A Three-Square Theorem

Lars Kadison
Institute of Mathematics and Physics, Roskilde University,
Postbox 260,4000 Roskilde, Denmark

Abstract
A prime p congruent to 1 or 3 (mod 8) may be written as

$$p = 2x^2 + y^2$$

for some integers x and y.

1 Introduction

This note grew out of presenting the theory of euclidean domains and its application to Fermat's two-square theorem in a course on abstract algebra at Roskilde University where we used the excellent textbook of I.N. Herstein [2]. A key ingredient in that presentation is the factorization of X^2+Y^2 over the complex numbers. Since $X^2+Y^2+Z^2$ factors into $(X+iY+kZ)(X-iY-kZ)$ over the quaternions, the hope arose that some kind of three-square theorem could be had similarly.

A moments experimentation yields numbers like $41 = 4^2 + 4^2 + 3^2$ and $17 = 2^2 + 2^2 + 3^2$, while neither 23 nor 13 may be written as a sum of three positive squares. These mysteries are happily resolved by considering prime (or irreducible) elements and unique factorization in the euclidean domain $\{x+yi+yk \mid x, y \ \ integers\}$, a subring of the real quaternions that is in fact isomorphic to $Z[\sqrt{-2}]$, the ring of integers of the field of rationals with $\sqrt{-2}$ adjoined. Gauss's lemma implies that -2 is a quadratic residue of primes congruent to 1 or 3 (mod 8). With these two facts one then proves

Theorem 1.1 *For any prime* $p \equiv 1, 3 \pmod 8$ *there exist integers* x *and* y *such that*

$$p = 2x^2 + y^2$$