Lagrange's Four-Square Theorem with Quaternions

Aaron Anderson for Olga Radko Math Circle

January 2022

1 Introduction

This handout is an attempt to explain the proof of Lagrange's Four-Square Theorem using quaternions.

Theorem 1.1 (Lagrange's Four-Square Theorem)**.** *Every natural number can be expressed as a sum of four perfect squares.*

Problem 1. Show that a natural number is the sum of four perfect squares if and only if it is the square of the magnitude of an integer quaternion (that is, a quaternion whose coordinates are all integers).

Problem 2. Show that Lagrange's Four-Square Theorem is true if every *odd prime number* can be expressed as the sum of four perfect squares.

2 Hurwitz Quaternions

In order to use quaternions, we will want to use a special set of them.

Definition 1. The *Hurwitz Quaternions* are the quaternions in the set

$$H = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\} \cup \left\{(a + \frac{1}{2}) + (b + \frac{1}{2})i + (c + \frac{1}{2})j + (d + \frac{1}{2})k : a, b, c, d \in \mathbb{Z}\right\}$$

consisting of all quaternions that either have all integer coordinates, or all integer-plus-$\frac{1}{2}$ coordinates.

Problem 3. Show that H is closed under addition, subtraction, and multiplication.

Problem 4. Show that if $q \in H$, then $|q|^2$ is a natural number.

At this point, we should sketch out the rest of the proof. Let p be an odd prime. We will factor p as a product $p = \alpha\beta$ of Hurwitz quaternions, where neither α nor β has magnitude 1. From this, we will show that α and β each have magnitude-squared p, and if necessary, modify them slightly to find an actual integer quaternion with magnitude-squared p, from which we deduce that p is the sum of four squares.

Throughout the rest of this section, assume $p = \alpha\beta$, where $\alpha, \beta \in H$ and $|\alpha|^2, |\beta|^2 > 1$. We will find such α and β later.

Problem 5. Show that $|\alpha|^2 = |\beta|^2 = p$.

Problem 6. If α or β has integer coordinates, show that p is the sum of four squares.

Problem 7. Assume neither α nor β has integer coordinates.

- Show that there is a Hurwitz quaternion $\omega = \frac{1}{2}(\pm 1 \pm i \pm j \pm k)$ such that $\gamma = \alpha + \omega$ has *even* integer coordinates.
- Show that $|\bar{\omega}\gamma - 1|^2 = |\alpha|^2 = p$.
- Show that $\bar{\omega}\gamma - 1$ has integer coordinates, and that p is the sum of four squares.

3 Euclidean Algorithm for Hurwitz Quaternions

In this section, we will develop a version of the Euclidean algorithm for Hurwitz quaternions, which we will use later to factor p. First we will show a sort of division by remainder property for Hurwitz quaternions. Compare this to the integer property where for any integers a, b with $a \neq 0$, there is an integer c (the remainder) with $0 \leq b - ac < |a|$. As we are generalizing properties of the integers to noncommutative quaternions, we will have to be extra-careful to avoid using commutativity.

Problem 8. Show that if q is a quaternion with rational coordinates, then there is a Hurwitz quaternion h with $|q - h| < 1$. (This is analogous to approximating rational numbers with integers by rounding.)

Problem 9. Show that for any Hurwitz quaternions a, b with $a \neq 0$, there is another Hurwitz quaternion c such that $|b - ac| < |a|$.

Now that we have this division-with-remainder property, we can use it to build a version of the Euclidean algorithm and find a sort of gcd:

Problem 10. Let a_0, a_1 be Hurwitz quaternions with $|a_0| \geq |a_1|$ and $a_0 \neq 0$.

Consider the algorithm given by repeating the following step: Given a_n, a_{n+1}, if we still have $|a_n| \geq |a_{n+1}|$ and $a_n, a_{n+1} \neq 0$, then let c be such that $|a_n - a_{n+1}c| < |a_{n+1}|$. Let $a_{n+2} = a_n - a_{n+1}c$.

Show that this algorithm eventually terminates with $a_{n+1} = 0$ for some n. Call a_n, the last nonzero term, $\text{gcld}(a_0, a_1)$.

Problem 11. Let a, b be Hurwitz quaternions with $|a| \geq |b|$ and $a \neq 0$.

Show that $\text{gcld}(a, b)$ is a Hurwitz quaternion with minimal norm such that there exist Hurwitz quaternions c, d such that $a = \text{gcld}(a, b)c$ and $b = \text{gcld}(a, b)d$.

Problem 12. Let a, b be Hurwitz quaternions with $|a| \geq |b|$ and $a \neq 0$. Show that there exist Hurwitz quaternions c, d such that $\text{gcld}(a, b) = ac + bd$.

4 Putting It All Together

In order to factor p, we will first factor an integer multiple of p into two Hurwitz quaternions that aren't purely real.

Problem 13. Show combinatorially that there exist numbers $l, m \in \{0, 1, \ldots, p-1\}$ such that $1 + l^2 + m^2 \equiv 0 \pmod{p}$.

Problem 14. Find l, m so that there is an integer k with $pk = (1 + li + mj)(1 - li - mj)$.

Now we want to use this factorization to split p. If we had natural numbers such that a divides bc, we could split a into a factor that divides b and a factor that divides c - specifically, $a = \gcd(a, b)\left(\frac{a}{\gcd(a,b)}\right)$. We attempt to replicate that logic with our gcld function.

Problem 15. Find a Hurwitz quaternion α such that:

- There exist Hurwitz quaternions β, γ such that $p = \alpha\beta$ and $1 - li - mj = \alpha\gamma$.
- There exist Hurwitz quaternions b, c such that $\alpha = pb + (1 - li - mj)c$.

It now suffices to show that $|\alpha|, |\beta| > 1$.

Problem 16. If $|\beta| = 1$, show that $(1-li-mj)/p$ is a Hurwitz quaternion, and find a contradiction.

Problem 17. If $|\alpha| = 1$, show that $(1+li+mj)/p$ is a Hurwitz quaternion, and find a contradiction.

Problem 18. Run back through the proof, and make sure you understand how it fits together.