INTEGER QUATERNIONS AND THE FOUR SQUARES THEOREM

The quaternions are defined to be all expressions of the form $q = x + yi + zj + wk$, added component by component, and multiplied according to the rules $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $jk = -kj = i$, and $ki = -ik = j$, which make the multiplication associative, but not commutative. We we define $\overline{q}$, the quaternionic conjugate of q, by $\overline{q} = x - yi - zj - wk$, and it turns out that $\overline{q_1 q_2} = \overline{q_2 q_1}$. We set $N(q) = q\overline{q} = x^2 + y^2 + z^2 + w^2$, and it follows from the product formula for the quaternionic conjugate that $N(q_1 q_2) = N(q_1)N(q_2)$.

An integer quaternion is a quaternion all of whose components are integers. Thus a positive integer is the sum of four squares if and only if it is the norm of an integer quaternion. The multiplicativity of the norm implies that if two integers are each the sum of four squares, then so is their product. It follows that we need only verify that every prime is the sum of four squares. Since some of the squares are allowed to be 0, and we have already verified that every prime not congruent to 3 $\pmod 4$ is the sum of two squares, we need only verify that every prime congruent to 3 $\pmod 4$ is the sum of four squares. We do this in several stages.

Let p be a prime congruent to 3 we wish to prove, at this stage, that mp is the sum of four squares for some $m < p$. We begin by observing that since -1 is not a quadratic residue $\pmod p$, there is no x relatively prime to p for which both x and $-x$ are quadratic residues. It follows, since exactly half the least residues are quadratic residues, that if x is relatively prime to p either x or $-x$ is a quadratic residue.

If $\frac{p-1}{2}$ is a quadratic residue $\pmod p$, then there exists an integer x with $x^2 \equiv \frac{p-1}{2} \pmod p$. Moreover, we may choose x between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$. Then $2x^2 + 1 \equiv 0 \pmod p$ so that $2x^2 + 1 = mp \leq \frac{(p-1)^2}{4} + 1 < p^2$, so that $m < p$. Otherwise, let r be the smallest positive least residue that is not a quadratic residue $\pmod p$. $1 < r < \frac{p-1}{2}$ and $-r$ is a quadratic residue. Now we can choose x and y, both between $-\frac{p-1}{2}$ and $\frac{p-1}{2}$, such that $x^2 \equiv r - 1 \pmod p$ and $y^2 \equiv -r \pmod p$. It follows that $x^2 + 1 + y^2 \equiv 0 \pmod p$ and therefore that $x^2 + 1 + y^2 = mp < p^2$, so that $m < p$ as before.

Now we need a descent argument. We assume $x^2+y^2+z^2+w^2 = mp$ with $1 < m < p$, and we wish to find x', y', z' and w' with $x'^2 + y'^2 + z'^2 + w'^2 = kp$ with $k < m$. If k is even, then x, y, z and w either all have the same parity, or two are even and two are odd. Without loss of generality, we may assume that x and y have the same parity and z and w have the same parity. In this case, we set $x' = \frac{x+y}{2}$, $y' = \frac{x-y}{2}$, $z' = \frac{z+w}{2}$, and $w' = \frac{z-w}{2}$. Then $x'^2 + y'^2 + z'^2 + w'^2 = \frac{m}{2}p$, and we have our descent.

If m is odd, we choose x_1, y_1, z_1, and w_1 congruent $\pmod m$ to x, y, z and w, respectively and strictly between $-\frac{m}{2}$ and $\frac{m}{2}$. We can do this because m is odd and therefore every integer is congruent $\pmod m$ to an integer in the given range. Since $x^2+y^2+z^2+w^2 \equiv 0 \pmod m$, it follows that $x_1^2 + y_1^2 + z_1^2 + w_1^2 = km < m^2$, so that $k < m$. We now set $q = x + yi + zj + wk$ and $q_1 = x_1 + y_1 i + z_1 j + w_1 k$, noting that $q\overline{q} = mp$, $q_1\overline{q}_1 = km$ and $q_1 = q + mq_2$ for some q_2. It follows that $q\overline{q}_1 = q(\overline{q}+mq_2) = m(p+q\overline{q}_2)$. Finally, we set $q' = x'+y'i+z'j+w'k = p+q\overline{q}_2 = \frac{q\overline{q}_1}{m}$. It follows that $q'\overline{q}' = \frac{q\overline{q}_1 q_1\overline{q}}{m^2} = kp$, and once again we have our descent. This completes the proof of the four squares theorem.

The prescription for expressing a prime congruent to 3 $\pmod 4$ as a sum of four squares is entirely constructive. To see this, let us consider the prime 43. Since 43 is not adjacent to a multiple of 8, 2 is a quadratic nonresidue $\pmod{43}$, and hence $-2 \equiv 41$ is a quadratic residue. In fact $16^2 = 256 \equiv -2 \pmod{43}$. This gives us the equation

$$1^2 + 1^2 + 16^2 = 6 \cdot 43,$$

. We pair the coefficients of like parity and taking half the sums and differences, we get

$$1^2 + 8^2 + 8^2 = 3 \cdot 43.$$

We now set $q = 1 + 8i + 8j$ and $q_1 = 1 - i - j = q - 3(3i + 3j)$, so that $q_2 = -3i - 3j$ and $\overline{q}_2 = 3i + 3j$. According to the algorithm laid out in the proof,

$$q' = 43 + q\overline{q}_2 = 43 + 3(1 + 8i + 8j)(i + j) = -5 + 3i + 3j,$$

and indeed $5^2 + 3^2 + 3^2 = 43$. In this case, we only had to use each form of the reduction once; in general we might have to use one or both types of reduction several times.