Quaternions and the four-square theorem

Background on Hamilton's Quaternions

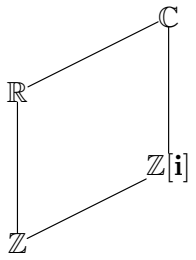
We have the complex numbers

$$\mathbb{C} = \{a + b_i : a, b \in \mathbb{R}\}$$

an their integral analogue,

$$\mathbb{Z}[\mathbf{i}] = \{a + b\mathbf{i} : a, b \in \mathbb{R}\},$$

the *Gaussian integers*, and we can draw a subring diagram accordingly.



A higher dimensional, but analogous, scenario was discovered by the Irish mathematician Wm. Rowan Hamilton in 1843 whilst crossing Dublin's Broom Bridge on his way into town.

Definition 1. *The* Hamilton Quaternions *are given by*

$$\mathbb{H} = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{R}\}$$

where

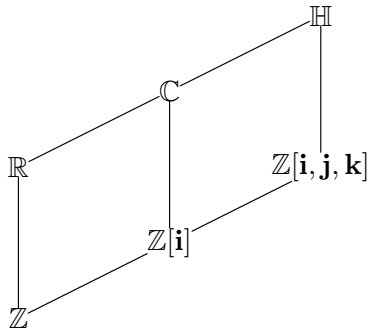
$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$$
$$\mathbf{ij} = \mathbf{k} = -\mathbf{ji}$$
$$\mathbf{jk} = \mathbf{i} = -\mathbf{kj}$$
$$\mathbf{ki} = \mathbf{j} = -\mathbf{ik},$$

and they are a ring.

We would like these to have have an integer analogue, and one possibility is

$$\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}] = \{a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} : a, b, c, d \in \mathbb{Z}\}.$$

Note that sum, difference, or product of things in $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$ return things in $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$. We could extend our subring lattice accordingly.



Examples: We have $1 + \mathbf{i} + \mathbf{j} + \mathbf{k} \in \mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$ and clearly the sum

$$(1 + \mathbf{i} + \mathbf{j} + \mathbf{k}) + (1 + \mathbf{i} + \mathbf{j} + \mathbf{k}) = 2 + 2\mathbf{i} + 2\mathbf{j} + 2\mathbf{k},$$

and difference

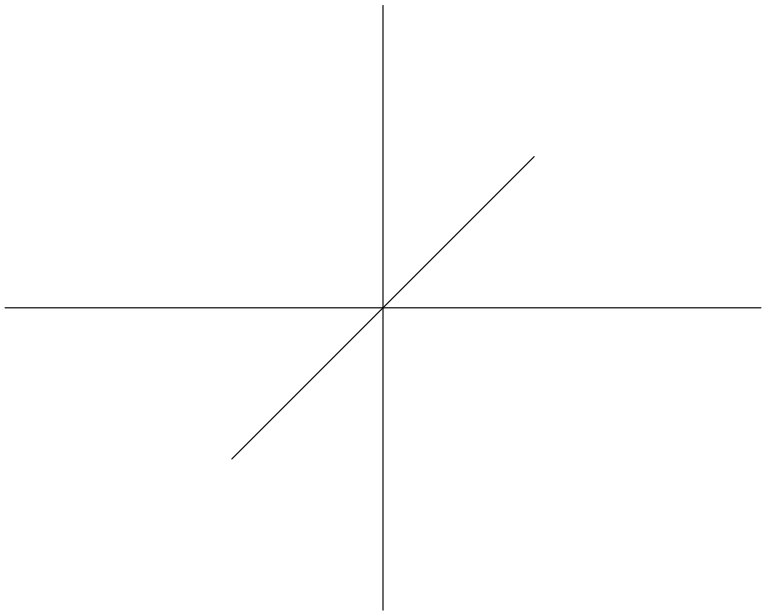
$$(1 + \mathbf{i} + \mathbf{j} + \mathbf{k}) - (1 + \mathbf{i} + \mathbf{j} + \mathbf{k}) = 0,$$

are in $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$, but a bit more work shows the product

$$\begin{aligned} & (1 + \mathbf{i} + \mathbf{j} + \mathbf{k})(1 + \mathbf{i} + \mathbf{j} + \mathbf{k}) \\ = \; & 1 + \mathbf{i} + \mathbf{j} + \mathbf{k} + \mathbf{i} - 1 + \mathbf{ij} + \mathbf{ik} + \mathbf{j} + \mathbf{ji} - 1 + \mathbf{jk} + \mathbf{k} + \mathbf{ki} + \mathbf{kj} - 1 \\ = \; & -2 + 2\mathbf{i} + 2\mathbf{j} + 2\mathbf{k} \end{aligned}$$

is also in $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$. So from our theorem yesterday, we know $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$ is a subring of $\mathbb{H}$.

The point $1 + \mathbf{i} + \mathbf{j} + \mathbf{k}$ can be thought of as the point one "unit out" in each dimension in $\mathbb{R}^4$. We can't visualize fully this (damn human brains), but it might help to think about it in three dimensions.



Recall, the distance of point $a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$ from the origin is just

$$\sqrt{(a-0)^2 + (b-0)^2 + (c-0)^2 + (d-0)^2} = \sqrt{a^2 + b^2 + c^2 + d^2}.$$

Definition 2. *We define a* norm *on* $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$ *by*

$$norm(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = a^2 + b^2 + c^2 + d^2,$$

noting that this is just the square of the distance of a point from the origin. This is multiplicative, that is

$$norm(q_1 q_2) = norm(q_1) norm(q_2)$$

Examples: We can use this norm to determine when a integer in $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$ is *prime*. Since

$$\text{norm}(-2 + 2\mathbf{i} + 2\mathbf{j} + 2\mathbf{k}) = 16$$

we know it can be decomposed. On the other hand,

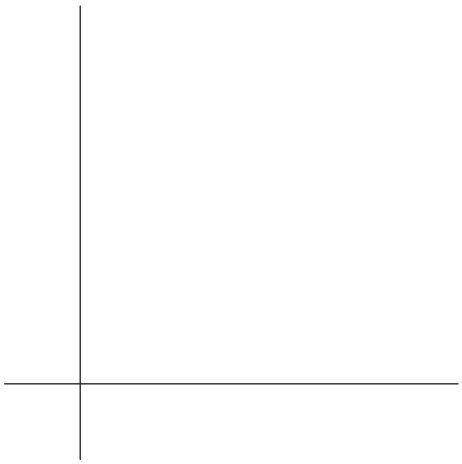
$$\text{norm}(-2 + \mathbf{i} + \mathbf{j} + \mathbf{k}) = 7,$$

and so it can't be decomposed. More generally, for $\beta \in \mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$, we have

- For $q_1, q_2 \in \mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$, we have

$$\text{norm}(\beta q_1 - \beta q_2) = \text{norm}(\beta(q_1 - q_2)) = \text{norm}(\beta)\text{norm}(q_1 - q_2)$$

- This means multiplying $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$ by β has the effect of stretching every distance by a factor of $\text{norm}(\beta)$ (note, this is a real number value).

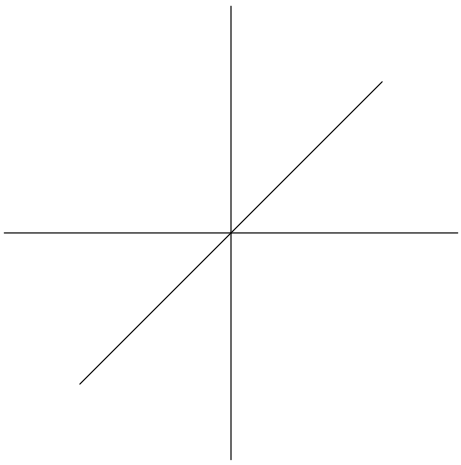


- This also means all angles are unchanged. So in particular,

$$\beta\mathbf{i}, \beta\mathbf{j}, \beta\mathbf{k}$$

  are all still perpendicular, and just shifted away from the origin.

- This means multiplication by β sends a "cube" in $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$ gets sent to a "cube" in $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$, possibly just stretching out the sides and rotating.



Division in the quaternions

To begin, we recall the division algorithm in the integers. We would like something similar to exist in the quaternions.

> **The Division Algorithm.** For any $a, b \in \mathbb{Z}$ there exists unique integers r and q with $0 \leq r < b$ such that $a = bq + r$.

Suppose $\alpha, \beta \in \mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$, and we want to write $\alpha = \beta\mu + \rho$, where $0 \leq \rho < \beta$ Then we would want to compute the remainder

$$\rho = \alpha - \mu\beta$$

which is the distance from α to the nearest "corner" in the multiplication by β grid. But if α is at the center of a cube, then

$$\alpha = \left(\mu + \frac{1}{2} + \frac{\mathbf{i}}{2} + \frac{\mathbf{j}}{2} + \frac{\mathbf{k}}{2}\right)\beta,$$

which may still be an element of $\mathbb{Z}[\mathbf{i}, \mathbf{j}, \mathbf{k}]$. And consequently,

$$\text{norm}(\alpha - \beta\mu) = \text{norm}\left(\beta\left(\frac{1}{2} + \frac{\mathbf{i}}{2} + \frac{\mathbf{j}}{2} + \frac{\mathbf{k}}{2}\right)\right) = \text{norm}(\beta)\left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) = \text{norm}(\beta).$$

Suppose we include all of the "center points" into the grid, this would be achieved by including

$$\frac{1 + \mathbf{i} + \mathbf{j} + \mathbf{k}}{2}$$

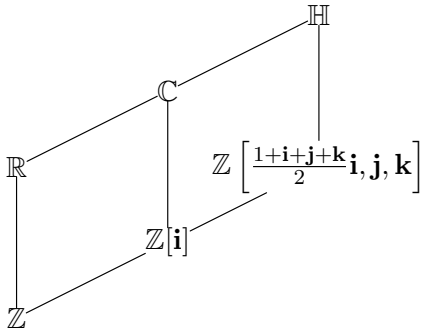
into the quaternion integers.

Definition 3. *The most practical integer analogue inside* $\mathbb{H}$ *is the* Hurwitz integers *which are the set*

$$\mathbb{Z}\left[\frac{1 + \mathbf{i} + \mathbf{j} + \mathbf{k}}{2}, \mathbf{i}, \mathbf{j}, \mathbf{k}\right] = \{a + b\frac{1 + \mathbf{i} + \mathbf{j} + \mathbf{k}}{2} + c\mathbf{i} + d\mathbf{j} + e\mathbf{k} : a, b, c, d, e \in \mathbb{Z}\}.$$

The are a ring, clearly an additive group, and now we know they also have the division algorithm!

- *An element in here is called a* Hurwitz prime *if it is not the product of two smaller ring elements.*
- *Note that every Hurwitz integer can be expressed as* $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}$ *where* $2a, 2b, 2c, 2d \in \mathbb{Z}$.



Examples: Primality can still be checked using norms, for example

$$\text{norm}\left(3+\frac{1+\mathbf{i}+\mathbf{j}+\mathbf{k}}{2}\right) = \text{norm}\left(\frac{7}{2}+\frac{\mathbf{i}}{2}+\frac{\mathbf{j}}{2}+\frac{\mathbf{k}}{2}\right) = \frac{49}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4} = \frac{52}{4} = 13,$$

so this is a Hurwitz prime!

Using the quaternions to prove the four square theorem

Definition 4. *Any complex number* $a+b\mathbf{i} \in \mathbb{C}$ *has a* conjugate

$$\overline{a+b\mathbf{i}} = a-b\mathbf{i},$$

and similarly, any $a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k} \in \mathbb{H}$ *has a conjugate*

$$\overline{a+b\mathbf{i}+c\mathbf{j}+d\mathbf{k}} = a-b\mathbf{i}-c\mathbf{j}-d\mathbf{k}.$$

The conjugate satisfies some properties, among them

- $\overline{r} = r$ *for* $r \in \mathbb{R}$.
- $\overline{q_1 q_2} = \overline{q_2}\,\overline{q_1}$.
- $q_1\overline{q_1} = norm(q_1)$.

Theorem 1. *If* p *is an ordinary prime but not a Hurwitz prime then*

$$p = a^2+b^2+c^2+d^2$$

where $2a, 2b, 2c, 2d \in \mathbb{Z}$.

Proof. Suppose that p is an ordinary prime but not a Hurwitz prime, so p has a nontrivial Hurwitz integer factorization

$$p = (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\gamma$$

where $2a, 2b, 2c, 2d \in \mathbb{Z}$ and γ a Hurwitz integer. Then conjugating both sides

$$p = \overline{p} = \overline{(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\gamma} = \overline{\gamma}(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}).$$

But now,

$$\begin{aligned} p^2 &= p\overline{p} \\ &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\gamma\overline{\gamma}(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) \\ &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\overline{(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})}\gamma\overline{\gamma} \\ &= (a^2 + b^2 + c^2 + d^2)\gamma\overline{\gamma}. \end{aligned}$$

But since p is prime, it must follow that $p = a^2 + b^2 + c^2 + d^2$. □

Theorem 2. *If p is an ordinary prime but not a Hurwitz prime then*

$$p = a^2 + b^2 + c^2 + d^2$$

where $a, b, c, d \in \mathbb{Z}$.

Proof. If $(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})$ is a Hurwitz integer, then

$$(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = \omega + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}$$

where a', b', c', d' are even integers and

$$\omega = \frac{\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k}}{2}.$$

Notice that $\text{norm}(\omega) = 1$, so in particular $\omega\overline{\omega} = 1$.

We know $p = a^2 + b^2 + c^2 + d^2$ where a, b, c, d are half integers from Theorem 1. But now

$$\begin{aligned} p &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})\overline{(a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})} \\ &= (a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k})(a - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}) \\ &= (\omega + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k})(\overline{\omega} - a' - b'\mathbf{i} - c'\mathbf{j} - d'\mathbf{k}) \\ &= (\omega + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k})\overline{\omega}\omega(\overline{\omega} - a' - b'\mathbf{i} - c'\mathbf{j} - d'\mathbf{k}) \\ &= (\omega + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k})\overline{\omega}\overline{(\omega + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k})\overline{\omega}} \end{aligned}$$

But focus on the first component for a moment,

$$\begin{aligned} (\omega + a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k})\overline{\omega} &= 1 + \overline{\omega}(a' + b'\mathbf{i} + c'\mathbf{j} + d'\mathbf{k}) \\ &= A + B\mathbf{i} + C\mathbf{j} + D\mathbf{k} \end{aligned}$$

where $A, B, C, D \in \mathbb{Z}$. But consequently,

$$p = (A + B\mathbf{i} + C\mathbf{j} + D\mathbf{k})\overline{(A + B\mathbf{i} + C\mathbf{j} + D\mathbf{k})} = A^2 + B^2 + C^2 + D^2.$$

□

If every odd prime p is the sum of 4 squares, then our work is done, since a product of a sum of four squares is again a sum of four squares

$$(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2) = (l^2+m^2+s^2+t^2).$$

This was shown by Euler in 1748. Notice that was 100 years before Hamilton!

Lemma 1. *If p is an odd prime then there are integers m and l such that p divides $1+m^2+l^2$.*

Proof. Let $p = 2n+1$ where $n \in \mathbb{Z}$. Then for any $m, l \in \{1, ..., n\}$, we have $m + l < p$ and so

$$m^2 \equiv l^2 \mod p \Rightarrow (m+l)(m-l) \equiv 0 \mod p \Rightarrow m = l.$$

This means there are $n+1$ incongruent choices for $l^2 \mod p$, and $n+1$ incongruent choices of $-1-m^2 \mod p$. But there are only $2n+1$ equivalence classes mod p, so for some choice of m, l we must have

$$l^2 \equiv -1 - m^2 \mod p,$$

in other words, $p \mid 1 + m^2 + l^2$. □

Theorem 3. *Every natural number is the sum of four squares.*

Proof. Suppose p is an odd prime, so $p = 2n+1$. Then Lemma 1 (a classical result of Lagrange) shows that

$$p \mid 1 + l^2 + m^2$$

for some integers l and m. This means that $p \nmid m$ and $p \nmid l$. But

$$1 + l^2 + m^2 = (1 + l\mathbf{i} + m\mathbf{j})(1 - l\mathbf{i} - m\mathbf{j}).$$

But now p must divide $(1 + l\mathbf{i} + m\mathbf{j})$ or $(1 - l\mathbf{i} - m\mathbf{j})$. But

$$\frac{1}{p} + \frac{\mathbf{i}}{p} + \frac{\mathbf{j}}{p} \text{ and } \frac{1}{p} - \frac{\mathbf{i}}{p} - \frac{\mathbf{j}}{p}$$

are both not Hurwitz integers, and hence aren't Hurwitz primes. Therefore p is the sum of 4 squares. Now the claim follows from Euler's identity. □