Now apply the norm on R to both sides of equation 1 and obtain

$$p^2 = (a^2 + 2b^2)(c^2 + 2d^2)$$

In general, nonunits $x + y\zeta$ satisfy $d(x + y\zeta) > 1$, hence $p = a^2 + 2b^2$. □

Remark 2.2 The alert reader will note that we also have $p = c^2 + 2d^2$ in the last line of the proof above, which seems to give another representation of p as a sum of three squares. However, $c + d\zeta$ and $a - b\zeta$ are associates by unique factorization in R and applying the involution to equation 1, so $a = \pm c$ and $b = \pm d$.

Corollary 2.1 *Any positive integer*

$$n = 2^{m_1} p_2^{m_2} \cdots p_k^{m_k} p_{k+1}^{2m_{k+1}} \cdots p_r^{2m_r}$$

where $p_i \equiv 1, 3 \pmod 8$ $(i = 2, \ldots, k)$
and $p_j \equiv 5, 7 \pmod 8$ $(j = k+1, \ldots, r)$
and $m_1, \ldots, m_r$ *are positive integers, is expressible as*

$$n = 2x^2 + y^2$$

for some integers x *and* y.

Proof. First note that $2(2x^2 + y^2) = 2y^2 + (2x)^2$. Now combine the theorem with lemma 2.3 in a routine induction argument. □

Remark 2.3 Since $x^2 \equiv 0, 1, 4 \pmod 8$ for all integers x, it follows that $x^2 + 2y^2$ does not assume the values 5 or 7 (mod 8). It is then routine to show that primes $\equiv 5, 7 \pmod 8$ are also prime elements in R. Then unique factorization in R shows that a product of distinct primes $\equiv 5, 7 \pmod 8$ is not of the form $2x^2 + y^2$ either. A routine argument then shows that the integers specified in the corollary exhaust the set of elements of the form $2x^2 + y^2$.