9

Quaternions Applied to Number Theory

In this chapter we shall use integer quaternions to show that every natural number is a sum of four perfect squares. This was first proved by J. L. Lagrange in 1770 (*Oeuvres*, Vol. 3, pp. 189-201).

As a warming up exercise, note that every integer is a sum of five cubes. Indeed, let m be an integer. Since $m - m^3 = -(m-1)m(m+1)$, it follows that $m - m^3$ is divisible by both 2 and 3, and hence by 6. Thus $x = (m - m^3)/6$ is an integer. Moreover, $m = m^3 + 6x = m^3 + (x+1)^3 + (x-1)^3 + (-x)^3 + (-x)^3$, a sum of five cubes. It is not known whether every integer can be written as a sum of four cubes.

About sums of non-negative cubes, it is known that every natural number, except 23 and 239, can be written as a sum of 8 non-negative cubes. As of 1971, it was not known whether the 8 could be lowered for large positive integers (Ellison [1971], pp. 10-36).

To prove the theorem of Lagrange, we shall require the following lemma, due to Euler.

Lemma 9.1. *For every odd prime p there exist integers x and y such that*

$$x^2 + y^2 + 1 = mp,$$

where m is an integer such that $0 < m < p$.

Proof: Let x range from 0 to $\frac{1}{2}(p-1)$. The squares x^2 all leave different remainders when divided by p. For suppose x_1^2 and x_2^2 leave the same remainder. Then $(x_1 + x_2)(x_1 - x_2) = x_1^2 - x_2^2$ is a multiple of p, hence p must divide $x_1 + x_2$ or $x_1 - x_2$. Without loss of generality, we may assume that

$x_1 > x_2$. Then $x_1 \neq x_2$ and

$$0 < x_1 + x_2 < p - 1, \qquad -\frac{p-1}{2} \leq x_1 - x_2 \leq \frac{p-1}{2},$$

hence p divides neither $x_1 + x_2$ nor $x_1 - x_2$. Thus we have a contradiction and the assertion has been proved.

Similarly, we can show that, as y ranges from 0 to $\frac{1}{2}(p-1)$, the numbers $-y^2 - 1$ all leave different remainders when divided by p.

As x and y range from 0 to $\frac{1}{2}(p-1)$, the set of all x^2 thus takes on $\frac{1}{2}(p+1)$ different values and so does the set of all $-y^2 - 1$. Since there are only p possible remainders when one divides by p, the two sets must overlap; hence there exist integers x and y in the given range such that $x^2 + y^2 + 1 = mp$ is a multiple of p. Moreover,

$$1 \leq mp \leq \tfrac{1}{4}(p-1)^2 + \tfrac{1}{4}(p-1)^2 + 1 < p^2,$$

hence $1 \leq m < p$, as required.

Following Lipschitz [1886], p. 404, we define an *integer quaternion* as a quaternion with integer coefficients.

Theorem 9.2. (Lagrange)
Every natural number n is the sum of four perfect squares, that is, n is the norm of an integer quaternion.

Proof: Since the norm of the product of integer quaternions is the product of their norms and since n is a product of primes, it suffices to show that every prime is the norm of an integer quaternion. Since $2 = 1^2 + 1^2 + 0^2 + 0^2$, it suffices to prove this for odd primes. Let p be any odd prime. Then we know from Euler's lemma that there is an integer quaternion x such that $N(x) = mp$ with $0 < m < p$. Pick $m = m_0$ as small as possible with this property. We claim that $m_0 = 1$.

First let us show that m_0 cannot be even. If it is, then so is $x_0^2 + x_1^2 + x_2^2 + x_3^2$, hence also $x_0 + x_1 + x_2 + x_3$ is even. There are three cases: either all the x_i are even, or they are all odd, or exactly two are even, say x_0 and x_1. In all three cases, $x_0 \pm x_1$ and $x_2 \pm x_3$ are even, hence

$$\frac{1}{2} m_0 p = \left(\frac{x_0 + x_1}{2}\right)^2 + \left(\frac{x_0 - x_1}{2}\right)^2 + \left(\frac{x_2 + x_3}{2}\right)^2 + \left(\frac{x_2 - x_3}{2}\right)^2$$

is the sum of four perfect squares. But $\frac{1}{2} m_0$ is a positive integer less than m_0, which contradicts the assumption that m_0 was chosen as small as possible.

We now know that m_0 is odd. Let z_i be the closest integer to $\frac{x_i}{m_0}$, hence $|\frac{x_i}{m_0} - z_i| < \frac{1}{2}$. (It cannot be equal to $\frac{1}{2}$, or else $m_0 = 2|x_i - m_0 z_i|$ would be even.)

Consider the integer quaternion $y = x - m_0 z$, where $z = z_0 + z_1 i_1 + z_2 i_2 + z_3 i_3$. Then

$$|y_i| = |x_i - m_0 z_i| < \tfrac{1}{2} m_0,$$

hence $N(y) < 4(\frac{1}{2}m_0)^2 = m_0^2$. But

$$N(y) = y\bar{y} = x\bar{x} - m_0(x\bar{z} + z\bar{x}) + m_0^2 z\bar{z}.$$

Write $x\bar{z} = w$, so $x\bar{z} + \bar{z}x = 2w_0$, where w_0 is the scalar part of w, and hence

$$N(y) = m_0 p - 2m_0 w_0 + m_0^2 N(z) = m_0 m_1,$$

where $m_1 = p - 2w_0 + m_0 N(z)$. Now $m_0 m_1 = N(y) < m_0^2$, hence $m_1 < m_0$.

Consider now the integer quaternion

$$y\bar{x} = x\bar{x} - m_0 z\bar{x} = m_0 p - m_0 z\bar{x} = m_0(p - z\bar{x}).$$

Then

$$m_0 m_1 m_0 p = N(y)N(\bar{x}) = N(y\bar{x}) = m_0^2 N(p - z\bar{x}),$$

hence

$$m_1 p = N(p - z\bar{x}).$$

Since $m_1 < m_0$, this would contradict the assumption that m_0 was chosen as small as possible, unless $m_1 = 0$.

This leaves only the possibility that $m_1 = 0$, hence $N(y) = 0$, hence $y = 0$, hence $x = m_0 z$, hence $m_0 p = N(x) = m_0^2 N(z)$, hence $p = m_0 N(z)$, hence $m_0 = 1$ or $m_0 = p$. But $m_0 < p$, so $m_0 = 1$, as was required.

Exercises

1. Express 239 as a sum of nine positive cubes.
2. Show that numbers of the form $8k + 7$ cannot be expressed as sums of three perfect squares.
3. Prove that every prime number of the form $4k+1$ can be expressed as the sum of two perfect squares. (Hint: imitate the above proof using complex integers instead of integer quaternions.)