whose least positive residues (mod p) are greater than $p/2$ has even parity. (Write $-2 \equiv p-2 \pmod{p}$, $-4 \equiv p-4 \pmod{p}$, etc., and count in the two cases p of the form 8n + 1 or of the form 8n + 3. □

Remark 2.1 By the same token (Gauss's lemma), -2 is a quadratic nonresidue of primes $p \equiv 5, 7 \pmod{8}$.

Lemma 2.2 *Let i, j, and k be the unit quaternions, and let $\zeta = i+k$. Then the set $R = \{a + b\zeta \mid a, b \text{ integers}\}$ is a commutative subring of the algebra of real quaternions. Moreover, R is isomorphic to the ring $Z[\sqrt{-2}]$ and is a euclidean domain.*

Proof. It is routine to check that R is a commutative subring of the quaternions containing the integers. Note that $\zeta^2 = -2$, so that the map given by $a + b\zeta \mapsto a + b\sqrt{-2}$ is an isomorphism of the rings R and $Z[\sqrt{-2}]$. Now the ring $Z[\sqrt{-2}]$ is known to be a Euclidean domain [1, Theorem 246], but we show it directly in an outline.

Note that R is an involutive subring of the quaternions, where $(a+b\zeta)^* = a-b\zeta$, and that it has norm d defined by $d(a+b\zeta) = a^2+2b^2 = (a+b\zeta)(a+b\zeta)^*$, a positive integer unless a = b = 0. Note that $d(uv) = d(u)d(v)$ for all u and v in R. To check that one has division with remainder one only has to copy the proof of the same for the Gaussian integers [2, theorem 3.8.1]. □

Lemma 2.3 *For any integers a, b, x, and y, we have the identity*

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

Proof. Note that $d((a + b\zeta)(x + y\zeta) = d((ax - 2by) + (bx + ay)\zeta)$
$= d(a + b\zeta)d(x + y\zeta)$. □

Theorem 2.1 *Given prime $p \equiv 1, 3 \pmod{8}$, there exist integers x and y such that*

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

Proof. By lemma 1 there is a solution x of $2x^2 \equiv -1 \pmod{p}$. Then p divides $2x^2 + 1$ both in Z and in the larger ring R. Since p divides $2x^2 + 1 = (1 + x\zeta)(1 - x\zeta)$, but p clearly divides neither $1 + x\zeta$ nor $1 - x\zeta$, it follows that p is not a prime element of the euclidean ring R. Whence p factors into nonunits

$$p = (a + b\zeta)(c + d\zeta) \tag{1}$$