4 Interi somma di più di due quadrati

Abbiamo già osservato, risolvendo l'equazione diofantea $X^2 + Y^2 = n$, che *non* ogni intero positivo si può scrivere come somma di due quadrati di interi (ad esempio: $3 = 1^2+1^2+1^2$, $6 = 2^2+1^2+1^2$, $15 = 3^2+2^2+1^2+1^2$). Si pone naturalmente il problema di trovare il numero minimo di quadrati di interi (relativi o, equivalentemente, non negativi) necessari in una somma per scrivere un qualunque intero positivo.

Per quanto riguarda il problema degli interi positivi, che si possono scrivere come somma di tre quadrati, ma non di due (ad esempio: $3 = 1^2+1^2+1^2$, $43 = 3^2+3^2+5^2$), possiamo senz'altro dire che esso è notevolmente più difficile di quello corrispondente per due o quattro quadrati. Una delle ragioni è che, a differenza di quanto accade nel caso della somma di due (o come vedremo anche nel caso di quattro quadrati), il prodotto di due interi che si possono scrivere come somma di tre quadrati non è, in generale, un intero somma di tre quadrati. (Ad esempio, $3 \cdot 21 = (1^2+1^2+1^2)(4^2+2^2+1^2) = 63 = 7^2+3^2+2^2+1^2$ oppure $3 \cdot 13 = (1^2+1^2+1^2)(3^2+2^2+0^2) = 39 = (6^2+1^2+1^2+1^2)$; mentre, al contrario, $3 \cdot 43 = 129 = 11^2+2^2+2^2$ è ancora ottenibile come somma di tre quadrati.)

A proposito di tale problema segnaliamo che, nel 1785, Legendre affermò che *ogni intero positivo od il suo doppio si può scrivere come somma di tre quadrati di interi*, risultato che egli dimostrò poi completamente nel 1798 come conseguenza del suo teorema generale che asserisce che *ogni intero positivo che non è del tipo* $4k$*, né del tipo* $8k+7$*, è somma di tre quadrati di interi*. Il risultato più generale concernente tale problema è il seguente teorema dimostrato da Gauss, il quale ha completato il lavoro iniziato da Legendre; i successivi contributi di Cauchy e Dirichlet riguardano semplificazioni della dimostrazione di Gauss.

Teorema 4.1. (A.M. Legendre, 1798; K.F. Gauss, 1801) *Un numero naturale* $n \geq 1$ *può essere scritto come somma di tre quadrati di interi se, e soltanto se,* $n \neq 4^e(8k+7)$*, con* e, k *interi,* $e, k \geq 0$.

Dimostrazione. Ci limitiamo a dimostrare la parte "soltanto se" di tale teorema, parte che non presenta particolari difficoltà.

Sia $n = x^2 + y^2 + z^2$ un numero intero, con $n \geq 1$. Per mostrare che $n \neq 4^e(8k+7)$, ragioniamo per induzione sull'intero $e \geq 0$. Dal momento che il quadrato di un intero è congruo a $0, 1$ e $4 \pmod 8$, allora n è congruo a $0, 1, 2, 3, 4, 5,$ o $6 \pmod 8$, cioè $n \neq 8k+7$, per ogni intero $k \geq 0$. Supponiamo

che fissato $e \geq 1$, $n \neq 4^{e-1}(8k+7)$, per ogni intero $k \geq 0$. Vogliamo mostrare che $n \neq 4^e(8k+7)$, per ogni intero $k \geq 0$. Se per assurdo $n = 4^e(8k+7)$, per qualche $k \geq 0$, allora $4 \mid n$, da cui x, y, z devono essere tutti pari e quindi $n/4 = 4^{e-1}(8k+7) = (x/2)^2 + (y/2)^2 + (z/2)^2$, e ciò è assurdo per l'ipotesi induttiva.

□

Osservazione 4.2. **(a)** Per la dimostrazione della parte "se" cfr., ad esempio, E. Landau [7] oppure L.J. Mordell [9].

(b) Se n è un numero naturale, $n \geq 1$, si può dimostrare che:

(1) se $n \equiv 0 \pmod 8$, allora, per infiniti valori di n (ad esempio, $n := 24 \cdot k^2$, $k \geq 1$), n può essere scritto come somma di tre quadrati di interi positivi ($24 \cdot k^2 = (4k)^2 + (2k)^2 + (2k)^2$) e, per infiniti valori di n (ad esempio, $n := 2^k$, per $k \geq 1$; risultato dimostrato da A. Hurwitz nel 1907, cfr. Esercizio 4.3 (b)), n *non* può essere scritto come somma di tre quadrati di interi positivi (cfr. Sierpiński [13, p. 406]);

(2) se $n \equiv 1 \pmod 8$, allora B. Jones e G. Pall nel 1939 hanno dimostrato che, tranne 1 e 25, tutti i numeri naturali di questo tipo si possono scrivere come somma di tre quadrati interi.

(3) se $n \equiv 4 \pmod 8$, allora $n = 8k + 4$ è somma di tre quadrati di interi positivi se, e soltanto se, $2k + 1$ gode della stessa proprietà (cfr. anche il successivo Esercizio 4.3 (a)).

(4) Se $n \equiv 6 \pmod 8$, allora n è somma di tre quadrati di interi (semplice conseguenza del Teorema 4.1), ma non è somma di due quadrati di interi, perché $n = 8k + 6 = 2(4k + 3)$.

Dal Teorema 4.1 discende che $7, 15, 23, 28, \ldots$ non sono somma di tre quadrati. Nel 1621, Bachet, nelle sue note alla *Arithmetica* di Diofanto, congetturò che ogni intero positivo si può scrivere come somma di quattro quadrati di interi, affermando tra l'altro di aver verificato tale congettura per tutti gli interi positivi $n \leq 325$. Fermat, in un'altra celebre annotazione, affermò di aver provato la Congettura di Bachet, usando il metodo della discesa infinita (cfr. la dimostrazione del successivo Teorema 4.7). Più tardi, egli sfidò gli altri cultori di tali problematiche suoi contemporanei a dimostrare questo risultato, in modo da verificare di non aver sopravvalutato questa sua notevole scoperta. Euler tentò a lungo di dare una dimostrazione

di tale risultato, ma ottenne soltanto dei risultati parziali. Lagrange, nel 1770, fu il primo a dare una dimostrazione completa della Congettura di Bachet, riconoscendo ad Euler un notevole contributo di idee che egli utilizzò nella sua dimostrazione.

Per dimostrare il Teorema di Lagrange dei quattro quadrati, procediamo, inizialmente, in una maniera analoga a quella seguita nel problema della decomposizione di un intero positivo come somma di due quadrati di interi.

Proposizione 4.3. (L. Euler, 1748) *Siano $n, m \in \mathbb{N}^+$. Se n e m possono essere scritti come somma di quattro quadrati di interi, allora anche nm può essere scritto come somma di quattro quadrati di interi.*

Dimostrazione. L'enunciato è una immediata conseguenza della seguente identità

$$\begin{aligned}(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2) = \\ = (ae+bf+cg+dh)^2+(af-be+ch-dg)^2+ \\ +(ag-ce+df-bh)^2+(ah-de+bg-cf)^2\ .\end{aligned} \tag{4.3.1}$$

□

Osservazione 4.4. La verifica di una identità, in particolare della identità (4.3.1), consiste in un banale sviluppo dei calcoli indicati ad ambo i membri dell'uguaglianza. La scoperta della identità (4.3.1), dovuta ad Euler, è stata fondamentale importanza per la risoluzione del problema in esame. Si noti che questa identità non è, al contrario di quella simile relativa alla somma di due quadrati, una semplice conseguenza di proprietà inerenti i numeri complessi. Essa è, invece, conseguenza delle proprietà algebriche di una struttura algebrica più riposta: i quaternioni.

A proposito delle identità, che sono strumenti ricorrenti di indagine in teoria dei numeri, Littlewood ha acutamente osservato che "ogni identità è banale, se è scoperta da ... qualcun altro".

Corollario 4.5. *Se ogni numero primo può essere scritto come somma di quattro quadrati di interi, allora ogni intero positivo può essere scritto come somma di quattro quadrati di interi.*

Dimostrazione. Immediata conseguenza della Proposizione 4.3.

□

Proposizione 4.6. *Per ogni primo p, esistono $x, y \in \mathbb{Z}$ in modo tale che*

$$x^2 + y^2 \equiv -1 \pmod{p} \ .$$

Dimostrazione. **Caso 1**: $p = 2$. Allora, basta porre $x = 1$, $y = 0$.

Caso 2: $p \equiv 1 \pmod 4$. Allora basta porre $y = 0$ e x uguale ad una soluzione della congruenza $X^2 \equiv -1 \pmod p$, esistente in quanto in tal caso $\left(\frac{-1}{p}\right) = 1$ (cfr. Proposizione I.6.6 (h)).

Caso 3: $p \equiv 3 \pmod 4$. Allora basta trovare un intero y tale che la congruenza

$$X^2 \equiv -(y^2 + 1) \pmod{p}$$

è risolubile, cioè, usando il simbolo di Legendre, un intero y tale che

$$\left(\frac{-(y^2+1)}{p}\right) = 1 \ .$$

Ma, poiché:

$$\left(\frac{-(y^2+1)}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{y^2+1}{p}\right) = -\left(\frac{y^2+1}{p}\right)$$

basta trovare un intero y tale che $\left(\frac{y^2+1}{p}\right) = -1$. Dal momento che tutti e soli gli interi a, tali che esiste $y \in \mathbb{Z}$ per cui $a \equiv y^2 \pmod p$ sono per definizione gli interi a tali che $\left(\frac{a}{p}\right) = 1$, allora basta determinare un intero $a \pmod p$ in modo tale che $\left(\frac{a}{p}\right) = 1$ e $\left(\frac{a+1}{p}\right) = -1$. È evidente che esistono interi che verificano tale proprietà (altrimenti, poiché $\left(\frac{1}{p}\right) = 1$, si avrebbe $\left(\frac{1+1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \ldots = \left(\frac{p-1}{p}\right) = 1$) (cfr. anche l'Esercizio I.6.19).

□

Teorema 4.7. (J. L. Lagrange, 1770) *Sia n un intero positivo. Allora, n può essere scritto come somma di quattro quadrati di interi.*

Dimostrazione. Per il Corollario 4.5, ci si può limitare al caso in cui $n = p$, con p primo. Se $p = 2$, allora $2 = 1^2 + 1^2 + 0^2 + 0^2$, dunque si può supporre p primo dispari. Consideriamo la congruenza in due indeterminate:

$$X^2 + Y^2 \equiv -1 \pmod{p} \ .$$

Per la Proposizione 4.6, tale congruenza è sempre risolubile, quindi possiamo trovare $t, x, y \in \mathbb{Z}$, con $|x|$, $|y| \leq p/2$, in modo tale che

$$x^2 + y^2 + 1 = tp \ .$$

Abbiamo, dunque, mostrato che un multiplo di p è somma di quattro quadrati, cioè $tp = x^2 + y^2 + z^2 + w^2$, con $x, y \in \mathbb{Z}$, $z = 1$, $w = 0$. Vogliamo, ora, dimostrare che tale proprietà vale per $t = 1$. Sappiamo che:

$$0 \lneqq t = \frac{x^2 + y^2 + 1}{p} \leq \frac{(p/2)^2 + (p/2)^2 + 1}{p} = p/2 + 1/p \lneqq p \ .$$

Sia k il più piccolo intero positivo tale che $kp = x_1^2 + y_1^2 + z_1^2 + w_1^2$, con $x_1, y_1, z_1, w_1 \in \mathbb{Z}$, e supponiamo, per assurdo, che $1 \lneqq k$ ($\lneqq p$). Siano x_2, y_2, z_2, w_2 elementi di $S := \{0, +1, -1, +2, -2, \ldots\}$, sistema completo di residui (mod k) *minimo in valore assoluto*, tali che $x_1 \equiv x_2 \pmod{k}$, $y_1 \equiv y_2 \pmod{k}$, $z_1 \equiv z_2 \pmod{k}$, $w_1 \equiv w_2 \pmod{k}$. Si ha, ovviamente, che $|x_2| \leq k/2$, $|y_2| \leq k/2$, $|z_2| \leq k/2$, $|w_2| \leq k/2$. Per le scelte effettuate è chiaro, che non può essere:

$$x_2 \equiv y_2 \equiv z_2 \equiv w_2 \equiv 0 \pmod{k} \ ,$$

perché, altrimenti, si avrebbe $kp \equiv 0 + 0 + 0 + 0 = 0 \pmod{k^2}$, da cui si avrebbe che $k \,|\, p$, donde un assurdo. Inoltre, non può essere

$$|x_2| = |y_2| = |z_2| = |w_2| = k/2 \ ,$$

perché altrimenti, si avrebbe $kp \equiv 4(k/2)^2 = k^2 \equiv 0 \pmod{k^2}$, da cui di nuovo un assurdo. Ora, risulta:

$$0 \equiv x_1^2 + y_1^2 + z_1^2 + w_1^2 \equiv x_2^2 + y_2^2 + z_2^2 + w_2^2 \pmod{k} \ ,$$

dunque, esisterà un intero t' in modo tale che:

$$x_2^2 + y_2^2 + z_2^2 + w_2^2 = t'k \quad \text{cioè} \quad t' = \frac{x_2^2 + y_2^2 + z_2^2 + w_2^2}{k} \ .$$

Per quanto sopra osservato, si ha:

$$1 \leq t' \lneqq \frac{(k/2)^2 + (k/2)^2 + (k/2)^2 + (k/2)^2}{k} = k \ .$$

D'altra parte, poiché kp e $t'k$ sono somma di quattro quadrati di interi, allora, per la Proposizione 4.3, anche il loro prodotto $k^2t'p$ è somma di quattro quadrati di interi, cioè per (4.3.1) risulta:

$$k^2t'p = a^2 + b^2 + c^2 + d^2 \ ,$$

con

$$\begin{aligned}
a &= x_1x_2 + y_1y_2 + z_1z_2 + w_1w_2 \equiv x_1^2 + y_1^2 + z_1^2 + w_1^2 \equiv 0 && (\text{mod } k),\\
b &= x_1y_2 - y_1x_2 + z_1w_2 - w_1z_2 \equiv x_1y_1 - y_1x_1 + z_1w_1 - w_1z_1 = 0 && (\text{mod } k),\\
c &= x_1z_2 - z_1x_2 + w_1y_2 - y_1w_2 \equiv x_1z_1 - z_1x_1 + w_1y_1 - y_1w_1 = 0 && (\text{mod } k),\\
d &= x_1w_2 - w_1x_2 + y_1z_2 - z_1y_2 \equiv x_1w_1 - w_1x_1 + y_1z_1 - z_1y_1 = 0 && (\text{mod } k).
\end{aligned}$$

Quindi, $t'p = (a/k)^2 + (b/k)^2 + (c/k)^2 + (d/k)^2$, dove a/k, b/k, c/k, $d/k \in \mathbb{Z}$ e $1 \leq t' \lneqq k$, donde una contraddizione per la minimalità della scelta di k.

□

Osservazione 4.8. (Problema di Waring) Nello stesso periodo in cui Lagrange dimostrava il teorema dei quattro quadrati, il matematico inglese E. Waring (1734–1798), nel suo libro *Meditationes Algebraicae* (1770) congetturava il seguente teorema:

Per ogni esponente intero positivo s, esiste un intero positivo k tale che ogni intero positivo n è somma di k potenze s–esime di interi non negativi.

Denotiamo con $g(s)$ *il più piccolo intero positivo k (qualora esistente) tale che ogni numero naturale è la somma di k potenze s–esime di interi non negativi.* Allora, con altre parole, il teorema congetturato da Waring assicura l'esistenza di un $g(s)$, per ogni $s \geq 1$.

La congettura di Waring fu provata da D. Hilbert nel 1909. Notiamo che:

(a) per $s = 1$, il Teorema di Waring è banalmente vero;

(b) per $s = 2$, il Teorema di Lagrange e i risultati già esposti sugli interi somma di quadrati assicurano che $g(2) = 4$;

(c) per $s = 3$, Waring congetturò che $g(3) = 9$, risultato che è stato provato da A. Wieferich nel 1909;

(d) per $s = 4$, Waring congetturò che $g(4) = 19$. Tale congettura è stata dimostrata da R. Balasubramanian, F. Dress e J.–H. Deshonilles nel 1985;

(e) per $s = 5$, J.R. Chen nel 1964 ha dimostrato che $g(5) = 37$.

In generale, da alcuni lavori di L.E. Dickson (1913), S.S. Pillai (1936), K. Mahler (1957) e R.M. Stemmler (1964) si ricava che:

$$g(s) = 2^s + [(3/2)^2] - 2$$

per $5 \leq s \leq 200.000$ e definitivamente per s.

Limitiamoci qui a dimostrare la seguente disuguaglianza:

Proposizione 4.9. *Per ogni intero $s \geq 2$, risulta*

$$g(s) \geq 2^s + [(3/2)^s] - 2 \ .$$

Dimostrazione. Sia $n := 2^s[(3/2)^s] - 1$. Dal momento che, per ogni numero reale positivo α, si ha ovviamente che $[\alpha] \leq \alpha$, allora:

$$n \leq 2^s(3^s/2^s) - 1 \lneqq 3^s \ .$$

Inoltre, per definizione di $g(s)$, si deve avere che

$$n = x_1^s + \cdots + x_{g(s)}^s \quad \text{con } x_i \in \mathbb{Z} \ , \ x_i \geq 0 \ .$$

Poiché $n < 3^s$, necessariamente si deve avere $x_i \lneqq 3$, per ogni indice i, $1 \leq i \leq g(s)$. Sia $\gamma_2 := \#\{x_i : 1 \leq i \leq g(s), x_i = 2\}$; $\gamma_1 := \#\{x_i : 1 \leq i \leq g(s), x_i = 1\}$; $\gamma_0 := \#\{x_i : 1 \leq i \leq g(s), x_i = 0\}$. Dunque $\gamma_0 + \gamma_1 + \gamma_2 = g(s) \geq \gamma_1 + \gamma_2$ ed, inoltre, $n = 2^s\gamma_2 + \gamma_1 \geq 2^s\gamma_2$. Quindi:

$$n + 1 = 2^s[(3/2)^s] \geq 2^s\gamma_2 + 1$$

da cui $[(3/2)^s] - 1 \geq \gamma_2$. Dunque, si ha

$$\begin{aligned} g(s) \geq \gamma_1 + \gamma_2 &= (n - 2^s\gamma_2) + \gamma_2 = \\ &= n - (2^s - 1)\gamma_2 \geq n - (2^s - 1)([(3/2)^2] - 1) = \\ &= 2^s + [(3/2)^s] - 2 \ . \end{aligned}$$

□

Osservazione 4.10. Per ogni intero positivo s, è stato definito un altro intero, denotato con $G(s)$, che per molti aspetti è anche più interessante di $g(s)$. L'intero $G(s)$ è, per definizione, *il più piccolo intero positivo k tale che ogni numero naturale sufficientemente grande (cioè, ogni numero naturale con al più un numero finito di eccezioni) è la somma di k potenze s–esime di interi non negativi*. Evidentemente risulta:

(a) $G(2) = g(2) = 4$;

(b) $G(s) \leq g(s)$, per $s \geq 3$.

Inoltre, non è troppo difficile dimostrare che $G(s) \geq s + 1$, per ogni $s \geq 2$. In una serie di lavori, pubblicati tra il 1919 e il 1928 (apparsi sotto il titolo generale di "Some problems of *partitio numerorum*"), Hardy e Littlewood, usando metodi analitici, hanno determinato delle limitazioni superiori per $G(s)$. La più semplice, ma anche la più "grossolana", è la seguente:

$$G(s) \leq s2^{s-1} + 1$$

successivamente migliorata, tra l'altro, con la seguente:

$$G(s) \leq (s-2)2^{s-1} + 5 \ .$$

Risultati ancora più soddisfacenti sono stati ottenuti da I. Vinogradov nella seconda metà degli anni venti e da H. Heilbroun nel 1936, che ha migliorato, semplificando anche le dimostrazioni, quelli di Vinogradov.

Sorprendentemente, non è ancora noto il valore di $G(3)$, anche se nel 1942 Y.V. Linnik ha mostrato che $G(3) \leq 7$ e, per quanto visto sopra, $4 \leq G(3)$. D'altro canto è noto che $G(4) = 16$, $G(5) \leq 21$ e $G(6) \leq 31$.

Per ulteriori informazioni ed una dettagliata bibliografia sul problema di Waring, rinviamo ai volumi di Hardy–Wright [6, p. 335–339] e Sierpiński [13, p. 427–430].

4 Esercizi e complementi

4.1. Esprimere 247 e 308 come somma di tre quadrati.

[*Soluzione*: $247 = 13 \cdot 19$ con:

$$13 = 3^2 + 2^2 + 0^2 + 0^2 \ ,$$
$$19 = 4^2 + 1^2 + 1^2 + 1^2 \ ,$$

dunque, utilizzando (3.3.1), abbiamo:

$$247 = (12+2)^2 + (3-8)^2 + (3-2)^2 + (3+2)^2 = 14^2 + 5^2 + 1^2 + 5^2 \ .$$

Si noti che tale scrittura non è unica, utilizzando ad esempio il fatto che $13 = 2^2 + 2^2 + 2^2 + 1^2$.

Dopo aver osservato che $308 = 2^2 \cdot 7 \cdot 11$ e che $7 = 2^2 + 1^2 + 1^2 + 1^2$ e $11 = 3^2 + 1^2 + 1^2 + 0^2$, si può dedurre che $308 = 8^2 + 8^2 + 12^2 + 6^2$.]

4.2. Dimostrare il Teorema di Lagrange (Teorema 4.7) supponendo di aver già dimostrato il Teorema di Legendre–Gauss (Teorema 4.1) (ovviamente, questo non sarebbe stato possibile a Lagrange perché il Teorema 4.1 è stato dimostrato, da un punto di vista temporale, dopo il Teorema 4.7).

[*Suggerimento*. Basta dimostrare che ogni primo dispari è somma di quattro quadrati. Se $p \equiv 1 \pmod 4$ allora p si scrive come somma di due quadrati (e, quindi, banalmente come somma di quattro quadrati). Se $p \equiv 3 \pmod 4$ allora $p - 1 = 4k + 2$ per qualche $k \geq 0$. Dunque $p-1 = 8h+6$ oppure $p-1 = 8h+2$ per qualche $h \geq 0$, rispettivamente se k è dispari oppure se k è pari. In entrambi i casi, per il Teorema di Legendre–Gauss, $p - 1 = a^2 + b^2 + c^2$ e quindi $p = a^2 + b^2 + c^2 + 1^2$.]

4.3. Mostrare che:

(a) Un numero naturale $n = 4k$, $k \geq 1$, è somma di tre quadrati di interi positivi se, e soltanto se, k gode della medesima proprietà.

(b) **(A. Hurwitz, 1907)** Se $n = 2^k$, $k \geq 1$, allora n *non* si può scrivere come somma di tre quadrati di interi positivi.

[*Suggerimento*. (a) è una semplice conseguenza del Teorema 4.1. Oppure, si noti che:

$$4k = a^2 + b^2 + c^2 \Leftrightarrow k = a_1^2 + b_1^2 + c_1^2 \quad \text{con } a = 2a_1,\ b = 2b_1,\ c = 2c_1 \ .$$

dove $a_1,\ b_1,\ c_1 \in \mathbb{Z}$ se e soltanto se $a,\ b,\ c \in \mathbb{Z}$, perché il quadrato di un qualunque intero è congruo a $0,\ 1 \pmod 4$.

(b) Per $k = 1, 2$ è ovvio. Se $k \geq 3$, l'enunciato discende da (a) per induzione su k perché se $2^k = 4 \cdot 2^{k-2} = a^2 + b^2 + c^2$ allora anche 2^{k-2} sarebbe somma di tre quadrati di interi.]

4.4. Usando il Teorema di Legendre–Gauss (Teorema 4.1), provare che un numero naturale è somma di tre quadrati di numeri razionali se, e soltanto se, è somma di tre quadrati di interi.

[*Suggerimento*. Sia $n = \frac{a^2}{d^2} + \frac{b^2}{d^2} + \frac{c^2}{d^2}$ con $a, b, c, d \in \mathbb{Z}$ e $d \neq 0$. Dunque $nd^2 = a^2 + b^2 + c^2$. Sia, per assurdo, $n = 4^e(8k + 7)$ con $e, k \geq 0$. Possiamo sempre porre:

$$d = 2^f(2h + 1) \ , \quad \text{per qualche } f, h \geq 0$$

e dunque otteniamo:

$$nd^2 = 4^{e+f}(8t + 7) \quad \text{dove } e + f, t \geq 0 \ .$$

Ciò contraddice il Teorema di Gauss perché nd^2 è somma di tre quadrati di interi.]

4.5. Mostrare che ogni intero non negativo n si può esprimere nella forma $a^2 \pm b^2 \pm c^2$ (infatti, nella forma $a^2 + b^2 \pm c^2$), per una oppurtuna scelta di $a, b, c \in \mathbb{Z}$.

[*Suggerimento*. Dato $n > 0$ è sempre possibile trovare $a \in \mathbb{Z}$ in modo tale che $n - a^2$ è un intero dispari positivo.
Infatti se a è il più grande intero non negativo tale che $n > a^2$ e se $n - a^2$ è pari, basta prendere $a' := a - 1$ ed allora $n - a'^2$ è dispari. Dunque, $n - a^2 = 2m + 1$ per qualche $a, m \geq 0$. Dalla identità

$$2m + 1 = (m + 1)^2 - m^2$$

ricaviamo che $n = a^2 + (m + 1)^2 - m^2$. Ad esempio, se $n = 11$, $11 - 3^2 = 2$ e $11 - 2^2 = 7$, quindi $7 = 2 \cdot 3 + 1$ e $11 = 2^2 + 4^2 - 3^2$.]

4.6. (L. Euler, 1749) Mostrare che se n si scrive come somma di quattro quadrati di interi dispari, allora n si può scrivere anche come somma di quattro quadrati di interi pari.

[*Suggerimento*. Sia $n = (2a + 1)^2 + (2b + 1)^2 + (2c + 1)^2 + (2d + 1)^2$. È subito visto che $(2a + 1)^2 + (2b + 1)^2 = 2[(a + b + 1)^2 + (a - b)^2]$. Dunque

$$\begin{aligned} n &= 2\left[(a + b + 1)^2 + (a - b)^2 + (c + d + 1)^2 + (c - d)^2\right] = \\ &= 2\left[(2\alpha + 1)^2 + 4\beta^2 + (2\gamma + 1)^2 + 4\delta^2\right] \end{aligned}$$

dove $a + b + 1 = 2\alpha + 1$, $c + d + 1 = 2\gamma + 1$ sono dispari e $a - b = 2\beta$, $c - d = 2\delta$ sono pari. Quindi

$$n = 4[(\alpha + \gamma + 1)^2 + (\alpha - \gamma)^2 + \beta^2 + \delta^2] \ . \quad]$$