UNIVERSITÀ STUDI DI UDINE

Scuola Superiore

Tesina di fine anno

RETICOLI E RAPPRESENTAZIONE DI NUMERI IN SOMME DI QUADRATI

RELATORE:
Prof: Corvaja Pietro
TUTOR:
Prof: Corvaja Pietro

STUDENTE:
Mignani Michele

Anno Accademico 2019/2020

Indice

Introduzione

In questo elaborato, verranno trattate alcune questioni relative alla teoria dei numeri, per mezzo di strumenti prettamente geometrici, quali i reticoli. Il problema principale che vogliamo analizzare riguarda la rappresentazione di numeri come somma di quadrati.

Nel primo capitolo introdurremo il concetto di reticolo e mostreremo come è possibile analizzare caratteristiche geometriche di tali entità per studiare proprietà algebriche di un anello. Vedremo infatti un metodo che ci permetterà di capire se un dominio è ad ideali principali e quindi se è dotato di fattorizzazione unica. Infine proveremo il Teorema 1.11 che risulterà fondamentale nei capitoli successivi.

Nel secondo capitolo definiremo la nozione di forma bilineare (e forma quadratica associata) e successivamente vedremo come ad ogni base di $\mathbb{R}^n$ se ne può associare una. Parleremo quindi anche di forme bilineari sugli interi e del loro legame con la teoria dei reticoli.

Nel terzo capitolo tratteremo il problema la cui soluzione anima tutto l'elaborato. Ci occuperemo di classificare tutti e soli i numeri che si rappresentano come somma di 2,3 e 4 quadrati. Giungeremo quindi al Teorema di Lagrange 3.10 uno dei più significativi riguardo l'argomento discusso.

1 Reticoli

1.1 Definizioni e proprietà principali

Definizione 1.1. Sia $n \in \mathbb{N}$ e $S = \{v_1, \dots, v_n\}$ una base di $\mathbb{R}^n$. Il reticolo associato ad S è

$$\Lambda_S := \{a_1 v_1 + \cdots + a_n v_n : \forall i \in \mathbb{N} \quad 1 \leq i \leq n \quad a_i \in \mathbb{Z}\}.$$

Definiamo inoltre il parallelogramma fondamentale di Λ_S

$$\mathscr{P}_S := \{b_1 v_1 + \cdots + b_n v_n : \forall i \in \mathbb{N} \quad 1 \leq i \leq n \quad 0 \leq b_i < 1\}$$

e infine il volume del reticolo Λ_S come il volume del parallelogramma fondamentale

$$\mathrm{Vol}(\Lambda_S) := \mathrm{Vol}(\mathscr{P}_S) = |\det(v_1 \ \dots \ v_n)|.$$

Notiamo che, sebbene un reticolo venga determinato univocamente dalla base S, non vale comunque il viceversa. Potrebbero quindi esistere due insiemi contenenti vettori diversi a cui è associato uno stesso reticolo. Sia $S = \{v_1, \dots, v_n\} \subset \mathbb{R}^n$ una base e $R = \{w_1, \dots, w_n\} \subset \Lambda_S$. Per costruzione, si avrà che $w_i = a_{i1} v_1 + \cdots + a_{in} v_n$. Sia $A \in \mathrm{M}_n(\mathbb{Z})$ la matrice di cambio base, cioè

$$A = \begin{pmatrix} a_{11} & \cdots & a_{n1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \cdots & a_{nn} \end{pmatrix}.$$

Allora si ha la seguente proposizione:

Proposizione 1.1. *Il reticolo Λ_S e il reticolo Λ_R coincidono se e solo se* $|\det(A)| = 1$.

Dimostrazione. ($\Rightarrow$) Se $\Lambda_S = \Lambda_R$ allora ogni vettore $v_i \in S$ si scrive come combinazione lineare intera di $\{w_1, \dots, w_n\}$. Supponiamo pertanto che $v_i = b_{i1} w_1 + \cdots + b_{in} w_n$ e quindi che $B = (b_{ij}) \in \mathrm{M}_n(\mathbb{Z})$ sia la matrice di cambio base associata. Allora $B = A^{-1}$ e quindi $A \in \mathrm{GL}_n(\mathbb{Z})$, da cui segue $|\det(A)| = 1$.

($\Leftarrow$) Se $|\det(A)| = 1$, allora $A^{-1} \in \mathrm{M}_n(\mathbb{Z})$. Quindi ogni vettore dell'insieme S si scrive come combinazione lineare intera dei vettori dell'insieme R, da cui segue $\Lambda_S \subset \Lambda_R$. Per ipotesi però $R = \{w_1, \dots, w_n\} \subset \Lambda_S$ e quindi $\Lambda_R \subset \Lambda_S$. Infine si ha $\Lambda_R = \Lambda_S$.

□

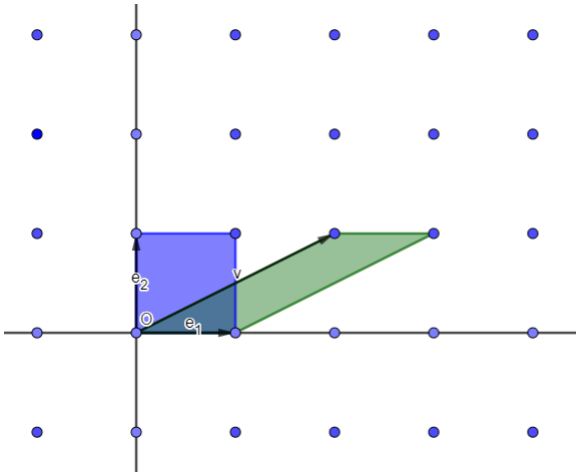

Figura 1: Il reticolo $\mathbb{Z}^2$ e due suoi parallelogrammi fondamentali

Dalla definizione 1.1 si evince che il parallelogramma fondamentale dipende unicamente dall'insieme S di vettori scelti. Abbiamo però visto nella proposizione precedente che uno stesso reticolo può essere descritto da due basi diverse, ammettendo quindi due parallelogrammi fondamentali diversi (cfr Figura 1). Questa osservazione mette a rischio la corretta definizione del volume di un reticolo. Abbiamo bisogno quindi della seguente proposizione.

Proposizione 1.2. *Siano $S = \{v_1, \dots, v_n\}$ e $R = \{w_1, \dots, w_n\}$ due insiemi di vettori linearmente indipendenti tali che $\Lambda_S = \Lambda_R$. Allora i parallelogrammi fondamentali associati all'insieme S e all'insieme R hanno lo stesso volume, ovvero* $\mathrm{Vol}(\mathscr{P}_S) = \mathrm{Vol}(\mathscr{P}_R)$.

Dimostrazione. Sia $A \in \mathrm{M}_n(\mathbb{Z})$ la matrice di passaggio dalla base S alla base R. Quindi $(v_1 \ \dots \ v_n)A = (w_1 \ \dots \ w_n)$. Dalla proposizione 1.1 si ha che $|\det(A)| = 1$ e per la definizione 1.1

$$\begin{aligned}\mathrm{Vol}(\mathscr{P}_R) &= |\det(w_1 \ \dots \ w_n)| = |\det((v_1 \ \dots \ v_n)A)| \\ &= |\det(v_1 \ \dots \ v_n)||\det(A)| = |\det(v_1 \ \dots \ v_n)| = \mathrm{Vol}(\mathscr{P}_S).\end{aligned}$$

□

1.2 Reticoli e domini ad ideali principali

La teoria dei reticoli risulta estremamente utile anche nel dimostrare se un certo anello è o meno ad ideali principali. Supponiamo di lavorare con un sottoanello di $\mathbb{C}$ del tipo

$$\mathbb{Z}[\alpha] = \{a + b\alpha : a, b \in \mathbb{Z} \text{ e } \alpha \in \mathbb{C} \setminus \mathbb{R}\}.$$

Allora possiamo associare a tale anello un reticolo Λ nel seguente modo:

$$\begin{pmatrix} x \\ y \end{pmatrix} \in \Lambda \text{ se e solo se } x + iy \in \mathbb{Z}[\alpha].$$

Ad ogni numero complesso $\beta = c + di$, possiamo inoltre associare in modo naturale la trasformazione di $\mathbb{R}^2$ corrispondente alla matrice

$$R_\beta = \begin{pmatrix} c & -d \\ d & c \end{pmatrix} \in \mathrm{M}_2(\mathbb{R}).$$

Osserviamo che con queste identificazioni, la somma tra due numeri complessi è associata alla somma dei vettori associati agli addendi e la moltiplicazione di un numero β per un altro, dà come risultato l'immagine di quest'ultima per l'applicazione R_β.

Così facendo, un ideale $\mathfrak{p} \subset \mathbb{Z}[\alpha]$ si può identificare con un sottoinsieme di Λ con le seguenti proprietà:

- È un reticolo poiché $(\mathfrak{p}, +)$ è un gruppo abeliano;
- È invariante per R_α poiché dato un elemento $x \in \mathfrak{p}$, $\alpha x \in \mathfrak{p}$.

Notiamo che un ideale sarà principale, cioè generato da un singolo elemento in $\mathbb{Z}[\alpha]$, quando il sottoreticolo ad esso associato sarà $M = \langle v, R_\alpha v \rangle$, per un certo vettore $v \in \Lambda$.

Dimostriamo adesso due teoremi fondamentali che ci permetteranno, alla luce di quanto visto sopra, di dire se un determinato anello della forma $\mathbb{Z}[\alpha]$ è ad ideali principali o no.

Teorema 1.3. *Sia $\Lambda \in \mathbb{R}^2$ un reticolo e siano v_1, v_2 due vettori linearmenti indipendenti di Λ. Allora $\Lambda = \langle v_1, v_2 \rangle$ se e solo se il parallelogramma fondamentale associato a tale base $\mathscr{P}_{\{v_1,v_2\}}$ non contiene punti del reticolo eccetto il vettore nullo.*

Dimostrazione. ($\Rightarrow$) Supponiamo che esista un vettore non nullo $w \in \Lambda \cap \mathscr{P}_{\{v_1,v_2\}}$. Allora w non si può scrivere come combinazione lineare a coefficienti interi di v_1 e di v_2 e quindi $\Lambda \neq \langle v_1, v_2 \rangle$.

($\Leftarrow$) Supponiamo che $\Lambda \neq \langle v_1, v_2 \rangle$, cioè esista un vettore $w \in \Lambda \setminus \langle v_1, v_2 \rangle$. Allora, poiché $\{v_1, v_2\}$ costituiscono una base di $\mathbb{R}^2$, si ha che

$$w = a_1 v_1 + a_2 v_2, \text{ con } a_1, a_2 \in \mathbb{R}.$$

Denotando con $\lfloor a \rfloor$ la parte intera di un numero reale a (il massimo intero minore o uguale ad a), si ha che $w - (\lfloor a_1 \rfloor v_1 + \lfloor a_2 \rfloor v_2)$ appartiene a Λ perché combinazione lineare di vettori nel reticolo. Inoltre si osserva che esso appartiene anche a $\mathscr{P}_{\{v_1,v_2\}}$ contro le ipotesi. □

Teorema 1.4. *Sia Λ un reticolo in $\mathbb{R}^2$ e siano v_1 un vettore di norma minima in Λ e v_2 un vettore di norma minima in $\Lambda \setminus \langle v_1 \rangle$. Allora $\Lambda = \langle v_1, v_2 \rangle$.*

Dimostrazione. Utilizziamo il Teorema 1.3 e mostriamo che l'esistenza di un punto $u \in \mathscr{P}_{\{v_1,v_2\}} \cap \Lambda$ implicherebbe la presenza di un vettore con norma minore a quella di v_1 o a quella di v_2. Il vettore u sarà della forma $t_1v_1 + t_2v_2$, con t_1 e t_2 appartenenti all'intervallo $[0, 1[$. Dividiamo l'analisi in quattro casi:

- $0 \leq t_1, t_2 < \frac{1}{2}$: allora $\|u\| < \|v_2\|$, infatti

$$\begin{aligned}\|u\|^2 = \|t_1v_1 + t_2v_2\|^2 &= t_1^2\|v_1\|^2 + t_2^2\|v_2\|^2 + 2t_1t_2\langle v_1, v_2\rangle \\ &< \frac{1}{2}\|v_2\|^2 + \frac{1}{2}\langle v_1, v_2\rangle \leq \frac{1}{2}\|v_2\|^2 + \frac{1}{2}\|v_1\|^2\|v_2\|^2 \leq \|v_2\|^2.\end{aligned}$$

- $0 \leq t_1 < \frac{1}{2}$ e $\frac{1}{2} \leq t_2 < 1$: allora $\|u - v_2\| < \|v_2\|$, infatti

$$\begin{aligned}\|u - v_2\|^2 &= \|t_1v_1 + (t_2 - 1)v_2\|^2 \\ &= t_1^2\|v_1\|^2 + (1 - t_2)^2\|v_2\|^2 + 2t_1(1 - t_2)\langle v_1, v_2\rangle \\ &< \frac{1}{2}\|v_2\|^2 + \frac{1}{2}\|v_2\|^2 = \|v_2\|^2.\end{aligned}$$

- $\frac{1}{2} \leq t_1 < 1$ e $0 \leq t_2 < \frac{1}{2}$: allora $\|v_1 - u\| < \|v_2\|$, infatti

$$\begin{aligned}\|v_1 - u\|^2 &= \|(1 - t_1)v_1 - t_2v_2\|^2 \\ &= (1 - t_1)^2\|v_1\|^2 + t_2^2\|v_2\|^2 - 2(1 - t_1)(t_2)\langle v_1, v_2\rangle \\ &< \frac{1}{2}\|v_2\|^2 < \|v_2\|^2.\end{aligned}$$

- $\frac{1}{2} \leq t_1, t_2 < 1$: allora $\|(v_1 + v_2) - u\| < \|v_2\|$, infatti

$$\begin{aligned}\|(v_1 + v_2) - u\|^2 &= \|v_1 + v_2 - t_1v_1 - t_2v_2\|^2 \\ &= \|(1 - t_1)v_1 + (1 - t_2)v_2\|^2 \\ &= (1 - t_1)^2\|v_1\|^2 + (1 - t_2)\|v_2\|^2 + \\ &+ 2(1 - t_1)(1 - t_2)\|v_1\|\|v_2\| \\ &< \frac{1}{2}\|v_2\|^2 + \frac{1}{2}\|v_2\|^2 < \|v_2\|^2,\end{aligned}$$

  dove nell'ultimo passaggio abbiamo utilizzato il fatto che v_1 e v_2 non sono lineramente indipendenti e quindi $\langle v_1, v_2\rangle < \|v_1\|\|v_2\|$.

□

Ne segue

Corollario 1.5. *Sia Λ un reticolo invariante per una rotazione $R \in \mathrm{Aut}(\mathbb{R}^2)$ e sia $v \in \Lambda$ un vettore di norma minima. Allora $\Lambda = \langle v, Rv \rangle$.*

Mostriamo ora alcuni esempi.

Esempio 1.6. Mostriamo che $\mathbb{Z}[i]$ è ad ideali principali. Un ideale $\mathfrak{p}$ è associabile ad un sottoreticolo invariante per R_i rotazione di $\frac{\pi}{2}$. Sia $v \in \mathfrak{p}$ un vettore non nullo di norma minima. Allora per il Corollario 1.5, $\mathfrak{p} = \langle v, R_i v \rangle$ e quindi ogni ideale di $\mathbb{Z}[i]$ è principale.

Esempio 1.7. Dimostriamo che $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}] = \mathbb{Z}[\alpha]$ è ad ideali principali. Sia R_α la trasformazione associata alla moltiplicazione per α. Dato un ideale $\mathfrak{p}$ e un suo vettore non nullo di norma minima v, dimostriamo che v e $R_\alpha v$ generano il sottoreticolo associato a $\mathfrak{p}$. Per far questo, ricorriamo al Teorema 1.3 e osserviamo che studiare $\mathfrak{p}$ è equivalente a studiare un ideale avente $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ come vettore di norma minima. Basta quindi dimostrare che nel parallelogramma fondamentale generato da $v_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ e $v_2 = R_\alpha v_1 = \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{7}}{2} \end{pmatrix}$, non ci sono vettori del reticolo, eccetto quello nullo.

Calcoliamo ora la norma del vettore w_1 congiungente origine e baricentro di $\mathscr{P}_{\{v_1,v_2\}}$.

$$\|w_1\|^2 = \|\frac{1}{2} + (\frac{1+\sqrt{-7}}{4})\|^2 = \|\frac{3}{4} + \frac{\sqrt{-7}}{4}\|^2 = 1.$$

Inoltre la norma del vettore w_2 che congiunge il baricentro e il punto corrispondente a v_1 vale

$$\|w_2\|^2 = \|\frac{1}{2} + \frac{1+\sqrt{-7}}{4} - 1\|^2 = \| - \frac{1}{4} + \frac{\sqrt{-7}}{4}\|^2 = \frac{1}{2}.$$

Quindi $\|w_2\| < 1$. Considerando che v_1 ha norma minima, si esclude l'esistenza di un altro vettore del reticolo in un qualsiasi parallelogramma in cui è diviso $\mathscr{P}_{\{v_1,v_2\}}$. Da questo segue la tesi.

Mostriamo infine un esempio di anello non ad ideali principali.

Esempio 1.8. Studiamo $\mathbb{Z}[\sqrt{-5}]$. In questo caso esiste un sottoreticolo che non è generato da un vettore e dall'immagine di tale vettore per l'applicazione associata a $i\sqrt{5}$. Prendiamo l'ideale $\mathfrak{p} = \langle 2, 1+\sqrt{-5} \rangle$, ovvero il reticolo $\Lambda = \langle v_1, v_2 \rangle = \langle \begin{pmatrix} 2 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ \sqrt{5} \end{pmatrix} \rangle$.

Tale reticolo è invariante per $R_{i\sqrt{5}} = \begin{pmatrix} 0 & -\sqrt{5} \\ \sqrt{5} & 0 \end{pmatrix}$ ed infatti

$$R_{i\sqrt{5}} \begin{pmatrix} 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 2\sqrt{5} \end{pmatrix} = -v_1 + 2v_2 \qquad R_{i\sqrt{5}} \begin{pmatrix} 1 \\ \sqrt{5} \end{pmatrix} = \begin{pmatrix} -5 \\ \sqrt{5} \end{pmatrix} = -3v_1 + v_2.$$

Il vettore di norma minima è v_1 e $R_{i\sqrt{-5}} v_1 = \begin{pmatrix} 0 \\ 2\sqrt{5} \end{pmatrix}$. Osserviamo però che il baricentro appartiene a $\Lambda \cap \mathscr{P}_{\{v_1, R_{i\sqrt{5}} v_2\}}$, visto che

$$\begin{pmatrix} 1 \\ \sqrt{5} \end{pmatrix} = v_2 \in \Lambda.$$

Per il Teorema 1.3, si evince che tale ideale non è principale.

1.3 Teoremi di Blichfeldt e di Minkowski

Osserviamo che, per come è stato definito, un reticolo è un insieme di vettori di $\mathbb{R}^n$. Dalla teoria sugli spazi affini si sa che, una volta fissato un punto privilegiato (origine del sistema di riferimento), esiste una corrispondenza biunivoca tra punti dello spazio affine e vettori della giacitura. Con un ragionamento analogo possiamo identificare i vettori di un reticolo $\Lambda \subset \mathbb{R}^n$ con un sottoinsieme di punti in $\mathbb{R}^n$. In virtù di questa osservazione, in seguito utilizzeremo le nozioni di punti e vettori nella stessa maniera.

I teoremi che tratteremo in questa sezione cercano di rispondere alla seguente domanda: *fissato un reticolo Λ e un sottoinsieme $A \subset \mathbb{R}^n$, sotto quali condizioni A contiene un punto non nullo del reticolo?* Il teorema di Minkowski fornisce delle condizioni sufficienti che garantiscono una risposta affermativa al problema posto.

Indichiamo alcune notazioni che risulteranno importanti.

Notazione 1.2. Sia $A \subset \mathbb{R}^n$ e sia $v \in \mathbb{R}^n$. Allora denotiamo

$$A + v = \{a + v \ : \ a \in A\}.$$

Notazione 1.3. Siano A e B due insiemi. Allora chiamiamo la loro unione *disgiunta* se i due insiemi sono disgiunti (cioè $A \cap B = \emptyset$) e scriviamo $A \sqcup B$.

Lemma 1.9. *Sia $S = \{v_1, \dots, v_n\} \subset \mathbb{R}^n$, Λ_S il reticolo associato e $\mathscr{P}_S$ il suo parallelogramma fondamentale. Allora*

$$\mathbb{R}^n = \bigsqcup_{v \in \Lambda_S} (v + \mathscr{P}_S). \tag{1}$$

Dimostrazione. I vettori di S costituiscono una base per $\mathbb{R}^n$. Sia $w \in \mathbb{R}^n$. Allora $w = a_1 v_1 + \cdots + a_n v_n$, con $a_i \in \mathbb{R}$. Denotiamo con $\lfloor a_i \rfloor$ la parte intera di a_i e con $\{a_i\}$ la sua parte frazionaria (cioè $\{a_i\} = a_i - \lfloor a_i \rfloor$). Quindi

$$w = \sum_{i=1}^{n} \lfloor a_i \rfloor v_i + \sum_{i=1}^{n} \{a_i\} v_i.$$

Ricordando ora che $\lfloor a_i \rfloor \in \mathbb{Z}$ e $0 \leq \{a_i\} < 1$, abbiamo decomposto w come un elemento del reticolo ($\sum_{i=1}^{n} \lfloor a_i \rfloor v_i \in \Lambda_S$) e uno del parallelogramma fondamentale ($\sum_{i=1}^{n} \{a_i\} v_i \in \mathscr{P}_S$).

Dimostriamo ora che l'unione è disgiunta. Siano quindi $w_1, w_2 \in \Lambda$, con $w_1 \neq w_2$ e mostriamo che

$$(w_1 + \mathscr{P}_S) \cap (w_2 + \mathscr{P}_S) = \emptyset.$$

Supponiamo per assurdo che l'intersezione non sia vuota e contenga un vettore u. Poiché S costituisce una base per $\mathbb{R}^n$, possiamo supporre che

$$w_1 = \sum_{i=1}^{n} a_i v_i \quad \text{e} \quad w_2 = \sum_{i=1}^{n} b_i v_i, \quad \text{con} \quad a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}.$$

Allora esistono $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n \in [0, 1[$ tali che

$$u = w_1 + \sum_{i=1}^{n} \alpha_i v_i = w_2 + \sum_{i=1}^{n} \beta_i v_i$$

$$\sum_{i=1}^{n} (a_i + \alpha_i) v_i = \sum_{i=1}^{n} (b_i + \beta_i) v_i.$$

Poiché i vettori di S sono linearmenrte indipendendi allora l'equazione precedente implica che $\forall i \in \{1, \ldots, n\} \quad a_i + \alpha_i = b_i + \beta_i$, ovvero $|a_i - b_i| = |\alpha_i - \beta_i| < 1$. Essendo a_i e b_i interi si conclude che per ogni i, $a_i = b_i$ contro l'ipotesi iniziale che $w_1 \neq w_2$. □

Teorema 1.10 (Blichfeldt)**.** *Sia $\Lambda \subset \mathbb{R}^n$ un reticolo e A un sottoinsieme aperto di $\mathbb{R}^n$, con $\mathrm{Vol}(A) > \mathrm{Vol}(\Lambda)$. Allora esistono in A due punti distinti w_1, w_2 tali che*

$$w_1 - w_2 \in \Lambda \setminus \{0\}$$

Dimostrazione. Sia S un sottoinsieme di $\mathbb{R}^n$ tale che $\Lambda_S = \Lambda$. Dalla (1) abbiamo che

$$A = A \cap \bigsqcup_{v \in \Lambda} (v + \mathscr{P}_S) = \bigsqcup_{v \in \Lambda} \{(v + \mathscr{P}_S) \cap A\}.$$

Passando ai volumi quindi si ottiene che

$$\mathrm{Vol}(A) = \sum_{v\in\Lambda} \mathrm{Vol}\{(v + \mathscr{P}_S) \cap A\} = \sum_{v\in\Lambda} \mathrm{Vol}\{\mathscr{P}_S \cap (A - v)\} = \sum_{v\in\Lambda} \mathrm{Vol}(\mathscr{P}_v),$$

con $\mathscr{P}_v := \mathscr{P}_S \cap (A - v)$. Poiché $\mathscr{P}_v \subset \mathscr{P}_S$, si ha che

$$\mathrm{Vol}(\mathscr{P}_v) \leq \mathrm{Vol}(\mathscr{P}_S) = \mathrm{Vol}(\Lambda).$$

Ricordando ora che per ipotesi $\mathrm{Vol}(A) > \mathrm{Vol}(\Lambda)$, si ottiene che

$$\sum_{v\in\Lambda} \mathrm{Vol}(\mathscr{P}_v) > \mathrm{Vol}(\mathscr{P}_S). \tag{2}$$

Se i $\mathscr{P}_v$ fossero a due a due disgiunti, allora non si potrebbe avere la (2), quindi esistono nel reticolo Λ due vettori v_1, v_2 distinti, tali che

$$\mathscr{P}_{v_1} \cap \mathscr{P}_{v_2} \neq \emptyset.$$

Sia $u \in \mathscr{P}_{v_1} \cap \mathscr{P}_{v_2}$. Allora

$$\begin{cases} u = w_1 + v_1 & \text{poiché } u \in \mathscr{P}_{v_1}, \\ u = w_2 + v_2 & \text{poiché } u \in \mathscr{P}_{v_2}, \end{cases}$$

con $w_1, w_2 \in A$. Quindi

$$w_1 - w_2 = (u - v_1) - (u - v_2) = v_1 - v_2 \in \Lambda \setminus \{0\}.$$

□

Da questo segue facilmente il teorema di Minkowski famoso in letteratura anche come teorema del corpo convesso-simmetrico. Prima di enunciarlo, presentiamo alcune definizioni.

Definizione 1.4. Sia $A \subset \mathbb{R}^n$. Allora A è:

- *simmetrico* se $\quad \forall x \quad x \in A \quad \rightarrow \quad -x \in A.$
- *convesso* se $\quad \forall x, y \in A \quad \forall t \in [0,1] \quad tx + (1-t)y \in A.$

Teorema 1.11 (Minkowski)**.** *Sia Λ un reticolo di $\mathbb{R}^n$ e sia $A \subset \mathbb{R}^n$ aperto, convesso e simmetrico con $\mathrm{Vol}(A) > 2^n \mathrm{Vol}(\Lambda)$. Allora esiste un vettore non nullo in $\Lambda \cap A$.*

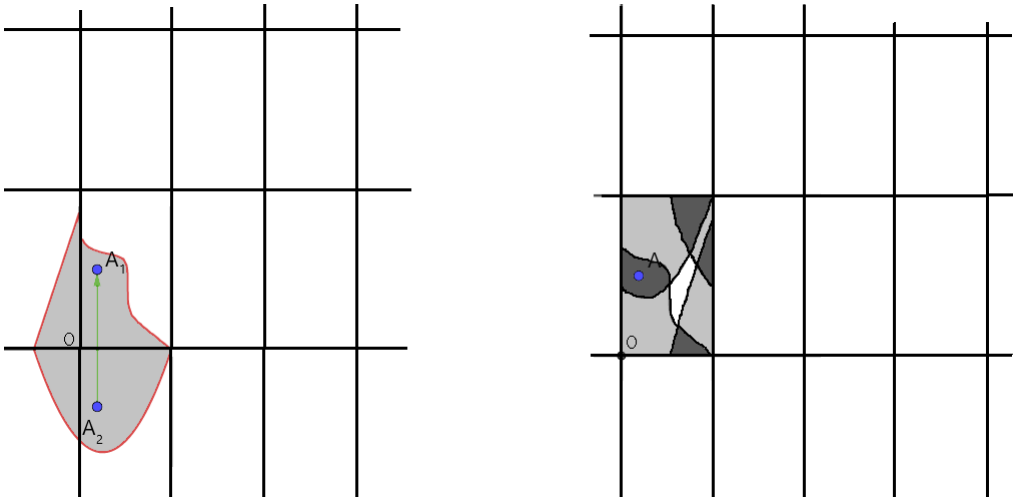

Figura 2: Teorema di Blichfeldt

Dimostrazione. Consideriamo

$$A' = \frac{1}{2}A = \left\{\frac{1}{2}v \ : \ v \in A\right\}.$$

Allora

$$\mathrm{Vol}(A') = \left(\frac{1}{2}\right)^n \mathrm{Vol}(A) > \left(\frac{1}{2}\right)^n 2^n \,\mathrm{Vol}(\Lambda) = \mathrm{Vol}(\Lambda).$$

Quindi possiamo applicare il Teorema di Blichfeldt 1.10 sull'insieme aperto A e quindi esistono $u_1, u_2 \in A'$ tali che

$$u_1 - u_2 \in \Lambda \setminus \{0\}.$$

Vogliamo ora dimostrare che $u_1 - u_2 \in A$, da cui seguirà, per quanto detto sopra, la tesi.

Per definizione di A', si ha che $2u_1, 2u_2 \in A$. Poiché A è simmetrico rispetto l'origine, si ha che $-2u_2 \in A$. Inoltre A è anche convesso e quindi

$$\frac{1}{2}(2u_1) + \frac{1}{2}(-2u_2) = u_1 - u_2 \in A.$$

□

Mostriamo ora alcune applicazioni dirette del Teorema di Minkowski 1.11.

Corollario 1.12. *Un qualsiasi sottoinsieme di punti di $\mathbb{R}^2$ simmetrico rispetto all'origine, convesso e aperto con area strettamente maggiore di 4 contiene almeno un punto con coordinate intere.*

Dimostrazione. Basta applicare il Teorema 1.11 con $\Lambda = \mathbb{Z}^2$. □

Il Teorema 1.11 fornisce anche un limite superiore sulla lunghezza minima dei vettori in un dato reticolo.

Corollario 1.13. *Sia Λ un reticolo di $\mathbb{R}^2$ con $\mathrm{Vol}(\Lambda) = k$. Allora esiste un vettore non nullo $v \in \Lambda$ con $\|v\| \leq 2\frac{\sqrt{k}}{\sqrt{\pi}}$*

Dimostrazione. Supponiamo che ogni vettore $v \in \Lambda \setminus \{0\}$ soddisfi $\|v\| > 2\frac{\sqrt{k}}{\sqrt{\pi}}$. Sia $w \in \Lambda$ un vettore del reticolo. Consideriamo in $\mathbb{R}^2$ il disco

$$\mathscr{C} = \{(x, y) \ : \ x^2 + y^2 \leq \|w\|^2\}.$$

Allora $\mathscr{C} \cap \Lambda$ è un insieme finito perché $\mathscr{C}$ è limitato. Quindi esiste almeno un vettore $u \in \mathscr{C} \cap \Lambda$ con norma minima. Sia $r = \|u\| > 2\frac{\sqrt{k}}{\sqrt{\pi}}$ e definiamo

$$\mathscr{S} = \{(x, y) \ : \ x^2 + y^2 < r^2\}.$$

Poiché $\mathscr{S}$ è un sottoinsieme aperto, simmetrico rispetto all'origine e convesso di $\mathbb{R}^n$ e

$$\mathrm{Vol}(\mathscr{S}) = r^2\pi > 4k = 2^2 \,\mathrm{Vol}(\Lambda),$$

per il teorema 1.11 si ha che esiste un vettore non nullo $s \in \mathscr{C} \cap \Lambda$. Poiché $s \in \mathscr{S}$, si ha che $\|s\| < r = \|u\|$, contro la minimalità di $\|u\|$. □

2 Forme quadratiche e reticoli

Incominciamo col definire i concetti di forma bilineari e forme quadratiche.

Definizione 2.1. Sia V uno spazio vettoriale su un campo $\mathbb{K}$ di caratteristica diversa da 2. Allora definiamo una funzione $b : V \times V \to \mathbb{K}$ *bilineare* se, dato un qualsiasi vettore $v \in V$, accade che:

- l'applicazione $b_v^{sx} : V \to \mathbb{K}$ tale che $w \mapsto b(v, w)$ è lineare;
- l'applicazione $b_v^{dx} : V \to \mathbb{K}$ tale che $w \mapsto b(w, v)$ è lineare.

Definiamo inoltre una forma bilineare b simmetrica se

$$\forall v, w \in V \quad b(v, w) = b(w, v).$$

Infine chiamiamo $q : V \to \mathbb{K}$ la forma quadratica associata a b se

$$\forall v \in V \quad q(v) = b(v, v).$$

Dalla definizione, discende quindi che conoscendo la forma bilineare, possiamo trovare facilmente la forma quadratica associata. In realtà però vale anche il viceversa. Conoscendo $q : V \to \mathbb{K}$, è possibile ricavare la forma bilineare $b : V \times V \to \mathbb{K}$, grazie alla seguente formula:

$$b(v, w) = \frac{1}{2}(q(v + w) - q(v) - q(w)).$$

D'ora in poi parleremo soltanto di forme bilineari simmetriche definite su uno spazio vettoriale di dimensione finita n.

In tal caso è possibile associare ad ogni forma quadratica una matrice $n \times n$. Scegliamo infatti una base $S = \{v_1, \ldots, v_n\}$ di V e poniamo

$$a_{ij} = b(v_i, v_j) \quad \text{per ogni } (i, j) \in \{1, \ldots, n\}^2.$$

Dato un vettore $\mathbf{x} = (x_1, \ldots, x_n) \in V$ nella base S, si ha

$$q(\mathbf{x}) = \sum_{i,j} a_{ij} x_i x_j.$$

Associando quindi a q la matrice

$$M_q = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix},$$

si ha

$$q(\mathbf{x}) = q\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = (x_1, \ldots, x_n) M_q \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}.$$

Introduciamo ora la nozione di equivalenza tra forme quadratiche.

Definizione 2.2. Siano f, g due forme quadratiche definite su uno stesso spazio vettoriale V su di un campo $\mathbb{K}$. Sia I un anello incluso in $\mathbb{K}$. Allora f è I-equivalente a g (in simboli $f \sim_I g$) se per ogni vettore $\mathbf{x} \in I^n$,

$$\exists T \in \mathrm{GL}_n(I) \text{ tale che } f(\mathbf{x}) = g(T(\mathbf{x})).$$

Si verifica facilmente che la relazione sopra introdotta è di equivalenza. Inoltre si ha la seguente proposizione.

Proposizione 2.1. *Siano f, g due forme quadratiche definite su uno stesso spazio vettoriale V su uno stesso campo $\mathbb{K}$ e siano $M_f, M_g \in \mathrm{M}_n(\mathbb{K})$ le matrici associate. Allora*

$$f \sim_I g \iff \exists A \in \mathrm{GL}_n(I) \text{ tale che } M_f = A^T M_g A.$$

Definiamo ora la forma quadratica intera associata ad una base di $\mathbb{R}^n$.

Definizione 2.3. Sia V uno spazio vettoriale su $\mathbb{R}$ di dimensione finita n e sia $S = \{v_1, \ldots, v_n\}$ una sua base. Allora la forma quadratica intera associata ad S, $f_S : \mathbb{Z}^n \to \mathbb{R}$ è così definita:

$$\forall \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Z}^n \quad f_S\left(\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}\right) = \|x_1 v_1 + \cdots + x_n v_n\|^2.$$

Cerchiamo ora di vedere quale relazione deve esserci tra due basi di $\mathbb{R}^n$ affinché le forme quadratiche ad esse associate siano $\mathbb{Z}$-equivalenti.

Lemma 2.2. *Siano $S = \{v_1, \ldots, v_n\}$ e $P = \{w_1, \ldots, w_n\}$ due basi di $\mathbb{R}^n$. Supponiamo che $w_i = a_{i1} v_1 + \cdots + a_{in} v_n$ e sia $A \in \mathrm{M}_n(\mathbb{Z})$ invertibile tale che*

$$A = \begin{pmatrix} a_{11} & \ldots & a_{n1} \\ \vdots & \ddots & \vdots \\ a_{1n} & \ldots & a_{nn} \end{pmatrix} \quad \textit{ovvero} \quad (v_1 \ldots v_n) A = (w_1 \ldots w_n).$$

Allora $f_S \sim_{\mathbb{Z}} f_P$.

Dimostrazione. Sia $\mathbf{x} = (x_1, \dots, x_n)^T$ un generico vettore di $\mathbb{Z}^n$. Allora si ottiene che

$$\begin{aligned} f_P(\mathbf{x}) &= (x_1 w_1 + \cdots + x_n w_n)^T (x_1 w_1 + \cdots + x_n w_n) = \\ &= (x_1 \dots x_n)(w_1 \dots w_n)^T (w_1 \dots w_n) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \\ &= (x_1 \dots x_n) A^T (v_1 \dots v_n)^T (v_1 \dots v_n) A \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \\ &= f_S(A\mathbf{x}). \end{aligned}$$

Poiché $A \in \mathrm{M}_n(\mathbb{Z})$ ed è invertibile, si ha la tesi. □

Il Lemma 2.2 può essere riformulato come segue:

Corollario 2.3. *Sia Λ un reticolo di $\mathbb{R}^n$. Scelte due basi di Λ, le forme quadratiche ad esse associate sono $\mathbb{Z}$-equivalenti.*

Ci preoccupiamo ora di capire sotto quale condizioni due basi definiscono forme quadratiche equivalenti. Nel prossimo teorema denotiamo con $\mathrm{O}_n(\mathbb{R})$ l'insieme delle isometrie di $\mathbb{R}^n$ e ricordiamo che $T \in \mathrm{O}_n(\mathbb{R}) \iff T^T T = I_n$.

Teorema 2.4. *Siano $S = \{v_1, \dots, v_n\}$ e $P = \{w_1, \dots, w_n\}$ due basi di $\mathbb{R}^n$. Allora per ogni $\mathbf{x} \in \mathbb{Z}^n$ si ha*

$$f_S(\mathbf{x}) = f_P(\mathbf{x}) \quad \iff \quad \exists T \in \mathrm{O}_n(\mathbb{R}) \text{ tale che } T(v_1 \dots v_n) = (w_1 \dots w_n).$$

Dimostrazione. ($\Leftarrow$)

$$\begin{aligned} f_P(\mathbf{x}) &= \mathbf{x}^T (w_1 \dots w_n)^T (w_1 \dots w_n)\mathbf{x} = \\ &= (\mathbf{x}^T (v_1 \dots v_n)^T T^T) T (v_1 \dots v_n)\mathbf{x} \\ &= \mathbf{x}^T (v_1 \dots v_n)^T (v_1 \dots v_n)\mathbf{x} \\ &= f_S(\mathbf{x}). \end{aligned}$$

($\Rightarrow$) Sia $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in \mathbb{Z}^n$. Allora dal fato che $f_S(\mathbf{x}) = f_P(\mathbf{x})$ si ha

$$\|x_1 v_1 + \cdots + x_n v_n\|^2 = \|x_1 w_1 + \cdots + x_n w_n\|^2.$$

Sia $T \in \mathrm{GL}_n(\mathbb{R})$ tale che $T(v_1 \dots v_n) = (w_1 \dots w_n)$. Allora T conserva le norme e quindi è un'isometria. □

Da cui discende immediatamente il seguente corollario.

Corollario 2.5. *Siano $S = \{v_1, \dots, v_n\}$ e $P = \{w_1, \dots, w_n\}$ due basi. Allora $f_S \sim_{\mathbb{Z}} f_P$ se e solo se esiste un'isometria $T \in \mathbb{R}^n$ e una matrice $A \in \mathrm{M}_n(\mathbb{Z})$ invertibile tale che*

$$T(v_1 \dots v_n) = (w_1 \dots w_n)A.$$

Dimostrazione. Sia $\mathbf{x}$ un generico vettore di $\mathbb{Z}^n$ e consideriamo la forma quadratica Φ_S che ad ogni vettore $\mathbf{y} \in \mathbb{Z}^n$ associa $f_S(A\mathbf{y})$. Si verifica facilmente che Φ_S è la forma quadratica associata alla base $(u_1 \dots u_n) = (w_1 \dots w_n)A$. È sufficiente ora applicare il Teorema 2.4.

□

Osserviamo che il Corollario 2.5 assume un significato profondo nella teoria delle forme quadratiche definite a partire da un reticolo. Infatti si ha

Corollario 2.6. *Siano $S = \{v_1, \dots, v_n\}$ e $P = \{w_1, \dots, w_n\}$ due basi. Chiamiamo poi Λ_S e Λ_P i due reticoli associati e f_S ed f_P le due forme quadratiche associate. Allora*

$$f_S \sim_{\mathbb{Z}} f_P \quad \iff \quad \exists T \in \mathrm{O}_n(\mathbb{R}) \text{ tale che } T(\Lambda_S) = \Lambda_P.$$

Dimostrazione. Per il Corollario 2.5 l'equivalenza tra le forme quadratiche è garantita se e solo se esiste $T \in \mathrm{O}_n(\mathbb{R})$ e $A \in \mathrm{M}_n(\mathbb{Z})$ invertibile tali che

$$T(v_1 \dots v_n) = (w_1 \dots w_n)A.$$

Poiché A è a coefficienti interi, $(w_1 \dots w_n)A$ ha come colonne vettori di Λ_P. Inoltre, essendo A invertibile, tali vettori costituiscono una base per il reticolo. Quindi, condizione necessaria e sufficiente affinché $f_S \sim_{\mathbb{Z}} f_P$ è che $T(\Lambda_S) = \Lambda_P$. □

Grazie a questo breve preambolo sulle forme quadratiche siamo ora in grado di capire meglio la correlazione tra reticoli e rappresentazioni di numeri in forme quadratiche.

Definizione 2.4. Sia $\mathbb{K}$ un campo ed I un suo sottoanello. Siano dati anche uno spazio vettoriale V su $\mathbb{K}$ ed una forma quadratica f su V. Allora un elemento n si dice I-rappresentabile secondo f se esiste un vettore $\mathbf{x} \in I^n$ tale che $f(\mathbf{x}) = n$.

In questa discussione prenderemo come campo $\mathbb{R}$, come suo sottoanello $\mathbb{Z}$ e come spazio vettoriale $\mathbb{R}^n$. Chiameremo quindi un numero naturale rappresentabile, se è $\mathbb{Z}$-rappresentabile. Osserviamo che se S è una base di $\mathbb{R}^n$, Λ_S il reticolo associato ed f_S la forma quadratica associata, allora per dire che un naturale n è rappresentabile secondo f_S deve esistere un vettore $v \in \Lambda_S$ con norma pari ad n. Abbiamo così ridotto, grazie alla teoria dei reticoli, un problema di teoria dei numeri ad un problema geometrico. Infatti n è rappresentabile secondo f_S se e solo se esiste un vettore nell'intersezione tra il reticolo Λ_S e il luogo dei punti distanti $\sqrt{n}$ dall'origine. Nelle sezioni in cui si tratterà la rappresentazione dei numeri in somme di quadrati, ci si ispirerà proprio a questo argomento. L'idea sarà però quella di intersecare il reticolo non più con una circonferenza, bensì con un disco di raggio opportuno.

3 Rappresentazioni dei numeri come somme di quadrati

Dopo aver visto alcune conseguenze del Teorema 1.11, ci soffermiamo in questa sezione su alcuni possibili utilizzi di tale risultato in teoria dei numeri.

3.1 Somme di due quadrati

Teorema 3.1. *Sia $n \in \mathbb{N}$. Allora esso si scrive come somma di due quadrati se e solo se ogni fattore primo $p \equiv 3 \pmod 4$ compare nella sua fattorizzazione con un esponente pari.*

Per dimostrare il teorema 3.1 abbiamo bisogno di alcuni lemmi. Il cuore di tutta la prova è il seguente:

Lemma 3.2. *Siano n, m due naturali che si scrivono come somma di quadrati. Allora anche nm si scrive come somma di quadrati.*

Dimostrazione. Le ipotesi garantiscono l'esistenza di a_1, a_2, b_1, b_2 tali che $n = a_1^2 + a_2^2$ e $m = b_1^2 + b_2^2$.

Allora

$$\begin{aligned} nm &= (a_1^2 + a_2^2)(b_1^2 + b_2^2) = a_1^2 b_1^2 + a_1^2 b_2^2 + a_2^2 b_1^2 + a_2^2 b_2^2 \\ &= a_1^2 b_1^2 + a_2^2 b_2^2 + -2a_1 a_2 b_1 b_2 + a_2^2 b_1^2 + a_1^2 b_2^2 + 2a_1 a_2 b_1 b_2 \\ &= (a_1 b_1 - a_2 b_2)^2 + (a_1 b_2 + a_2 b_1)^2. \end{aligned}$$

□

Osserviamo che il Lemma 3.2 fornisce una dimostrazione della moltiplicatività della norma nel campo $\mathbb{C}$ ed in particolare in $\mathbb{Z}[i]$. Infatti dato un numero complesso $x_1 + ix_2$, definiamo la funzione norma $|\cdot|$ come segue:

$$|(x_1 + ix_2)| = \sqrt{x_1^2 + x_2^2},$$

ovvero

$$|(x_1 + ix_2)|^2 = x_1^2 + x_2^2.$$

Supponiamo di avere due compleesi $a_1 + ia_2$ e $b_1 + ib_2$. Allora il loro prodotto è $(a_1 b_1 - a_2 b_2) + i(a_1 b_2 + a_2 b_1)$ e dalla dimostrazione precedente, si evince che la norma del prodotto è il prodotto delle norme dei fattori.

L'utilità di questo lemma risiede nella possibilità di concentrarsi solo sugli elementi primi in $\mathbb{Z}$. Per prima cosa notiamo che non tutti i primi possono effettivamente scriversi come somma di due quadrati.

Lemma 3.3. *Sia n un numero naturale che si scrive come somma di due quadrati. Allora $n \not\equiv 3 \pmod 4$.*

Dimostrazione. Supponiamo $n = a^2 + b^2$, con $a, b \in \mathbb{N}$. Riducendo tale equazione modulo 4 e notando che, dato un qualsiasi numero c, c^2 ha resto 0 o 1 modulo 4, la classe di resto di n non potrà essere 3. □

Quindi gli unici primi dispari candidati a scriversi come somma di quadrati sono della forma 4k+1. Vediamo con il prossimo teorema che effettivamente questi si rappresentano nella maniera voluta.

Teorema 3.4. *Tutti e soli i primi che si scrivono come somma di due quadrati sono il 2 e quelli della forma 4k+1.*

Dimostrazione. Dimostriamo inizialmente che tutti i primi che soddisfano le ipotesi si scrivono come somma di due quadrati. Poiché $2 = 1^2+1^2$, studiamo solo il caso $p = 4k + 1$.

Dobbiamo trovare due interi u, v tali che $p = u^2+v^2$. Questo è equivalente a dire che esistono due interi *non entrambi nulli* con le seguenti proprietà:

(a) p divide $u^2 + v^2$;

(b) $u^2 + v^2 < 2p$.

L'idea è quella di costruire un reticolo Λ appropriato in cui

$$\forall \begin{pmatrix} a \\ b \end{pmatrix} \in \Lambda, \qquad p|(a^2 + b^2)$$

e poi considerarne l'intersezione con il disco di raggio $\sqrt{2p}$.

Poiché $p \equiv 1 \ (mod\ 4)$, si ha che esiste $z \in \mathbb{Z}$ tale che $z^2 \equiv -1 \ (mod\ p)$. Infatti $\mathbb{F}_p^*$ ha cardinalità divisibile per 4 ed essendo ciclico, ammette un elemento z di tale ordine. Da questo si conclude che z^2 ha ordine 2 ma non è 1, quindi $z^2 = -1$. Consideriamo i vettori $v_1 = \begin{pmatrix} p \\ 0 \end{pmatrix}$ e $v_2 = \begin{pmatrix} z \\ 1 \end{pmatrix}$. Essi sono linearmente indipendenti e verifichiamo che il reticolo da loro generato $\Lambda_{\{v_1,v_2\}}$ ha le proprietà volute.

Prendiamo un elemento generico $w = \begin{pmatrix} a \\ b \end{pmatrix} \in \Lambda_{\{v_1,v_2\}}$. Allora

$$w = c_1v_1 + c_2v_2 = (c_1p + c_2z, c_2).$$

$$a^2 + b^2 = c_1^2p^2 + c_2^2(z^2 + 1) + 2pc_1c_2z = c_1^2p^2 + c_2^2p + 2pc_1c_2z \equiv 0 \ (mod\ p).$$

Consideriamo ora il sottoinsieme di $\mathbb{R}^2$:

$$\mathscr{C} = \{(x, y) : x^2 + y^2 < 2p\}.$$

Esso è un insieme aperto, convesso e simmetrico rispetto l'origine con volume pari a $2p\pi$. Il volume del reticolo è

$$\mathrm{Vol}(\Lambda_{\{v_1,v_2\}}) = \left| \det \begin{pmatrix} p & z \\ 0 & 1 \end{pmatrix} \right| = p.$$

Visto che $4\,\mathrm{Vol}(\Lambda_{\{v_1,v_2\}}) = 4p < 2\pi p$, possiamo applicare il teorema di Minkowski 1.11. Pertanto esiste un vettore *non nullo* $(u, v)^T \in \Lambda \cup \mathscr{C}$. Ora tale vettore soddisfa la proprietà (a) poiché appartiene al reticolo Λ e la (b) poiché appartiene a $\mathscr{C}$. Da cui si conclude che $p = u^2 + v^2$.

Sia ora p un generico primo che non sia della forma $4k + 1$ e non sia 2 e dimostriamo che non si può scrivere come somma di due quadrati. Se $p \neq 2$ allora p è dispari e quindi non può essere della forma $4k + 2$ o della forma $4k$. Ne segue quindi che p è della forma $4k + 3$. Ricordando ora il Lemma 3.3 si conclude. □

Lemma 3.5. *I primi q della forma $4k + 3$ sono primi in $\mathbb{Z}[i]$.*

Dimostrazione. Supponiamo che $q|\alpha\beta$ e mostriamo che $q|\alpha$ o $q|\beta$. Poiché $q|\alpha\beta$, si avrà che q divide $(\alpha\beta\bar{\beta}\bar{\alpha}) = N(\alpha)N(\beta)$ in $\mathbb{Z}[i]$. Dal fatto che $q, N(\alpha), N(\beta) \in \mathbb{Z}$, si evince che q divide $N(\alpha)N(\beta)$ anche in $\mathbb{Z}$. Assumiamo quindi che $q|N(\alpha) = a^2 + b^2$ con $\alpha = a + bi$. Se $q|a$, allora $0 \equiv a^2 + b^2 \equiv b^2 \ (mod\ q)$, quindi $q|b$ e allora $q|\alpha$. Se invece $q \nmid a$, a è invertibile in $\mathbb{F}_q$ e posto $ba^{-1} = c$, si avrebbe che $c^2 \equiv -1 \ (mod\ q)$ cioè esisterebbe un elemento in $\mathbb{F}_q$ di ordine 4, il che va contro l'ipotesi $q \equiv 3 \ (mod\ 4)$. □

Siamo ora pronti a dimostrare il Teorema 3.1.

Dimostrazione Teorema 3.1. ($\Leftarrow$) Sia q un primo della forma $4k+3$ che divide n. Dimostriamo che ha esponente pari. Poiché n si scrive come somma di quadrati, esisterà $\alpha \in \mathbb{Z}[i]$ tale che $n = \alpha\bar{\alpha}$. Dal momento che q è primo in $\mathbb{Z}[i]$ (Lemma 3.5), si può assumere senza perdità di generalità che $q|\alpha$. Allora $\alpha = q\alpha'$ e $q|\bar{\alpha}$ quindi $n = q^2\alpha'\bar{\alpha}'$ e $q^2|n$. Supponiamo quindi che $q^k|n$ con k dispari. Allora iterando il procedimento visto sopra concluderemo che anche $q^{k+1}|n$, da cui la tesi.

($\Rightarrow$) Supponiamo che

$$n = 2^t(p_1^{a_1} \cdots p_s^{a_s})(q_1^{2b_1} \cdots q_h^{2b_h}),$$
$$\text{con } t, a_1, \ldots, a_s, b_1, \ldots, b_h \in \mathbb{N}, \quad p_i \equiv 1 \ (mod\ 4) \text{ e } q_j \equiv 3 \ (mod\ 4).$$

Notiamo che n risulta in questo modo essere prodotto di elementi tutti rappresentabili e quindi in virtù del lemma 3.2, anche n si scrive come somma di due quadrati. □

3.2 Somme di quattro quadrati

In questa sezione, dimostreremo che ogni numero naturale si scrive come somma di quattro quadrati.

Iniziamo la discussione con un lemma analogo al 3.2 che ci permetterà di restringere lo studio ai numeri primi.

Lemma 3.6 (Identità di Eulero)**.** *Siano $n, m \in \mathbb{N}$ numeri esprimibili come somma di quattro quadrati. Allora anche nm si rappresenta come somma di quattro quadrati.*

Dimostrazione. Siano dati $n = a^2 + b^2 + c^2 + d^2$ e $m = e^2 + f^2 + g^2 + h^2$. Allora

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

□

Osservazione 3.7. Possiamo trovare una certa correlazione tra il Lemma 3.2 e il Lemma 3.6. Mentre il primo porta ad una dimostrazione della moltiplicatività della norma in $\mathbb{C}$, il secondo la prova in $\mathbb{H}$. Il corpo dei quaternioni (indicato con $\mathbb{H}$) è un'estensione non commutativa di $\mathbb{C}$.

Possiamo introdurre in $\mathbb{R}$ le unità immaginarie i, j, k, legate dalle seguenti relazioni:

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ ij &= -ji = k \\ jk &= -kj = i \\ ki &= -ik = j \end{aligned}$$

Definiamo quindi

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

Chiameremo a la parte reale di q (in simboli $\mathrm{Re}(q)$) e un quaternione sarà *puro* se $\mathrm{Re}(q) = 0$. Osserviamo che possiamo definire una biezione $f : \mathbb{H} \to \mathbb{R} \times \mathbb{R}^3$ in modo tale che

$$f(q) = f(a + bi + cj + dk) = (\mathrm{Re}(q), \mathbf{q}) = \left(a, \begin{pmatrix} b \\ c \\ d \end{pmatrix}\right).$$

Questa funzione ci aiuterà a definire la somma $\tilde{+}$ ed il prodotto $\tilde{\cdot}$ tra due quaternioni q_1 e q_2. In particolare:

$$q_1 \tilde{+} q_2 = f^{-1}(\mathrm{Re}(q_1) + \mathrm{Re}(q_2), \mathbf{q_1} + \mathbf{q_2})$$
$$q_1 \tilde{\cdot} q_2 = f^{-1}(\mathrm{Re}(q_1)\,\mathrm{Re}(q_2) - (\langle \mathbf{q_1}, \mathbf{q_2} \rangle), \mathrm{Re}(q_1)\mathbf{q_2} + \mathrm{Re}(q_2)\mathbf{q_1} + \mathbf{q_1} \wedge \mathbf{q_2}),$$

dove $\langle \mathbf{q_1}, \mathbf{q_2} \rangle$ denota il prodotto scalare tra i due vettori e $\mathbf{q_1} \wedge \mathbf{q_2}$ il prodotto vettoriale.

Per il calcolo dell'inverso di un quaternione, risulterà utile il concetto di coniugato. Sia $q \in \mathbb{H}$. Allora il coniugato

$$\bar{q} = f^{-1}(\mathrm{Re}(q), -\mathbf{q}),$$

ovvero se $q = a + bi + cj + dk$, si ha

$$\bar{q} = a - bi - cj - dk.$$

Grazie a tale definizione si può costruire la funzione norma $|\cdot| : \mathbb{H} \to \mathbb{R}$ tale che

$$q = a + bi + cj + dk \mapsto q\bar{q} = a^2 + b^2 + c^2 + d^2.$$

Notiamo immediatamente che

$$|q| = 0 \iff q = 0 \quad \text{e} \quad q \neq 0 \to q^{-1} = \frac{\bar{q}}{|q|}.$$

Si evince quindi che $(\mathbb{H}, \tilde{+}, \tilde{\cdot})$ è un corpo, dotato di una norma $(|\cdot|)$ moltiplicativa per il Lemma 3.6

Il lemma 3.6 permette di provare che ogni numero si scrive come somma di quattro quadrati, dimostrando unicamente che ogni primo si scrive in tal modo. Inoltre osserviamo che $2 = 1^2 + 1^2 + 0^2 + 0^2$, quindi possiamo anche restringerci al caso p dispari.

Utilizziamo ora lo stesso procedimento applicato nello studio dei primi rappresentabili come somma di due quadrati. Dire infatti che un primo p è somma di quattro quadrati equivale a sostenere l'esistenza di quattro interi u, v, w, t con le seguenti proprietà:

(a) $(u, v, w, t) \neq (0, 0, 0, 0)$;

(b) $u^2 + v^2 + w^2 + t^2 < 2p$;

(c) $p|(u^2 + v^2 + w^2 + t^2)$.

Dobbiamo quindi costruire un reticolo Λ con

$$\forall \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} \in \Lambda \qquad p|(a^2+b^2+c^2+d^2)$$

e poi considerarne l'intersezione con la sfera

$$\mathscr{S} = \{(x,y,z,w) \in \mathbb{R}^4 : x^2+y^2+z^2+w^2 < 2p\}.$$

Per la costruzione del reticolo Λ sarà utile il seguente lemma.

Lemma 3.8. *Sia p un numero primo dispari. Allora*

$$\exists r, s \in \mathbb{Z} \quad con \quad r^2+s^2+1 \equiv_p 0.$$

Dimostrazione. Consideriamo le due funzioni

$$f, g : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}, \qquad \text{con } f(x) = x^2 \text{ (mod p)} \quad \text{e} \quad g(x) = -1 - x^2 \text{ (mod p)}.$$

La tesi equivale a dimostrare l'esistenza di interi r, s tali che $f(r) = g(s)$. Cerchiamo di calcolare $|f(\mathbb{Z})|$ e $|g(\mathbb{Z})|$.

Sicuramente $f(x) = f(-x)$ e anche $g(x) = g(-x)$. Dimostriamo inoltre che $f(x) = f(y)$ implica $x = y$ oppure $x = -y$. Infatti l'equazione $t^2 = f(x)$ nella variabile t, può avere al massimo due soluzioni distinte, essendo $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$ un campo. Allora si ottiene

$$\begin{aligned} f(x) = f(y) \quad &\text{se e solo se} \quad x \equiv_p \pm y \\ g(x) = g(y) \quad &\text{se e solo se} \quad x \equiv_p \pm y. \end{aligned}$$

Quindi, considerando che p è dispari e che per ogni elemento non nullo x, esso è diverso dal suo opposto e hanno la stessa immagine,

$$|f(\mathbb{Z})| = |g(\mathbb{Z})| = \frac{p+1}{2}.$$

Si deduce, utilizzando il principio dei cassetti ($|f(\mathbb{Z})| + |g(\mathbb{Z})| = p+1 > p$) la tesi.

□

Teorema 3.9. *Ogni primo p si scrive come somma di quattro quadrati.*

Dimostrazione. Se $p = 2$, allora $2 = 1^2 + 1^2 + 0^2 + 0^2$. Possiamo quindi assumere p dispari.

Grazie al teorema 3.8 esistono r, s interi con $r^2+s^2+1 \equiv_p 0$. Consideriamo i vettori

$$v_1 = \begin{pmatrix} p \\ 0 \\ 0 \\ 0 \end{pmatrix}, \quad v_2 = \begin{pmatrix} 0 \\ p \\ 0 \\ 0 \end{pmatrix} \quad v_3 = \begin{pmatrix} r \\ s \\ 1 \\ 0 \end{pmatrix}, \quad v_4 = \begin{pmatrix} s \\ -r \\ 0 \\ 1 \end{pmatrix}.$$

Tali vettori sono linearmente indipendenti e in particolare

$$\mathrm{Vol}(\Lambda) = \det \begin{pmatrix} p & 0 & r & s \\ 0 & p & s & -r \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} = p^2.$$

Dimostriamo che il reticolo così costruito ha la proprietà richiesta, cioè

$$\forall u \in \Lambda \quad p \text{ divide } \|u\|^2.$$

Essendo un generico vettore del reticolo, u si scriverà come $c_1v_1 + c_2v_2 + c_3v_3 + c_4v_4$. Allora

$$\|u\|^2 = \langle u, u\rangle = \langle c_1v_1 + c_2v_2 + c_3v_3 + c_4v_4, c_1v_1 + c_2v_2 + c_3v_3 + c_4v_4\rangle.$$

Ora, considerando la bilineraità del prodotto scalare e il fatto che p divide tutte le componenti di v_1 e di v_2, si ottiene

$$\langle c_1v_1 + c_2v_2 + c_3v_3 + c_4v_4, c_1v_1 + c_2v_2 + c_3v_3 + c_4v_4\rangle = \langle c_3v_3 + c_4v_4, c_3v_3 + c_4v_4\rangle.$$

Osservando poi che v_3 e v_4 sono perpendicolari e che le loro norme sono multiple di p,

$$\|u\|^2 = \langle c_3v_3 + c_4v_4, c_3v_3 + c_4v_4\rangle = c_3^2\|v_3\|^3 + c_4^2\|v_4\|^2 \equiv 0 \pmod p.$$

Consideriamo ora la sfera aperta $\mathscr{S}$ di raggio $\sqrt{2p}$. Tale sottoinsieme di $\mathbb{R}^4$ è simmetrico rispetto all'origine, aperto e convesso. Inoltre il suo volume è

$$\mathrm{Vol}(\mathscr{S}) = \frac{\pi^2}{2}(\sqrt{2p}^4) = 2\pi^2p^2 > 16p^2 = 2^4\,\mathrm{Vol}(\Lambda).$$

Possiamo pertanto applicare il teorema di Minkowski 1.11 e affermare l'esistenza di un vettore *non nullo* $s = (u, v, w, t)^T \in \Lambda \cap \mathscr{S}$. In particolare gli interi u, v, w, t soddisfano la proprietà (a), la proprietà (b) perché s appartiene alla sfera $\mathscr{S}$ ed infine la proprietà (c) perché s appartiene al reticolo Λ. Quindi si conclude che $p = u^2 + v^2 + w^2 + t^2$. □

Siamo ora pronti a dimostrare il teorema principale.

Teorema 3.10. *Ogni numero naturale si scrive come somma di quattro quadrati.*

Dimostrazione. Sia $n \in \mathbb{N}$ e supponiamo che $n = p_1 \cdots p_t$. Allora procediamo per induzione su t.

Se $t = 1$, si ha che n è un primo e quindi si ha la tesi per il Teorema 3.9.

Se $t > 1$, allora $n = p_1 \cdots p_t = (p_1 \cdots p_{t-1})p_t$. Per ipotesi induttiva $p_1 \cdots p_{t-1}$ si rappresenta come somma di quattro quadrati e per il Teorema 3.9 anche p_t. Quindi per il Lemma 3.6, n si scrive come somma di quadrati. □

3.3 Somme di tre quadrati

Utilizzando l'idea che ha ispirato il caso dei due quadrati e quello dei quattro quadrati, studieremo ora quali numeri si rappresentano come somma di tre quadrati. Una risposta parziale al problema viene data dal seguente lemma.

Lemma 3.11. *I numeri del tipo $n = 4^a(8b+7)$ non si possono scrivere come somma di tre quadrati.*

Dimostrazione. Distinguiamo per semplicità due casi:

- $a = 0$. Supponiamo che $n = 8b + 7$ e dimostriamo che non si può esprimere come somma di 3 quadrati. Infatti se fosse $n = x^2 + y^2 + z^2$, ricordando che solo 0, 1 e 4 sono residui quadratici modulo 8, si ha che $n \not\equiv_7 8$.

- $a \geq 1$. Proviamo dapprima che se $4n$ si rappresenta come somma di 3 quadrati, allora anche n si scrive in questa maniera. Assumiamo che $4n = x^2 + y^2 + z^2$. Ricordando che solo 0 e 1 sono residui quadratici modulo 4, si ottiene che affinché $4|(x^2 + y^2 + z^2)$, ogni addendo deve essere divisibile per 4. Quindi chiamando

  $$\bar{x} = \frac{x}{2} \quad \bar{y} = \frac{y}{2} \quad \bar{z} = \frac{z}{2},$$

  si ha che

  $$n = \frac{4n}{4} = \frac{x^2 + y^2 + z^2}{4} = \left(\frac{x}{2}\right)^2 + \left(\frac{y}{2}\right)^2 + \left(\frac{z}{2}\right)^2 = \bar{x}^2 + \bar{y}^2 + \bar{z}^2.$$

  Supponiamo quindi che la tesi del nostro lemma non sia vera. Consideriamo l'insieme

  $$A = \{a \in \mathbb{N} : 4^a(8b + 7) \text{ è rappresentabile}\}.$$

  Allora A non è vuoto e, essendo sottoinsieme di $\mathbb{N}$, ammette minimo $\alpha \geq 1$, visto che il caso $a = 0$, è stato scartato all'inizio. Per quanto detto precedentemente, si ha che $(\alpha - 1) \in A$, contro l'ipotesi di minimalità di α. Si conclude così l'assurdo.

□

In realtà, i numeri del tipo $4^a(8b+7)$ sono *tutti e soli* quelli non esprimibili come somma di tre quadrati. Notiamo però che non possiamo utilizzare teoremi analoghi ai Lemmi 3.2 e 3.6. Grazie ad essi siamo stati in grado di affermare che il prodotto tra somme di due (quattro) quadrati è ancora esprimibile come somma di due (quattro) quadrati. Nel caso dei tre quadrati non possiamo far ricorso ad argomenti di questo tipo e quindi non possiamo limitare il nostro studio ai soli elementi primi di $\mathbb{N}$. Il motivo di questa impossibilità è spiegata dal seguente teorema.

Teorema 3.12. *Non esistono tre forme bilineari $F, G, H : \mathbb{R}^3 \times \mathbb{R}^3 \to \mathbb{R}$ tali che, dati due qualsiasi vettori $\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}, \mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}$ in $\mathbb{R}^3$, si abbia*

$$(x_1^2 + x_2^2 + x_3^2)(y_1^2 + y_2^2 + y_3^2) = F(\mathbf{x}, \mathbf{y})^2 + G(\mathbf{x}, \mathbf{y})^2 + H(\mathbf{x}, \mathbf{y})^2.$$

Dimostrazione. Supponiamo che

$$F(\mathbf{x}, \mathbf{y}) = \sum_{i,j} f_{ij} x_i y_j \quad G(\mathbf{x}, \mathbf{y}) = \sum_{i,j} g_{ij} x_i y_j \quad H(\mathbf{x}, \mathbf{y}) = \sum_{i,j} h_{ij} x_i y_j.$$

Sia

$$\mathbf{z} = \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} F(\mathbf{x}, \mathbf{y}) \\ G(\mathbf{x}, \mathbf{y}) \\ H(\mathbf{x}, \mathbf{y}) \end{pmatrix}.$$

Allora si ha

$$(x_1^2 + x_2^2 + x_3^2)(y_1^2 + y_2^2 + y_3^2) = (z_1^2 + z_2^2 + z_3^2) \tag{3}$$

Abbiamo quindi che

$$\begin{aligned} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} &= \begin{pmatrix} \sum_{i,j} f_{ij} x_i y_j \\ \sum_{i,j} g_{ij} x_i y_j \\ \sum_{i,j} h_{ij} x_i y_j \end{pmatrix} = \\ &= y_1 \begin{pmatrix} \sum_i f_{i1} x_i \\ \sum_i g_{i1} x_i \\ \sum_i h_{i1} x_i \end{pmatrix} + y_2 \begin{pmatrix} \sum_i f_{i2} x_i \\ \sum_i g_{i2} x_i \\ \sum_i h_{i2} x_i \end{pmatrix} + y_3 \begin{pmatrix} \sum_i f_{i3} x_i \\ \sum_i g_{i3} x_i \\ \sum_i h_{i3} x_i \end{pmatrix} = \\ &= \begin{pmatrix} \sum_i f_{i1} x_i & \sum_i f_{i2} x_i & \sum_i f_{i3} x_i \\ \sum_i g_{i1} x_i & \sum_i g_{i2} x_i & \sum_i g_{i3} x_i \\ \sum_i h_{i1} x_i & \sum_i h_{i2} x_i & \sum_i h_{i3} x_i \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = \end{aligned}$$

$$= \left(x_1 \begin{pmatrix} f_{11} & f_{12} & f_{13} \\ g_{11} & g_{12} & g_{13} \\ h_{11} & h_{12} & h_{13} \end{pmatrix} + x_2 \begin{pmatrix} f_{21} & f_{22} & f_{23} \\ g_{21} & g_{22} & g_{23} \\ h_{21} & h_{22} & h_{23} \end{pmatrix} + \right.$$
$$\left. + x_3 \begin{pmatrix} f_{31} & f_{32} & f_{33} \\ g_{31} & g_{32} & g_{33} \\ h_{31} & h_{32} & h_{33} \end{pmatrix} \right) \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} =$$
$$= (x_1 A_1 + x_2 A_2 + x_3 A_3) \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix} = A \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}.$$

Da (3) si evince che

$$\mathbf{z}^T \mathbf{z} = z_1^2 + z_2^2 + z_3^2 = \mathbf{y}^T A^T A \mathbf{y}.$$

Il membro di sinistra di (3) si può scrivere come

$$(x_1^2 + x_2^2 + x_3^2)\mathbf{y}^T \mathbf{y} = \mathbf{y}^T (x_1^2 + x_2^2 + x_3^2) I_3 \mathbf{y}.$$

Quindi si ottiene che

$$\mathbf{y}^T A^T A \mathbf{y} = \mathbf{y}^T (x_1^2 + x_2^2 + x_3^2) I_3 \mathbf{y}$$

e poiché deve valere per ogni $\mathbf{y} \in \mathbb{R}^3$, si ha

$$(x_1^2 + x_2^2 + x_3^2) I_3 = A^T A.$$

Ricordando che $A = x_1 A_1 + x_2 A_2 + x_3 A_3$,

$$A^T A = x_1^2 A_1^T A_1 + x_2^2 A_2^T A_2 + x_3^2 A_3^T A_3 +$$
$$+ x_1 x_2 (A_1^T A_2 + A_2 A_1^T) + x_1 x_3 (A_1^T A_3 + A_3^T A_1) + x_2 x_3 (A_2^T A_3 + A_3^T A_2)$$

Poiché tale uguaglianza vale per ogni $x_1, x_2, x_3 \in \mathbb{R}$, allora si ottiene che

$$A_1^T A_1 = I_3 \quad A_2^T A_2 = I_3 \quad \text{e} \quad A_1^T A_2 = -A_2^T A_1.$$

Questo sistema però non ammette soluzione se lavoriamo con spazi vettoriali V di dimensione dispari. Dalle prime due uguaglianze ricaviamo, infatti, che $|\det(A_1)| = |\det(A_2)| = 1$. Quindi $A_1^T A_2$ e $A_2^T A_1$ hanno lo stesso determinante e ciò è incompatibile con l'ultima ($\det(I_3) = -1$). Da qui discende quindi l'assurdo. □

Ci preoccupiamo ora di mostrare che i numeri non della forma $4^a(8b+7)$ si rappresentano effettivamente nella forma voluta. Per provare ciò abbiamo bisogno di introdurre un nuovo simbolo e dimostrare alcuni lemmi preparatori.

Notazione 3.1 (Simbolo di Legendre)**.** Sia a un intero e p un primo dispari. Allora definiamo

$$\left(\frac{a}{p}\right) := \begin{cases} +1 & \text{se esiste } n \text{ tale che } n^2 \equiv_p a; \\ 0 & \text{se } p|a; \\ -1 & \text{altrimenti.} \end{cases}$$

Se $\left(\frac{a}{p}\right) = +1$, chiameremo a residuo quadratico modulo p.

Introduciamo adesso alcuni teoremi che mettono in luce alcune caratteristiche del simbolo di Legendre, tra cui la *legge di reciprocità quadratica*, dapprima in un caso particolare e poi in un caso più generale.

Teorema 3.13. *Sia p un primo dispari. Allora*

$$\left(\frac{a}{p}\right) \equiv_p a^{\frac{p-1}{2}}.$$

Dimostrazione. Se $a \equiv_p 0$, la tesi è vera. Supponiamo quindi che $p \nmid a$. Il gruppo $(\mathbb{F}_p \setminus \{0\}, \cdot)$ è un gruppo ciclico. Quindi sia g un generatore. Allora $a \equiv_p g^i$ per un certo i, da cui

$$\left(\frac{a}{p}\right) = (-1)^i.$$

Se i è pari, si ha

$$a^{\frac{p-1}{2}} \equiv_p g^{i\frac{p-1}{2}} \equiv_p g^{\frac{i}{2}(p-1)} \equiv_p 1.$$

Se $i = 2k+1$ è dispari, invece,

$$a^{\frac{p-1}{2}} \equiv_p g^{i\frac{p-1}{2}} \equiv_p g^{(2k+1)\frac{p-1}{2}} \equiv_p g^{k(p-1)} g^{\frac{p-1}{2}} \equiv_p g^{\frac{p-1}{2}}.$$

Ma

$$g^{\frac{p-1}{2}} \equiv_p -1,$$

infatti $(g^{\frac{p-1}{2}})^2 = g^{p-1} \equiv_p 1$ e $g^{\frac{p-1}{2}} \not\equiv_p 1$, in quanto se lo fosse, g non sarebbe generatore. □

Teorema 3.14. *Sia p un primo dispari. Allora per ogni intero a, b si ha*

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

Dimostrazione. Per il teorema 3.13,

$$\left(\frac{ab}{p}\right) \equiv_p (ab)^{\frac{p-1}{2}} \equiv_p a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv_p \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Allora p divide $\left(\frac{ab}{p}\right) - \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Dal momento che il simbolo di Legendre può valere solo $-1, 0, +1$, si ha che tale differenza può unicamente assumere i valori compresi tra -2 e $+2$. Essendo p dispari, tale differenza deve essere pari a 0, cioè la tesi. □

Teorema 3.15 (Reciprocità quadratica 1)**.** *Se p e q sono distinti numeri primi dispari, allora*

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

Inoltre se p è un primo dispari

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Per una dimostrazione di tale teorema si rimanda a [1]

Notazione 3.2 (Simbolo di Jacobi)**.** Siano $a, b \in \mathbb{Z}$ e b dispari, con $b = p_1 \cdots p_k$, primi non necessariamente distinti. Definiamo

$$\left(\frac{a}{b}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right),$$

dove $\left(\frac{a}{p_i}\right)$ indica il simbolo di Legendre.

Esistono dei teoremi analoghi a quelli visti sopra per il simbolo di Legendre. In particolare

Teorema 3.16. *Sia m un numero dispari. Allora per ogni intero a, b si ha*

$$\left(\frac{ab}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right).$$

Teorema 3.17 (Reciprocità quadratica 2)**.** *Sia $m \in \mathbb{N}$ dispari. Allora*

- $$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}.$$
- $$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}.$$

- *Siano $m, n \in \mathbb{N}$ entrambi dispari. Allora*

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\left(\frac{n}{m}\right).$$

Lo scopo di questa sezione sarà dimostrare il seguente

Teorema 3.18. *I numeri naturali che si rappresentano come somma di 3 quadrati sono tutti e soli quelli* non *del tipo* $4^a(8b+7)$.

In virtù del Lemma 3.11, rimane da provare che i numeri che non sono della forma $4^a(8b+7)$ si scrivono come somma di tre quadrati. La dimostrazione che seguiremo noi sfrutta le proprietà dei reticoli e il Teorema di Minkowski 1.11. La difficoltà risiede nel costruire il reticolo giusto che permette di giungere alla tesi. Per far questo avremo quindi bisogno di un altro teorema.

Teorema 3.19 (Dirichlet)**.** *Siano a, b degli interi con $b > 0$ e coprimi. Allora l'insieme*

$$\{a + kb \mid k \in \mathbb{N}\}$$

contiene infiniti numeri primi.

Ora siamo pronti a dimostrare il Teorema 3.18. La dimostrazione si articolerà in vari punti.

Dimostrazione. Possiamo limitarci a dimostrare l'asserto per un intero m libero da quadrati. Pertanto dall'enunciato del teorema e da questa osservazione, si esclude che la classe di resto di m modulo 8 sia 0,4 o 7. Supponiamo che $m = p_1 \cdots p_r$ e analizziamo il caso in cui $m \equiv_8 3$. In particolare quindi $p_1, \ldots, p_r$ sono primi dispari.

(a)

$$\text{Esiste } q \text{ primo tale che } \forall i \quad 1 \leq i \leq r \qquad \left(\frac{-2q}{p_i}\right) = 1 \text{ e } q \equiv_4 1. \tag{4}$$

Richiediamo quindi che $-2q$ sia un residuo quadratico modulo p_i ed, essendo p_i dispari e -2 invertibile modulo p_i, questo equivale a dire che $q \equiv_{p_i} \alpha_i$, per un'opportuna classe di resto α_i. Quindi q deve essere tale che

$$\begin{cases} q \equiv_4 1 \\ q \equiv_{p_1} \alpha_1 \\ \ldots \\ q \equiv_{p_r} \alpha_r \end{cases}.$$

Poiché i p_i sono dispari, per ogni i essi sono coprimi con 4 e inoltre sono anche coprimi tra loro visto che m è libero da quadrati. Si può applicare il teorema cinese del resto e quindi esiste una soluzione β e tutte e sole le soluzioni del sistema sono della forma $\beta + 4kp_1 \cdots p_r = \beta + 4km$. Ora per il teorema di Dirichlet 3.19 ($4m$ e β sono coprimi, visto che β non può essere pari e $\alpha_i \neq 0$) si ha l'esistenza di un primo q della forma $\beta + 4km$, da cui la tesi.

(b)

Esistono due interi b, h con b dispari, tali che $b^2 - 4hq = -m$.

Incominciamo col dimostrare che $\left(\frac{-m}{q}\right) = 1$. Per il punto precedente, si ha che

$$\forall i \qquad \left(\frac{-2q}{p_i}\right) = 1.$$

Quindi,

$$1 = \prod_{i=1}^{r}\left(\frac{-2q}{p_i}\right) = \prod_{i=1}^{r}\left(\frac{-2}{p_i}\right)\left(\frac{q}{p_i}\right) = \left(\frac{-2}{m}\right)\prod_{i=1}^{r}\left(\frac{q}{p_i}\right).$$

Per il Teorema 3.15,

$$\left(\frac{q}{p_i}\right) = (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\left(\frac{p_i}{q}\right) = \left(\frac{p_i}{q}\right),$$

dove nell'ultima uguaglianza abbiamo utilizzato il fatto che $q \equiv_4 1$. Quindi,

$$1 = \left(\frac{-2}{m}\right)\prod_{i=1}^{r}\left(\frac{q}{p_i}\right) = \left(\frac{-2}{m}\right)\prod_{i=1}^{r}\left(\frac{p_i}{q}\right) = \left(\frac{-2}{m}\right)\left(\frac{m}{q}\right),$$

da cui

$$\left(\frac{-2}{m}\right) = \left(\frac{m}{q}\right). \tag{5}$$

Considerando che $q \equiv_4 1$, cioè $\left(\frac{-1}{q}\right) = 1$, si ha

$$\left(\frac{-m}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{m}{q}\right) = \left(\frac{m}{q}\right).$$

Infine

$$\left(\frac{-2}{m}\right) = \left(\frac{-1}{m}\right)\left(\frac{2}{m}\right) = (-1)^{\frac{m-1}{2}}(-1)^{\frac{m^2-1}{8}} = 1,$$

quindi per (5), si ha la tesi.

Esiste perciò $b \in \mathbb{Z}$ con $b^2 \equiv_q -m$, ovvero esiste $h_1 \in \mathbb{Z}$ tale che

$$b^2 - qh_1 = -m.$$

Possiamo supporre senza perdita di generalità che b sia dispari. Infatti se non lo fosse, basta prendere $b+q$ che è un numero dispari e $(b+q)^2 \equiv_q b^2 \equiv_q -m$. Studiando ora l'equazione modulo 4, si osserva che $b^2 \equiv_4 1$ poiché abbiamo supposto b dispari e $m \equiv_4 -1$, visto che $m \equiv_8 3$. Allora si ottiene che $qh_1 \equiv_4 0$ e, dal momento che $4 \nmid q$, $4|h_1$. Quindi esiste $h \in \mathbb{Z}$ tale che $b^2 - 4qh = -m$.

(c)

$$\text{Esiste } t \text{ intero con } t^2 \equiv_m (-2q)^{-1}.$$

Dal primo punto, sappiamo che

$$\forall i \quad 1 \leq i \leq r \qquad \left(\frac{-2q}{p_i}\right) = 1.$$

Questo significa che fissato p_i, esiste s_i, tale che $s_i^2 \equiv_{p_i} -2q$. Sicuramente s_i è invertibile modulo p_i. Infatti se non lo fosse, $p_i|2q$ e quindi si avrebbe $\left(\frac{-2q}{p_i}\right) = 0 \neq 1$.

Chiamiamo $t_i = s_i^{-1}$. Allora

$$t_i^2 \equiv_{p_i} s_i^{-2} \equiv_{p_i} (-2q)^{-1}.$$

Avendo un sistema del tipo

$$\begin{cases} x \equiv_{p_1} (-2q)^{-1} \\ \dots \\ \dots \\ x \equiv_{p_r} (-2q)^{-1} \end{cases}$$

la soluzione esiste (i vari primi sono tra loro coprimi poiché m è libero da quadrati) ed è unica modulo $p_1 \cdots p_r = m$. Sia t tale che per ogni i, $t \equiv_{p_i} t_i$. Allora t^2 è soluzione del sistema, ma anche $(-2q)^{-1}$ è soluzione e quindi per il teorema cinese del resto si conclude che $t^2 \equiv_m (-2q)^{-1}$.

(d) Definiamo ora in $\mathbb{R}^3$ la sfera

$$\mathscr{S} := \{(u, v, w)^T \in \mathbb{R}^3 : u^2 + v^2 + w^2 < 2m\},$$

con volume $\mathrm{Vol}(\mathscr{S}) = \frac{4}{3}\pi(2m)^{\frac{3}{2}}$. Consideriamo poi i tre vettori

$$v_1 = \begin{pmatrix} 2tq \\ \sqrt{2q} \\ 0 \end{pmatrix}, \qquad v_2 = \begin{pmatrix} tb \\ \frac{b}{\sqrt{2q}} \\ \sqrt{\frac{m}{2q}} \end{pmatrix} \qquad v_3 = \begin{pmatrix} m \\ 0 \\ 0 \end{pmatrix}$$

e il reticolo Λ associato. Esso avrà volume $\mathrm{Vol}(\Lambda) = m^{\frac{3}{2}}$.

(e) Per il Teorema di Minkowski 1.11, essendo $2^3 \mathrm{Vol}(\Lambda) < \mathrm{Vol}(\mathscr{S})$, esiste un vettore non nullo $(u, v, w)^T \in \Lambda \cap \mathscr{S}$. Proviamo che

$$u^2 + v^2 + w^2 = m.$$

Per far questo basta provare che tale somma è intera e divisibile per m.

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = xv_1 + yv_2 + zv_3 = \begin{pmatrix} 2xtq + ytb + zm \\ x\sqrt{2q} + \frac{by}{\sqrt{2q}} \\ y\sqrt{\frac{m}{2q}} \end{pmatrix}.$$

Allora

$$\begin{aligned} u^2 + v^2 + w^2 &= (2tqx + tby + mz)^2 + \left(x\sqrt{2q} + \frac{by}{\sqrt{2q}}\right)^2 + \left(y\sqrt{\frac{m}{2q}}\right)^2 \\ &= (4t^2q^2 + 2q)x^2 + \left(t^2b^2 + \frac{b^2+m}{2q}\right)y^2 + m^2z^2 + \\ &+ (4t^2qb + 2b)xy + (4tqm)xz + (2tbm)yz \end{aligned}$$

Ricordando ora che $b^2 + m = 4qh \in \mathbb{Z}$, si ha che tale somma è intera. Per dimostrare che è divisibile per m, osserviamo che per costruzione $t^2 \equiv_m (-2q)^{-1}$. Da cui,

$$\begin{aligned} u^2 + v^2 + w^2 &\equiv_m (-2q + 2q)x^2 + \left(b^2t^2 + \frac{b^2}{2q} + \frac{m}{2q}\right)y^2 + \\ &+ (-2b + 2b)xy \\ &\equiv_m \left(b^2t^2 + \frac{b^2}{2q} + \frac{m}{2q}\right)y^2. \end{aligned}$$

Supponiamo quindi che

$$\left(b^2t^2 + \frac{b^2}{2q} + \frac{m}{2q}\right)y^2 \equiv_m \alpha.$$

Allora, poiché $2q$ è invertibile modulo m, si ottiene che

$$(b^2t^2(2q) + b^2 + m)y^2 \equiv_m 2q\alpha.$$

Poiché $b^2t^2(2q) \equiv_m -b^2$,

$$2q\alpha \equiv_m 0 \qquad \text{cioè} \qquad \alpha \equiv_m 0.$$

Pertanto $(b^2t^2 + \frac{b^2}{2q} + \frac{m}{2q})y^2 \equiv_m 0$ e cioè $u^2 + v^2 + w^2 \equiv_m 0$.

(f) Poniamo

$$R = 2tqx + tby + mz \quad \text{e} \quad \ell = qx^2 + bxy + hy^2.$$

Allora si ha

$$u^2 + v^2 + w^2 = R^2 + 2\ell. \tag{6}$$

Mostriamo ora che 2ℓ si scrive come somma di due quadrati e in particolare per il Lemma 3.2 basta provare che ℓ si scrive come somma di due quadrati. Dimostriamo quindi che se p è un primo e $p^{2k+1}|\ell$ ma $p^{2k+2} \nmid \ell$, allora $p \equiv_4 1$. Distinguiamo due casi:

- $p \nmid m$: Per (6), poiché $p|\ell$, si ha che $m \equiv_p R^2$, cioè $\left(\frac{m}{p}\right) = 1$. Ora:
  - $p = q$: si conclude poiché $q \equiv_4 1$;
  - $p \neq q$: da come è stata definita ℓ, si ha

$$\begin{aligned} 4q\ell &= 4q^2x^2 + 4qbxy + 4qhy^2 \\ &= (2qx + by)^2 + (4qh - b^2)y^2 \\ &= (2qx + by)^2 + my^2 \\ &= e^2 + my^2. \end{aligned}$$

  Quindi $p^{2k+1}|(e^2 + my^2)$.
  Se $y \not\equiv_p 0$, allora y è invertibile e quindi $-m$ è un residuo quadratico modulo p. Dal fatto che $\left(\frac{-m}{p}\right) = 1$, si deduce che $\left(\frac{-1}{p}\right) = \left(\frac{m}{p}\right)$. Ora ricordiamo che $m \equiv_p R^2$, ovvero $\left(\frac{m}{p}\right) = 1$. Pertanto $\left(\frac{-1}{p}\right) = 1$ e infine $p \equiv_4 1$.
  Se $y \equiv_p 0$, allora $p|e$. Quindi $p^2|(e^2 + my^2)$. Chiamando quindi

$$e_1 = \frac{e}{p} \quad \text{e} \quad y_1 = \frac{y}{p},$$

  $p^{2k-1}|(e_1^2 + my_1^2)$. Si può continuare con questo procedimento finché non si arriva ad un certo $e_r = \frac{e}{p^r}$ e $y_r = \frac{y}{p^r}$, con $y_r \not\equiv_p 0$. In tal caso allora, $p^{2t+1}|(e_r^2 + my_r^2)$ e quindi si conclude che $\left(\frac{-m}{p}\right) = 1$, da cui discende come sopra la tesi.

- $p|m$: poiché $p|\ell$ e $m = R^2 + 2\ell$, $p|R^2$ e quindi $p|R$. Inoltre

$$m = R^2 + \frac{1}{2q}[(2qx + by)^2 + my^2]. \tag{7}$$

Quindi $p|(2qx + by)^2 + my^2$. Poiché m è libero da quadrati, $p^2 \nmid m$ ma $p|m$, cioè $p|(2qx + by)$. Ora riprendendo l'equazione (7) si ha

$$2qm = 2qR^2 + (2qx + by)^2 + my^2. \tag{8}$$

Ora poiché p divide $m, (2qx + by)$ e R, si ha

$$2q\frac{m}{p} = 2q\frac{R^2}{p} + \frac{(2qx + by)^2}{p} + \frac{m}{p}y^2.$$

Vedendo questa equazione modulo p, si ottiene

$$2q\frac{m}{p} \equiv_p \frac{m}{p}y^2.$$

Visto che $p^2 \nmid m$, $\frac{m}{p}$ è invertibile modulo p e quindi

$$2q \equiv_p y^2, \text{ cioè } \left(\frac{2q}{p}\right) = 1.$$

Ma $p|m$, quindi per (4) si ha

$$\left(\frac{2q}{p}\right)\left(\frac{-1}{p}\right) = \left(\frac{-2q}{p}\right) = 1 = \left(\frac{2q}{p}\right).$$

Da cui si evince

$$\left(\frac{-1}{p}\right) = 1 \qquad \text{cioè} \qquad p \equiv_4 1.$$

Analizziamo il caso in cui $m \equiv_8 1$ oppure $m \equiv_8 5$. Ragionando come (a) si riesce a trovare il primo q tale che

$$\forall i \quad 1 \le i \le r \qquad \left(\frac{-q}{p_i}\right) = 1 \text{ e } q \equiv_4 1. \tag{9}$$

Successivamente, si può dimostrare che

$$\left(\frac{-m}{q}\right) = 1.$$

Infatti

$$\forall i \qquad \left(\frac{-q}{p_i}\right) = 1.$$

Quindi

$$1 = \prod_{i=1}^{r}\Big(\frac{-q}{p_i}\Big) = \prod_{i=1}^{r}\Big(\frac{-1}{p_i}\Big)\Big(\frac{q}{p_i}\Big) = \Big(\frac{-1}{m}\Big)\prod_{i=1}^{r}\Big(\frac{q}{p_i}\Big).$$

Per il teorema di reciprocità quadratica, visto che $q \equiv_4 1$, si ha $\left(\frac{q}{p_i}\right) = \left(\frac{p_i}{q}\right)$. Quindi

$$1 = \Big(\frac{-1}{m}\Big)\prod_{i=1}^{r}\Big(\frac{p_i}{q}\Big) = \Big(\frac{-1}{m}\Big)\Big(\frac{m}{q}\Big).$$

Da cui $\left(\frac{-1}{m}\right) = \left(\frac{m}{q}\right)$. Poiché $q \equiv_4 1$, $\left(\frac{-1}{q}\right) = 1$, si ha

$$\Big(\frac{-m}{q}\Big) = \Big(\frac{-1}{q}\Big)\Big(\frac{m}{q}\Big) = \Big(\frac{m}{q}\Big).$$

Considerando che

$$\Big(\frac{-1}{m}\Big) = (-1)^{\frac{m-1}{2}} = 1,$$

otteniamo che $\left(\frac{-m}{q}\right) = \left(\frac{m}{q}\right) = 1$. Ragionando come (b)

$$\exists b \in \mathbb{Z} \text{ dispari } \exists h \in \mathbb{Z} \qquad b^2 - qh = -m.$$

Si può infine dimostrare che

$$\exists t \in \mathbb{Z} \ : \ t^2 \equiv_m (-q)^{-1}.$$

Definiamo poi i vettori

$$v_1 = \begin{pmatrix} tq \\ \sqrt{q} \\ 0 \end{pmatrix} \qquad v_2 = \begin{pmatrix} tb \\ \frac{b}{\sqrt{q}} \\ \sqrt{\frac{m}{q}} \end{pmatrix} \qquad \begin{pmatrix} m \\ 0 \\ 0 \end{pmatrix} \tag{10}$$

e il reticolo Λ costruito a partire da tale base di $\mathbb{R}^3$. Consideriamo

$$\mathscr{S} := \left\{ \begin{pmatrix} u \\ v \\ w \end{pmatrix} \ : \ u^2 + v^2 + w^2 < 2m \right\}.$$

Come per il caso $m \equiv_8 3$, si dimostra che preso un qualsiasi vettore in $\Lambda \cap \mathscr{S}$, la somma dei quadrati delle componenti è pari ad m. Per il teorema di Minkowski 1.11 esiste un vettore non nullo

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} = xv_1 + yv_2 + zv_3 \in \Lambda \cap \mathscr{S}$$

e quindi

$$u^2 + v^2 + w^2 = m = R^2 + \ell,$$

$$\text{con} \quad R := (xtq + ytb + zm) \text{ e } \ell := qx^2 + 2bxy + hy^2. \tag{11}$$

Si dimostra infine, con un ragionamento analogo a quanto visto sopra, (basta considerare $q\ell$ laddove si analizzava $4q\ell$) che ℓ si scrive come somma di due quadrati e si giunge alla tesi.

Infine ci dedichiamo al caso in cui $m \equiv_8 2$ oppure $m \equiv_8 6$. In questo caso, poiché m è libero da quadrati ed è pari, si avrà che $m = 2m_1$, con $m_1 = p_1 \cdots p_r$ dispari. Ragionando come sopra possiamo trovare un primo q con $\left(\frac{-q}{p_i}\right) = 1$ e inoltre, se $m \equiv_8 2$, $q \equiv_8 1$, invece se $m \equiv_8 6$, $q \equiv_8 5$. In entrambi i casi comunque $q \equiv_4 1$. Possiamo ora dimostrare che $\left(\frac{-m}{q}\right) = 1$. Utilizzando i risultati sulla reciprocità quadratica, si ha

$$1 = \prod_{i=1}^{r}\left(\frac{-q}{p_i}\right) = \left(\prod_{i=1}^{r}\left(\frac{-1}{p_i}\right)\right)\left(\prod_{i=1}^{r}\left(\frac{q}{p_i}\right)\right) = \left(\frac{-1}{m_1}\right)\prod_{i=1}^{r}\left(\frac{p_i}{q}\right) = \left(\frac{-1}{m_1}\right)\left(\frac{m_1}{q}\right).$$

Quindi $\left(\frac{-1}{m_1}\right) = \left(\frac{m_1}{q}\right)$. Poiché $q \equiv_4 1$, $\left(\frac{-m_1}{q}\right) = \left(\frac{m_1}{q}\right)$. Infine

$$\left(\frac{-m}{q}\right) = \left(\frac{-2}{q}\right)\left(\frac{m_1}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{2}{q}\right)\left(\frac{-1}{m_1}\right) = (-1)^{\frac{q-1}{2}}(-1)^{\frac{q^2-1}{8}}(-1)^{\frac{m_1-1}{2}} = 1.$$

Esistono quindi $b \in \mathbb{Z}$ e $h \in \mathbb{Z}$ con $b^2 - qh = -m$. Analogamente a quanto visto sopra, esiste $t \in \mathbb{Z}$ tale che $t^2 \equiv_m (-q)^{-1}$. Si definiscono poi i vettori come in (10) e si applica il teorema di Minkowski 1.11. Si ha quindi un vettore non nullo

$$\begin{pmatrix} u \\ v \\ w \end{pmatrix} \in \Lambda \cap \mathscr{S} : u^2 + v^2 + w^2 = m = R^2 + \ell,$$

con ℓ ed R definite come in (11). Si conclude dimostrando che ℓ si scrive come somma di 2 quadrati. □

Possiamo ora fornire inoltre un'altra dimostrazione del Teorema 3.10 utilizzando il Teorema 3.18.

Teorema 3.10. Per il teorema 3.18 i numeri non del tipo $4^a(8b + 7)$ si scrivono come somma di tre quadrati e pertanto anche come somma di quattro quadrati (dal momento che $0 = 0^2$). Basta quindi dimostrare che i numeri $n = 4^a(8b + 7)$ si scrivono come somma di quattro quadrati. Infatti

$$n = 4^a(8b + 7) = 4^a(8b + 6) + 4^a = m + (2^a)^2,$$

con $m = 4^a(8b + 6)$. In particolare m si scrive come somma di tre quadrati, da cui la tesi. $\square$

4 Bibliografia

Riferimenti bibliografici

[1] G.H. Hardy e E.M. Wright, *An introduction to the Theory of Numbers*. Oxford University, 1960.

[2] J.W.S Cassels, *Rational Quadratic Forms*. Academic Press Inc. (London) LTD., 1978.

[3] Ramin Takloo-Bighash, *A Pythagorean Introduction to Number Theory*. Springer, 2018.