The Two-Squares Theorem

Anthony Kable

The odd prime numbers $(3, 5, 7, 11, 13, 17, 19, 23, \dots)$ may be divided into two lists according to their remainder when divided by 4. Half the primes $(5, 13, 17, 29, 37, 41, \dots)$ leave a remainder of 1 when divided by 4 and the other half $(3, 7, 11, 19, 23, 31, \dots)$ leave a remainder of 3. Girard noticed long ago (around 1625) that the primes on the first list can all be written as a sum of two squares $(5 = 1^2 + 2^2, \dots, 41 = 5^2 + 4^2, \dots)$ as far as he could check. Euler proved (around 1747) that this pattern continues for all the primes on the first list; he wrestled with the problem for a couple of years before he solved it. This assures us that no matter how large a prime we take from the first list (for example, 5915587277) we will always succeed at writing it as a sum of two squares $(5915587277 = 76621^2 + 6694^2)$. I will explain my favorite way to prove this fact. This way was discovered around 1971 by Heath-Brown and simplified around 1990 by Zagier.