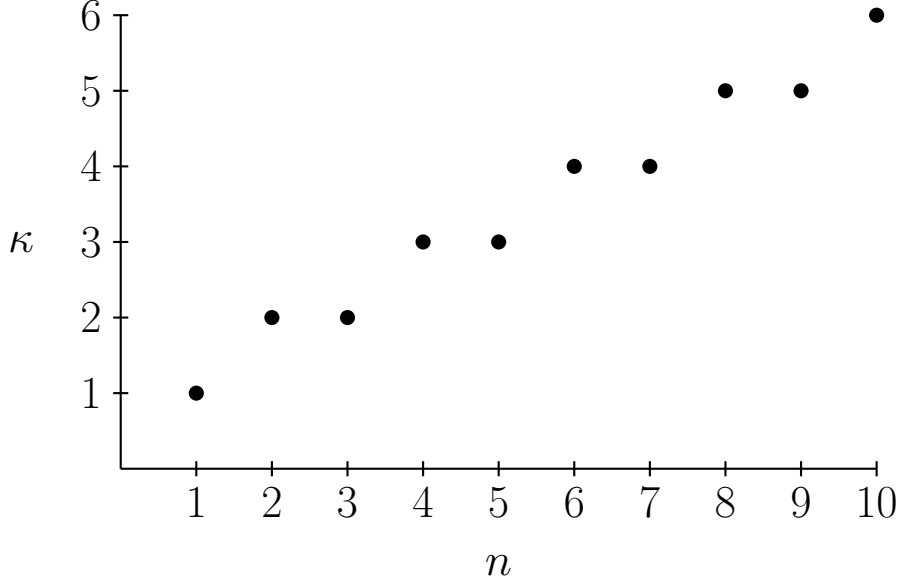


Figure 2: The number of equivalence classes  $\kappa$  when  $p = m = 2$  is  $\lfloor n/2 \rfloor + 1$ .

**Corollary 2.6.** *The number of solutions  $(a, b)$  to*

$$a^2 + b^2 = (x^2 + y^2)^n,$$

where  $a, b \in \mathbb{Z}[x, y]$ , is  $4n + 4$ .

*Proof.* It is sufficient to count the orbits of a representative from each equivalence class, where the group action is  $\mathfrak{S}_2^\pm \times \mathfrak{S}_2^\pm$ .

Case I:  $n = 2z$  for some  $z \in \mathbb{Z}$ .

There are  $z + 1$  equivalence classes. We choose  $z + 1$  representatives of the form  $(x - iy)^j(x + iy)^k$ , with  $0 \leq j \leq n/2$  and  $j + k = n$ . When  $j = k$ , the representative is  $(x - iy)^z(x + iy)^z = (x^2 + y^2)^z$ . This gives the tuple  $(x^2 + y^2, 0)$ , which has an orbit of order 4. Otherwise, we write the representative as  $(x + iy)^{k-j}(x^2 + y^2)^j$ . As  $k - j$  is even, let  $k - j = 2w$ . We have

$$\begin{aligned} (x + iy)^{2w} &= x^{2w} - \binom{2w}{2} x^{2w-2} y^2 + \cdots + \binom{2w}{2w-2} x^2 y^{2w-2} (-1)^{w-1} + y^{2w} (-1)^w \\ &\quad + i \left( \binom{2w}{1} x^{2w-1} y + \cdots + \binom{2w}{2w-1} x y^{2w-1} (-1)^{w-1} \right). \end{aligned} \quad (2.1)$$

As a tuple, this has two entries, where the first is the real part of equation (2.1) and the second entry is the imaginary part. The order of the stabilizer is 8 — the two variables can be rearranged and their signs switched. This may require the sign of an entire expression to

be switched, depending on the parity of  $w$ . As  $|\mathfrak{S}_2^\pm \times \mathfrak{S}_2^\pm| = 64$ , the order of each orbit is also 8.

Thus in Case I there are  $8z + 4 = 4(n + 1)$  solutions to  $a^2 + b^2 = (x^2 + y^2)^n$ .

Case II:  $n = 2z + 1$  for some  $z \in \mathbb{Z}$ .

There are  $z + 1$  equivalence classes. We choose  $z + 1$  representatives of the form  $(x - iy)^j(x + iy)^k$ , with  $0 \leq j \leq n/2$  and  $j + k = n$ . It is impossible to choose  $j$  such that  $\text{Im}((x - iy)^j(x + iy)^k) = 0$ . We write the representative as  $(x + iy)^{k-j}(x^2 + y^2)^j$ . As  $k - j$  is odd, let  $k - j = 2w + 1$ . We have

$$\begin{aligned} (x + iy)^{2w+1} &= x^{2w+1} - \binom{2w+1}{2} x^{2w-1} y^2 + \cdots + \binom{2w+1}{2w} x y^{2w} (-1)^w \\ &\quad + i \left( \binom{2w+1}{1} x^{2w} y + \cdots + \binom{2w+1}{2w-1} x^2 y^{2w-1} (-1)^{w-1} + y^{2w+1} (-1)^w \right). \end{aligned} \quad (2.2)$$

As a tuple, this has two entries, where the first is the real part of equation (2.2) and the second entry is the imaginary part. The order of the orbit of the tuple under the group action is 8, which can be verified similarly to Case I.

Thus the number of solutions in Case II is  $8(z + 1) = 4(2w + 1) + 4 = 4n + 4$ .  $\square$

### 3 The case where $p = m = 4$

In this section we examine the case where  $p = m = 4$  in equation (1.1). This case is approached by factoring the identities into quaternions in  $\mathbb{L}[x, y, z, w]$ . The quaternions' lack of multiplicative commutativity precludes the technique used in the proof of Theorem 2.5, so experimental data becomes more important.

Two methods of gathering experimental data about the number of equivalence classes are used. In the first method, the program *numeric\_comparison* is used to calculate specific numerical values of the identities in order to separate them into equivalence classes. If two identities fulfill a different set of solutions, they are not equivalent.

For  $n = 2$ , a sample of this process appears in Table 1. This program provides a lower bound on the number of identities, but cannot prove that two identities are equivalent.

To show that identities are in the same equivalence class, the *symbolic\_comparison* program uses particular group actions from  $\mathfrak{S}_4^\pm \times \mathfrak{S}_4^\pm$  to prove equivalence. An image of this process appears in Figure 3. This program provides an upper bound on the number of identities, but cannot prove that two identities are not equivalent.

The two programs agree on the values for  $n = 1$  to 4. This data appears in Table 2.



Identity Value	(3.1)	(3.2)	(3.3)	(3.4)	(3.5)	(3.6)	(3.7)	(3.8)
$0^2 + 0^2 + 0^2 + 0^2 = 0^2$								
$0^2 + 0^2 + 0^2 + 1^2 = 1^2$								
$0^2 + 0^2 + 0^2 + 2^2 = 2^2$								
$0^2 + 0^2 + 0^2 + 3^2 = 3^2$								
$0^2 + 0^2 + 0^2 + 4^2 = 4^2$								
$0^2 + 1^2 + 2^2 + 2^2 = 3^2$								
$1^2 + 1^2 + 1^2 + 1^2 = 2^2$								
$2^2 + 2^2 + 2^2 + 2^2 = 4^2$								

Table 1: Small data values used by *numeric\_comparison* to differentiate between equivalence classes of identities. Shaded cells indicate that the particular value of  $a^2 + b^2 + c^2 + d^2 = e^2$  was a particular value of the identity.

$n$	$\kappa$
1	1
2	8
3	48
4	965

Table 2: The conjectured number of equivalence classes  $\kappa$  in the case where  $p = m = 4$ .

**Theorem 3.1.** *In the case where  $p = m = 4$  and  $n = 2$ , the following identities arise from 8 different equivalence classes.*

$$(x^2 - y^2 - z^2 - w^2)^2 + (2xy)^2 + (2xz)^2 + (2xw)^2 = (x^2 + y^2 + z^2 + w^2)^2 \quad (3.1)$$

$$(x^2 - y^2 - z^2 + w^2)^2 + (2xy - 2zw)^2 + (2xz + 2yw)^2 + (0)^2 = (x^2 + y^2 + z^2 + w^2)^2 \quad (3.2)$$

$$(x^2 + y^2 + z^2 + w^2)^2 + (0)^2 + (0)^2 + (0)^2 = (x^2 + y^2 + z^2 + w^2)^2 \quad (3.3)$$

$$(x^2 - y^2 - 2zw)^2 + (2xy + z^2 - w^2)^2 + (xz - yz + xw + yw)^2 + (xz - yz + xw + yw)^2 = (x^2 + y^2 + z^2 + w^2)^2 \quad (3.4)$$

$$(x^2 - y^2)^2 + (2xy - z^2 - w^2)^2 + (xz + yz + xw + yw)^2 + (-xz - yz + xw + yw)^2 = (x^2 + y^2 + z^2 + w^2)^2 \quad (3.5)$$

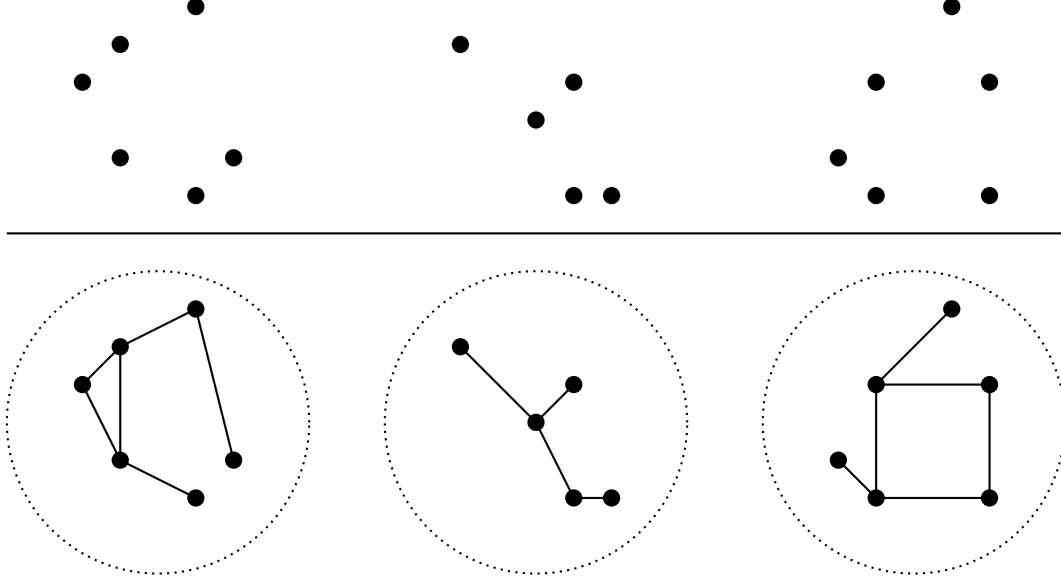


Figure 3: The program *symbolic\_comparison* finds particular equivalence relations that link different identities together, showing that they belong to the same equivalence class. In practice, there are orders of magnitude more identities (represented as dots) and many more equivalence classes (the connected subgraphs) than shown here. Moreover, the program had access to enough elements of the group action so that the subgraphs were usually complete.

$$(x^2 + y^2)^2 + (-z^2 - w^2)^2 + (xz + yz + xw - yw)^2 + (-xz + yz + xw + yw)^2 = (x^2 + y^2 + z^2 + w^2)^2 \quad (3.6)$$

$$(x^2 - yz - yw - zw)^2 + (xy + xz + yz - w^2)^2 + (-y^2 + xz + xw + zw)^2 + (xy - z^2 + xw + yw)^2 = (x^2 + y^2 + z^2 + w^2)^2 \quad (3.7)$$

$$(x^2 - yz + yw - zw)^2 + (xy + xz - yz - w^2)^2 + (y^2 + xz + xw + zw)^2 + (xw - xy - z^2 + yw)^2 = (x^2 + y^2 + z^2 + w^2)^2 \quad (3.8)$$

Furthermore, each identity is generated by a product of quaternions.

*Proof.* Identity (3.1) follows from taking the norm of the quaternion product

$$(x + iy + jz + kw)(x + iy + jz + kw) = (x^2 - y^2 - z^2 - w^2) + i(2xy) + j(2xz) + k(2xw).$$

Identity (3.2) follows from taking the norm of the quaternion product

$$(x + iy + jz + kw)(x + iy + jz - kw) = (x^2 - y^2 - z^2 + w^2) + i(2xy - 2zw) + j(2xz + 2yw) + k(0).$$

Identity (3.3) follows from taking the norm of the quaternion product

$$\begin{aligned} & (x + iy + jz + kw)(x - iy - jz - kw) \\ &= (x^2 + y^2 + z^2 + w^2) + i(0) + j(0) + k(0). \end{aligned}$$

Identity (3.4) follows from taking the norm of the quaternion product

$$\begin{aligned} & (x + iy + jz + kw)(x + iy + jw + kz) \\ &= (x^2 - y^2 - 2zw) + i(2xy + z^2 - w^2) \\ &+ j(xz - yz + xw + yw) + k(xz - yz + xw + yw). \end{aligned}$$

Identity (3.5) follows from taking the norm of the quaternion product

$$\begin{aligned} & (x + iy + jz + kw)(x + iy + jw - kz) \\ &= (x^2 - y^2) + i(2xy - z^2 - w^2) \\ &+ j(xz + yz + xw + yw) + k(-xz - yz + xw + yw). \end{aligned}$$

Identity (3.6) follows from taking the norm of the quaternion product

$$\begin{aligned} & (x + iy + jz + kw)(x - iy + jw - kz) \\ &= (x^2 + y^2) + i(-z^2 - w^2) \\ &+ j(xz + yz + xw - yw) + k(-xz + yz + xw + yw). \end{aligned}$$

Identity (3.7) follows from taking the norm of the quaternion product

$$\begin{aligned} & (x + iy + jz + kw)(x + iz + jw + ky) \\ &= (x^2 - yz - yw - zw) + i(xy + xz + yz - w^2) \\ &+ j(-y^2 + xz + xw + zw) + k(xy - z^2 + xw + yw). \end{aligned}$$

Finally, Identity (3.8) follows from taking the norm of the quaternion product

$$\begin{aligned} & (x + iy + jz + kw)(x + iz + jw - ky) \\ &= (x^2 - yz + yw - zw) + i(xy + xz - yz - w^2) \\ &+ j(y^2 + xz + xw + zw) + k(xw - xy - z^2 + yw). \end{aligned} \quad \square$$

**Conjecture 3.2.** *In the case where  $p = m = 4$  and  $n = 2$ , there are exactly 8 equivalence classes, which have representatives given in Theorem 3.1.*

*Remark 3.3.* The cardinality of each equivalence class in the set of solutions to  $a^2 + b^2 + c^2 + d^2 = (x^2 + y^2 + z^2 + w^2)^2$  can be calculated using the group action under  $\mathfrak{S}_4^\pm \times \mathfrak{S}_4^\pm$ . The orders of these orbits are, respectively, 1536, 1152, 8, 2304, 4608, 2304, 3072, 3072. Naturally, all of those numbers are factors of  $|\mathfrak{S}_4^\pm \times \mathfrak{S}_4^\pm| = 2^{14}3^2$ . The programs *numeric\_comparison* and *symbolic\_comparison* both used the space of all products of relevant quaternions, giving a different list of cardinalities: 4, 3, 8, 6, 12, 6, 8, 8. In fact, the programs were able to ignore large portions of this space for theoretical reasons, which is why the cardinalities in this list are smaller. In particular, this list represents the number of nodes in the connected subgraphs found by *symbolic\_comparison*. This list is almost the first list scaled down by a factor of 384, but the third term is inconsistent for reasons involving conjugates that are discussed more fully in the proof of Theorem 6.1.

## 4 Conjecture for $p = m = 4$ and $n \in \mathbb{N}$

The conjecture in this section was made in collaboration with Professor David Leep.

We conjecture that when  $p = m = 4$  and  $n \in \mathbb{N}$ , all identities of the form  $\tau_1^2 + \tau_2^2 + \tau_3^2 + \tau_4^2 = (x_1^2 + x_2^2 + x_3^2 + x_4^2)^n$  can be written as a product of Lipschitz quaternions. This is made more precise in Conjecture 4.1.

**Conjecture 4.1.** *Let  $(a, b, c, d)$  be a tuple such that*

$$a^2 + b^2 + c^2 + d^2 = (x^2 + y^2 + z^2 + w^2)^n,$$

*where  $a, b, c, d \in \mathbb{Z}[x, y, z, w]$ . Let  $\alpha = a + bi + cj + dk$ . Then  $\alpha = \beta_1 \beta_2 \cdots \beta_n$ , where  $\beta_u \in \mathbb{L}[x, y, z, w]$  for  $u$  in  $1, \dots, n$ . Moreover, let  $\beta_u = a' + b'i + c'j + d'k$ . Then the following tuple equivalence holds:  $(a', b', c', d') \simeq (x, y, z, w)$ .*

Conjecture 4.1 would be true if every  $\alpha \in \mathbb{L}[x, y, z, w]$  had a nontrivial factorization over  $\mathbb{L}[x, y, z, w]$  given that the norm  $N(\alpha)$  has a nontrivial factorization over  $\mathbb{Z}[x, y, z, w]$

However, Beauregard [1] provides a counterexample: The quaternion

$$x^2 y^2 - 1 + (x^2 - y^2)i + 2xyj$$

is an irreducible in  $\mathbb{L}[x, y, z, w]$ , but its norm is not an irreducible in  $\mathbb{Z}[x, y, z, w]$ . Thus Conjecture 4.1 remains unproven.

## 5 Proof of Conjecture 4.1 when $n = 1$

I have proved Conjecture 4.1 in the case where  $n = 1$ .

Recall that  $\theta \in \mathbb{Z}[x, y, z, w]$  is a *monomial* if  $\theta$  is of the form  $Cx^{e_1}y^{e_2}z^{e_3}w^{e_4}$ , where  $C \in \mathbb{Z}$  and  $e_1, e_2, e_3, e_4 \in \mathbb{N} \cup \{0\}$ . Two monomials  $u$  and  $v$  are *similar*, denoted  $u \sim v$ , if they are equal or only differ in their coefficient. We denote the degree of  $\theta$  with respect to the variable  $x$  by  $\deg_x \theta = e_1$ . We use analogous notation for the other three variables.

*Remark 5.1.* Any element of  $\mathbb{Z}[x, y, z, w]$  is a sum of monomials.

**Lemma 5.2.** *If  $a, b, c, d \in \mathbb{Z}[x, y, z, w]$ , and*

$$a^2 + b^2 + c^2 + d^2 = x^2 + y^2 + z^2 + w^2,$$

*then  $(a, b, c, d) \simeq (x, y, z, w)$ .*

*Proof.* Write each of  $a, b, c, d$  as sums of monomials, that is,

$$a = \theta_{11} + \theta_{12} + \cdots + \theta_{1\alpha},$$

$$b = \theta_{21} + \theta_{22} + \cdots + \theta_{2\beta},$$

$$c = \theta_{31} + \theta_{32} + \cdots + \theta_{3\gamma},$$

$$d = \theta_{41} + \theta_{42} + \cdots + \theta_{4\delta},$$

where the monomial  $\theta_{ij}$  is not similar to the monomial  $\theta_{ik}$  for  $j \neq k$ .

Let  $S$  be the *multiset* of all the preceding  $\theta$ 's. We select a particular element  $\omega$  from  $S$  in the following manner. Let  $S_1$  be the set of all  $\theta \in S$  such that  $\deg_x \theta$  is the maximum possible for all  $\theta \in S$ . Let  $S_2$  be the set of all  $\theta \in S_1$  such that  $\deg_y \theta$  is the maximum possible for all  $\theta \in S_1$ . Let  $S_3$  be the set of all  $\theta \in S_2$  such that  $\deg_z \theta$  is the maximum possible for all  $\theta \in S_2$ . Finally, let  $S_4$  be the set of all  $\theta \in S_3$  such that  $\deg_w \theta$  is the maximum possible for all  $\theta \in S_3$ . Let  $\omega$  be an element of  $S_4$ . We can write  $\omega = Cx^{e_1}y^{e_2}z^{e_3}w^{e_4}$ , where  $C \in \mathbb{Z}$  and  $e_1, e_2, e_3, e_4 \in \mathbb{N} \cup \{0\}$ .

We first assume that  $\deg_x \omega > 1$ . In the expression  $a^2 + b^2 + c^2 + d^2$ , there must be at least one monomial similar to  $\omega^2$  that cancels the term  $\omega^2 = C^2x^{2e_1}y^{2e_2}z^{2e_3}w^{2e_4}$ . Let one of these monomials be  $\psi$ . Assume for the moment that  $\psi$  is not formed from squaring a monomial in  $S$ , but rather from a product of two nonsimilar monomials. In other words,  $\psi = \psi' \cdot \psi''$ , where  $\psi' \not\sim \psi''$  and  $\psi', \psi'' \in S$ . Since  $\omega$  was chosen to have maximal  $x$ -degree, we have  $\deg_x \psi' \leq \deg_x \omega$  and  $\deg_x \psi'' \leq \deg_x \omega$ . As  $\omega^2 \sim \psi = \psi' \cdot \psi''$ , we have  $\deg_x \omega^2 = \deg_x \psi' + \deg_x \psi''$  and immediately have  $\deg_x \omega = \deg_x \psi' = \deg_x \psi''$ . Thus  $\psi', \psi'' \in S_1$ . Continuing in this manner with the other variables, we conclude that  $\psi'$  and  $\psi''$  are similar monomials. This contradicts the fact that  $\psi' \not\sim \psi''$ . Hence  $\psi$  was formed by the square of a monomial in  $S$ . However, this implies the coefficient of  $\psi$  is positive. Furthermore, the coefficient of any monomial similar to  $\omega^2$  must be positive, so  $\omega^2$  cannot be canceled. This is a contradiction, so  $\deg_x \omega \leq 1$ . Thus no monomial in  $S$  has  $x$ -degree more than 1. Analogously, we can show that no monomial in  $S$  has  $y$ -degree,  $z$ -degree, or  $w$ -degree more than 1.

By setting the three variables  $y, z, w$  equal to zero, we see that  $S$  contains exactly one monomial similar to  $x$ , namely  $x$  or  $-x$ . The same is true for the other three variables. Moreover, there are no constants in  $S$ .

Assume that  $\theta_{11} \sim x$  and  $\theta_{12} \sim y$ . Then  $a^2$  contains a monomial similar to  $xy$ , which can only be canceled by another product of monomials similar to  $x$  and  $y$ . However, we showed that  $S$  has no such other monomials. Thus each coordinate  $(a, b, c, d)$  contains exactly one of  $\pm x, \pm y, \pm z, \pm w$ .

Assume that the coordinate that contains  $\pm x$  also contains another monomial  $A = Dx^{f_1}y^{f_2}z^{f_3}w^{f_4}$ , where  $D \in \mathbb{Z}$  and  $f_1, f_2, f_3, f_4 \in \{0, 1\}$ . Then  $A^2$  has degrees (with respect to each variable) of either 0 or 2. To cancel  $A^2$ , we must find a product of two monomials in  $S$  that is similar to  $A^2$ . As no monomial in  $S$  has a degree (with respect to any variable) of two, any monomial similar to  $A^2$  must itself be a square of a monomial similar to  $A$ . In this case, the coefficients are positive and will not cancel. Thus there can be no such monomial  $A$ , so the only monomials in  $S$  are the four desired ones.  $\square$

## 6 Enumerative Consequences of Conjecture 4.1

**Theorem 6.1.** *Assuming Conjecture 4.1 holds, then the number of solutions  $(a, b, c, d)$  to*

$$a^2 + b^2 + c^2 + d^2 = (x^2 + y^2 + z^2 + w^2)^n, \quad (6.1)$$

where  $a, b, c, d \in \mathbb{Z}[x, y, z, w]$ , is at most

$$8 \cdot \frac{47^{n+1} - 1}{46} = 8 \cdot \left\lfloor \frac{47^{n+1}}{46} \right\rfloor = 8 \sum_{i=0}^n 47^i.$$

*Proof.* If Conjecture 4.1 holds, any solution  $(a, b, c, d)$  can be viewed as a quaternion  $a + bi + cj + dk = \beta_1 \beta_2 \cdots \beta_n$  where the  $\beta_i$  are quaternions from the following set:

$$T_1 = \{\pm a' \pm b'i \pm c'j \pm d'k : \{a', b', c', d'\} = \{x, y, z, w\}\}.$$

Note that  $|T_1| = 2^4 4! = 384$ . Thus there are at most  $384^n$  unique solutions to equation (6.1). Using the fact that

$$\beta_1 \beta_2 \cdots \beta_i \beta_{i+1} \cdots \beta_n = \beta_1 \beta_2 \cdots \beta_i u u^{-1} \beta_{i+1} \cdots \beta_n,$$

where  $u \in \{\pm 1, \pm i, \pm j, \pm k\}$  is a unit of  $\mathbb{L}$ , we can specify that every  $\beta_i$  except the first has  $a' = x$  without losing any solutions. Thus the number of unique solutions to equation (6.1) is at most  $384 \cdot 48^{n-1}$ . Alternatively, we can factor out a unit from the first factor  $\beta_1$  to ensure that it has  $a' = x$ , so the resulting product is of the form  $u \beta_1 \beta_2 \cdots \beta_n$ , where each  $\beta_i$  belongs to

$$T_2 = \{x \pm b'i \pm c'j \pm d'k : \{b', c', d'\} = \{y, z, w\}\},$$

with  $|T_2| = 2^3 3! = 48$ .

If any two consecutive  $\beta$ 's are conjugates, we can combine them to form  $x^2 + y^2 + z^2 + w^2$ . As this is a real number, we can factor it out. The product is now of the form

$$(x^2 + y^2 + z^2 + w^2)^\gamma u \beta_1 \beta_2 \cdots \beta_{n-2\gamma},$$

with  $\gamma$  ranging over  $0, 1, \dots, \lfloor n/2 \rfloor$ .

Assume  $n$  is even. When  $\gamma = n/2$ , the product is of the form  $(x^2 + y^2 + z^2 + w^2)^{n/2} u$ , so there are 8 unique values, one for each unit. When  $\gamma = n/2 - 1$ , the product is of the form  $(x^2 + y^2 + z^2 + w^2)^{n/2-1} u \beta_1 \beta_2$ . Although  $\beta_1$  can be any element of  $T_2$ ,  $\beta_2$  cannot be equal to  $\bar{\beta}_1$ , so the number of solutions in this case is  $8 \cdot 48 \cdot 47$ . The same restriction applies for all  $\gamma < n/2$ . For  $\gamma < n/2$ , the number of solutions is  $8 \cdot 48 \cdot 47^{n-2\gamma-1}$ . Summing over all possible

values of  $\gamma$ , the number of solutions is

$$\begin{aligned}
8 + 8 \cdot 48 \cdot 47 + 8 \cdot 48 \cdot 47^3 + \cdots + 8 \cdot 48 \cdot 47^{n-1} &= 8 + 8 \cdot 48 \cdot 47 \cdot \frac{47^{2 \cdot n/2} - 1}{47^2 - 1} \\
&= 8 + 8 \cdot 47 \cdot \frac{47^n - 1}{47 - 1} \\
&= 8 \left( 1 + \frac{47(47^n - 1)}{46} \right) \\
&= 8 \left( \frac{46 + (47^{n+1} - 47)}{46} \right) \\
&= 8 \left( \frac{47^{n+1} - 1}{46} \right).
\end{aligned}$$

Now assume  $n$  is odd. When  $\gamma = (n - 1)/2$ , the product is of the form  $(x^2 + y^2 + z^2 + w^2)^{(n-1)/2} u \beta_1$ , so there are  $8 \cdot 48$  unique solutions. When  $\gamma = (n - 1)/2 - 1 = (n - 3)/2$ , the product is of the form  $(x^2 + y^2 + z^2 + w^2)^{(n-3)/2} u \beta_1 \beta_2 \beta_3$ . Although  $\beta_1$  can be any element of  $T_2$ ,  $\beta_2 \neq \overline{\beta_1}$  and  $\beta_3 \neq \overline{\beta_2}$ , so the number of solutions in this case is  $8 \cdot 48 \cdot 47^2$ . The same restriction applies for all  $\gamma < (n - 1)/2$ . For  $\gamma < (n - 1)/2$ , the number of solutions is  $8 \cdot 48 \cdot 47^{n-2\gamma-1}$ . Summing over all values of  $\gamma$ , the number of solutions is

$$\begin{aligned}
8 \cdot 48 + 8 \cdot 48 \cdot 47^2 + 8 \cdot 48 \cdot 47^4 + \cdots + 8 \cdot 48 \cdot 47^{n-1} &= 8 \cdot 48 \cdot \frac{47^{2 \cdot (n+1)/2} - 1}{47^2 - 1} \\
&= 8 \cdot \frac{47^{n+1} - 1}{47 - 1}. \quad \square
\end{aligned}$$

*Remark 6.2.* Note that the proof of Theorem 6.1 gives an upper bound for the number of solutions.

## 7 Conclusion

This paper is a significant advance over the author's previous estimate in [2] of the number of equivalence classes when  $p = m = 4$  and  $n = 2$ . Using the two new computational methods discussed in Section 3, the upper bound has been reduced from 57 to 8, assuming Conjecture 4.1 holds.

It is notable that the number of solutions when  $p = m = 2$  increases linearly in  $n$ , but the number of solutions when  $p = m = 4$  is asymptotic to an exponential function in  $n$ .

Future steps include the following:

1. A proof of Conjecture 4.1 would solidify Theorem 6.1 and provide more theoretical insight into the nature of these identities.

2. Experimental data shows that Theorem 6.1 gives the exact number of solutions in the cases where  $n = 0, 1, 2, 3$ . This data was collected by applying the group action of  $\mathfrak{S}_4^\pm \times \mathfrak{S}_4^\pm$  to a representative from each equivalence class and counting the unique identities. It seems plausible that for all  $n$  the expression  $8 \sum_{i=0}^n 47^n$  is a lower bound as well as an upper bound.
3. It is difficult to approach the equation  $\sum_{j=1}^p \tau_j^2 = (\sum_{i=1}^m x_i^2)^n$  in cases besides  $p = m = 2$  and  $p = m = 4$ , since the only division rings with a norm are the reals, the complex numbers, the quaternions, and the 8-dimensional octonions, as was proven by Hurwitz in [4]. I may be able to approach the case  $p = m = 8$  using the octonions, although the lack of associativity presents new challenges. Alternatively, I may be able to adapt the proof of Theorem 6.1 to cases when  $p$  and  $m$  take on values less than four.

## References

- [1] R. A. BEAUREGARD, When is  $F[x, y]$  a unique factorization domain?, *Proceedings of the American Mathematical Society* **117** (1993), 67–70.
- [2] T. EHRENBORG, Pythagorean Quintuples and Quaternions, preprint 2018.
- [3] W. HAMILTON, On Quaternions; or on a new System of Imaginaries in Algebra, *The London, Edinburgh and Dublin Philosophical Magazine and Journal of Science* **25** (1844), 10–13.
- [4] A. HURWITZ, Über die Komposition der quadratischen Formen, *Mathematische Annalen* **88** (1922), 1–25.
- [5] D. E. JOYCE, Euclid’s Elements, Book X, Proposition 29, <https://mathcs.clarku.edu/~djoyce/java/elements/elements.html>.