In questa nota dimostriamo che ogni numero naturale è somma di quattro quadrati e che un numero naturale n è somma di due quadrati se e solo se $\mathrm{ord}_p(n)$ è pari per ogni primo $p \equiv 3 \pmod 4$.

1. Due quadrati.

Definiamo la norma $N : \mathbf{C} \longrightarrow \mathbf{R}$ tramite $N(x) = x\overline{x} = |x|^2 = a^2 + b^2$ dove $x = a + bi$ con $a, b \in \mathbf{R}$. Allora $N(x) \geq 0$ per ogni $x \in \mathbf{C}$ e $N(x) = 0$ se e solo se $x = 0$. La norma è moltiplicativa nel senso che $N(xy) = N(x)N(y)$ per ogni $x, y \in \mathbf{C}$. Con $\mathbf{Z}[i]$ indichiamo l'anello degli interi di Gauss. La norma di x è intera se $x \in \mathbf{Z}[i]$.

Lemma 1. *Per ogni $z \in \mathbf{C}$ esiste $q \in \mathbf{Z}[i]$ con $|z - q| < 1$.*

Dimostrazione. Sia $z = u + iv$ con $u, v \in \mathbf{R}$. Sia a l'intero più vicino ad u e b l'intero più vicino a v. Definiamo $q = a + bi$. Si ha quindi che $|u - a| \leq \frac{1}{2}$ e $|v - b| \leq \frac{1}{2}$. Questo implica che $|z - q| \leq (\frac{1}{2})^2 + (\frac{1}{2})^2 = \frac{1}{2} < 1$ come richiesto.

Corollario 2. *L'anello $\mathbf{Z}[i]$ è un dominio ad ideali principali.*

Dimostrazione. Seguiamo la dimostrazione che ogni dominio Euclideo è un dominio ad ideali principali.

Sia $I \subset \mathbf{Z}[i]$ un ideale. Se $I = 0$, allora è certamente principale. Supponiamo che $I \neq 0$. Sia $x \in I$ non nullo con norma *minimale*. Dimostriamo che x genera I: sia $y \in I$ un elemento arbitrario. Per il Lemma 1 applicato al quoziente $z = y/x \in \mathbf{C}$. Allora esiste $q \in \mathbf{Z}[i]$ con $|y/x - q| < 1$. Moltiplichiamo per $|x|$ e troviamo che $|y - qx| < |x|$ e quindi $N(y - qx) < N(x)$. Poiché $y - qx$ appartiene all'ideale I e la norma $N(x)$ è minimale, abbiamo necessariamente che $N(y - qx) = 0$ e quindi $y - qx = 0$. In altre parole, si ha che $y = qx$ e quindi y appartiene all'ideale generato da x.

Questo dimostra che $I = (x)$ come richiesto.

Proposizione 3. *Sia $p \neq 2$ un primo. Allora p è somma di due quadrati se e solo se $p \equiv 1 \pmod 4$.*

Dimostrazione. Se $p = a^2 + b^2$ con $a, b \in \mathbf{Z}$, allora a è pari e b è dispari o viceversa. Questo implica che $a^2 \equiv 0 \pmod 4$ e $b^2 \equiv 1 \pmod 4$ o vicerversa. In ogni caso si trova che $p = a^2 + b^2 \equiv 1 \pmod 4$.

Viceversa, sia $p \equiv 1 \pmod 4$. Allora il gruppo $\mathbf{Z}_p^*$ ha ordine divisibile per 4. Poiché $\mathbf{Z}_p^*$ è ciclico, esiste un elemento di ordine 4. In altre parole, esiste $z \in \mathbf{Z}$ con $z^2 \equiv -1 \pmod p$. Possiamo supporre (e supponiamo) che $-p/2 < z < p/2$.

Per il Corollario 2, l'ideale I di $\mathbf{Z}[i]$ generato da p e $z - i$ è principale. Abbiamo che $I = (a + bi)$ con $a, b \in \mathbf{Z}$. Il fatto che $p = \lambda(a + bi)$ per $\lambda \in \mathbf{Z}[i]$, implica che $N(a + bi) = a^2 + b^2$ divide $N(p) = p^2$. Ci sono quindi tre possibilità: $a^2 + b^2$ è uguale a 1, p oppure a p^2.

Il fatto che $z - i$ appartiene all'ideale generato da $a + bi$ implica che $a^2 + b^2$ divide $N(z - i) = z^2 + 1$. Poichè z soddisfa $|z| < p/2$, abbiamo che $z^2 + 1 < p^2/4 + 1 < p^2$. Vediamo quindi che $a^2 + b^2$ non può essere uguale a p^2.

Per vedere che a^2+b^2 non può essere neanche uguale a 1, verifichiamo che *ogni* elemento dell'ideale $I = (p, z-i)$ ha norma divisibile per p. Sia $y \in I$. Allora $y = \lambda p + \mu(z-i)$ con $\lambda, \mu \in \mathbf{Z}[i]$. La norma di y è data da

$$\begin{aligned} N(y) &= (\lambda p + \mu(z-i))(\overline{\lambda} p + \overline{\mu}(z+i)), \\ &= \lambda\overline{\lambda}p^2 + p\left(\lambda\overline{\mu}(z+i) + \overline{\lambda}\mu(z-i)\right) + \mu\overline{\mu}(z^2+1). \end{aligned}$$

Per costruzione, l'intero z^2+1 è divisibile per p. Poiché $\lambda\overline{\lambda}$, $\mu\overline{\mu}$ e $\lambda\overline{\mu}(z+i) + \overline{\lambda}\mu(z-i)$ sono in $\mathbf{Z}$, l'espressione a destra è un intero divisibile per p.

Quindi, a^2+b^2 non è uguale né a p^2 né a 1. L'unica possibilità rimasta è che $p = a^2+b^2$ come richiesto.

Esempio. Sia $p = 20112011201120112011201120112011201120112217$. Allora

$$p = 39563309597395626 1^2 + 211174253594663936^2.$$

Teorema 4. *Sia $n \in \mathbf{Z}_{\geq 1}$. Allora n è somma di due quadrati se e solo se $\mathrm{ord}_p(n)$ è pari per ogni primo $p \equiv 3 \pmod 4$.*

Dimostrazione. Sia $n = a^2 + b^2$ con $a, b \in \mathbf{Z}$ e sia p un primo congruo a 3 modulo 4. Se p non divide n, allora $\mathrm{ord}_p(n) = 0$ è pari. Supponiamo che p divida n. Allora si ha che $a^2 + b^2 \equiv 0 \pmod p$. Se a non è divisibile per p, allora a è invertibile modulo p e si ha che $(b/a)^2 \equiv -1 \pmod p$. Questo implica che la classe di b/a modulo p ha ordine 4 nel gruppo $\mathbf{Z}_p^*$. Il Teorema di Lagrange implica che 4 divide $p-1 = \#\mathbf{Z}_p^*$ e si ha quindi che $p \equiv 1 \pmod 4$. Contraddizione.

Allora p divide a e quindi anche b. Questo implica che p^2 divide n e quindi

$$\frac{n}{p^2} = (\frac{a}{p})^2 + (\frac{b}{p})^2.$$

Per induzione il teorema vale per n/p^2 e quindi $\mathrm{ord}(\frac{n}{p^2})$ è pari. Poiché si ha che $\mathrm{ord}(n) = \mathrm{ord}(\frac{n}{p^2}) + 2$, anche $\mathrm{ord}_p(n)$ è pari, come richiesto.

2. Quattro quadrati.

Sia $\mathbf{H}$ il corpo dei quaternioni di Hamilton. Il coniugio $\overline{x}$ di un elemento $x \in \mathbf{H}$ della forma $x = a + bi + cj + dk$ con $a, b, c, d \in \mathbf{R}$ è dato da $\overline{x} = a - bi - cj - dk$. Si ha che $\overline{xy} = \overline{y}\,\overline{x}$ per ogni $x, y \in \mathbf{H}$. La norma $N : \mathbf{H} \longrightarrow \mathbf{R}$ è definita da $N(x) = x\overline{x} = |x|^2 = a^2 + b^2 + c^2 + d^2$ dove $x = a + bi + cj + dk$ con $a, b, c, d \in \mathbf{R}$. Allora $N(x) \geq 0$ per ogni $x \in \mathbf{H}$ e $N(x) = 0$ se e solo se $x = 0$. La norma è moltiplicativ nel senso che $N(xy) = N(x)N(y)$ per ogni $x, y \in \mathbf{H}$.

Sia W l'anello dei quaternioni di Hurwitz. Si ha quindi che

$$\begin{aligned} W &= \mathbf{Z}[i, j, k, \frac{1+i+j+k}{2}], \\ &= \{\frac{a+bi+cj+dk}{2} \in \mathbf{H} : a, b, c, d \in \mathbf{Z} \text{ tutti pari o tutti dispari}\}. \end{aligned}$$

Per esempio, il quaternione $\epsilon = \frac{1+i+j+k}{2}$ è un elemento di W, ma $\frac{1}{2} + i$ no. Ogni $x \in W$ ha la forma $a+bi+cj+dk$ con $a, b, c, d \in \mathbf{Z}$ oppure $\epsilon + (a+bi+cj+dk)$ con $a, b, c, d \in \mathbf{Z}$. Dal fatto che $\epsilon^2 = \epsilon - 1$ segue facilmente che il prodotto di due elementi in W sta ancora in W e che W è un sottoanello di $\mathbf{H}$. Per $x \in W$ si ha che $x + \overline{x} \in \mathbf{Z}$ e che $N(x) = x\overline{x} \in \mathbf{Z}$. Questo segue dal fatto che $a^2 + b^2 + c^2 + d^2$ è divisibile per 4 quando a, b, c, d sono interi che hanno la stessa parità.

Lemma 5. *Per ogni $z \in \mathbf{H}$ esiste $q \in W$ con $N(z-q) < 1$.*

Dimostrazione. Sia $z = u + iv + iw + kt$ con$u, v, w, t \in \mathbf{R}$. Sia $q = a + bi + cj + dk$ dove a, b, c, d sono gli interi più vicini ad u, v, w, t rispettivamente. I numeri reali $u - a$, $v - b$, $w - c$ e $t - d$ appartengono quindi all'intervallo $[-\frac{1}{2}, \frac{1}{2}]$. Poiché $N(z-q)$ è la somma dei loro quadrati, si ha che $N(z-q) \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1$.

Se la disugualianza è stretta abbiamo finito. Se abbiamo ugualianza, allora i numeri $u - a$, $v - b$, $w - c$ e $t - d$ sono per forza tutti uguali a $\pm\frac{1}{2}$. In questo caso il quaternione $z = u + iv + iw + kt$ è uguale a la somma di un quaternione del tipo $\frac{\pm 1 \pm i \pm j \pm k}{2}$ e $x = a + bi + cj + dk$. Dunque $z \in W$ e possiamo prendere $q = z$.

Questo dimostra il lemma.

La stima del Lemma 5 non è ottimale. Per i fanatici spieghiamo adesso come ottenere la stima ottimale. Ad ogni modo, questo risultato non è necessario per la dimostrazione del fatto che ogni numero naturale è somma di quattro quadrati.

Osservazione. *Per ogni $z \in \mathbf{H}$ esiste $q \in W$ con $N(z-q) \leq \frac{1}{2}$.*

Dimostrazione. Sia $z = u+iv+iw+kt$ per certi $u, v, w, t \in \mathbf{R}$. Come nella dimostrazione del Lemma 5 definiamo $q = a+bi+cj+dk$ dove a, b, c, d sono gli interi più vicini ad u, v, w, t rispettivamente. Sia (x_1, x_2, x_3, x_4) il vettore delle differenze $(u-a, v-b, w-c, t-d)$. Si ha che $|x_i| \leq \frac{1}{2}$ per ogni i e quindi che $N(z-q) = \sum_{i=1}^4 x_i^2 \leq 1$. Se $\sum_{i=1}^4 x_i^2 \leq \frac{1}{2}$, abbiamo finito.

Supponiamo ora che $\sum_{i=1}^4 x_i^2 > \frac{1}{2}$. Sia $u \in W$ dato da $e = \epsilon_1 + \epsilon_1 i + \epsilon_1 j + \epsilon_1 k$, dove $\epsilon_i = \pm\frac{1}{2}$ ha lo stesso segno di x_i per ogni i. Questo implica che $(x_i - \epsilon_i)^2 = (|x_i| - |\epsilon_i|)^2$ e che $x_i^2 \leq |\epsilon_i x_i|$ per ogni i. Sia $q' = q - u$. Si ha che q' appartiene a W. Stimiamo la norma $N(z-q') = \sum_{i=1}^4 (x_i - \epsilon_i)^2$:

$$\sum_{i=1}^4 (x_i - \epsilon_i)^2 \;=\; \sum_{i=1}^4 (|x_i| - |\epsilon_i|)^2 \;=\; \sum_{i=1}^4 (x_i^2 - 2|x_i\epsilon_i| + \epsilon_i^2) \;\leq\; -\sum_{i=1}^4 x_i^2 + 1 \;\leq\; \frac{1}{2}.$$

Quindi in questo caso q' è il quaternione cercato.

Lemma 6. *Ogni ideale sinistro di W è principale.*

Dimostrazione. Copiamo la dimostrazione del Lemma 2. L'unica complicazione è il fatto che W non è commutativo.

Sia I un ideale non nullo di W e sia $x \in I$ un elemento non nullo di norma minimale. Allora x genera I nel senso che $I = \{\lambda x : \lambda \in W\}$. Per vedere questo, sia $y \in I$ arbitrario. Consideriamo il quoziente yx^{-1} in $\mathbf{H}$. Per il Lemma 5 esiste $q \in W$ tale che $N(yx^{-1} - q) <$

1. Moltiplicando per $N(x)$ troviamo che $N(y-qx) < N(x)$. L'elemento $y-qx$ appartiene all'ideale I e non può avere norma $< N(x)$, eccetto quando $y-qx=0$. Abbiamo quindi che $y=qx$ e il lemma segue.

Lemma 7. *Per ogni primo p esistono $u, v \in \mathbf{Z}$ tali che $u^2+v^2+1 \equiv 0 \pmod{p}$.*

Dimostrazione. I due sottoinsiemi $A = \{v^2+1 : v \in \mathbf{Z}_p\}$ e $B = \{-u^2 : u \in \mathbf{Z}_p\}$ hanno tutti e due $\frac{p+1}{2}$ elementi. Poiché $\#A + \#B > \#\mathbf{Z}_p$, necessariamente $A \cap B \neq \emptyset$. Questo dimostra il lemma.

Proposizione 8. *Ogni numero primo ha la forma $N(x)$ per un x nell'anello di Hurwitz W.*

Dimostrazione. Siano $u, v \in \mathbf{Z}$ come nel Lemma 7. Possiamo supporre che $|u|, |v| < p/2$. Consideriamo l'ideale sinistro I di W generato da p e $1+ui+vj$. Per il Lemma 6 l'ideale I è principale. Sia x un generatore. Allora $p = \lambda x$ con $\lambda \in W$. Questo implica che $N(x)$ divide $N(p) = p^2$. Si sa quindi che $N(x)$ è uguale a 1, p opure p^2. Dal fatto che $1+ui+vj = \mu x$ per un certo $\mu \in \mathbf{Z}$, segue che $N(x)$ divide $1+u^2+v^2 < 1+2\cdot(p/2)^2 < p^2$. Questo implica che $N(x) \neq p^2$.

Per escludere la possibilità che $N(x)=1$, dimostriamo che ogni elemento dell'ideale $I = (p, 1+ui, vj)$ ha norma divisibile per p. Sia $y = I$. Allora si ha che $y = \lambda p + \mu(1+ui, vj)$ con $\lambda, \mu \in W$. Calcoliamo

$$\begin{aligned} N(y) &= (\lambda p + \mu(1+ui, vj))(\overline{\lambda} p + (1-ui-vj)\overline{\mu}, \\ &= \lambda\overline{\lambda}p^2 + \left(\lambda(1-ui-vj)\overline{\mu} + \mu(1+ui+vj)\overline{\lambda}\right) p + \mu\overline{\mu}(1+u^2+v^2). \end{aligned}$$

Per costruzione l'intero $1+u^2+v^2$ è divisibile per p. Poiché $\lambda\overline{\lambda}$, $\mu\overline{\mu}$ e

$$\lambda(1-ui-vj)\overline{\mu} + \mu(1+ui+vj)\overline{\lambda} = \lambda(1-ui-vj)\overline{\mu} + \overline{\lambda(1-ui-vj)\overline{\mu}}$$

sono in $\mathbf{Z}$, l'espressione a destra è un intero divisibile per p, come richiesto.

Theorem 9. *Ogni numero naturale è somma di quattro quadrati.*

Dimostrazione. Sia n un numero naturale. Allora n è prodotto di numeri primi. Per la Proposizione 8 ogni primo è norma di un quaternione di Hurwitz. Poiché $N(yz) = N(y)N(z)$ per ogni $y, z \in W$, si ha quindi che $n = N(x)$, per un $x \in W$.

Se x ha la forma $x = a+bi+cj+dk$ con $a, b, c, d \in \mathbf{Z}$, allora si ha che $n = a^2+b^2+c^2+d^2$ e la dimostrazione è completa. Se invece $x = \frac{a_1+a_2i+a_3j+a_4k}{2}$ con a_1, a_2, a_3, a_4 dispari, facciamo vedere che esiste $u \in W$ di norma 1 tale che $\overline{u}x = a+bi+cj+dk$ con $a, b, c, d \in \mathbf{Z}$ e quindi $n = N(\overline{u}x) = a^2+b^2+c^2+d^2$.

Infatti, sia $u = \frac{u_1+u_2i+u_3j+u_4k}{2}$ dove $u_i = 1$ se $a_i \equiv 1 \pmod 4$ e $u_i = -1$ se $a_i \equiv 3 \pmod 4$ per ogni i. Si ha $N(u) = \frac{1}{4}+\frac{1}{4}+\frac{1}{4}+\frac{1}{4} = 1$ e $x = u+2y$ dove y è un quaternione a coefficienti interi. Allora il quaternione $\overline{u}x = \overline{u}(u+2y) = 1+2\overline{u}y$ ha coefficienti interi, come richiesto.

Questo dimostra il teorema.

Esempio. Il numero $n = 201120112011201120112011201120112215$ è uguale a

$$32794599076662750 7^2+2308169545127268 74^2+193306634377412161^2+54107464978905213^2.$$

3. Tre quadrati.

Lemma 10. *Se $n = 4^k(7 + 8m)$ con $k, m \in \mathbf{Z}_{\geq 0}$, allora n non è somma di tre quadrati.*

Dimostrazione. Sia $n = 4^k(7 + 8m)$ e supponiamo che $n = a^2 + b^2 + c^2$ con $a, b, c \in \mathbf{Z}$. Se a, b, c sono tutti pari, allora n è divisibile per 4 ed abbiamo che $\frac{n}{4} = 4^{k-1}(7 + 8m)$. Per induzione, $\frac{n}{4}$ non è una somma di tre quadrati, contraddicendo il fatto che $\frac{n}{4} = (\frac{a}{2})^2 + (\frac{b}{2})^2 + (\frac{c}{2})^2$.

Quindi, almeno uno di a, b, c è dispari. Diciamo che a è dispari e quindi $a^2 \equiv 1 \pmod 8$. Supponiamo prima che b e c abbiano la stessa parità. Questo implica che n è dispari e quindi $k = 0$ e $n \equiv 7 \pmod 8$. Se $b \equiv c \equiv 0 \pmod 2$, allora $b^2 + c^2 \equiv 0 \pmod 4$ e quindi $n = a^2 + b^2 + c^2 \equiv 1 \pmod 4$. Contraddizione. Se invece $b \equiv c \equiv 1 \pmod 2$, allora $b^2 + c^2 \equiv 2 \pmod 8$ e quindi $n = a^2 + b^2 + c^2 \equiv 3 \pmod 8$. Contraddizione.

In conclusione, b e c non hanno la stessa parità. Diciamo che b è dispari, mentre c è pari. Allora $b^2 \equiv 1 \pmod 4$ e $c^2 \equiv 0 \pmod 4$. Troviamo che $n = a^2 + b^2 + c^2 \equiv 2 \pmod 4$. Contraddizione.

Questo dimostra il lemma.

Teorema 11. *Ogni $n \in \mathbf{Z}_{\geq 0}$ che non ha la forma $n = 4^k(7 + 8m)$ con $k, m \in \mathbf{Z}_{\geq 0}$, è somma di tre quadrati.*

Dimostrazione. Si veda: Cassels, J.W.S. and Fröhlich, A.: *Algebraic Number Theory*, Exercise 4, p. 357 (Academic Press 1967)