Dimostriamo che ogni numero naturale è somma di 4 quadrati. Sia

$$\mathbf{H} = \{a + bi + cj + dk : a, b, c, d \in \mathbf{R}\}$$

il corpo dei quaternioni. Si sa che la norma $N\colon \mathbf{H} \longrightarrow \mathbf{R}$ data da $N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2$ è moltiplicativa. Sia R il sottoanello di $\mathbf{H}$ dei *quaternioni interi*

$$R = \{a + bi + cj + dk : a, b, c, d \in \mathbf{Z}\}.$$

Per la moltiplicatività della norma, basta dimostrare che ogni numero primo p è somma di 4 quadrati. Visto che $2 = 1^2 + 1^2 + 0^2 + 0^2$, possiamo supporre che $p > 2$.

Sia $p > 2$ un numero primo. Consideriamo il sottoinsieme di R dato da

$$A = \{x \in R : N(x) \text{ è divisibile per } p\}.$$

Lemma. *L'insieme A contiene un elemento non nullo di norma $< p^2$.*

Dimostrazione. I due sottoinsiemi $\{y^2 + 1 : y \in \mathbf{Z}_p\}$ e $\{-z^2 : z \in \mathbf{Z}_p\}$ di $\mathbf{Z}_p$ hanno $(p+1)/2$ elementi ciascuno e hanno quindi intersezione non vuota. In altre parole, esistono $y, z \in \mathbf{Z}$ tali che $1 + y^2 + z^2 \equiv 0 \pmod p$. Il quaternione $\alpha = 1 + yi + zj$ appartiene quindi ad A. Possiamo scegliere y, z con $|y|, |z| < p/2$. In quel caso la norma di α soddisfa $N(\alpha) < p^2/4 + p^2/4 + 1 < p^2$, come richiesto.

Sia $\beta \in A$ un elemento non nullo di norma minimale. Sia $q \in R$ il quaternione intero più vicino al quoziente $p\beta^{-1} \in \mathbf{H}$. Abbiamo quindi che $N(p\beta^{-1} - q) \leq 1/4 + 1/4 + 1/4 + 1/4 = 1$. Se scriviamo $r = p - q\beta$, allora $N(r) \leq N(\beta)$. Poiché $N(\beta)$ è divisibile per p, lo è anche

$$N(r) = (p - q\beta)(p - \overline{q\beta}) = p^2 - p(q\beta + \overline{q\beta}) + N(q)N(\beta).$$

Il 'resto' r è quindi un elemento di A. Per la minimalità di $N(\beta)$ abbiamo quindi che $r = 0$ oppure $N(r) = N(\beta)$.

Se $r = 0$, allora $p = q\beta$ e per la moltiplicatività delle norma $N(\beta)$ divide $N(p) = p^2$. Se $N(r) = N(\beta)$, abbiamo che $p\beta^{-1} - q = \pm\frac{1}{2} \pm \frac{1}{2}i \pm \frac{1}{2}j \pm \frac{1}{2}k$ e quindi $p = q'\beta$ per qualche $q' \in \mathbf{H}$ che ha la forma $\frac{1}{2}(a + bi + cj + dk)$ con a, b, c, d interi dispari. Siccome

$$N(q') = \frac{a^2 + b^2 + c^2 + d^2}{4}$$

è intera (!), vediamo che anche in questo caso $N(\beta)$ divide $N(p) = p^2$.

In ogni caso, concludiamo che $N(\beta) = 1$, p oppure p^2. Dal fatto che β sta in A, segue che $N(\beta)$ è divisibile per p. Il lemma implica che $N(\beta) < p^2$. Abbiamo quindi che $N(\beta) = p$. In altre parole, p è somma di 4 quadrati, come richiesto.

Per esempio $71 = 7^2 + 3^2 + 3^2 + 2^2$, ma anche $71 = 6^2 + 5^2 + 3^2 + 1^2$. In quanti modi 71 è somma di quattro quadrati? In generale, per un numero naturale n, sia $r(n)$ il numero

di modi di scrivere n come somma di 4 quadrati di numeri interi. Con la teoria delle forme modulari si sa dimostrare che per $n \geq 1$ vale

$$r(n) = \begin{cases} 8\sigma(n); & \text{se } n \text{ non è divisibile per 4,} \\ 8\sigma(n) - 32\sigma(n/4) & \text{se } n \text{ è divisibile per 4,} \end{cases}$$

dove $\sigma(n)$ indica la somma dei divisori positivi di n. In termini di serie di potenze, abbiamo quindi che

$$\sum_{v \in \mathbf{Z}^4} X^{\|v\|^2} = 1 + 8 \sum_{n \geq 1} \frac{nX^n}{1 - X^n} - 32 \sum_{n \geq 1} \frac{nX^{4n}}{1 - X^{4n}}.$$