Alma Mater Studiorum · Università di Bologna

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI

Corso di Laurea in Matematica

Terne pitagoriche e somme di quadrati

Tesi di Laurea in Teoria dei numeri

Relatore:
Chiar.mo Prof.
Calogero Tinaglia

Presentata da:
Chimienti Fabrizio

Terza Sessione
Anno Accademico 2009/2010

Indice

Introduzione

Il problema di stabilire quali numeri siano rappresentabili come somma di due quadrati è molto antico; alcuni enunciati che ad esso si riferiscono appaiono nell'*Aritmetica* di Diofanto (circa 250 a.C.), ma il loro significato preciso non è chiaro. La vera risposta alla questione fu data per la prima volta dal matematico olandese Albert Girard nel 1625, e nuovamente da Fermat un po' più tardi. E' probabile che Fermat potesse provare i propri enunciati, ma le prime dimostrazioni di cui si sappia con certezza sono quelle pubblicate da Eulero nel 1749.
In seguito generalizzeremo il problema a somme di tre quadrati, che fu dimostrato completamente da Gauss nelle sue *Disquisitiones arithmeticae*, e infine a somme di quattro quadrati (il numero minimo per ottenere ogni numero naturale) la cui prima dimostrazione fu esibita nel 1770 da Lagrange.
Inizialmente tratteremo il problema di individuare quando la somma di due quadrati è a sua volta un quadrato, ovvero trovare le *terne pitagoriche*, ossia le terne ordinate di interi x, y, z che sono soluzioni dell'equazione:

$$x^2 + y^2 = z^2$$

e che quindi si possano pensare come lunghezze dei lati di un triangolo rettangolo: x, y, i cateti e z l'ipotenusa. Si trova che il terzo elemento della terna, cioè la z (ossia l'ipotenusa) deve essere somma di due quadrati e forse

ciò ha dato origine al problema di trovare i naturali che sono somme di due quadrati ossia i naturali N tali che si abbia:

$$a^2 + b^2 = N$$

con a, b interi, e più in generale i naturali che sono somme di due quadrati.

$$C^2 = A^2 + B^2$$

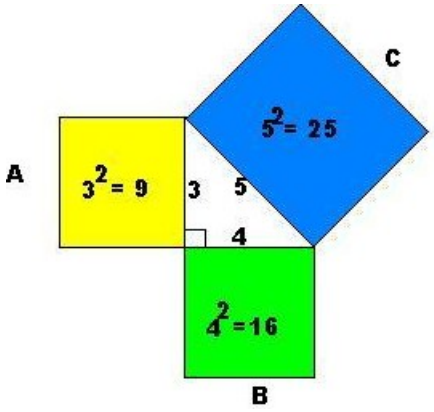

Figura 1: Esempio di applicazione del teorema di Pitagora

Capitolo 1

Terne pitagoriche

Definizione 1.1 (**Terna pitagorica**)**.** Si chiama *terna pitagorica* ogni terna ordinata di numeri interi che sia soluzione dell'equazione

$$x^2 + y^2 = z^2. \tag{1.1}$$

Questo particolare problema è molto antico, infatti se ne trova una soluzione nel lemma 1 relativo alla proposizione 29 del decimo libro degli *'Elementi'* di Euclide. Il nome terna pitagorica però deriva dal teorema di Pitagora, da cui deriva il fatto che ad ogni triangolo rettangolo con lati di lunghezza intera corrisponda una terna pitagorica e viceversa.

Innanzitutto consideriamo il caso in cui $xyz = 0$. Naturalmente la terna nulla (0, 0, 0) è pitagorica, infatti sostituendo all'equazione (1.1) si vede che la terna ne è una soluzione. Le terne non nulle hanno sempre x o y non nulli e $z \neq 0$. Quindi le terne saranno della forma $(a\ 0, \pm a)$, $(0, a, \pm a)$ $\forall a \in \mathbb{Z}$ e $a \neq 0$.
Premettiamo le seguenti definizioni al fine di capire meglio i discorsi successivi.

Definizione 1.2. Si dice che un intero $b \neq 0$ *divide* un intero a o che b è un *divisore* di a o che a è un *multiplo* di b e si scrive $b|a$ se esiste un intero c

tale che $a = bc$ (ovviamente a è multiplo anche di c e c è divisore di a).

Definizione 1.3 (**Numero primo**)**.** Un naturale diverso da 0 si dice *primo* quando è $\neq 1$ e ha come divisori solo 1 e se stesso.

Definizione 1.4 (**Massimo comun divisore**)**.** Dati x, y interi si dice *massimo comun divisore* di x e y il numero naturale d che è il massimo tra i divisori comuni ad x e y e si scrive $d = MCD(x, y)$ oppure $d = (x, y)$

Definiamo un tipo particolare di terna:

Definizione 1.5 (**Terna pitagorica primitiva**)**.** Una terna pitagorica si dice *primitiva* se e soltanto se gli interi x, y, z sono coprimi, ovvero $MCD(x, y, z) = 1$ Dall'equazione (1.1) si osserva che una qualsiasi terna pitagorica (x, y, z) è primitiva se e soltanto se gli interi sono coprimi a due a due.

Detto questo capiamo bene che la terna nulla non è primitiva, infatti $MCD(0, 0, 0) = 0$ e le uniche terne primitive con un un elemento nullo sono ottenute tutte da $(0, 1, 1)$ cambiando i segni e permutando la prima con la seconda componente, questo perché $MCD(0, 1, 1) = 1$.
Le terne pitagoriche proporzionali ad una stessa terna primitiva x, y, z sono tutte e sole quelle date da mx, my, mz ($\forall m \in \mathbb{Z}$). Infatti se (x, y, z) è una terna pitagorica primitiva anche la terna (mx, my, mz) è primitiva perché essendo $x^2 + y^2 = z^2$ è anche $m^2(x^2 + y^2) = m^2z^2$ e quindi $(mx)^2 + (my)^2 = (mz)^2$ ossia mx, my, mz è pitagorica. Viceversa se X, Y, Z è una terna pitagorica non primitiva, ossia $X^2 + Y^2 = Z^2$ e X, Y, Z non sono coprimi allora sarà $MCD(X, Y, Z) = m$ e quindi $X = mx$, $Y = my$, $Z = mz$ con x, y, z coprimi ed essendo $(mx)^2 + (my)^2 = (mz)^2$ sarà $m^2(x^2 + y^2) = m^2z^2$ e dividendo per m^2 si ha $x^2 + y^2 = z^2$ e quindi x, y, z è una terna pitagorica primitiva.
Si ha subito che, fissata una terna (x, y, z) non nulla e con $xyz \neq 0$, da questa si ottengono altre 15 terne cambiando i segni e permutando x con y.

Tra queste sedici terne se ne trovano due con $x > 0$, $y > 0$, $z > 0$ ed esse si ottengono una dall'altra permutando x con y.
Per questo motivo di solito si determinano solo le terne primitive con $x > 0$, $y > 0$, $z > 0$ ed a meno dello scambio di x con y.

1.1 Determinazione delle terne pitagoriche primitive

Si dimostra facilmente che: *Se una conica $\mathcal{C}$ ha equazione cartesiana a coefficienti interi e se ha un punto razionale R allora ha infiniti punti razionali.*
I punti razionali di $\mathcal{C}$ sono tutti e soli i punti di intersezione di $\mathcal{C}$ con le rette intere (ossia con equazione a coefficienti razionali e quindi interi) del fascio di centro R. Il metodo dovuto a Klein sarà applicato nella prima parte della dimostrazione che ci darà le terne pitagoriche primitive. Osserviamo che con questo metodo il problema di determinare i punti razionali di una conica a coefficienti interi è ricondotto a quello di trovarne uno.

Teorema 1.1.1. *Le terne pitagoriche primitive x, y, z, con $xyz \neq 0$ e $x > 0$, $y > 0$, $z > 0$, a meno dell'ordine di x, y e dei segni di x, y, z sono tutte e sole le terne date da:*

$$x = 2ab, \qquad y = a^2 - b^2, \qquad z = a^2 + b^2 \tag{1.2}$$

con a, $b \in \mathbb{Z}$, $0 < b < a$, a e b con parità diversa (ovvero se a è pari b dev'essere dispari o viceversa) e $MCD(a, b) = 1$

Dimostrazione. **metodo di Klein**

Possiamo vedere geometricamente che l'equazione (1.1) rappresenta un cono circolare retto di $\mathbb{R}^3$ con il vertice nell'origine degli assi cartesiani. Come nella figura:

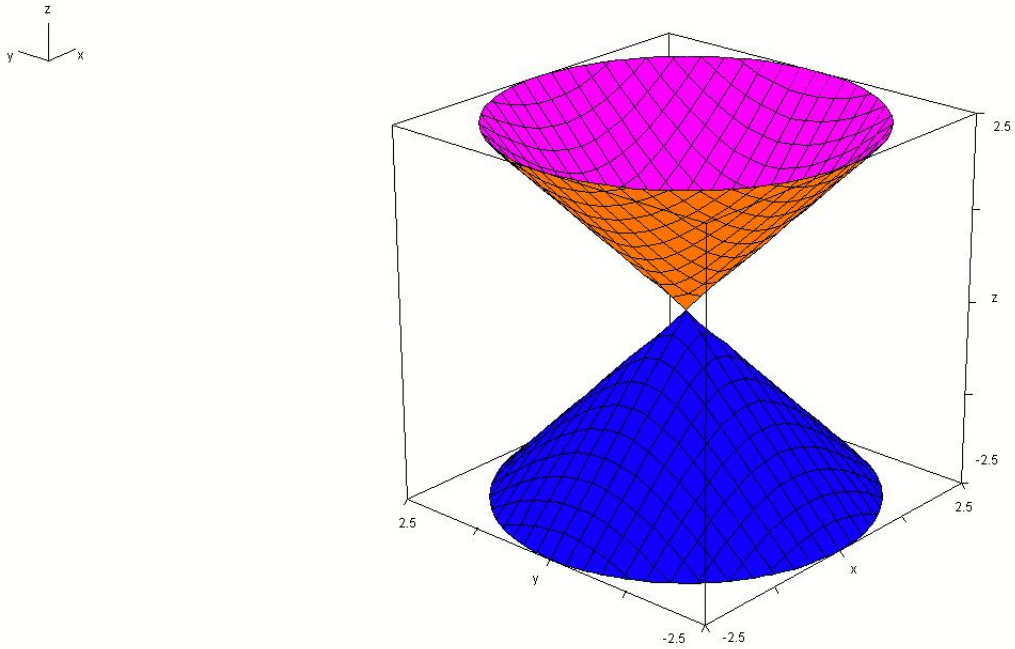

Figura 1.1: Rappresentazione grafica in $\mathbb{R}^3$ di $x^2 + y^2 = z^2$

Quindi dal punto di vista geometrico il problema è trovare i punti a coordinate intere del cono di equazione $x^2 + y^2 = z^2$ con vertice nell'origine.

In ogni terna pitagorica non nulla $z \neq 0$. Dividendo $x^2 + y^2 = z^2$ per z^2 si ottiene:

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1 \tag{1.3}$$

Ponendo:

$$X = \frac{x}{z} \qquad Y = \frac{y}{z} \tag{1.4}$$

e sostituendo nella (1.3) si ottiene:

$$X^2 + Y^2 = 1 \tag{1.5}$$

che nel piano cartesiano rappresenta la circonferenza di centro l'origine e raggio 1.

Poiché stiamo cercando le terne pitagoriche primitive e quindi $MCD(x, y) =$

$MCD(y,\, z) = 1$, per le (1.4), per trovare tali terne basta trovare i punti razionali della circonferenza (1.5)

Poiché $\mathcal{C}$ passa per il punto $A(0,\, -1)$ che è razionale quindi possiamo applicare il metodo di Klein. Una retta r del fascio di rette di centro A è data da $Y = mX - 1$ e quindi $r \cap \mathcal{C}$ è dato dal sistema:

$$\begin{cases} Y = mX - 1 \\ X^2 + Y^2 = 1 \end{cases} \tag{1.6}$$

L'equazione risolvente del sistema è $X[(1+m^2)X - 2m] = 0$. Sostituendo nella prima equazione di (1.6), con la soluzione $X = 0$ si ha il punto A, mentre con la soluzione $X = \frac{2m}{1+m^2}$ si ha il punto P di coordinate:

$$\begin{cases} X = \frac{2m}{1+m^2} \\ \\ Y = \frac{m^2-1}{1+m^2} \end{cases}$$

Per quanto detto nella sezione sui punti razionali di una conica, P è razionale se e solo se r è razionale e ciò accade se e solo se m è razionale, allora posso porre $m = \frac{a}{b}$ con $a,\, b \in \mathbb{Z}$, $b \neq 0$ e $MCD(a,\, b) = 1$ si ottiene che:

$$\begin{cases} X = \frac{2ab}{a^2+b^2} \\ \\ Y = \frac{a^2-b^2}{a^2+b^2} \end{cases}$$

Sostituendo quanto ottenuto in (1.4) si ottiene:

$$\begin{cases} x = \frac{2ab}{a^2+b^2} z \\ \\ y = \frac{a^2-b^2}{a^2+b^2} z \end{cases}$$

Se $ab \neq 0$ e $a \neq b$ poiché $MCD(a,\, b) = 1$ è anche:

$$MCD(2ab, a^2 + b^2) = MCD(a^2 + b^2, a^2 - b^2) \leq 2. \tag{1.7}$$

Infatti se $MCD(a^2+b^2,\ a^2-b^2) = d$ si ha $a^2+b^2 = dp$, $a^2-b^2 = dq$ con $MCD(p,\ q) = 1$. Sommando e sottraendo si ottiene $2a^2 = d(p+q)$, $2b^2 = d(p-q)$. Poiché $MCD(a^2,\ b^2) = 1$ può aversi solo:
$d = 1$ con p e q entrambi dispari oppure $d = 2$ e p e q con parità diversa.
Se $d = 1$, poiché $p = a^2+b^2$ è dispari si ha $MCD(2ab,\ a^2+b^2) = MCD(ab,\ a^2+b^2)$.
Se $MCD(ab, a^2+b^2) = n$ si ha $ab = nh$, $a^2+b^2 = nk$ con n dispari. Poiché $MCD(a,\ b) = 1$ sarà $n = n_1n_2, h = h_1h_2$, $a = n_1h_1$, $b = n_2h_2$ e $(n_1h_1)^2+(n_2h_2)^2 = n_1n_2k$.
Si avrà $(n_1h_1)^2 = n_2[n_1k-n_2(h_2)^2]$ ed anche $(n_2h_2)^2 = n_1[n_2k-n_1(h_1)^2]$.
Poiché $1 = MCD(a,b) = MCD(n_1h_1, n_2) = MCD(n_2h_2, n_1)$ le due relazioni sono vere se e soltanto se $n_1 = n_2 = 1$ ossia se e soltanto se $n = 1$. Se $d = 2$, poiché $a^2+b^2 = 2p$ si ha $MCD(2ab, a^2+b^2) = MCD(2ab, p)$. Se $MCD(ab,p) = n$ si ha $ab = nh$, $2p = a^2+b^2 = 2nk$ con n dispari. Ragionando come sopra sarà $n = n_1n_2$, $h = h_1h_2, a = n_1h_1, b = n_2h_2$ e $(n_1h_1)^2+(n_2h_2)^2 = 2n_1n_2k$ e si prova che queste relazioni sono possibili se e soltanto se $n_1 = n_2 = 1$ ossia $n = 1$. Con ciò abbiamo provato la (1.7).
Se $d = 1$, la terna x, y, z è intera se e solo se z è un intero multiplo di a^2+b^2 e quindi $z = (a^2+b^2)t$ con t intero arbitrario.
Pertanto le terne pitagoriche sono tutte e solo quelle date da:

$$x = 2abt, \qquad y = (a^2-b^2)t, \qquad z = (a^2+b^2)t. \tag{1.8}$$

Tale terna è primitiva se e soltanto se $|t| = 1$ e gli interi a e b hanno parità diversa. Se $d = 2$ la terna x, y, z è intera se e solo se z è un intero multiplo di p e quindi $z = pt$ con t intero arbitrario. Pertanto le terne pitagoriche sono tutte e sole quelle date da $x = abt$, $y = qt$, $z = pt$ ossia:

$$x = abt, \qquad 2y = (a^2-b^2)t, \qquad 2z = (a^2+b^2)t. \tag{1.9}$$

Tale terna è primitiva se e soltanto se $|t| = 1$. Proviamo che, posto $|t| = 1$, scambiando x con y la (1.8) è una delle (1.9). Gli interi a, b non possono

avere parità diversa perché altrimenti y e z non sarebbero interi e la terna non sarebbe intera; non possono essere entrambi pari perché 2 sarebbe divisore comune di x, y, z e la terna non sarebbe primitiva; quindi a e b debbono essere entrambi dispari inoltre abbiamo già detto che è a, $b \in \mathbb{Z}$ con $0 < b < a$. Poniamo $a = 2h + 1$, $b = 2k + 1$ con h, $k \in \mathbb{Z}$ e $0 \leq k < h$. Sostituendo nelle (1.9) con $|t| = 1$ si ottiene:

$$x = (2h+1)(2k+1), \qquad y = 2(h-k)(h+k+1), \qquad z = \frac{1}{2}[(2h+1)^2+(2k+1)^2]. \tag{1.10}$$

Ponendo $m = h - k$, $n = h + k + 1$ si ha: $2h + 1 = n + m$, $2k + 1 = n - m$ e si ottiene:

$$x = (n+m)(n-m), \qquad y = 2mn, \qquad z = \frac{1}{2}[(n+m)^2 + (n-m)^2]$$

ossia:

$$x = n^2 - m^2, \qquad y = 2mn, \qquad z = n^2 + m^2 \tag{1.11}$$

ove per definizione $0 < m < n$ (perché $k < h$) e m, n hanno parità diversa ed inoltre poiché la terna (1.11) coincide con la (1.8) con $|t| = 1$, la quale è primitiva allora anche $MCD(m, n) = 1$. Quindi, scambiando in (1.11) x con y si ottengono le stesse formule di (1.8) con $|t| = 1$ ossia le (1.2).

□

Osservazioni

Ora ci chiediamo se posto n intero positivo esiste una terna primitiva tale che:

1. $n = z$, si nota da (1.2) che è possibile se e solo se n è dispari ed è la somma di due quadrati coprimi. Perciò non solo z^2 deve essere somma di due quadrati ma anche z. Quindi si ha: l'equazione $x^2 + y^2 = n$ ha soluzioni intere se e solo se $n = M^2k$ oppure $n = 2M^2k$ con $M \geq 1$, e k libero da quadrati e prodotto di primi p della forma $4h + 1$. Questo punto verrà affrontato in maniera più dettagliata nel capitolo sulle **somme di quadrati**.

2. $n = y$ o $n = x$ ricordando la (1.2) si nota che scrivere un numero n come differenza di due quadrati non è un problema, perché si ha subito che n è la differenza del quadrato della semisomma meno il quadrato della semidifferenza di due divisori complementari u e v di n ove u e v sono qualsiasi se n è dispari, sono entrambi pari se n è multiplo di 4 mentre se $n = 2(2h+1)$ è pari e non è multiplo di 4 non si può scrivere come differenza di due quadrati.

1.1.1 Relazione tra i numeri di Fibonacci e le terne pitagoriche

Definizione 1.6 (Serie di Fibonacci)**.** Si chiama *serie* o *successione di Fibonacci* l'insieme dei naturali ottenuti per ricorsione da:

$$F_n = F_{n-1} + F_{n-2} \quad con \quad F_1 = 1 \quad e \quad F_0 = 0. \tag{1.12}$$

I naturali F_n si dicono *numeri di Fibonacci*

Teorema 1.1.2. *Scelti comunque quattro termini consecutivi della serie di Fibonacci, a, b, c, d, troviamo una terna pitagorica formata da:*

$$x = ad, \qquad y = 2bc, \qquad z = b^2 + c^2$$

Dimostrazione. Essendo $c = a + b$ sarà $a = c - b$, $d = b + c$, b e c coprimi perché numeri di Fibonacci consecutivi. Si ha $x = (c - b)(c + b)$ e quindi si ottiene:

$$x = c^2 - b^2, \qquad y = 2bc, \qquad z = b^2 + c^2. \tag{1.13}$$

Se a è dispari solo uno dei naturali b e c è pari e quindi, a meno dello scambio di x con y, la (1.13) coincide con la (1.8).

Se invece a è pari anche d sarà pari e b e c entrambi dispari e coprimi. Quindi la terna x, y, z non è primitiva perché tutte le componenti sono pari. Dividendo per 2 si ottiene la terna:

$$x' = \frac{c^2 - b^2}{2}, \qquad y' = bc, z' = \frac{c^2 + b^2}{2}$$

ossia

$$2x' = c^2 - b^2, \qquad y' = bc, \qquad 2z' = b^2 + c^2 \tag{1.14}$$

e questa, a meno dello scambio di x' con y', coincide con la (1.9). □

Capitolo 2

Somme di quadrati

Risolviamo ora il problema principale, inizialmente troveremo quali sono i numeri naturali somma di due quadrati per poi ampliare questa somma a tre e quattro quadrati. Ci fermeremo a quattro in quanto vedremo che ogni numero naturale può essere scritto come somma di quattro quadrati.
In seguito verrà introdotto il teorema di Hurwitz riguardo al fatto che il prodotto di una somma di due, quattro e otto quadrati è ancora una somma di quadrati. E otto è il massimo numero di quadrati per cui vale questa proprietà.

2.1 Somme di due quadrati

Il problema che ora ci poniamo è il seguente:
dato un naturale n trovare se esistono due naturali x, y tali che $x^2 + y^2 = n$.
Ovvero trovare i punti a coordinate naturali nel seguente grafico in $\mathbb{R}^3$
Al fine di dimostrare i seguenti teoremi premettiamo:

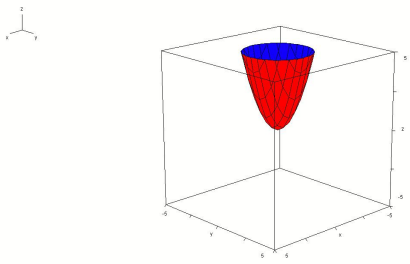

Figura 2.1: Rappresentazione grafica in $\mathbb{R}^3$ di $z = x^2 + y^2$

2.1.1 Richiami

1. **Congruenza**. Fissato $n \in \mathbb{Z}$, due interi a e b si dicono *congruenti modulo* n se $n|(a-b)$ (ovvero se $\exists c \in \mathbb{Z}$ tale che $(a-b) = nc$); si scrive $a \equiv b \pmod{n}$ oppure $a \equiv_n b$ e si legge a è congruo a b modulo n. Per indicare la congruenza modulo n, utilizzeremo in seguito solo la seconda delle due scritture sopracitate.

2. **Teorema di Chevalley**. Sia p primo. Se la congruenza algebrica:

$$f(x_1, x_2, ..., x_i, ..., x_n) \equiv_p 0 \tag{2.1}$$

in n incognite ha grado $m < n$ (ossia $grad(f) = m < n$) e se il termine noto di f è zero allora la congruenza ha almeno un soluzione $\overline{x_1}, ..., \overline{x_i}, ..., \overline{x_n}$ diversa da quella nulla (ossia è $f(\overline{x_1}, ..., \overline{x_i}, ..., \overline{x_n}) \equiv_p 0$ con $\overline{x_j} \not\equiv_p 0$ per qualche j).

3. **Residuo quadratico**. Un intero a si dice *residuo quadratico rispetto a* p se è un quadrato rispetto a p (p primo dispari) ossia se la congruenza:

$$x^2 \equiv_p a \tag{2.2}$$

ha soluzione.

4. I residui quadratici sono i quadrati di tutti e soli i primi $\frac{p-1}{2}$ residui ossia:

$$1, 2^2, 3^2, ..., r^2, ..., \left(\frac{p-1}{2}\right)^2$$

Se c è un non residuo quadratico allora i non residui quadratici sono tutti e soli:

$$c, 2^2c, 3^2c, ..., r^2c, ..., c\left(\frac{p-1}{2}\right)^2$$

Si osservi che se a è il quadrato di b allora è il quadrato anche di $-b$ e se $1 \leq b \leq \frac{p-1}{2}$, essendo $-b = p - b$, sarà $\frac{p-1}{2} < -b \leq p - 1$. Quindi possiamo dire che i residui quadratici sono quelli soprascritti.

5. **Simbolo di Legendre**. Sia a un numero intero e p un numero primo dispari, si definisce il *simbolo di Legendre* il numero:

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \textit{se } \text{p } \textit{divide } a \\ 1 & \textit{se } \text{a } \textit{residuo quadratico} \\ -1 & \textit{se } \text{a } \textit{non residuo quadratico} \end{cases}$$

Si osservi che nel simbolo di Legendre a (ossia il numeratore) è arbitrario mentre p (ossia il denominatore) è un primo dispari. Detto questo si può enunciare la prima proprietà dell'elenco precedente nel seguente modo:
Per il simbolo di Legendre vale la proprietà moltiplicativa $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ e quindi si ha subito che $\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)...\left(\frac{q_h}{p}\right)$ essendo $q_1, ..., q_h$ i fattori primi della fattorizzazione standard di a che hanno esponente dispari.

6. La congruenza $x^2 \equiv_p -1$ ha soluzione se e solo se p è un primo della forma $4k + 1$ ossia -1 è un residuo quadratico di p se e solo se p è un primo della forma $4k + 1$ cioè:

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \textit{se } p = 4k + 1 \\ -1 & \textit{se } p = 4k + 3 \end{cases}$$

7. Se -1 è non residuo quadratico di p (ossia se p è un primo della forma $4k - 1$) allora i non residui quadratici sono tutti gli opposti dei residui

quadratici (ossia se a è un non residuo quadratico allora esiste x tale che $a \equiv_p -x^2$)

Per dimostrarlo basta ripetere quanto detto nel richiamo numero 4 ponendo $c = -1$.

2.1.2 Somme di quadrati

Detto questo possiamo notare il fatto che se n un quadrato è $\equiv_4 0$ oppure $\equiv_4 1$ infatti:

1. Se n è pari allora pongo $n = 2k$, $k \in \mathbb{N}$ quindi $n^2 = (2k)^2 = 4k^2 \equiv_4 0$ $\forall\ k \in \mathbb{N}$.

2. Se n è dispari allora pongo $n = (2k+1)$, $k \in \mathbb{N}$ quindi $n^2 = (2k+1)^2 = 4k^2 + 4k + 1 \equiv_4 1\ \forall\ k \in \mathbb{N}$.

Quindi la somma di due quadrati è congrua modulo 4 a 0 oppure 1 oppure 2 perché, per quanto detto sopra, posso avere solo tre situazioni possibili, $0+0=0$, $0+1=1$ e $1+1=2$. Allora se n è delle forma $4k+3$, $k \in \mathbb{N}$, non è somma di due quadrati perché, per quanto detto, tale somma non è mai congrua a 3 modulo 4. Allora posso enunciare il seguente teorema:

Teorema 2.1.1. *Condizione necessaria perché un naturale n sia somma di due quadrati è che i fattori primi di n della forma $4k+3, k \in \mathbb{N}$ abbiano esponente pari o meglio deve essere:*

$$n = M^2N \qquad oppuren = 2M^2N \tag{2.3}$$

con N prodotto di primi della forma $4k+1$

Dimostrazione. Se n non ha fattori primi della forma $4k+3$, non c'è niente da provare.
Mentre sia $n = mp$ e $p = 4k+3$ è un fattore primo di n. Se $x^2 + y^2 = n$ si ha $x^2 + y^2 = mp$ ovvero $x^2 + y^2 \equiv_p 0$ quindi $x^2 \equiv_p -y^2$. Poiché -1 è un

non residuo quadratico modulo p, allora per il richiamo numero 7, $(-1)y^2$ è un non residuo quadratico e quindi non può essere congruente ad un residuo quadratico. Pertanto la congruenza è vera se e soltanto se sono vere le due congruenze $x^2 \equiv_p 0$ e $y^2 \equiv_p 0$ e quindi anche le due congruenze $x \equiv_p 0$ e $y \equiv_p 0$. Sarà $x = pX$, $y = pY$ e $n = p^2(X^2 + Y^2) = p^2 m_1$ ed m_1 è somma di quadrati. Allora allo stesso modo si prova che se $p|m_1$ allora $m_1 = p^2(r^2+s^2)$ e quindi $n = p^4(r^2+s^2)$. Ciò prova che p deve avere esponente pari e lo stesso deve accadere per tutti gli altri fattori primi della forma $4k-1$.

□

Si osservi che nelle (2.3) tra i fattori primi di M oltre a quelli della forma $4k+3$ possono esserci 2 e fattori primi della forma $4k+1$.

Per determinare i naturali somme di due quadrati è fondamentale sapere che si ha la seguente identità:

$$(r^2 + s^2)(x^2 + y^2) = (rx + sy)^2 + (ry - sx)^2 \tag{2.4}$$

che si verifica subito e che mostra che il prodotto di somme di due quadrati è ancora una somma di due quadrati. Se $n = r^2 + s^2$ e pongo $x = y = 1$, si ha $2n = (r + s)^2 + (r - s)^2$

Teorema 2.1.2. *Un primo p della forma $4k+1$ è somma di due quadrati in modo unico.*

Dimostrazione. Si ha che esistono sempre due naturali x, y tali che la somma dei loro quadrati è un multiplo di p. Infatti poiché $p = 4k+1$ si ha che -1 è un residuo quadratico rispetto a p e quindi esiste x tale che $x^2 \equiv_p -1$ ossia $x^2 + 1 \equiv_p 0$ ossia esiste m naturale tale che $x^2 + 1 = mp$. Quindi è vero che esistono x, y tali che:

$$x^2 + y^2 = mp \tag{2.5}$$

Possiamo supporre $m < p$ perché (dividendo x e y per p e prendendo i relativi resti eventualmente quelli negativi) possiamo scegliere $|x| \leq 2k, |y| \leq 2k$ e

avremo $mp = x^2 + y^2 \leq 8k^2 < 16k^2 < 16k^2 + 8k + 1 = p^2$ ossia $mp < p^2$ e $m < p$. Si osservi che la (2.5) dice anche che $x^2 + y^2 \equiv_m 0$. Siano r, s tali che:

$$x \equiv_m r, \qquad y \equiv_m s \tag{2.6}$$

Per le proprietà delle congruenze che lasciano inalterato il modulo, sarà :

1. Allora $x^2 \equiv_m r^2$, $y^2 \equiv_m s^2$ e quindi $r^2 + s^2 \equiv_m 0$ ossia $r^2 + s^2 = am$ e ragionando come prima prendendo $|r| \leq \frac{m}{2}$, $|s| \leq \frac{m}{2}$ per questo possiamo supporre $a < m$.

2. $x^2 \equiv_m xr$, $y^2 \equiv_m ys$ e quindi $xr + ys \equiv_m 0$ ossia $xr + ys = bm$.

3. $xy \equiv_m xs$, $yx \equiv_m yr$ e quindi $xs - yr \equiv_m xy - yx \equiv_m 0$ ossia $xs - yr = cm$.

Si nota che $a \neq 0$ perché altrimenti sarebbe $r = s = 0$ e dalle (2.6) si avrebbe $x = mu$, $y = mv$ che sostituiti nella (2.5) danno $p = m(u^2 + v^2)$ e ciò è assurdo perché p è primo. Per l'identità (2.4) abbiamo che:

$$am^2p = (x^2+y^2)(r^2+s^2) = (xr+ys)^2+(xs-yr)^2 = b^2m^2+c^2m^2 = m^2(b^2+c^2)$$

ovvero:

$$b^2 + c^2 = ap \tag{2.7}$$

Siamo quindi nelle stesse condizioni di (2.5). Ragionando allo stesso modo sulla (2.7) come per la (2.5) si troverà che $a' \neq 0$ e $a' < a$ tale che $a'p$ è somma di due quadrati. Così procedendo si arriverà a trovare $a'' = 1$. Per dimostrare l'unicità, supponiamo che:

$$p = x^2 + y^2 = X^2 + Y^2. \tag{2.8}$$

Sappiamo che la congruenza $z^2 + 1 \equiv_p 0$ ha precisamente due soluzioni, che sono della forma $z \equiv_p \pm h$. Pertanto:

$$x \equiv_p \pm hy \qquad e \qquad X \equiv_p \pm hY.$$

Poiché i segni di x, y, X, Y non hanno rilevanza, possiamo assumere che:

$$x \equiv_p hy \qquad e \qquad X \equiv_p hY. \tag{2.9}$$

Moltiplichiamo tra loro le due equazioni della (2.8), e applichiamo l'identità (2.4). Otterremo:

$$p^2 = (x^2 + y^2)(X^2 + Y^2) = (xX + yY)^2(xY - yX)^2.$$

Ora $xY - yX \equiv_p 0$, per la (2.9). Pertanto entrambi i numeri sulla sinistra sono multipli di p, e tutti i termini dell'equazione si possono dividere per p^2. Ci si ridurrà così ad una equazione che esprime 1 come somma di due quadrati interi, e l'unica possibilità è $(\pm 1)^2 + 0^2$. Dunque, nell'equazione precedente uno dei due numeri $xX + yY$, $xY - yX$ dev'essere 0. Se $xY - yX = 0$ allora, poiché x, y e X, Y sono coprimi, o $x = X$ e $y = Y$ oppure $x = -X$ e $y = -Y$. Similmente, se $xX + yY = 0$, seguirà che o $x = Y$ e $y = -X$ oppure $x = -Y$ e $y = X$. In ogni caso, le due rappresentazioni nella (2.8) essenzialmente coincidono.

□

Per quanto detto ne viene il seguente corollario:

Corollario 2.1.3. *Un naturale n è somma di due quadrati se e soltanto se:*

$$n = M^2N \qquad oppure \qquad n = 2M^2N \tag{2.10}$$

con N prodotto di primi della forma $4k + 1$

Inoltre si può dimostrare che:

Teorema 2.1.4. *Ogni naturale che non è della forma $4^h(8k + 7)$, $h \geq 0$ intero, è somma di tre quadrati.*

La difficoltà della dimostrazione del precedente teorema stà nel fatto che nel caso di 3 quadrati non esiste un' identità come la (2.4)

Inoltre abbiamo il seguente teorema:

Teorema 2.1.5. *Ogni naturale è somma di quattro quadrati.*

Premettiamo il seguente corollario:

Corollario 2.1.6. *La congruenza*

$$x^2 + y^2 + 1 \equiv_p 0 \tag{2.11}$$

è risolubile.

Dimostrazione. Eulero esibì una semplice argomentazione che stabilisce la solubilità della (2.13) senza alcun calcolo. Scriviamo la congruenza come:

$$x^2 + 1 \equiv_p -y^2.$$

Qualsiasi non-residuo quadratico modulo p è rappresentabile come congruente a qualche numero della forma $-y^2$, poiché -1 è non-residuo per ogni primo della forma $4k + 3$. Pertanto, per verificare la congruenza di sopra, è sufficiente trovare un residuo quadratico R e un non-residuo quadratico N tali che $R + 1 = N$. Se definiamo N come il *primo* non-residuo quadratico nella successione 1, 2, 3, ... questa condizione è ovviamente verificata, e la solubilità della congruenza (2.13) ne segue. Osserviamo che la solubilità della (2.13) è un caso particolare del *teorema di Chevalley* (richiamo numero 2), in quel contesto si è visto che la congruenza:

$$x^2 + y^2 + z^2 \equiv_p 0$$

è risolubile, con x, y, z non tutti congrui a 0. Supponendo $z \not\equiv_p 0$, e definendo X e Y in modo tale che $x \equiv_p Xz$, $y \equiv_p Yz$ avremo $X^2 + Y^2 + 1 \equiv_p 0$. □

Dimostrazione. **Teorema 2.1.5**

La dimostrazione è simile a quella del caso di due quadrati. E' prima ricondotta al caso dei primi della forma $4k + 3$ (gli altri primi, 2 compreso,

sono somme di due quadrati e quindi anche di quattro) perché prima si fa vedere la seguente identità che verrà adoperata nella dimostrazione.

$$(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2) =$$
$$(ax+by+cz+dt)^2+(bx-ay+dz-ct)^2+$$
$$+(cx-dy-az+bt)^2+(dx+cy-bz-at)^2 \tag{2.12}$$

la quale mostra che il prodotto di somme di quattro quadrati è ancora una somma di quattro quadrati. La dimostrazione di divide in due parti, la prima è provare che un opportuno multiplo mp di p, dove $0 < m < p$, è rappresentabile come somma di quattro quadrati. La seconda parte consiste nel dedurre da ciò che p stesso è rappresentabile. Per quanto riguarda il primo passo è sufficiente provare che la congruenza:

$$x^2+y^2+1 \equiv_p 0 \tag{2.13}$$

è risolubile, ma questo è vero per il corollario 2.1.6. Perciò possiamo scegliere una soluzione in cui x e y sono numericamente minori di $\frac{1}{2}p$, e abbiamo:

$$mp = x^2+y^2+1^2+0^2,$$

con

$$m < \frac{1}{p}\left(\frac{1}{4}p^2+\frac{1}{4}p^2+1\right) < p.$$

Arriviamo ora alla seconda parte della dimostrazione, partendo dal fatto che mp è rappresentabile come:

$$mp = a^2+b^2+c^2+d^2, \tag{2.14}$$

per qualche m tale che $0 < m < p$. Dimostreremo che, se $m > 1$, esiste qualche numero r con $0 < r < m$ che abbia la stessa proprietà di m. Ripetendo l'argomentazione, seguirà che il numero 1 ha quella proprietà, e dunque che p stesso è rappresentabile come somma di quattro quadrati.

Iniziamo riducendo a, b, c, d rispetto al modulo m determinando cioè numeri A, B, C, D che siano congruenti rispettivamente ad a, b, c, d modulo m e che soddisfino $-\frac{1}{2}m < A \leq \frac{1}{2}m$, e così via, per B, C, D. Si ha allora:

$$mr = A^2 + B^2 + C^2 + D^2 \tag{2.15}$$

per qualche intero r. Questo numero r non può essere 0, in quanto A, B, C, D sarebbero in tal caso tutti nulli, ed a, b, c, d sarebbero tutti multipli di m. Dalla (2.14) dedurremmo la divisibilità di mp per m^2, ossia la divisibilità di p per m, il che è impossibile poiché p è primo mentre m è maggiore di 1 ma minore di p.

Per quanto riguarda la grandezza di r, si ha:

$$r = \frac{1}{m}(A^2 + B^2 + C^2 + D^2) \leq \frac{1}{m}\left(\frac{1}{4}m^2 + \frac{1}{4}m^2 + \frac{1}{4}m^2 + \frac{1}{4}m^2\right) = m.$$

Così com'è, ciò non è ancora sufficiente; ci serve sapere che r è strettamente minore di m. La possibilità che $r = m$ si può rappresentare solo se A, B, C, D sono tutti uguali a $\frac{1}{2}m$. In tal caso m sarà pari, e A, B, C, D saranno tutti congrui a $\frac{1}{2}m$ modulo m. Ma allora $a^2 \equiv_{m^2} \frac{1}{4}m^2$, e similmente per b, c, d. Ora la (2.14) implicherebbe $mp \equiv_{m^2} 0$, e abbiamo già visto che ciò è impossibile. Ne segue che il numero r nella (2.15) soddisfa $0 < r < m$.
Proseguiamo la dimostrazione moltiplicando assieme le equazioni (2.14) e (2.15), e applicando l'identità (2.12). Si perviene a:

$$m^2rp = x^2 + y^2 + z^2 + w^2, \tag{2.16}$$

dove x, y, z, w sono le quattro espressioni nella parte destra della (2.12). Tutte queste espressioni rappresentano numeri divisibili per m. Infatti:

$$x = aA + bB + cC + dD \equiv_m a^2 + b^2 + c^2 + d^2 \equiv_m 0$$

e

$$y = aB - bA - cD + dC \equiv_m ab - ba - cd + dc \equiv_m 0$$

con simili risultati per z e w. Possiamo cancellare m^2 da entrambi i termini dell'equazioni (2.16), e ottenere una rappresentazione per rp come somma di quattro quadrati. □

In seguito ci si è chiesti fino a quale dimensione valgano identità come la (2.4) e la (2.12). Infatti nel 1845 Arthur Cayley scoprì l'identità nel caso di dimensione 8, ovvero:

$$(X_1^2 + ... + X_8^2)(Y_1^2 + ... + Y_8^2) = Z_1^2 + ... + Z_8^2$$

dove:

$$Z_1 = X_1Y_1 - X_2Y_2 - X_3Y_3 - X_4Y_4 - X_5Y_5 - X_6Y_6 - X_7Y_7 - X_8Y_8,$$

$$Z_2 = X_1Y_2 + X_2Y_1 + X_3Y_4 - X_4Y_3 + X_5Y_6 - X_6Y_5 - X_7Y_8 + X_8Y_7,$$

$$Z_3 = X_1Y_3 - X_2Y_4 + X_3Y_1 + X_4Y_2 + X_5Y_7 + X_6Y_8 - X_7Y_5 - X_8Y_6,$$

$$Z_4 = X_1Y_4 + X_2Y_3 - X_3Y_2 + X_4Y_1 + X_5Y_8 - X_6Y_7 + X_7Y_6 - X_8Y_5,$$

$$Z_5 = X_1Y_5 - X_2Y_6 - X_3Y_7 - X_4Y_8 + X_5Y_1 + X_6Y_2 + X_7Y_3 + X_8Y_4,$$

$$Z_6 = X_1Y_6 + X_2Y_5 - X_3Y_8 + X_4Y_7 - X_5Y_2 + X_6Y_1 - X_7Y_4 + X_8Y_3,$$

$$Z_7 = X_1Y_7 + X_2Y_8 + X_3Y_5 - X_4Y_6 - X_5Y_3 + X_6Y_4 + X_7Y_1 - X_8Y_2,$$

$$Z_8 = X_1Y_8 - X_2Y_7 + X_3Y_6 - X_4Y_5 - X_5Y_4 - X_6Y_3 + X_7Y_2 + X_8Y_1.$$

Si osservi che per la (2.4) si ha:

$$Z_1 = rx + sy$$

$$Z_2 = -sx + ry$$

e per la (2.12):

$$Z_1 = ax + by + cz + dt$$

$$Z_2 = bx - ay + dz - ct$$

$$Z_3 = cx - dy - az + bt$$

$$Z_4 = dx + cy - bz - at$$

e le matrici relative sono matrici di similitudini ossia righe e le colonne danno vettori a due a due ortogonali e con la stessa norma. Infatti nel caso di quattro quadrati si può ottenere l'identità (2.12) come segue. Dato un vettore intero $b(a,b,c,d)$ si consideri una delle similitudini di $\mathbb{R}^4$ di rapporto $||b|| = \sqrt{a^2+b^2+c^2+d^2}$, ad esempio la similitudine data da:

$$X' = \begin{pmatrix} a & b & c & d \\ b & -a & d & -c \\ c & -d & -a & b \\ d & c & -b & -a \end{pmatrix} X$$

Se $X(x,y,z,t)$ e se A è la matrice scritta sopra si ha:

$$||X'||^2 = (AX)^t(AX) = X^tA^tAX = X^t \begin{pmatrix} ||b||^2 & 0 & 0 & 0 \\ 0 & ||b||^2 & 0 & 0 \\ 0 & 0 & ||b||^2 & 0 \\ 0 & 0 & 0 & ||b||^2 \end{pmatrix} X =$$

$$= X^t(||b||^2X) = ||b||^2||X||^2 = (a^2+b^2+c^2+d^2)(x^2+y^2+z^2+t^2).$$

D'altra parte è $X'(ax+by+cz+dt, bx-ay+dz-ct, cx-dy-az+bt, dx+cy-bz-at)$ e quindi $||X'||^2 = (ax+by+cz+dt)^2 + (bx-ay+dz-ct)^2 + (cx-dy-az+bt)^2 + (dx+cy-bz-at)^2$ e quindi si ha la (2.12).
Si osservi che il rapporto di similitudine è appunto $\frac{||X'||}{||X||} = ||b||$.
Questo fatto può essere generalizzato nel modo seguente, considero $B = ||X||P$ con $X(X_1, X_2, ..., X_n)$, P matrice ortogonale, ossia $PP^t = I$ e $Z = BY$, quindi:

$$ZZ = (BY)^t(BY) = Y^t(B^tB)Y = Y^t(||X||P^t||X||P)Y = Y^t||X||^2(P^tP)Y =$$

$$= ||X||^2IY^tY = ||X||^2||Y||^2$$

In seguito furono fatte molte ipotesi, ma la risposta a tale domanda venne data solo nel 1898 con il seguente teorema:

Teorema 2.1.7 (di Hurwitz)**.** *Sia K un campo con caratteristica diversa da 2. Gli unici valori di n per i quali è valida l'identità:*

$$(X_1^2 + ... + X_n^2)(Y_1^2 + ... + Y_n^2) = Z_1^2 + ... + Z_n^2 \tag{2.17}$$

dove le Z_k sono funzioni bilineari di X_i e Y_i, a coefficienti in K, sono $n = 1, 2, 4, 8$.

Bibliografia

[1] H. Davenport, *Aritmetica superiore*, Zanichelli, 1994.

[2] G. Everest, T. Ward, *An Intriduction to Number Theory*. Springer,2005.

[3] C. V. Eynden, *Elementary Number Theory*. Mc Grow Hill, 2001.

[4] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*. Oxford University Press, 1979.

[5] A. R. Rajwade, *Squares*, Cambridge University Press, 1993.

[6] J. H. Silverman, *A Friendly Introduction to Number Theory*. Prentice-Hall, 2001.