Lagrange's Four-Square Theorem

A Complete Treatment

December 2025

1 The Algebra of Quaternions

Definition 1.1 (Hamilton Quaternions). The algebra of Hamilton quaternions $\mathbb{H}$ is the four-dimensional real vector space with basis $\{1, i, j, k\}$ equipped with multiplication determined by $i^2 = j^2 = k^2 = ijk = -1$. From these: $ij = k$, $jk = i$, $ki = j$, and $ji = -k$, $kj = -i$, $ik = -j$.

Definition 1.2 (Conjugation). For $\alpha = a+bi+cj+dk \in \mathbb{H}$, the conjugate is $\bar{\alpha} := a-bi-cj-dk$.

Lemma 1.3 (Conjugation Properties). For all $\alpha, \beta \in \mathbb{H}$:

(i) $\overline{\bar{\alpha}} = \alpha$
(ii) $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$
(iii) $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$
(iv) $\alpha \in \mathbb{R}$ if and only if $\bar{\alpha} = \alpha$

Proof. Parts (i), (ii), (iv) follow from the definition. For (iii), verify on basis elements: $\overline{ij} = \bar{k} = -k$ and $\bar{j}\bar{i} = (-j)(-i) = ji = -k$. ■

Definition 1.4 (Norm and Trace). For $\alpha = a + bi + cj + dk \in \mathbb{H}$:

- $N(\alpha) := \alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2$
- $\mathrm{Tr}(\alpha) := \alpha + \bar{\alpha} = 2a$

Lemma 1.5 (Norm and Trace Properties). For all $\alpha \in \mathbb{H}$:

(i) $N(\alpha) = \alpha\bar{\alpha} = \bar{\alpha}\alpha \in \mathbb{R}_{\geq 0}$
(ii) $\mathrm{Tr}(\alpha) = 2\,\mathrm{Re}(\alpha) \in \mathbb{R}$
(iii) $N(\alpha)$ and $\mathrm{Tr}(\alpha)$ commute with all quaternions
(iv) For $\alpha \neq 0$, $\alpha^{-1} = \bar{\alpha}/N(\alpha)$

Proof. For (i), direct computation shows $\alpha\bar{\alpha} = \bar{\alpha}\alpha = a^2 + b^2 + c^2 + d^2$. Parts (ii)–(iv) follow immediately. ■

Theorem 1.6 (Multiplicativity of Norm). For all $\alpha, \beta \in \mathbb{H}$: $N(\alpha\beta) = N(\alpha)N(\beta)$.

Proof. $N(\alpha\beta) = (\alpha\beta)\overline{(\alpha\beta)} = (\alpha\beta)(\bar{\beta}\bar{\alpha}) = \alpha(\beta\bar{\beta})\bar{\alpha} = \alpha N(\beta)\bar{\alpha} = N(\beta)\alpha\bar{\alpha} = N(\beta)N(\alpha) = N(\alpha)N(\beta)$. The step $\alpha N(\beta)\bar{\alpha} = N(\beta)\alpha\bar{\alpha}$ uses Lemma 1.5(iii). ■

Corollary 1.7 (Euler's Four-Square Identity). For all $a, b, c, d, e, f, g, h \in \mathbb{R}$:

$(a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2)$ is a sum of four squares.

Proof. Set $\alpha = a+bi+cj+dk$ and $\beta = e+fi+gj+hk$. Then $N(\alpha)N(\beta) = N(\alpha\beta)$ by Theorem 1.6. Expanding $\alpha\beta = (ae - bf - cg - dh) + (af + be + ch - dg)i + (ag - bh + ce + df)j + (ah + bg - cf + de)k$, the result follows. ■

2 The Hurwitz Quaternions

Definition 2.1 (Lipschitz Quaternions). $\mathcal{L} := \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\}$.

Definition 2.2 (Hurwitz Quaternions). $\mathcal{H} := \{\alpha \in \mathbb{H} : \text{all coordinates of } \alpha \text{ lie in } \mathbb{Z}, \text{ or all lie in } \mathbb{Z}+\frac{1}{2}\}$.

Definition 2.3. Define $\omega := (1 + i + j + k)/2$.

Lemma 2.4 (Coset Decomposition). $\mathcal{H} = \mathcal{L} \cup (\mathcal{L} + \omega)$, a disjoint union.

Proof. Integral Hurwitz quaternions are precisely $\mathcal{L}$. Half-integral ones have the form $(a + \frac{1}{2}) + (b + \frac{1}{2})i + (c + \frac{1}{2})j + (d + \frac{1}{2})k = (a + bi + cj + dk) + \omega \in \mathcal{L} + \omega$. The cosets are disjoint since $\omega \notin \mathcal{L}$. ■

Lemma 2.5 (Integrality of Norm and Trace). For all $\alpha \in \mathcal{H}$: $N(\alpha) \in \mathbb{Z}_{\geq 0}$ and $\mathrm{Tr}(\alpha) \in \mathbb{Z}$.

Proof. For integral α, immediate. For half-integral $\alpha = (a_0 + a_1 i + a_2 j + a_3 k)/2$ with a_i odd:

$4N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2$. Each $a_i^2 \equiv 1 \pmod 4$, so $4N(\alpha) \equiv 4 \pmod 4$, hence $N(\alpha) \in \mathbb{Z}$.

$\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha} = a_0 \in \mathbb{Z}$ (since a_0 is an odd integer). ■

Lemma 2.6 (Conjugation Preserves $\mathcal{H}$). For all $\alpha \in \mathcal{H}$, $\bar{\alpha} \in \mathcal{H}$.

Proof. If $\alpha = a + bi + cj + dk \in \mathcal{H}$, then $\bar{\alpha} = a - bi - cj - dk$ has the same coordinate type (all integral or all half-integral). ■

Lemma 2.7 (Closure under Multiplication). For all $\alpha, \beta \in \mathcal{H}$, we have $\alpha\beta \in \mathcal{H}$.

Proof.

Case 1: Both integral. $\mathcal{L}$ is closed under multiplication (products of integers are integers).

Case 2: One integral, one half-integral. Let $\alpha \in \mathcal{L}$ with coordinates $(a_0, a_1, a_2, a_3) \in \mathbb{Z}^4$, and $\beta = B/2$ where $B \in \mathcal{L}$ has all odd coordinates. Then $\alpha\beta = (\alpha B)/2$.

Set $C := \alpha B \in \mathcal{L}$. Each coordinate of C is an integer (being a sum of products of integers). We show all coordinates of C have the same parity.

Each coordinate of C is a signed sum of four terms $a_r B_s$. Since $B_s \equiv 1 \pmod 2$, we have $a_r B_s \equiv a_r \pmod 2$. Since negation preserves parity ($-x \equiv x \pmod 2$), each coordinate is $\equiv a_0 + a_1 + a_2 + a_3 \pmod 2$.

Hence all coordinates of C share the same parity, so $\alpha\beta = C/2$ has all coordinates in $\mathbb{Z}$ or all in $\mathbb{Z} + \frac{1}{2}$. Thus $\alpha\beta \in \mathcal{H}$.

Case 3: Both half-integral. Write $\alpha = A/2, \beta = B/2$ where $A, B \in \mathcal{L}$ have all odd coordinates. Then $\alpha\beta = AB/4$.

Write $A_i = 2a_i' + 1$ and $B_j = 2b_j' + 1$ for $a_i', b_j' \in \mathbb{Z}$. Then:

$$A_i B_j = (2a_i' + 1)(2b_j' + 1) = 4a_i'b_j' + 2(a_i' + b_j') + 1 \equiv 1 + 2(a_i' + b_j') \pmod 4$$

Define $S_A := a'_0 + a'_1 + a'_2 + a'_3 \pmod 2$ and $S_B := b'_0 + b'_1 + b'_2 + b'_3 \pmod 2$.

The coordinate formulas for AB are:

$$R = A_0B_0 - A_1B_1 - A_2B_2 - A_3B_3$$

$$I = A_0B_1 + A_1B_0 + A_2B_3 - A_3B_2$$

Computing $R \pmod 4$:

$$R \equiv [1 + 2(a'_0 + b'_0)] - [1 + 2(a'_1 + b'_1)] - [1 + 2(a'_2 + b'_2)] - [1 + 2(a'_3 + b'_3)]$$

$$\equiv (1 - 1 - 1 - 1) + 2[(a'_0 + b'_0) - (a'_1 + b'_1) - (a'_2 + b'_2) - (a'_3 + b'_3)]$$

$$\equiv -2 + 2[(a'_0 - a'_1 - a'_2 - a'_3) + (b'_0 - b'_1 - b'_2 - b'_3)]$$

Since $-x \equiv x \pmod 2$, we have $a'_0 - a'_1 - a'_2 - a'_3 \equiv a'_0 + a'_1 + a'_2 + a'_3 = S_A \pmod 2$, and similarly for B. Thus:

$$R \equiv -2 + 2(S_A + S_B) \equiv 2(S_A + S_B - 1) \pmod 4$$

Computing $I \pmod 4$:

$$I \equiv [1 + 2(a'_0 + b'_1)] + [1 + 2(a'_1 + b'_0)] + [1 + 2(a'_2 + b'_3)] - [1 + 2(a'_3 + b'_2)]$$

$$\equiv (1 + 1 + 1 - 1) + 2[(a'_0 + b'_1) + (a'_1 + b'_0) + (a'_2 + b'_3) - (a'_3 + b'_2)]$$

$$\equiv 2 + 2[(a'_0 + a'_1 + a'_2 - a'_3) + (b'_0 + b'_1 - b'_2 + b'_3)]$$

$$\equiv 2 + 2(S_A + S_B) \equiv 2(S_A + S_B + 1) \pmod 4$$

Similarly, $J \equiv K \equiv 2(S_A + S_B + 1) \pmod 4$.

Since $R - I \equiv 2(S_A + S_B - 1) - 2(S_A + S_B + 1) = -4 \equiv 0 \pmod 4$, we have $R \equiv I \equiv J \equiv K \pmod 4$.

Each coordinate of AB is even (being a signed sum of four odd numbers), so all are $\equiv 0$ or all $\equiv 2 \pmod 4$. Hence $\alpha\beta = AB/4$ has all coordinates in $\mathbb{Z}$ or all in $\mathbb{Z} + \frac{1}{2}$. Thus $\alpha\beta \in \mathcal{H}$. ■

Corollary 2.8. $\mathcal{H}$ is a subring of $\mathbb{H}$.

Theorem 2.9 (Units). $\mathcal{H}^\times = \{\pm 1, \pm i, \pm j, \pm k\} \cup \{(\varepsilon_0 + \varepsilon_1 i + \varepsilon_2 j + \varepsilon_3 k)/2 : \varepsilon_i \in \{\pm 1\}\}$, consisting of 8 integral and 16 half-integral units.

Proof. $\varepsilon \in \mathcal{H}^\times$ iff $N(\varepsilon) = 1$. For integral ε: $a^2 + b^2 + c^2 + d^2 = 1$ with $a, b, c, d \in \mathbb{Z}$ gives 8 solutions. For half-integral ε: $(a_0^2 + a_1^2 + a_2^2 + a_3^2)/4 = 1$ with a_i odd requires each $a_i^2 = 1$, giving 16 solutions. ■

Corollary 2.10. $\varepsilon \in \mathcal{H}^\times \Leftrightarrow N(\varepsilon) = 1 \Leftrightarrow \varepsilon^{-1} = \bar{\varepsilon}$.

---

3 Euclidean Structure

Lemma 3.1 (Covering Radius). For any $\gamma \in \mathbb{H}$, there exists $q \in \mathcal{H}$ with $N(\gamma - q) \leq 1/2$.

Proof. Write $\gamma = (x_0, x_1, x_2, x_3)$ with $x_i \in \mathbb{R}$. For each i, let $m_i \in \mathbb{Z}$ be a nearest integer to x_i, and set $\delta_i := x_i - m_i \in [-1/2, 1/2]$. Define $q_0 := m_0 + m_1 i + m_2 j + m_3 k \in \mathcal{L}$.

Signed half-shift. For each i, set $\varepsilon_i := +1$ if $\delta_i \geq 0$, and $\varepsilon_i := -1$ if $\delta_i < 0$. Define:

$$\omega' := (\varepsilon_0 + \varepsilon_1 i + \varepsilon_2 j + \varepsilon_3 k)/2$$

This is one of the 16 half-integral units ($N(\omega') = 1$), so $q_1 := q_0 + \omega' \in \mathcal{H}$.

Error analysis. The coordinates of $\gamma - q_1$ are $\delta_i - \varepsilon_i/2$. By construction, $|\delta_i - \varepsilon_i/2| = 1/2 - |\delta_i| =: \eta_i \in [0, 1/2]$.

Set $S_0 := N(\gamma - q_0) = \sum \delta_i^2$ and $S_1 := N(\gamma - q_1) = \sum \eta_i^2$.

Bound. For $t \in [0, 1/2]$: $t^2 + (1/2 - t)^2 = 2(t - 1/4)^2 + 1/8 \in [1/8, 1/4]$.

Summing: $4 \cdot (1/8) \leq S_0 + S_1 \leq 4 \cdot (1/4)$, i.e., $1/2 \leq S_0 + S_1 \leq 1$.

Therefore $\min(S_0, S_1) \leq (S_0 + S_1)/2 \leq 1/2$. Take $q \in \{q_0, q_1\}$ achieving the minimum. ■

Theorem 3.2 (Right Euclidean Property). For $\alpha, \beta \in \mathcal{H}$ with $\beta \neq 0$, there exist $q, r \in \mathcal{H}$ with $\alpha = \beta q + r$ and $N(r) < N(\beta)$.

Proof. Set $\gamma := \beta^{-1}\alpha \in \mathbb{H}$. By Lemma 3.1, choose $q \in \mathcal{H}$ with $N(\gamma - q) \leq 1/2$. Then $r := \alpha - \beta q = \beta(\gamma - q)$.

Since $\beta \neq 0$ and $\beta \in \mathcal{H}$, we have $N(\beta) \in \mathbb{Z}_{\geq 1}$ (by Lemma 2.5). Thus:

$$N(r) = N(\beta)N(\gamma - q) \leq N(\beta) \cdot (1/2) < N(\beta). \quad \blacksquare$$

Theorem 3.3 (Left Euclidean Property). For $\alpha, \beta \in \mathcal{H}$ with $\beta \neq 0$, there exist $q, r \in \mathcal{H}$ with $\alpha = q\beta + r$ and $N(r) < N(\beta)$.

Proof. Set $\gamma := \alpha\beta^{-1}$ and proceed symmetrically. ■

---

4 Divisibility and Factorisation

Definition 4.1. For $\alpha, \beta \in \mathcal{H}$: $\beta \mid_r \alpha$ (β right-divides α) if $\alpha = \beta\gamma$ for some $\gamma \in \mathcal{H}$.

Lemma 4.2 (Prime Norm Implies Irreducibility). If $N(\alpha) = p$ for a prime $p \in \mathbb{Z}$, then α is irreducible in $\mathcal{H}$.

Proof. Suppose $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathcal{H}$. Then $N(\beta)N(\gamma) = N(\alpha) = p$. Since $N(\beta), N(\gamma) \in \mathbb{Z}_{\geq 0}$ (Lemma 2.5) and p is prime, either $N(\beta) = 1$ or $N(\gamma) = 1$. By Corollary 2.10, that factor is a unit. ■

---

5 Existence of Small Norm Representatives

Lemma 5.1. For any odd prime p, there exist $x, y \in \mathbb{Z}$ with $x^2 + y^2 + 1 \equiv 0 \pmod{p}$.

Proof. Consider the sets:

$$A := \{x^2 \bmod p : 0 \leq x \leq (p-1)/2\}$$

$$B := \{-1 - y^2 \bmod p : 0 \leq y \leq (p-1)/2\}$$

Each set has cardinality $(p+1)/2$: the values x^2 for $x = 0, 1, \ldots, (p-1)/2$ are distinct modulo p (if $x^2 \equiv x'^2$ with $0 \leq x < x' \leq (p-1)/2$, then $p \mid (x'-x)(x'+x)$, but $0 < x' - x < p$ and $0 < x' + x < p$, contradiction).

Since $|A| + |B| = p + 1 > p$, the sets intersect. Thus $x^2 \equiv -1 - y^2 \pmod{p}$ for some x, y. ■

Corollary 5.2. For any odd prime p, there exists $\alpha \in \mathcal{L}$ with $N(\alpha) = mp$ for some $0 < m < p$.

Proof. By Lemma 5.1, choose $x, y \in \mathbb{Z}$ with $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ and $|x|, |y| \leq (p-1)/2$. Set $\alpha := x + yi + j \in \mathcal{L}$. Then:

$$N(\alpha) = x^2 + y^2 + 1 \equiv 0 \pmod{p}$$

and

$$N(\alpha) \leq 2 \cdot ((p-1)/2)^2 + 1 = (p-1)^2/2 + 1 < p^2$$

Since $0 < N(\alpha) < p^2$ and $p \mid N(\alpha)$, we have $N(\alpha) = mp$ for some $0 < m < p$. ■

---

6 Representation of Odd Primes

Lemma 6.1 (Reduction Lemma). For $\alpha \in \mathcal{H}$ and integer $m \geq 1$, there exists $\beta \in \mathcal{H}$ with:

(i) $\alpha - \beta \in m\mathcal{H}$ (equivalently, $(\alpha - \beta)/m \in \mathcal{H}$)
(ii) $N(\beta) \leq m^2/2$

Proof. Consider $\gamma := \alpha/m \in \mathbb{H}$. By Lemma 3.1, choose $q \in \mathcal{H}$ with $N(\gamma - q) \leq 1/2$. Set $\beta := \alpha - mq$.

Since $\mathcal{H}$ is closed under multiplication by integers (multiplying coordinates by an integer preserves the "all integral or all half-integral" condition), we have $mq \in \mathcal{H}$. By closure under subtraction, $\beta = \alpha - mq \in \mathcal{H}$.

Finally, $N(\beta) = N(m(\gamma - q)) = m^2 N(\gamma - q) \leq m^2/2$. ■

Theorem 6.2. Every odd prime p is the norm of some $\alpha \in \mathcal{H}$.

Proof. By Corollary 5.2, there exists $\alpha_0 \in \mathcal{H}$ with $N(\alpha_0) = m_0 p$ for some $0 < m_0 < p$.

Descent. We show: given $\alpha \in \mathcal{H}$ with $N(\alpha) = mp$ where $1 < m < p$, there exists $\alpha' \in \mathcal{H}$ with $N(\alpha') = m'p$ for some $0 < m' < m$.

By Lemma 6.1, choose $\beta \in \mathcal{H}$ with $\alpha - \beta \in m\mathcal{H}$ and $N(\beta) \leq m^2/2$. Write $\alpha = \beta + m\eta$ where $\eta := (\alpha - \beta)/m \in \mathcal{H}$.

Claim: $N(\beta) \equiv 0 \pmod{m}$.

Proof of Claim: Expanding $N(\alpha) = N(\beta + m\eta)$:

$$N(\beta + m\eta) = (\beta + m\eta)(\bar{\beta} + m\bar{\eta}) = \beta\bar{\beta} + m(\beta\bar{\eta} + \eta\bar{\beta}) + m^2\eta\bar{\eta}$$

Now $\bar{\eta} \in \mathcal{H}$ by Lemma 2.6, and $\beta\bar{\eta} \in \mathcal{H}$ by Lemma 2.7. Also, $\beta\bar{\eta} + \eta\bar{\beta} = \beta\bar{\eta} + \overline{\beta\bar{\eta}} = \mathrm{Tr}(\beta\bar{\eta}) \in \mathbb{Z}$ by Lemma 2.5.

Hence $N(\alpha) = N(\beta) + m \cdot \mathrm{Tr}(\beta\bar{\eta}) + m^2 N(\eta) \equiv N(\beta) \pmod{m}$.

Since $N(\alpha) = mp \equiv 0 \pmod{m}$, we have $N(\beta) \equiv 0 \pmod{m}$. ■

Write $N(\beta) = mm'$ for some integer $m' \geq 0$. Since $N(\beta) \leq m^2/2$, we have $m' \leq m/2 < m$.

Case $m' = 0$: Then $\beta = 0$, so $\alpha = m\eta$, giving $N(\alpha) = m^2 N(\eta)$, hence $mp = m^2 N(\eta)$, so $p = mN(\eta)$. Since $m > 1$ and p is prime, $m \mid p$, forcing $m = p$. But $m < p$ by hypothesis (we start with $m_0 < p$ and strictly decrease m at each step). Contradiction.

Case $0 < m' < m$: Compute $\bar{\beta}\alpha = \bar{\beta}(\beta + m\eta) = N(\beta) + m\bar{\beta}\eta = m(m' + \bar{\beta}\eta)$.

Since $m' \in \mathbb{Z} \subseteq \mathcal{H}$ and $\bar{\beta}\eta \in \mathcal{H}$ (by Lemmas 2.6 and 2.7), we have $m' + \bar{\beta}\eta \in \mathcal{H}$. Define $\alpha' := \bar{\beta}\alpha/m = m' + \bar{\beta}\eta \in \mathcal{H}$.

Then $N(\alpha') = N(\bar{\beta})N(\alpha)/m^2 = N(\beta)N(\alpha)/m^2 = (mm')(mp)/m^2 = m'p$.

Since $0 < m' < m$, the descent continues. By induction, we reach $m = 1$, giving $\alpha \in \mathcal{H}$ with $N(\alpha) = p$. ■

---

7 Integral Representation

Lemma 7.1 (Conversion). If $\alpha \in \mathcal{H}$ is half-integral with $N(\alpha) = p$ for an odd prime p, then there exists a half-integral unit $u \in \mathcal{H}^\times$ with $\alpha u \in \mathcal{L}$.

Proof. Write $\alpha = A/2$ where $A \in \mathcal{L}$ has all odd coordinates. Let $u = E/2$ where $E = (\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)$ with $\varepsilon_i \in \{\pm 1\}$. Then $\alpha u = AE/4$.

By Lemma 2.7 Case 3 (applied with $B = E$), the coordinates R, I, J, K of AE satisfy $R \equiv I \equiv J \equiv K \pmod 4$, with:

$$R \equiv 2(S_A + S_E - 1) \pmod 4$$

where $S_A = a_0' + a_1' + a_2' + a_3' \pmod 2$ with $A_i = 2a_i' + 1$, and S_E is defined similarly for E.

For $\varepsilon_i \in \{\pm 1\}$: $\varepsilon_i = 1$ gives $e_i' = 0$; $\varepsilon_i = -1$ gives $e_i' = -1$. Thus $S_E \equiv$ (number of $\varepsilon_i = -1$) $\pmod 2$.

For $\alpha u \in \mathcal{L}$, we need $R \equiv 0 \pmod 4$, equivalently $S_A + S_E \equiv 1 \pmod 2$.

If $S_A \equiv 0 \pmod 2$, choose an odd number of $\varepsilon_i = -1$, giving $S_E \equiv 1$.

If $S_A \equiv 1 \pmod 2$, choose an even number of $\varepsilon_i = -1$, giving $S_E \equiv 0$.

Either way, $S_A + S_E \equiv 1 \pmod 2$, so $\alpha u \in \mathcal{L}$ with $N(\alpha u) = N(\alpha) = p$. ■

Theorem 7.2 (Lagrange's Four-Square Theorem). Every $n \in \mathbb{Z}_{\geq 1}$ can be expressed as $n = a^2 + b^2 + c^2 + d^2$ for some $a, b, c, d \in \mathbb{Z}$.

Proof.

Step 1 (Small cases). $1 = 1^2 + 0^2 + 0^2 + 0^2$ and $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Step 2 (Odd primes). Let p be an odd prime. By Theorem 6.2, $p = N(\alpha)$ for some $\alpha \in \mathcal{H}$.

If $\alpha \in \mathcal{L}$ (integral), write $\alpha = a + bi + cj + dk$ with $a, b, c, d \in \mathbb{Z}$, and $p = a^2 + b^2 + c^2 + d^2$.

If α is half-integral, Lemma 7.1 provides a unit u with $\alpha u \in \mathcal{L}$ and $N(\alpha u) = p$. Write $\alpha u = a + bi + cj + dk$ with $a, b, c, d \in \mathbb{Z}$.

Step 3 (General n). By Corollary 1.7, the product of two sums of four squares is a sum of four squares. Since every $n \geq 1$ factors as a product of primes, and each prime is a sum of four squares by Steps 1–2, so is n. ■

---

8 Summary

The proof rests on five pillars:

1. **Norm multiplicativity** in $\mathbb{H}$ (Theorem 1.6), yielding Euler's four-square identity.
2. **Closure of $\mathcal{H}$** under multiplication with explicit mod-4 parity analysis (Lemma 2.7).
3. **Covering radius** $1/\sqrt{2}$ of the Hurwitz lattice via signed half-shift (Lemma 3.1).
4. **Descent** using the Reduction Lemma with bound $N(\beta) \leq m^2/2$, ensuring $m' \leq m/2 < m$ at each step (Theorem 6.2).
5. **Conversion** from half-integral to integral quaternions via parity-controlled unit multiplication (Lemma 7.1).

The non-commutativity of $\mathbb{H}$ requires care with the conjugation reversal $\overline{\alpha\beta} = \bar{\beta}\bar{\alpha}$ and explicit verification that $\mathrm{Tr}(\beta\bar{\eta}) \in \mathbb{Z}$, but the centrality of the norm ensures the descent mirrors the structure of the Gaussian integer proof for sums of two squares.