Section 19. Sums of Four Squares

Note. In this section, we prove that every positive integer can be written as a sum of four squares of integers (some of which may be zero).

Note. Diophantus of Alexandria (circa 200 CE–circa 284 CE)) in his *Arithmetica* seems to have assumed that every positive integer is a sum of 2, 3, or 4 squares of positive integers (see Section 3. Linear Diophantine Equations for more information on Diophantus). In 1621, Claude Bachet (October 9, 1581–February 26, 1638) published a Latin translation of Diophantus' *Artihmetica*, and he stated this sum of squares claim as an unproved theorem in the "notes" section. (As a passing comment, it is this version of *Arithmetica* in which Fermat makes the marginal note that led to his "Last Theorem," as discussed in the previous section.) Sometimes the result is known as Bachet's Conjecture. In considering sums of squares, Leonhard Euler (April 15, 1707–September 18, 1783) made partial progress and showed that the product of two sums of four squares is again a sum of four squares (our Lemma 19.1), and that the equation $1 + x^2 + y^2 \equiv 0 \pmod{p}$ has a solution for every prime p (our Lemma 19.2). In 1770, Joseph Louis Lagrange (January 25, 1736–April 10, 1813), using Euler's results, gave a proof that every positive integer is a sum of 4 squares (some of which may be zero); for this reason, the result is often called "Lagrange's Four-Square Theorem." Euler presented a simpler proof in 1773. (Some of these historical details are from Dudley's pages 151 and 152, others from the Wikipedia page on Lagranges Four-Square Theorem and the MacTutor History of Mathematics Archive's page of Bachet.)

Note 19.A. Before the proof, we need several lemmas. The proof of the first result is straightforward and only requires multiplication to verify:

$$(a^2+b^2+c^2+d^2)(r^2+s^2+t^2+u^2) = (ar+bs+ct+du)^2$$

$$+(as-br+cu-dt)^2+(at-bu-cr+ds)^2+(au+bt-cs-dr)^2.$$

Lemma 19.1. The product of two sums of four squares is a sum of four squares.

Note. By Lemma 19.1, to prove Lagrange's Four-Square Theorem it is sufficient to show that every *prime* is the sum of four squares.

Lemma 19.2. If p is an odd prime, then the equation $1+x^2+y^2 \equiv 0 \pmod{p}$ has a solution with $0 \leq x < p/2$ and $0 \leq y < p/2$.

Lemma 19.3. For every odd prime p, there is a positive integer m, $m < p$, such that the equation $mp = x^2+y^2+z^2+w^2$ has a solution.

Lemma 19.4. If m and p are odd, with $1 < m < p$, and $mp = x^2+y^2+z^2+w^2$, then there is a positive integer k_1 with $1 \leq k_1 < m$ such that $k_1 p = x_1^2+y_1^2+z_1^2+w_z^2$ for some integers x_1, y_1, z_1, w_1.

Note. We combine Lemmas 19.3 and 19.4 into the following.

Lemma 19.A. Every prime p can be written as the sum of four integer squares.

Note. We now have the equipment to easily prove Lagrange's Four-Square Theorem.

Theorem 19.1. Lagrange's Four-Square Theorem.
Every positive integer can be written as the sum of four integer squares.

Note. An alternative proof of Lagrange's Four-Square Theorem can be given using techniques from modern algebra. A proof using a subring of the noncommutative division ring of the quaternions is given in my online supplemental notes for Introduction to Modern Algebra 2 (MATH 4137/5137) on Section 7.4. Integral Quaternions and the Four-Square Theorem.

Revised: 4/20/2022