December 4, 2008

Theorem 9.14 in my book, *Basic Quadratic Forms*, reads as follows:

*If $1 \leq n \leq 4$, then a positive integer is a sum of $n$ integer squares if and only if it is a sum of $n$ rational squares.*

From this theorem the theorems of Lagrange, Fermat, and Gauss on sums of $n \leq 4$ squares are deduced in succession as corollaries. My proof of Theorem 9.14 is based on the claim that the unimodular $\mathbb{Z}$-lattices of form $L \cong \langle 1, \dots, 1 \rangle$ of rank $n \leq 4$, which have class number 1 (by Hermite's inequality on the minimum), are also $\mathbb{Z}$-maximal. The proof of $\mathbb{Z}$-maximality is correct for $n \leq 3$, but a reader has pointed out that the claim is false for $n = 4$: over the ring $\mathbb{Z}_2$ of 2-adic integers the lattice $L_2 = \mathbb{Z}_2 L$ is not $\mathbb{Z}_2$-maximal, and hence $L$ is not $\mathbb{Z}$-maximal. In fact if $\{e_1, \dots, e_4\}$ is an orthonormal basis for $L$, and $e_1' = \frac{1}{2}(e_1 + e_2 + e_3 + e_4)$, then the integral $\mathbb{Z}$-lattice $M = \mathbb{Z}e_1' + \mathbb{Z}e_2 + \mathbb{Z}e_3 + \mathbb{Z}e_4$ (this is the **Hurwitz lattice**) is $\mathbb{Z}$-maximal. This follows from the fact that over $\mathbb{Z}_2$ there is the splitting

$$M_2 \cong \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \perp \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$$

in the basis $\{e_1', e_2, e_3 - e_4, e_1 - e_4\}$. (In my maximality argument over $\mathbb{Z}_2$ I overlooked this lattice.) Notice that $M \supset L$ and $(M : L) = 2$.

Here is a way to correct the error. In the proof of Theorem 9.14, retain the present proofs when $n = 2$ and $n = 3$, but if $n = 4$ defer the proof until after the corollaries. After the theorem ( proved for $n = 2$ and 3), deduce Fermat's Two-Square Theorem and Gauss's Three-Square theorem (the present Corollaries 9.16 and 9.17). With Gauss's Theorem in hand, to prove Lagrange's Theorem (the present Corollary 9.15)—and simultaneously complete the proof of Theorem 9.14—it remains only to show that every positive integer of the form $n = 4^\nu(8k + 7)$, with $k \in \mathbb{Z}$, can be expressed as a sum of four integer squares, and here are two arguments.

**Argument 1 for Lagrange's Theorem**. By Gauss's Theorem the equation

$$n - 4^\nu = 4^\nu(8k + 6) = x^2 + y^2 + z^2$$

is solvable with $x, y, z \in \mathbb{Z}$, and hence $n = (2^\nu)^2 + x^2 + y^2 + z^2$.

**Argument 2 for Lagrange's Theorem**. Let $L \cong \langle 1, 1, 1, 1 \rangle$ as before. For each prime $p \neq 2$ the localization $L_p$ is $\mathbb{Z}_p$-maximal; and since the underlying $\mathbb{Q}_p$-space is universal there is a representation $n \longrightarrow L_p$. Trivially there is a representation $7 \longrightarrow L_2$; and by the Local Square Theorem every integer of the form $8k+7$ has the form $7\varepsilon^2$ for some 2-adic unit $\varepsilon$, hence it is also represented by $L_2$, and therefore there is a representation $n = 2^{2\nu}(8k + 7) \longrightarrow L_2$. Since $L$ has class number 1, this proves Lagrange's Theorem.

With Lagrange's Theorem in hand, the proof of Theorem 9.14 when $n = 4$ is now complete.