Problema J121. For an even integer n consider a positive integer N having exactly n^2 divisors greater than 1. Prove that N is the fourth power of an integer.

Proposed by Titu Andreescu, University of Texas at Dallas, USA

Solution by Ercole Suppa, Teramo, Italy

Let us begin by proving the following:

LEMMA. If an odd prime p divides the sum of the squares of two relatively prime integers, then it must be of the form $4k + 1$.

Proof. Let a, b be two relatively prime integers and p an odd prime such that $p \mid a^2 + b^2$. We have $a^2 \equiv -b^2 \pmod{p}$. Hence by raising the congruence to the power $(p - 1)/2$ we obtain

$$a^{p-1} \equiv (-1)^{\frac{p-1}{2}} b^{p-1} \pmod{p}$$

But, since $(a, b) = 1$, the numbers a, b are not divisible by p, whence, by the Fermat's little Theorem $a^{p-1} \equiv b^{p-1} \equiv 1 \pmod{p}$. Therefore

$$(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

and this implies that $(p-1)/2$ is even, because p is an odd prime. Thus p must be of the form $4k + 1$ as desired. ■

Coming back to the problem, let $N = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$ be the prime factorization of N. Employing the well known formula on the number of divisors of N we get

$$(a_1 + 1)(a_1 + 1) \cdots (a_1 + 1) = n^2 + 1$$

Since $(n, 1) = 1$ by the LEMMA we have that the prime factors of $n^2 + 1$ are all of the form $4k + 1$. Therefore for each $i \in \{1, 2, \ldots, r\}$ there exist $b_i \in \mathbb{Z}$ such that $a_i + 1 = 4b_i + 1$ (since the product of numbers congruent to 1 mod 4 is congruent to 1 mod 4). Consequently

$$N = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} = p_1^{4b_1} p_2^{4b_2} \cdots p_r^{4b_r} = \left(p_1^{b_1} p_2^{b_2} \cdots p_r^{b_r}\right)^4$$

and the proof is complete. □