A simple consequence of this theorem is that any positive integer that factors into powers of 2, powers of primes $\equiv 1, 3 \pmod 8$, and even powers of the other primes, is also representable as a sum of three squares, two of which are identical. This is a consequence of the identity

$$(a^2 + 2b^2)(x^2 + 2y^2) = (ax - 2by)^2 + 2(ay + bx)^2$$

Now Lagrange's theorem states that any positive integer is the sum of four or fewer nonzero squares. The less well-known Gauss-Legendre theorem states that numbers not of the form $4^a(8n + 7)$ are the sum of only three or fewer nonzero squares. Though the theorem above provides more specific information for the numbers specified in corollary 2.1, it can also be viewed as a good and easily puchased partial result toward the Gauss-Legendre theorem, a theorem with a thorny reputation.

This note is intended as a didactic supplement to the excellent textbooks of Herstein [2] and Hardy-Wright [1]. For example, the abstract and the corollary in this note could be posed as a problem with lemmas 2.1,2.2, and 2.3 below given as hints. Then the Gauss-Legendre theorem can be mentioned as a complete answer to which integers are representable as a sum of three squares. Although the author is unaware of any mention of theorem 1.1 in the literature, it is a safe bet that it has been noticed a few hundred years ago and is reaching folklore status by now.

2 Euclidean Rings Strike Again!

Lemma 2.1 *Let p be a prime such that $p \equiv 1, 3 \pmod 8$. Then $2x^2 \equiv -1 \pmod p$ has a solution.*

Proof. It suffices to show that -2 is a quadratic residue of p, for if $y^2 \equiv -2 \pmod p$, then an inverse x of y as an element of the field of p elements Z_p satisfies $2x^2 \equiv -1 \pmod p$.

Now Gauss's lemma [1][1, Theorem 92] implies that -2 is indeed a quadratic residue of p, since the number of members of the set

$$-2, \quad -4, \quad , -6, \ldots \quad , \frac{p-1}{2}(-2)$$

[1]See the appendix for a presentation of Gauss's lemma compatible with a course on abstract algebra.