Università degli Studi di Salerno

FACOLTÀ DI SCIENZE MATEMATICHE, FISICHE E NATURALI
Corso di Laurea in Matematica

Decomposizione di Interi in Somme di Potenze

Tesi di Laurea in Teoria dei Numeri

Relatore:
Chiar.ma Prof.
P. Longobardi

Candidato:
Matr. 0510100229
Dino Festi

Anno Accademico
2009/2010

Indice

Sommario

Scopo del lavoro è lo studio di come e quando un intero può essere rappresentato come somma di potenze k-esime, con k intero positivo.

Nel primo capitolo studiamo le n–ple pitagoriche, che sono la naturale generalizzazione delle terne pitagoriche: definiamo infatti $(n+1)$–pla pitagorica una $(n+1)$–pla di numeri interi $(x_1, \ldots, x_n, y)$ tali che $x_1^2 + \ldots + x_n^2 = y^2$.
Mediante alcune considerazioni riusciamo a dare una completa parametrizzazione delle $(n+1)$–ple pitagoriche. Abbiamo infatti che:

$$\begin{aligned} vx_i &= 2u_n u_i \qquad\qquad i = 1, \ldots, n-1 \\ vx_n &= u_1^2 + \cdots + u_{n-1}^2 - u_n^2 \\ vy &= u_1^2 + \cdots + u_n^2 \end{aligned}$$

con $u_n^2 < u_1^2 + \ldots + u_{n-1}^2$ e $v = MCD(2u_1u_n, \ldots, 2u_{n-1}u_n, u_1^2 + \ldots + u_{n-1}^2 - u_n^2)$. Tale parametrizzazione risulta inoltre essere anche unica al variare dei parametri $u_1, u_2, \ldots, u_n$, a meno di un fattore moltiplicativo.

Nel secondo Capitolo ci concentriamo sullo studio della rappresentazione degli interi come somma di quadrati. Il Capitolo si apre con un' identità, nota come identità di Fibonacci–Brahmagupta, che afferma che se due numeri possono essere rappresentati come somma di due quadrati, tale è il loro prodotto. Questo risultato ci consente di limitare il nostro studio ai numeri primi. Il Teorema 2.1 ci fornisce un' importante informazione in tal senso, affermando che tutti i primi della forma $4k+1$ e 2 possono essere scritti come somma di due quadrati, invece i primi della forma $4k+3$ non possono essere rappresentati in tal modo. Di questo Teorema, provato ora con considerazioni sulle involuzioni, secondo l' idea di Zagier del 1990, forniremo anche una dimostrazione alternativa nel Capitolo 6. Dopo aver visto che tutti e soli gli interi nella cui fattorizzazione canonica non compaiono primi della forma $4k+3$ elevati a potenze dispari possono essere scritti come somma di due quadrati, mostriamo che esistono infiniti interi che non possono essere scritti come somma di meno di quattro quadrati: questi numeri sono tutti i numeri della forma $4^n(8k+7)$. Attraverso l' utilizzo di due lemmi (uno dei quai dovuto a Eulero) riusciamo poi a dimostare il Teorema 2.7, che afferma che ogni numero primo si può rappresentare come somma di al più quattro quadrati. Da tale Teorema, grazie all' identità di Fibonacci–Brahmagupta che ci assicura che il prodotto di due numeri che sono somma di quattro quadrati è anch'esso somma di quattro quadrati, deriva dunque che tutti gli interi possono essere rappresentati mediante al più quattro quadrati. Tale

affermazione costituisce il Teorema 2.8 (dovuto a Lagrange), che è il Teorema conclusivo del capitolo.

Lo studio degli interi come somme di quarte potenze è invece trattato nel terzo Capitolo, che si apre fornendo una stima superiore del numero di quarte potenze necessarie a rappresentare ogni intero (Teorema 3.1): tale stima è ottenuta utlizzando i risultati presentati nel Capitolo 2, in particolare utilizzando il Teorema 2.8, e afferma che 53 quarte potenze sono sufficienti a rappresentare qualsiasi intero; il Teorema 3.2 ci fornisce invece una stima inferiore, affermando che i numeri della forma $16^n \cdot 31$ non possono essere rappresentati mediante meno di 16 quarte potenze.

Nel quarto Capitolo introduciamo la Congettura di Waring, secondo la quale per ogni intero k esite un intero, indicato con $g(k)$, tale che ogni intero può essere rappresentato mediante al più $g(k)$ k-esime potenze. La congettura è stata provata da Hilbert nel 1909. Nel Capitolo introdurremo anche la funzione $G(k)$, definita come il minimo numero di potenze k–esime necessario a rappresentare ogni intero sufficientemente grande. Nel capitolo sono forniti alcuni risultati riguardanti le stime di $g(k)$ e $G(k)$, le più importanti delle quali sono quelle dovute a Eulero e Vaughan:

$$g(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2$$

e

$$G(k) < k(3 \lg k + 4.2)$$

rispettivamente.

Dopo aver trattato la rappresentazione degli interi solo come somma di potenze, nel Capitolo 5 trattiamo invece la rappresentazione degli interi come somma e differenze di potenze, e indichiamo con $w(k)$ il numero minimo di potenze k–esime necessarie a rappresentare in tal modo ogni intero. Banalmente $w(k) \leq g(k)$, e pertanto dalla dimostrazione della congettura di Waring deriva l' esistenza anche di $w(k)$. Nel capitolo riusciamo a determinare $w(2) = 3$, mentre riusciamo solo a dare una stima (per quanto precisa) di $w(3)$: ovvero che $4 \leq w(3) \leq 5$.

Nel Capitolo 6 trattiamo invece la Teoria dei Reticoli Geometrici: sfrutteremo alcuni risultati raggiunti in tale ramo per dare una dimostrazione alternativa del Teorema 2.1. Per definire un reticolo dobbiamo considerare nel piano due rette non parallele, r e s, e due distanze, d_1 e d_2; consideriamo quindi la famiglia delle rette parallele a r e distanti da r un multiplo intero della distanza d_1; analogamente consideriamo la famiglia delle rette parallele a s e distanti da s un multiplo intero della distanza d_2. Chiamiamo queste rette *fili* del reticolo. Le intersezioni dei fili determinano i *punti* del reticolo. I parallelogrammi determinati da coppie di fili del reticolo vicine si diranno *parallelogrammi base*. Se, dato

un sistema di riferimento cartesiano del piano, supponiamo che l' origine $O = (0, 0)$ sia un punto del reticolo, e che $OABC$ sia un parallelogrammo base, e definiamo $\vec{p} = (k, l)$ e $\vec{q} = (m, n)$ come i vettori determinati dai lati OA e OC, allora otteniamo che i punti del reticolo sono tutti e soli i punti determinati dal vettore $\vec{r} = u \cdot \vec{p} + v \cdot \vec{q}$, con u e v interi, che possono essere espressi anche come i punti (x, y) del piano reale tale che:

$$(x, y) = u(k, l) + v(m, n) = (uk + vm, ul + vn).$$

Dopo questo risultato vengono fornite alcune proprietà dei Reticoli Geometrici, fino ad arrivare ad enunciare il Teorema 6.2, che consente di calcolare l' area di un qualunque poligono del reticolo conoscendo solamente quanti punti del reticolo sono al suo interno e quanti sul suo perimetro. Dopo tale Teorema dimostriamo il Teorema 6.3, dovuto a Minkowsky, che è uno dei più importanti nella Teoria dei Reticoli Geometrici, e che afferma che:
I) In un reticolo di punti nel quale i parallelogrammi base hanno area d, ogni regione convessa, centrata in un punto del reticolo e simmetrica rispetto al suo centro, con area maggiore di 4d, contiene almeno un altro punto del reticolo al suo interno oltre al suo centro.
II) Se l' area della regione è esattamente 4d, allora oltre al suo centro c'è sicuramente un altro punto del reticolo al suo interno o sulla sua frontiera.
Come applicazione del Teorema di Minkowski riusciamo a dimostrare la Proposizione 6.5, che afferma che in ogni reticolo di punti esiste sempre un punto del reticolo diverso dall' origine interno alla circonferenza descritta dall' equazione $x^2 + y^2 = \frac{4d}{\pi}$ con d che rappresenta l' area del parallelogramma base del reticolo.
Questa Proposizione, insieme alla Proposizione 6.4, ci consente di dare una dimostrazione alternativa del Teorema 2.1, presentato nel Capitolo 2.

Nel settimo e ultimo Capitolo concentriamo la nostra attenzione su una particolare classe di equazioni diofantee: le equazioni del tipo

$$y^n = x_1^n + \ldots + x_n^n$$

che possono essere viste come una generalizzazione alternativa delle terne pitagoriche. Nel capitolo presentiamo alcune soluzioni per n che va da 3 a 9. In particolare è presente la parametrizzazione delle soluzioni nel caso $n = 3$ e $n = 5$. Inoltre si fornisce l' unica soluzione conosciuta per $n = 8$, mentre non si riesce a fornire alcuna soluzione per $n = 6$ e $n = 9$.

Capitolo 1

n–ple pitagoriche

Con $n \geq 2$ una $(n+1)$–pla $(x_1, \ldots, x_n, y)$ di numeri interi é detta pitagorica se $x_1^2 + \ldots + x_n^2 = y^2$, in piú é detta primitiva se $MCD(x_1, \ldots, x_n, y) = 1$. Cercheremo ora di fornire una parametrizzazione completa delle $(n+1)$–ple pitagoriche. Consideriamo dunque

$$x_1^2 + \ldots + x_n^2 = y^2 \tag{1.1}$$

con $x_1, \ldots, x_n, y > 0$ e $MCD(x_1, \ldots, x_n, y) = 1$; avremo che $x_1^2 + \ldots + x_{n-1}^2 = y^2 - x_n^2$ e quindi

$$x_1^2 + \ldots + x_{n-1}^2 = (y - x_n)(y + x_n) \tag{1.2}$$

Sia ora d il massimo comune divisore di $x_1, \ldots, x_{n-1}, y - x_n$, esisteranno allora degli interi u_i tali che $x_i = du_i$ per ogni $i = 1, \ldots, n-1$ e $y - x_n = du_n$, con $MCD(u_1, \ldots, u_n) = 1$. Da ció deriva che $y + x_n = y - x_n + 2x_n = du_n + 2x_n$. Possiamo dunque scrivere la (1.2) come

$$d^2(u_1^2 + \ldots + u_{n-1}^2) = du_n(du_n + 2x_n) \tag{1.3}$$

ossia

$$d(u_1^2 + \ldots + u_{n-1}^2) = u_n(du_n + 2x_n) \tag{1.4}$$

Da $y + x_n = -(y - x_n) + 2y = 2y - du_n$ segue poi

$$d(u_1^2 + \ldots + u_{n-1}^2) = u_n(du_n + 2x_n) = u_n(2y - du_n) \tag{1.5}$$

Abbiamo dunque le seguenti due uguaglianze

$$2u_n x_n = d(u_1^2 + \ldots + u_{n-1}^2 - u_n^2) \tag{1.6}$$

$$2u_n y = d(u_1^2 + \ldots + u_{n-1}^2 + u_n^2) \tag{1.7}$$

Notiamo ora che x_n e d sono coprimi, in quanto un divsore comune c é anche divisore di $x_n, x_1, \ldots, x_{n-1}, y$, divide anche il massimo comune divisore di $x_1, \ldots, x_n, y$ che é 1 per ipotesi. Sicché c divide 1, possiamo allora concludere che $c = 1$. Dalla (1.6) possiamo allora dedurre che x_n divide $u_1^2 + \ldots + u_{n-1}^2 - u_n^2$, esiste dunque un naturale v tale che

$$vx_n = u_1^2 + \ldots + u_{n-1}^2 - u_n^2 \tag{1.8}$$

per cui la (1.6) comporta che:

$$2u_n = dv \tag{1.9}$$

Ora, ricordando che per ogni $i = 1, \ldots, n-1$ riesce che $x_i = du_i$, avremo che

$$vx_i = vdu_i = 2u_n u_i \quad i = 1, \ldots, n-1 \tag{1.10}$$

Moltiplicando per v la (1.7) e utilizzando la (1.9) avremo che $2vu_n y = vd(u_1^2 + \cdots + u_{n-1}^2 + u_n^2) = 2u_n(u_1^2 + \cdots + u_{n-1}^2 + u_n^2)$, dividendo per $2u_n$ il primo e l' ultimo termine dell' uguaglianza riesce dunque

$$vy = u_1^2 + \cdots + u_{n-1}^2 + u_n^2 \tag{1.11}$$

Abbiamo dunque ottenuto le seguenti relazioni:

$$vx_i = 2u_n u_i \qquad i = 1, \ldots, n-1 \tag{1.12}$$
$$vx_n = u_1^2 + \cdots + u_{n-1}^2 - u_n^2 \tag{1.13}$$
$$vy = u_1^2 + \cdots + u_n^2 \tag{1.14}$$

Dalla (1.13) deriva che $u_n^2 < u_1^2 + \cdots + u_{n-1}^2$ in quanto $v, x_n > 0$. Quindi scegliendo $u_1, \ldots, u_n$ che soddisfino tale condizione e prendendo v tale che sia il massimo comune divisore di $2u_1u_n, \ldots, 2u_{n-1}u_n, u_1^2 + \cdots + u_{n-1}^2 - u_n^2$ otteniamo $x_1, \ldots, x_n, y$ che soddisfino la (1.1) e tali che il loro massimo comune divisore sia 1.

Per esempio, scelti $n = 4, u_1 = 2, u_2 = 3, u_3 = 6$ e $u_4 = 5$, con tale procedimento resta individuata la quintupla pitagorica $(10, 15, 30, 12, 34)$.

Mostriamo ora che una soluzione é individuata da una sola sequenza di interi, dato il loro rapporto: $u_1 : u_2 : \cdots : u_n$ (quindi a meno di un fattore moltiplicativo). Poiché ci interessano solo i rapporti possiamo porre $x_i := u_i$ per ogni $i = 1, \ldots, n-1$, troveremo poi l' appropriato u_n. Dalla posizione fatta e dalla (1.12) deriva che:

$$vx_i = 2u_n x_i,\ i = 1, \ldots, n-1 \tag{1.15}$$

e quindi:

$$v = 2u_n \tag{1.16}$$

Andando quindi a sostituire nella (1.13) otteniamo che

$$2u_n x_n = x_1^2 + \cdots + x_{n-1}^2 - u_n^2 = y^2 - x_n^2 - u_n^2$$

E dunque abbiamo che

$$0 = y^2 - x_n^2 - u_n^2 - 2u_n x_n = y^2 - (x_n + u_n)^2 = (y - x_n - u_n)(y + x_n + u_n)$$

da cui

$$u_n = y - x_n \quad \text{oppure} \quad u_n = -y - x_n$$

Poiché u_n é un intero é positivo, possiamo conludere che $u_n = y - x_n$. Abbiamo dunque raggiunto il seguente risultato:

Teorema 1.1. *Tutte le soluzioni intere dell' equazione $x_1^2 + \cdots + x_n^2 = y^2$ sono date dalle formule:*

$$\begin{aligned} vx_i &= 2u_n u_i \qquad i = 1, \ldots, n-1 \\ vx_n &= u_1^2 + \cdots + u_{n-1}^2 - u_n^2 \\ vy &= u_1^2 + \cdots + u_n^2 \end{aligned}$$

con $u_n^2 < u_1^2 + \ldots + u_{n-1}^2$ e $v = MCD(2u_1u_n, \ldots, 2u_{n-1}u_n, u_1^2 + \ldots + u_{n-1}^2 - u_n^2)$, e sono uniche al variare del sistema dei parametri $u_1, u_2, \ldots, u_n$ a meno di un fattore moltiplicativo.

Capitolo 2

Interi come somme di quadrati

In questa sezione studieremo quando un intero si puó scrivere come somma di quadrati, iniziando con lo studio degli interi che si possono scrivere come somma di soli due quadrati.
Consideriamo a tal fine la seguente identitá, nota come identitá di Fibonacci – Brahmagupta, ma forse nota giá a Diofanto nel III secolo:

$$(x^2 + y^2)(u^2 + v^2) = (xu - yv)^2 + (xv - yu)^2$$

Questa identitá ci dice che se due numeri sono rappresentabili come somma di due quadrati, allora lo é anche il loro prodotto. Questo discorso si puó ovviamente ampliare a un numero n di interi. Possiamo dunque considerare dapprima solo i numeri primi. Dobbiamo allora chiederci quando un numero primo é rappresentabile come somma di due quadrati.
A tal proposito esiste un risultato completo, che enunciamo e dimostriamo di seguito mediante considerazioni sulle involuzioni secondo l' idea di Zagier del 1990, ma di cui forniremo anche una dimostrazione alternativa nel Capitolo 6 (Teorema 6.6).

Teorema 2.1. *Tutti i primi della forma $4k + 1$ e 2 possono essere scritti come somma di due quadrati. I primi della forma $4k + 3$ non possono essere scritti in questo modo.*

Dimostrazione. L' ultima affermazione é ovvia. Per dimostrarla basta osservare che il quadrato di un numero dispari é congruo 1 modulo 4, mentre il quadrato di un numero pari é congruo 0 modulo 4. Quindi la somma di due quadrati puó essere congrua 0, 1 o 2, ma mai 3 modulo 4; pertanto i numeri della forma $4k + 3$ (che sono congrui 3 modulo 4) non possono essere scritti come somma di due quadrati. Anche il fatto che 2 si puó

scrivere come somma di due quadrati é banale, in quanto $2 = 1^2 + 1^2$.
Ci rimane da dimostrare che tutti i primi della forma $4k + 1$ possono essere scritti come somma di due quadrati. Per farlo ripercorreremo la dimostrazione trovata da Zagier nel 1990, in cui é fondamentale il concetto di involuzione.
Dati un insieme M e un' applicazione σ di M in M, tale applicazione si dirá un' involuzione se e soltanto se $\sigma(\sigma(x)) = x$ per ogni x in M. Quindi un' involuzione é un' applicazione biettiva e coincide con la sua inversa; per esempio ogni simmetria è un' involuzione.
Un' involuzione ripartisce gli elementi dell' insieme su cui è definita in sottoinsiemi di ordine minore o uguale di 2: possiamo infatti associare all' elemento m l' elemento $\sigma(m)$; notiamo che il sottoinsieme ottenuto da m è lo stesso di quello ottenuto da $\sigma(m)$, poichè $\sigma(\sigma(m)) = m$; notiamo inoltre che un tale sottoinsieme ottenuto da m ha ordine 1 solo se $\sigma(m) = m$, ovvero solo se m è fissato da σ. Da ciò possiamo dedurre che, data un' involuzione su un insieme finito M, il numero di elementi fissati dall' involuzione è pari (dispari) se anche il numero degli elementi di M è pari (dispari), in quanto gli altri elementi, quelli non fissati, sono sicuramente in numero pari, poichè raggruppati in sottoinsiemi di ordine 2.
A questo punto lo schema della dimostrazione di Zagier è il seguente: dato p primo, consideriamo l' insieme delle soluzioni intere dell' equazione

$$x^2 + 4yz = p. \tag{2.1}$$

Ci basta provare che se p è della forma $4k + 1$ allora l' equazione ammette una soluzione per cui $y = z$, infatti in tal caso $p = x^2 + (2y)^2$.
Una soluzione per cui $z = y$ è un elemento fissato dall' involuzione σ sull' insieme delle soluzioni dell' equazione (2.1) , con σ definita come:

$$\sigma(x, y, z) = (x, z, y). \tag{2.2}$$

A questo punto ci basta provare che il numero delle soluzioni è dispari, perchè in tal caso esisterà sicuramente un elemento fissato da σ.
A tal scopo consideriamo l' involuzione τ sull' insieme delle soluzioni della (2.1), definita come segue:

$$\tau(x, y, z) = \begin{cases} (x + 2z, z, y - x - z) & \text{se } x < y - z \\ (2y - x, y, x - y + z) & \text{se } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{se } 2y < x \end{cases}$$

Si può dimostrare che tale applicazione è ben definita ed è un' involuzione. Per prima cosa notiamo che $x \neq 2y$ e $x \neq y - z$, perchè altrimenti avremmo che

$$p = x^2 + 4yz = 4y^2 + 4yz = 4y(y + z) \tag{2.3}$$

oppure

$$p = x^2 + 4yz = (y - z)^2 + 4yz = (y + z)^2 \tag{2.4}$$

che sono due eventualità impossibili a verificarsi, in quanto p è primo. Verifichiamo inoltre che ogni soluzione della (2.1) viene portata in una soluzione da τ; questo deriva dalle identità:

$$(x + 2z)^2 + 4z(y - x - z) = x^2 + 4yz \tag{2.5}$$

$$(x - 2y)^2 + 4y(x - y + z) = x^2 + 4yz \tag{2.6}$$

Sia ora $\tau(x, y, z) = (x', y', z')$.
Se $x < y - z$, allora $x' = x + 2z > 2z = 2y'$. Quindi una soluzione del primo tipo diventa una soluzione del terzo tipo.
Analogamente si prova che una soluzione del terzo tipo viene portata in una soluzione del primo tipo e che una soluzione del secondo tipo rimane una soluzione del secondo tipo. Per questo motivo soluzioni del primo e terzo tipo non possono essere fissati da τ , dobbiamo allora cercate eventuali soluzioni fissate da τ tra le soluzioni del secondo tipo. Una soluzione che sia fissata deve soddisfare il fatto che $z = z' = x - y + z$ da cui si ha che $x - y = 0$ e quindi che $x = y$. In tal caso $p = x^2 + 4yz = x(x + 4z)$ da cui, poichè p è primo, si ha che $x = y = 1$.
Se $p = 4k + 1$ allora $(1, 1, k)$ è una soluzione fissata (ed è anche l' unica, per quanto visto). Esiste dunque un solo elemento fissato da τ nell' insieme delle soluzioni intere dell' equazione (2.1), e pertanto le soluzioni sono in numero dispari. Con ciò abbiamo completato la dimostrazione. □

Un numero non divisibile da primi della forma $4k+3$ sarà allora rappresentabile come somma di due quadrati. Se consideriamo un siffatto numero e lo si moltiplica per un quadrato arbitrario, avremo che il prodotto sarà ancora rappresentabile mediante somma di due quadrati, infatti se $n = a^2 + b^2$ allora $nm^2 = (a^2+b^2)m^2 = (am)^2+(bm)^2$. Notiamo che tale prodotto può essere divisibile per primi della forma $4k + 3$, ma compariranno elevati a potenze pari (in quanto derivano dal quadrato). Otteniamo dunque che se nella fattorizzazione canonica di un intero n non compaiono primi della forma $4k + 3$ elevati a potenze dispari, allora n si può scrivere come somma di due quadrati.

Il primo a dimostrare che tale condizione è anche necessaria fu Eulero.

Diamo ora una proposizione che ci consentirà di illustrare il risultato ottenuto da Eulero:

Proposizione 2.2. *Siano a e b numeri naturali, allora $a^2 + b^2$ non ammette divisori della forma $4k - 1$ coprimi con a e b.*

Dimostrazione. Consideriamo un numero naturale della forma $4k-1$ che ha un multiplo che si può scrivere come somma di due quadrati le cui basi sono coprime con $4k - 1$. Sia c il più piccolo di questi numeri e sia $a_1^2 + b_1^2$ il suo multiplo, con a_1 e b_1 naturali coprimi con c. Sia a_1 che b_1 distano al più $\frac{c}{2}$ dal più vicino multiplo di c, quindi esistono degli interi q, r, a_2, b_2 tali che $a_1 = cq + a_2$ e $b_1 = cr + b_2$ con $|a_2|, |b_2| \leq \frac{c}{2}$. Notiamo che poichè c è coprimo con a_1 e b_1, a_2 e b_2 sono diversi da zero. Abbiamo dunque che $0 < a_1^2 + b_1^2 = (cq + a_2)^2 + (cr + b_2)^2 = c(cq^2 + cr^2 + 2qa_2 + 2rb_2) + (a_2^2 + b_2^2)$.
Ma c divide $a_1^2 + b_1^2$ e anche $c(cq^2 + cr^2 + 2qa_2 + 2rb_2)$, quindi c divide la loro differenza, ovvero c divide $a_2^2 + b_2^2$. Ma notiamo ora che a_2 e b_2 sono coprimi con c: infatti il massimo comune divisore tra a_2 e c dividerà anche a_1 (per la scelta di a_2), ma quindi, dividendo sia c che a_2, dividerà anche il massimo comun divisore di a_1 e c, che è 1, in quanto c e a_1 sono coprimi; pertanto anche il massimo comun divisore tra a_2 e c deve essere 1; discorso analogo per b_2.
Sia ora d il massimo comune divisore di a_2 e b_2, esisteranno dunque due interi a_3 e b_3 tali che $a_2 = da_3$ e $b_2 = db_3$, con a_3 e b_3 coprimi. Poichè c è coprimo sia con a_2 che con b_2 avremo che c è coprimo anche con d, ma c divide $a_2^2 + b_2^2 = d^2(a_3^2 + b_3^2)$, pertanto c deve dividere $a_3^2 + b_3^2$; esiste dunque un intero c' tale che $a_3^2 + b_3^2 = cc'$. È ovvio che $|a_3| \leq |a_2|$ e $|b_3| \leq |b_2|$, e dunque segue che $cc' = a_3^2 + b_3^2 \leq a_2^2 + b_2^2 \leq \frac{c^2}{4} + \frac{c^2}{4} < c^2$ da cui si ha che $c' < c$.
Mostriamo ora che c' ha un divisore della forma $4k - 1$. Ricordiamo che il quadrato di un numero pari è divisibile per 4, e il quadrato di un numero dispari è congruo 1 modulo 8. Poichè a_3 e b_3 sono coprimi almeno uno di loro deve essere dispari; allora $a_3^2 + b_3^2$ è della forma $4m + 1$ oppure $8m + 2$ rispettivamente se uno dei due è pari o sono entrambi dispari. Abbiamo allora che l' uguaglianza $cc' = a_3^2 + b_3^2$ può valere solo se anche c' è della forma $4k - 1$ (nel primo caso) o della forma $2(4k - 1)$ (nel secondo caso). Inoltre c' è coprimo con a_3 e b_3, poichè se ne dividesse uno, dividendo anche la somma dei loro quadrati, dovrebbe dividere anche l' altro mentre a_3 e b_3 sono coprimi. Possiamo dunque concludere che c' (o $\frac{c'}{2}$) è un intero minore di c, della forma $4k - 1$ che divide la somma di due quadrati le cui basi sono coprime con c' (o $\frac{c'}{2}$). Questo contraddice il fatto che c sia il minimo di questi numeri. Siamo giunti un assurdo, pertanto un siffatto c non esiste. □

Teorema 2.3. *Tutti e soli i numeri nella cui fattorizzazione canonica non appaiano primi della forma* $4k+3$ *elevati a potenze dispari possono essere scritti come somma di due quadrati.*

Dimostrazione. Siano a e b naturali e sia c il loro massimo comune divisore positivo, allora esistono interi a_1, b_1 tali che $a = ca_1, b = cb_1$ con a_1 e b_1 coprimi. Abbiamo dunque che $a^2 + b^2 = c^2(a_1^2 + b_1^2)$. Notiamo che un primo della forma $4k+3$ (cioè un primo della forma $4k-1$) non può dividere la somma $a_1^2 + b_1^2$ altrimenti dovrebbe essere divisore di uno dei due termini (per la Proposizione precedente), e quindi anche dell' altro; di conseguenza questo primo dividerebbe il massimo comune divisore di a_1 e b_1, che sono coprimi, dovrebbe quindi dividere 1, il che è impossibile. Pertanto la massima potenza di un siffato primo che divida la somma $a^2 + b^2$ deve essere la stessa che divide c^2, e deve quindi essere pari. □

Notiamo che la condizione espressa nel teorema precedente è abbastanza restrittiva, in quanto ci sono infiniti numeri che non la soddisfano; inoltre tali numeri ricorrono spesso tra i naturali.

Cosa accade se aumentiamo il numero di quadrati? Attraverso facili controesempi (per esempio notando che 7 si può scrivere solo come $2^4+1^4+1^4+1^4$) si può dedurre che 3 quadrati non sono ancora abbastanza per rappresentare tutti gli interi, ma si ottengono comunque delle informazioni. Nel caso della somma di due quadrati abbiamo trovato utile studiare il residuo dei quadrati modulo 4; nel caso della somma di 3 quadrati è utile studiare il residuo dei quadrati modulo 8: il quadrato di un numero pari è divisibile per 4, quindi sarà congruo 0 o 4 modulo 8, il quadrato di un numero dispari invece sarà sempre congruo 1 modulo 8: infatti sia $n = 2k+1$ con k naturale, allora $n^2 = 4k^2 + 4k + 1 = 4k(k+1) + 1 \equiv 1 (mod\, 8)$. Da queste osservazioni possiamo dunque concludere che:

- la somma dei quadrati di tre numeri pari è congrua 4 o 0 modulo 8;
- la somma dei quadrati di due numeri pari e uno dispari è congrua 1 o 5 modulo 8;
- la somma dei quadrati di un numero pari e due dispari è congrua 2 o 6 modulo 8;
- la somma dei quadrati di tre numeri dispari è congrua 3 modulo 8.

Vediamo dunque che la somma di 3 quadrati non può mai essere congrua 7 modulo 8. Dunque tutti i numeri della forma $8k+7$ non possono essere rappresentati come somma di 3 quadrati. In particolare vale il seguente teorema:

Teorema 2.4. *Tutti i numeri della forma $4^n(8k+7)$, con n e k interi non negativi, non possono essere scritti come somma di tre quadrati.*

Dimostrazione. Sia $N = 4^n(8k+7)$ somma di tre quadrati, con n il più piccolo esponente per cui ciò è vero. Per il ragionamento precedente si ha che $n > 0$, quindi N sarà divisibile per 4, Sempre per quanto detto precedentemente possiamo dunque affermare che N è la somma dei quadrati di tre numeri pari, a, b, c. Sia allora $N' := (\frac{a}{2})^2 + (\frac{b}{2})^2 + (\frac{c}{2})^2 = \frac{N}{4} = 4^{n-1}(8k+7)$. Ma allora N' è la somma di tre quadrati con $n-1 < n$, il che è in contraddizione con l' ipotesi iniziale che n è il più piccolo esponente per cui ciò accade. Abbiamo dunque raggiunto un assurdo; pertanto non esiste un siffatto N. □

Gauss provò che tutti i numeri che non hanno quella forma possono essere scritti come somma di tre quadrati, ma la dimostrazione è molto complicata. Lagrange fu il primo a dimostrare che ogni numero intero può essere scritto come somma di 4 quadrati. Dopo di lui ci sono state varie dimostrazioni, noi ne presenteremo una che farà uso dei seguenti lemmi:

Lemma 2.5 (Eulero). *Dato un primo p, esistono interi x, y tali che*
$x^2 + y^2 + 1 \equiv 0 (mod\, p)$

Dimostrazione. Supponiamo $p > 3$ (il caso $p = 2, 3$ è banale). Consideriamo le seguenti successioni di $\frac{p+1}{2}$ termini:

$$1, 1^2 + 1, 2^2 + 1, \ldots, (\frac{p-1}{2})^2 + 1$$

e

$$0, -1^2, -2^2, \ldots, -(\frac{p-1}{2})^2$$

L' unione dei sostegni delle due successioni è composto da $p+1$ elementi, pertanto ce ne devono essere almeno 2 congrui modulo p. Due elementi appartenenti alla stessa successione non possono essere congrui: infatti se così fosse avremmo due interi x_1, x_2 tali che $|x_i| \leq \frac{p-1}{2}$ con $i = 1, 2$ e $x_1^2 + 1 \equiv x_2^2 + 1 (mod\, p)$ oppure $-x_1^2 \equiv -x_2^2 (mod\, p)$. Entrambe queste congruenze sono equivalenti a

$$x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2) \equiv 0 (mod\, p)$$

Poichè p è primo tale equazione è soddisfatta soltanto se $x_1 \equiv \pm x_2 (mod\, p)$. Ma questo è impossibile poichè $0 < |x_1 - x_2| < \frac{p-1}{2}$ e $0 < x_1 + x_2 < p - 1$. Quindi i due elementi appartengono a sequenze differenti. Esistono dunque interi x e y tali che $x^2 + 1 \equiv -y^2 (mod\, p)$ cioè tali che $x^2 + y^2 + 1 \equiv 0 (mod\, p)$. □

Lemma 2.6. *Siano m e r interi maggiori di 1 e si considerino r espressioni lineari $L_i(u_1, \ldots, u_k) = a_{i,1}u_1 + \cdots + a_{i,k}u_k$ con $k > r$ e $a_{i,j}$ intero con $i = 1, \ldots, r$ e $j = 1, \ldots, k$. Siano inoltre $h_1, \ldots, h_k$ numeri reali positivi tali che $h_1 \cdot h_2 \cdot \ldots \cdot h_k \geq m^r$, allora il sistema*

$$\begin{cases} L_1(u_1, \ldots, u_k) \equiv 0 (mod\, m) \\ \vdots \\ L_r(u_1, \ldots, u_k) \equiv 0 (mod\, m) \end{cases}$$

ammette una soluzione intera $(\bar{u_1}, \ldots, \bar{u_k}) \neq (0, \ldots, 0)$ tale che $|\bar{u_i}| \leq h_i$ con $i = 1, \ldots, k$

Dimostrazione. La dimostrazione è simile a quella del Lemma 2.5. Consideriamo la sequenza di r–uple di numeri

$$L_1, L_2, \ldots, L_r$$

dove

$$L_i = L_i(z_1, \ldots, z_k)$$

e per ogni $i = 1, \ldots, k$ ogni z_i assume tutti i valori tra 0 e $[h_i]$. Dalle ipotesi abbiamo che

$$([h_1] + 1)([h_2] + 1) \ldots ([h_k] + 1) > h_1 \cdot \ldots \cdot h_k \geq m^r$$

Se consideriamo i resti delle componenti delle r–ple ci sono m^r possibili valori, e quindi ci sono più r–ple che possibili combinazioni, pertanto ci devono essere due r–ple tali che le loro componenti abbiano lo stesso resto modulo m, cioè esistono due r–ple congrue modulo m. Siano queste due r–ple corrispondenti ai parametri $z_1, \ldots, z_k$ e $z'_1, \ldots, z'_k$, avremo che

$$a_{i,1}z_1 + \cdots + a_{i,k}z_k \equiv a_{i,1}z'_1 + \cdots + a_{i,k}z'_k (mod\, m)$$

per $i = 1, \ldots, r$. Poniamo allora $\bar{u_j} = z_j - z'_j$, con $j = 1, \ldots, k$, da cui segue che

$$L_i(\bar{u_1}, \ldots, \bar{u_k}) \equiv 0 (mod\, m), \qquad i = 1, \ldots, r.$$

Inoltre abbiamo che

$$|\bar{u_j}| = |z_j - z'_j| \leq h_j, \qquad j = 1, \ldots, k$$

e non tutti gli $\bar{u_j}$ sono zero, poichè le due k–ple di parametri sono differenti. Con questo abbiamo provato l' asserto del lemma. □

Grazie a questi due lemmi siamo in grado di dimostrare che ogni primo si può scrivere come somma di quattro quadrati.

Teorema 2.7. *Ogni numero primo p si può rappresentare come somma di quattro quadrati.*

Dimostrazione. Sia p un primo maggiore di 3 (ciò non lede la generalità in quanto 2 e 3 sono rappresentabili come somma di quattro quadrati). Per il Lemma 2.5 esistono x e y interi tali che:

$$x^2 + y^2 + 1 \equiv 0 (mod\, p). \tag{2.7}$$

Consideriamo dunque le forme lineari:

$$L_1 = xu_1 + yu_2 - u_3 \quad e \quad L_2 = -yu_1 + xu_2 - u_4$$

Siano $m = p$ e $h_i = \sqrt{p}$ con $i = 1, \ldots, 4$, abbiamo allora che $h_1 \cdot \ldots \cdot h_4 = p^2 \geq m^r = p^2$. Possiamo allora applicare il Lemma 2.6, per cui esistono u_1, u_2, u_3, u_4 non tutti nulli tali che $|u_i| < \sqrt{p}$ con $i = 1, \ldots, 4$ e

$$L_1(u_1, u_2, u_3, u_4) \equiv L_2(u_1, u_2, u_3, u_4) \equiv 0 \, (mod\, p). \tag{2.8}$$

Possiamo allora scrivere, applicando la (2.7) e la (2.8) che $0 \equiv (x^2 + y^2 + 1)(u_1^2 + u_2^2) = (u_1^2+u_2^2)(x^2+y^2)+(u_1^2+u_2^2) = (xu_1+yu_2)^2+(xu_2-yu_1)^2+u_1^2+u_2^2 \equiv u_3^2+u_4^2+u_1^2+u_2^2 (mod\, p)$. Notare che l' ultima congruenza vale in quanto u_1, u_2, u_3, u_4 sono soluzioni di $L_1 = L_2 = 0$. Quindi possiamo dire che

$$u_1^2 + u_2^2 + u_3^2 + u_4^2 \equiv 0 (mod\, p) \tag{2.9}$$

Quindi abbiamo che $u_1^2+u_2^2+u_3^2+u_4^2$ è divisibile per p, e inoltre $0 < u_1^2+u_2^2+u_3^2+u_4^2 < 4p$. Pertanto $u_1^2 + u_2^2 + u_3^2 + u_4^2 = p, 2p, 3p$.

- Se $u_1^2 + u_2^2 + u_3^2 + u_4^2 = p$ allora abbiamo finito.
- Se $u_1^2+u_2^2+u_3^2+u_4^2 = 2p$ gli u_i hanno a due a due la stessa parità (cioè o sono tutti pari, o tutti dispari, o due pari e due dispari). Supponiamo che u_1 e u_2 abbiano la stessa parità, e quindi anche u_3 e u_4 avranno uguale parità, e moltiplichiamo per due ambo i membri, abbiamo che

  $$4p = (u_1 + u_2)^2 + (u_1 - u_2)^2 + (u_3 + u_4)^2 + (u_3 - u_4)^2$$

  Ogni base sarà pari (in quanto somma o differenza di termini con la stessa parità) possiamo dividere per 4 ambo i membri, e quindi avremo scritto p come somma di quattro quadrati.

- Se $u_1^2 + u_2^2 + u_3^2 + u_4^2 = 3p$ allora una base sarà divisibile per 3 e le altre no. Infatti ricordiamo che il quadrato di un numero non divisibile per 3 è sempre congruo 1 modulo 3. Quindi poichè $u_1^2 + u_2^2 + u_3^2 + u_4^2 = 3p \equiv 0(mod\, 3)$ le uniche possibilità sono che o sono tutte e quattro le basi divisibili per 3 o una è divisibile per 3 e le altre no. Se sono tutte divisibili per 3 allora la somma dei loro quadrati è divisibile per 9, ma p è un primo maggiore di 3 e quindi $3p$ non può essere divisibile per 9. Rimane pertanto solo la possibilità che una base sia divisibile per 3 e le altre no. Assumiamo allora, senza ledere la generalità, che u_4 sia divisibile per 3 e le altre basi abbiano resto 1 se divise per 3 (se hanno resto 2 le rimpiazziamo con i loro opposti). Moltiplicando per 3 ambo i membri avremo che

  $$9p = (u_1 + u_2 + u_3)^2 + (u_1 - u_2 + u_4)^2 + (u_2 - u_3 + u_4)^2 + (u_3 - u_1 + u_4)^2$$

  . Inoltre ogni base è divisibile per 3, pertanto la somma dei loro quadrati è divisibile per 9. Dividendo ambo i membri per 9 avremo rappresentato p come somma di quattro quadrati.

Quindi in ogni caso siamo riusciti a rappresentare p come somma di 4 quadrati, abbiamo dunque dimostrato l' asserto. □

Siamo ora in grado di dimostrare il teorema dimostrato da Lagrange:

Teorema 2.8 (di Lagrange). *Ogni intero n può essere rappresentato come somma di quattro quadrati.*

Dimostrazione. Abbiamo dimostrato nel Teorema 2.7 che ogni primo si può scrivere come somma di quattro quadrati, vale inoltre la seguente identità, dovuta a Eulero:

$$\begin{aligned}(x^2 + y^2 + z^2 + u^2)(r^2 + s^2 + t^2 + v^2) =& (xr + ys + zt + uv)^2 + (xs - yr - zv + ut)^2 + \\ &+ (xt + yv - zr - us)^2 + (xv - yt + zs - ur)^2\end{aligned}$$

che ci assicura che se due numeri possono essere scritti come somma di quattro quadrati allora tale è anche il loro prodotto. Ma ogni numero può essere scritto come prodotto di primi, che possono essere scritti come somma di quattro quadrati, pertanto ogni numero può essere scritto come somma di quattro quadrati. □

Dal Teorema 2.8 abbiamo dunque che ogni intero può essere scomposto in due addendi che sono la somma di al più due quadrati, ma quindi, per il Teorema 2.3, questi addendi, nella loro fattorizzazione, possono presentare fattori del tipo $4k+3$ elevati solo a potenze pari. Se noi al contrario provassimo questa proprietà (ovvero che ogni intero può essere

scomposto in due addendi nella cui decomposizione i fattori del tipo $4k+3$ compaiono elevati solo a potenze pari) allora avremmo dimostrato il Teorema 2.8 direttamente dal Teorema 2.3. Eulero spese molto tempo tentando di dimostrare il Teorema 2.8 in questo modo, senza riuscirvi. Fino ad ora nessuno ci è riuscito e una tale dimostrazione non esiste.

Notiamo che oltre a sapere quando un numero può essere scritto come somma di due quadrati, può essere interessante sapere in quanti modi si può scriverlo. Per esempio si ha la seguente proposizione, di cui non forniremo la dimostrazione:

Proposizione 2.9. *Sia n un intero e siano τ_1 e τ_3 i numeri dei divisori di n della forma $4k+1$ e $4k+3$ rispettivamente. Si ha allora che il numero di modi in cui n si può scrivere come somma di due quadrati è $4(\tau_1 - \tau_3)$.*

Capitolo 3

Interi come somme di quarte potenze

Dopo aver visto come si possono decomporre gli interi in somme di quadrati, è naturale chiedersi se e come si possono decomporre in somme di potenze successive. La decomposizione in cubi è molto complessa e per questo non sarà qui trattata, mentre studieremo la rappresentazione di un intero come somma di quarte potenze, per cui ci potranno essere d' aiuto i risultati raggiunti nello studio della rappresentazione degli interi come somma di quadrati. A tal scopo notiamo la seguente identità:

$$(a+b)^4 + (a-b)^4 = 2(a^4 + 6a^2b^2 + b^4) \tag{3.1}$$

da cui si ha che:

$$\begin{aligned}(a+b)^4 + (a-b)^4 + (a+c)^4 + (a-c)^4 + (a+d)^4 + (a-d)^4 + \\ + (b+c)^4 + (b-c)^4 + (b+d)^4 + (b-d)^4 + (c+d)^4 + \\ + (c-d)^4 = 6(a^2+b^2+c^2+d^2)^2\end{aligned}$$

Applicando il Teorema 2.8 abbiamo che i numeri della forma $6n^2$ possono essere scritti come somma di al più 12 quarte potenze. Ma applicando di nuovo tale teorema abbiamo che tutti i multipli di 6 si possono scrivere come somma di al più 48 quarte potenze. Infine se dividiamo un numero per 6 otteniamo un resto compreso tra 0 e 5; aggiungengo al più cinque volte 1^4 avremo ottenuto il numero desiderato. Abbiamo quindi mostrato che ogni intero si può scrivere come somma di al più 53 quarte potenze.

Con questo ragionamento abbiamo provato il seguente Teorema:

Teorema 3.1. *Ogni intero n può essere scritto come somma di al più 53 quarte potenze.*

53 quarte potenze sembrano troppe rispetto a quante siano davvero necessarie, tuttavia si possono trovare infiniti numeri che richiedono almeno 16 quarte potenze per essere rappresentati, come ci è mostrato dal seguente teorema.

Teorema 3.2. *I numeri della forma* $16^n \cdot 31$ *non possono essere rappresentati come somma di meno di 16 quarte potenze.*

Dimostrazione. L' asserto è banalmente vero per $n = 0$, infatti $16^0 \cdot 31 = 31$ può ammettere come addendi solo 1^4 e 2^4, quest' ultimo al più una volta, sicchè l' espressione col minimo numero di addendi è $31 = 2^4 + 15 \cdot 1^4$. Consideriamo dunque il resto delle quarte potenze modulo 16:

- se la base m è pari, allora 16 divide m^4;
- se la base m è dispari, ovvero $m = 2k+1$, allora $m^4 = 16k^4+32k^3+24k^2+8k+1 \equiv 8k^2 + 8k + 1 = 8k(k + 1) + 1 \equiv 1(mod\,16)$

Supponiamo ora che $n = 16^m \cdot 31$ sia il più piccolo intero di questa forma a poter essere rappresentato come somma di al più 15 quarte potenze. Ovviamente n non può essere 31 per quanto visto prima, quindi $m \neq 0$ e dunque 16 divide n, per cui $n \equiv 0(mod\,16)$. Allora tutti gli addendi devono essere pari, altrimenti si avrebbe che $n \equiv t(mod\,16)$ con t il numero di addendi dispari. Quindi $n = 16^m \cdot 31 = \sum_{i=1}^{15} a_i^4$ con a_i pari per ogni $i = 1, \ldots, 15$. Possiamo allora considerare $\sum_{i=1}^{15} (\frac{a_i}{2})^4 = \frac{1}{16} \sum_{i=1}^{15} a_i^4 = \frac{1}{16} \cdot 16^m \cdot 31 = 16^{m-1} \cdot 31$. Quindi anche il numero $16^{m-1} \cdot 31$ può essere scritto come somma di al più 15 potenze, e inoltre è minore di $16^m \cdot 31$, ma ciò è un assurdo poichè avevamo assunto che $16^m \cdot 31$ fosse il minimo. L' assurdo deriva dall' esistenza di un siffatto numero, da cui la tesi del teorema. □

Abbiamo quindi trovato due limitazioni per il numero di quarte potenze necessario a rappresentare tutti gli interi: questo numero deve essere compreso tra 16 e 53. Notiamo che le due limitazioni differiscono di molto, si potrebbe quindi pensare di provare a ridurre la limitazione superiore (per quanto abbiamo visto è infatti impossibile aumentare quella inferiore). Provando a rappresentare alcuni interi come somma di quarte potenze infatti si vede i casi più sfavorevoli sono dati da 31 (che, come abbiamo visto, richiede 15 quarte potenze), 47 (17), 63 (18), 79 (19). Dopo 79, anche proseguendo per molti interi, non si trovano numeri che richiedono più di 19 quarte potenze per essere rappresentati. Vedremo in seguito che 19 è proprio il minimo numero necessario a rappresentare ogni intero come somma di quarte potenze.

Capitolo 4

Congettura di Waring

Finora abbiamo studiato il problema di determinare se e quando un intero si può scrivere come somma di quadrati o quarte potenze. Generalizzando questo problema si può studiare se e quando un intero si può scrivere come somma di potenze k–esime. Il primo a porsi tale problema fu Waring, che nella sua opera *Meditationes algebricae*, composta tra il 1770 e il 1782, congetturò che per ogni intero k esistesse un numero intero, che noi indicheremo con $g(k)$, tale che ogni numero intero si potesse scrivere come somma di al più $g(k)$ potenze k–esime. Tale congettura fu provata da Hilbert nel 1909. Abbiamo già provato che $g(2) = 4$ e $19 \leq g(4) \leq 53$. Si intuisce, ed è confermato da alcune prove empiriche, che $g(k)$ sia determinato dai numeri piccoli, nella cui rappresentazione compaiono solo 1^k o 2^k. Basandosi su questa idea, Eulero ottenne il seguente risultato:

$$g(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2. \tag{4.1}$$

Wieferich nel 1909 mostrò che vale l' uguaglianza per $k = 3$, ovvero $g(3) = 2^3 + [\frac{27}{8}] - 2 = 8 + 3 - 2 = 9$. Tale dimostrazione fu completata da Kempner nel 1912.

Poichè quindi $g(k)$ è determinato sostanzialmente dai piccoli numeri, diviene interessante determinare $G(k)$,definito come il numero di k–esime potenze necessario per rappresentare ogni intero abbastanza grande e tale che esistano infiniti interi che non possano essere rappresentati come somma di meno di $G(k)$ potenze k–esime. Dai Teoremi 2.4 e 2.8 sappiamo che $G(2) = 4$ e dal Teorema 3.2 sappiamo che $G(4) \geq 16$.

Nel corso degli ultimi anni il problema di Waring è stato molto studiato; riportiamo di seguito alcuni importanti risultati raggiunti: Hardy e Littlewood, in una serie di articoli tra il 1919 e il 1928 utilizzarono le funzioni a variabili complesse per dare una serie di

stime superiori di $G(k)$, fino ad arrivare alla seguente limitazione:

$$G(k) \leq (k-2)2^{k-1} + 5. \tag{4.2}$$

In seguito Vinogradov combinando i metodi di Hardy e Littlewood con dei nuovi mostrò che queste stime potevano essere migliorate. Nel 1989 Vaughan diede una miglior stima di $G(k)$:

$$G(k) < k(3 \lg k + 4.2) \tag{4.3}$$

Per k molto grandi questa stima è minore della stima inferiore di $g(k)$ fornita nella (4.1). Questo vuol dire che, sotto alcune condizioni vale l' uguaglianza:

$$g(k) = 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2 \tag{4.4}$$

con $k \geq 7$. Se questa condizione non è soddisfatta allora $g(k)$ è dato da una formula simile alla (4.3). Ci vollero poi ben 40 anni per determinare $g(4), g(5)$ e $g(6)$. L' ultimo fu $g(4) = 19$, come fu dimostrato nel 1986 da Balasubramanian, Deshuillers e Dress. Per quanto riguarda la condizione sopramenzionata si sa che solo un numero finito di numeri può non soddisfarla, il più piccolo dei quali è maggiore di 200.000 . Molti matematici sono dell' opinione che non esistano numeri che non soddisfino tale proprietà.

Landau nel 1909 provò che $G(3) \leq 8$, e nel 1939 Dickson dimostrò che gli unici interi che richiedono nove cubi per essere rappresentati sono 23 e 239. Wieferich poi mostrò che solo 15 interi richiedono otto cubi per essere rappresentati, da cui deriva che $G(3) \leq 7$. Ad oggi il più grande numero conosciuto che richiede sette cubi per essere rappresentato è 8042.

Nel 1933 Hardy e Littlewood mostrarono che $G(4) \leq 19$; nel 1939 Davenport dimostrò che $G(4) = 16$. Brüdern, migliorando i metodi usati da Vaughan, dimostrò che $G(5) \leq 18$. Nel 1993 Vaughan e Wooley mostrarono che $G(8) \leq 42$.

Hardy e Littlewood congetturarono che $G(k) \leq 2k + 1$ eccetto per il caso in cui $k = 2^m$ con $m \geq 2$, nel qual caso congetturarono che $G(k) = 4k$. I risultati ottenuti non contraddicono tale congettura, in quanto $G(4) = 16 = 4 \cdot 4$. Nel determinare $G(k)$ è di aiuto sapere quanti numeri, fino a un certo limite x, possono essere scritti come somma di k k–esime potenze. Landau mostrò che per $k = 2$ al crescere di x questo numero tende asintoticamente a $\frac{cx}{\sqrt{\ln x}}$ con c un' opportuna costante positiva. Per $k \geq 3$ non sappiamo nulla sulla loro distribuzione.

Si può congetturare, fissato un naturale k, che il numero di interi positivi minori di x che si possono scrivere come somma di al più k k–esime potenze sia maggiore di x^{1-h}, con h un reale positivo e con x sufficientemente grande. Nel 1950 Davenport trovò che per $k = 3$ questo numero è maggiore di $x^{\frac{47}{55}-h}$ se x è sufficientemente grande.

Nel 1938 Erdos e Mahler provarono che il numero di interi positivi della forma $a^k + b^k$ minori di x è maggiore di $cx^{\frac{2}{k}}$ e minore di $x^{\frac{2}{k}}$, con c un' opportuna costante numerica positiva. Hardy e Littlewood congetturarono che per ogni h il numero delle soluzioni dell' equazione $n = x_1^h + \ldots + x_h^h$ è minore di n^h,per n sufficientemente grande. Questo è vero per $k = 2$, ma per $k = 3$ Mahler dimostrò che non vale. Non sappiamo quale sia la situazione per $k > 3$.

Diamo ora un breve riepilogo delle stime ottenute per $g(k)$ e $G(k)$ nella seguente tabella:

k	$g(k)$	$G(k)$
2	4	4
3	9	$\leq$7
4	19	16
5	37	$\leq$17
6	73	$\leq$24
7	143	$\leq$33
8	279	$\leq$42
9	548	$\leq$51
10	1079	$\leq$59
11	2132	$\leq$67
12	4223	$\leq$76
13	8384	$\leq$84
14	16673	$\leq$92
15	33203	$\leq$100

Capitolo 5

Rappresentazione di interi come somme e differenze di potenze

Finora abbiamo studiato come rappresentare gli interi solo come somma di potenze. In questo capitolo indagheremo invece su come si possano rappresentare gli interi utilizzando anche differenze di potenze. A tal scopo possiamo limitarci a studiare gli interi non negativi, in quanto la rappresentazione dei negativi sarà ottenuto cambiando i segni della rappresentazione di questi.
La rappresentazione degli interi come somma di potenze non è altro che un caso particolare della rappresentazione degli interi come somma e differenza di potenze, e pertanto, sfruttando la dimostrazione di Hilbert della congettura di Waring, possiamo ammettere che per ogni intero k esiste un numero $w(k)$ tale che ogni intero si può scrivere come somma e differenza di al più $w(k)$ k–esime potenze. Ovviamente si avrà che:

$$w(k) \leq g(k).$$

Studiamo ora il caso per $k = 2$:
Notiamo che $n^2-(n-1)^2 = 2n-1$, quindi tutti i numeri dispari si possono rappresentare come differenza di due quadrati. Invece per i numeri pari abbiamo che $2n = (2n-1)+1 = n^2 - (n-1)^2 + 1^2$. Quindi tutti i numeri possono essere rappresentati mediante al più tre quadrati, da cui $w(2) \leq 3$.
Notiamo ora che nel Capitolo 2 abbiamo visto che ci sono infiniti numeri che non possono essere rappresentati come somma di due quadrati, esaminiamo se tali numeri possono essere rappresentati come differenza di due quadrati: osservando che $a^2-b^2 = (a+b)(a-b)$ e che $(a+b)+(a-b) = 2a$ abbiamo che tutti e due i fattori devono essere pari, o tutti e due dispari; il loro prodotto sarà dunque dispari o divisibile per 4. Notiamo allora che il doppio di un numero dispari non può essere scomposto in fattori che abbiano la stessa

parità, pertanto non può essere rappresentato come differenza di quadrati. Abbiamo dunque provato che $w(k) \geq 3$, da cui segue $w(k) = 3$.
È anche vero che ci sono infiniti numeri per cui sono necessari tre quadrati nella loro rappresentazione, come nel caso dei numeri della forma $6(2k+1)^2$, che sono il doppio di un numero dispari: $3(2k+1)^2$ e che quindi non possono essere rappresentati come differenza di 2 quadrati, e inoltre nella loro fattorizzazione c'è un primo della forma $4k+3$ (precisamente 3) elevato a una potenza dispari (1 o 3), e pertanto non può essere rappresentato nemmeno come somma di due quadrati. Abbiamo dunque dimostrato il seguente Teorema:

Teorema 5.1. *Ogni intero può essere rappresentato come somma di tre quadrati con segni misti. Inoltre ci sono infiniti numeri che non sono rappresentabili come somma o differenza di due quadrati.*

Per quanto riguarda il caso $k = 3$, ci può aiutare la seguente identità:

$$(m+1)^3 - 2m^3 + (m-1)^3 = 6m \tag{5.1}$$

che mostra che tutti i multipli di 6 possono essere rappresentati da al più quattro cubi. Notiamo che $n^3 - n$ è sempre divisibile per 6, e quindi per la (5.1) avremo che:

$$n^3 - n = 6m = (m+1)^3 - 2m^3 + (m-1)^3 \tag{5.2}$$

da cui

$$n = n^3 - (m+1)^3 + 2m^3 - (m-1)^3 \tag{5.3}$$

Quindi ogni intero può essere rappresentato mediante al più cinque cubi, sicchè $w(3) \leq 5$. Possiamo anche trovare una limitazione inferiore per $w(3)$ notando che il cubo di un numero non divisibile per 3 è adiacente a un numero divisibile per 9 e, ovviamente, il cubo di un numero divisibile per 3 è divisibile per 9. Sia infatti $n = 3t + e$ con $e = \pm 1$, per cui

$$e^2 = 1 \tag{5.4}$$

e

$$e^3 = e \tag{5.5}$$

Sfruttando la (5.4) e la (5.5) avremo che $n^3 = (3t+e)^3 = 27t^3 + 27t^2e + 9te^2 + e^3 = 9(3t^3 + 3t^2e + t) + e$ che è un numero adiacente a 9.
Da ciò segue che i numeri della forma $9m+4$ non possono essere rappresentati con meno di quattro cubi. Abbiamo allora dimostrato il seguente teorema:

Teorema 5.2. *Ogni intero può essere rapprsentato come somma con segni misti di al più cinque cubi, ma ci sono infiniti numeri che non possono essere scritti come somma (sempre con segni misti) di meno di quattro cubi.*
Pertanto $4 \leq w(3) \leq 5$.

Oltre questa buona stima di $w(3)$ si conosce l' esatto valore di $w(k)$ solo per $k = 2$. A parte questo si sa molto poco riguardo la funzione $w(k)$.

Capitolo 6

Reticoli Geometrici

In questo capitolo daremo un esempio di come branche della matematica che possono sembrare molto lontane tra di loro, siano in realtà collegate. Infatti attraverso risultati di Teoria dei Reticoli Geometrici arriveremo a dimostrare un teorema riguardante la Teoria dei Numeri già enunciato nel Capitolo 2 (il Teorema 2.1).

Consideriamo nel piano due rette non parallele, r e s, e due distanze, d_1 e d_2; a questo punto consideriamo la famiglia delle rette parallele a r e distanti da r un multiplo intero della distanza d_1; analogamente consideriamo la famiglia delle rette parallele a s e distanti da s un multiplo intero della distanza d_2. Chiamiamo queste rette *fili* del reticolo. Le intersezioni dei fili determinano i *punti* del reticolo. I parallelogrammi determinati da coppie di fili del reticolo vicine si diranno *parallelogrammi base*.
Consideriamo un sistema di riferimento cartesiano tale che l' origine O si un punto del reticolo, sia $OABC$ un parallelogrammo base e siano $\vec{p}$ e $\vec{q}$ i vettori determinati dai lati OA e OC.
Dall' origine O possiamo raggiungere un qualsiasi punto R del reticolo percorrendo la retta determinata da OA fino al punto d' intersezione con la retta parallela alla direzione di OC e passante per R, e poi continuando lungo tale retta fino a R. Il primo tratto è un multiplo intero (anche negativo) di $\vec{p}$, il secondo di $\vec{q}$: possiamo dunque scrivere il vettore $\vec{r} := \vec{OR}$ come

$$\vec{r} = u \cdot \vec{p} + v \cdot \vec{q} \tag{6.1}$$

con u e v interi e univocamente determinati. Notiamo che muovendo l' origine O di un vettore $\vec{r} = u \cdot \vec{p} + v \cdot \vec{q}$, con u e v interi, essa finisce sempre in un punto del reticolo.

Siano $(k, l), (m, n)$ e (x, y) le coordinate dei punti determinati dai vettori $\vec{p}, \vec{q}$ e $\vec{r}$;

dalla (6.1) abbiamo quindi che

$$(x, y) = u(k, l) + v(m, n) = (uk + vm, ul + vn) \tag{6.2}$$

Abbiamo visto dunque che il generico punto del reticolo ha coordinate

$$\begin{cases} x = uk + vm \\ y = ul + vn \end{cases}$$

con u e v interi. Notiamo ora che per $(u, v) = (0, 0), (1, 0), (0, 1)$ otteniamo i punti O, A, C di coordinate $(0, 0), (k, l), (m, n)$ rispettivamente, e pertanto l'area di un parallelogramma base sarà:

$$d = \left| det \begin{pmatrix} 0 & 0 & 1 \\ k & l & 1 \\ m & n & 1 \end{pmatrix} \right| = |kn - lm| \tag{6.3}$$

Abbiamo dunque dimostrato il seguente teorema:

Teorema 6.1. *I punti di un reticolo di parallelogrammi sono tutti e soli i punti determinati dal vettore $\vec{r} = u \cdot \vec{p} + v \cdot \vec{q}$, con u e v interi, che possono essere espressi anche come i punti (x, y) del piano reale tale che:*

$$(x, y) = u(k, l) + v(m, n) = (uk + vm, ul + vn).$$

Inoltre l' area di un parallelogramma base è $d = |kn - lm|$.

I reticoli hanno molte proprietà, di seguito ne enunciamo due fondamentali:

Proprietá. *I) Traslando il reticolo in modo che un dato punto del reticolo finisca su di un altro punto del reticolo, ogni punto del reticolo finirà su di un altro punto del reticolo, ovvero avremo traslato il reticolo in se stesso.*
II) Esiste un numero reale positivo δ tale che la distanza tra due punti distinti del reticolo è sempre maggiore o uguale a δ.

Dimostrazione. I) Per verificare tale proprietà dobbiamo far vedere che ogni punto del reticolo si sovrappone a un altro punto del reticolo e ogni punto del reticolo è immagine di un altro punto del reticolo. Notiamo allora che per ogni famiglia di fili del reticolo esiste un filo del reticolo che passa per il punto immagine del punto traslato, e che questi fili sono paralleli a quelli che passano per il punto considerato inizialmente. I fili di queste famiglie sono paralleli e equispaziati, e quindi la famiglia iniziale è traslata in se stessa. Analogamente per l' altra famiglia di fili del reticolo. Per questo motivo anche i punti del reticolo (che sono le intersezioni di tali famiglie) sono traslati in se stessi.

II) Dato un punto del reticolo, consideriamo i 4 parallelogrammi base di cui è vertice. Questi insieme determinano un parallelogramma che ha dimensioni doppie rispetto a un parallelogramma base, e l' unico punto del reticolo a esso interno è proprio il punto dato. La minore delle due misure del parallelogramma base gode pertanto della proprietà richiesta. □

Le rette che passano per almeno 2 punti del reticolo saranno dette *rette* del reticolo; i fili del reticolo pertanto sono anche rette. Similmente definiamo *vettori* del reticolo, *intervalli* del reticolo e *poligoni* del reticolo i vettori, intervalli e poligoni che hanno per estremi punti del reticolo.
Sfruttando i precedenti risultati si possono dimostrare anche le seguenti proprietà:

Proprietá. *III) In un reticolo di punti, una retta o contiene al più un punto, o ne contiene infiniti equispaziati.*
IV) Se da un qualsiasi punto del reticolo tracciamo una retta parallela a una data retta del reticolo, allora anche questa retta sarà una retta del reticolo, che passerà per infiniti punti equispaziati.
V) Il simmetrico di un punto del reticolo rispetto a un altro punto del reticolo o rispetto al punto medio di un intervallo del reticolo è ancora un punto del reticolo.

Dato un reticolo, a volte può essere interessante conoscere l' area di un parallelogramma del reticolo conoscendo solamente quanti punti del reticolo esso contiene. A tal proposito vale il seguente teorema:

Teorema 6.2. *Sia d l' area del parallelogramma base del reticolo, e consideriamo un poligono del reticolo che contiene h punti del reticolo, di cui b sul suo perimetro; allora l' area T del poligono del reticolo è data dalla formula:*

$$T = \big(b + \frac{h}{2} - 1\big)d\,. \tag{6.4}$$

Questo teorema quindi prova anche che in un reticolo l' area di un poligono è determinata solo dal numero di punti del reticolo che vi appartengono, e non dal tipo di poligono.

Con il seguente Teorema, che è uno dei più importanti nella Teoria dei Reticoli Geomerici, mostreremo invece che regioni del reticolo che soddisfino certe condizioni, devono contenere necessariamente dei punti del reticolo al proprio interno.

Teorema 6.3 (di Minkowski). *I) In un reticolo di punti nel quale i parallelogrammi base hanno area d, ogni regione convessa, centrata in un punto del reticolo e simmetrica rispetto al suo centro, con area maggiore di $4d$, contiene almeno un altro punto del reticolo al suo interno oltre al suo centro.*
II) Se l' area della regione è esattamente $4d$, allora oltre al suo centro c'è sicuramente un altro punto del reticolo al suo interno o sulla sua frontiera.

Dimostrazione. I) Consideriamo nel piano un reticolo di punti L in cui i parallelogrammi base hanno area d. Sia T un regione del piano centrata nel punto del reticolo O, simmetrica rispetto al proprio centro, convessa e con area maggiore di $4d$. Consideriamo allora un parallelogramma base del reticolo $OABC$ e consideriamo ogni altro filo del reticolo parallelo ai fili del reticolo passanti per OA e OC. A questo punto siamo in grado di ricoprire il reticolo con parallelogrammi che hanno area $4d$. Sia $KLMN$ uno di questi parallelogrammi, e si traslino in esso tutti quei parallelogrammi che intersecano T insieme con la parte di T che essi contengono. In questo modo avremo traslato in $KLMN$ una regione con area maggiore di $4d$ (in quanto T ha area maggiore di $4d$), pertanto esiste un punto P coperto da almeno 2 regioni di T che sono state traslate. Fissiamo i punti di due regioni che coprono P e poi riportiamole indietro traslandole di volta in volta di una distanza pari alla lunghezza di uno dei due lati del parallelogramma e secondo la sua direzione. Siano P_1 e P_2 i due punti di T la cui immagine è P. Mettendo insieme i due percorsi abbiamo un percorso da P_1 a P_2 che è formato da segmenti paralleli a OA o a OC ma lunghi il doppio rispettivamente. Sia ora P_3 il simmetrico di P_1 rispetto a O; P_3 è ancora un punto di T, in quanto T è simmetrico rispetto a O. Consideriamo il cammino da P_3 a P_2, ottenuto unendo il segmento che va da P_3 a P_1 con il cammino ottenuto precedentemente che va da P_1 a P_2 passando per P (vedi Figura 6.1): se lo contraiamo fino a farne la metà otteniamo che O è l' immagine di P_1 e Q è l' immagine di P_2. Quindi Q è un punto del reticolo in quanto ottenuto da O (che è un punto del reticolo) attraverso un cammino costituito da segmenti paralleli ad OA o a OC e della loro lunghezza. Q appartiene al segmento P_3P_2 e quindi anche a T, poichè T è convesso. Infine notiamo che Q è distinto da O, poichè sono immagini di punti distinti mediante la contrazione .
II) La dimostrazione precedente può essere ripercorsa interamente anche nel caso in cui l' area della regione è esattamente $4d$ se il parallelogramma $KLMN$ ha ancora un punto coperto da due regioni traslate. Tuttavia nelle ipotesi della II) questo non è assicurato. Se ciò non accade (cioè non ci sono punti coperti da due regione di T traslate) vuol dire che le porzioni di T, con le proprie frontiere, traslate con i parallelogrammi, coprono esattamente $KLMN$. Questo contiene 9 punti del reticolo. Notiamo che O viene traslato

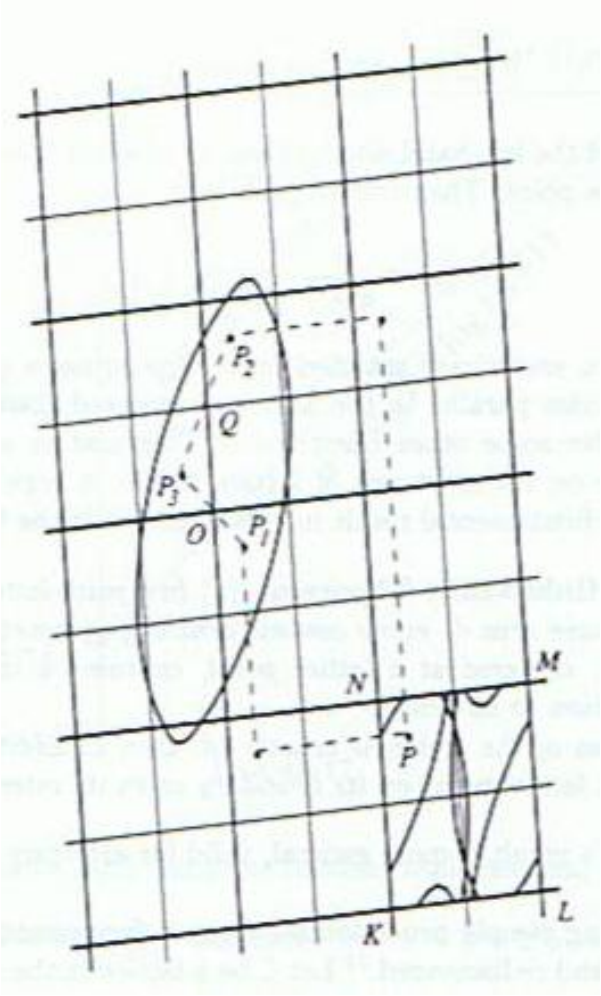

Figura 6.1:

nei quattro vertici di $KLMN$ quando trasliamo i parallelogrammi che intersecano T, e O non può avere altre immagini per come abbiamo ricoperto il reticolo. I restanti 5 punti di $KLMN$ devono pertanto essere immagine di un altro punto interno a T o appartenente alla sua frontiera; per la natura della traslazione questo punto deve essere un punto del reticolo, e pertanto abbiamo dimostrato l' asserto. □

Come applicazione del Teorema di Minkowski possiamo dimostrare il seguente Teorema:

Proposizione 6.4. *Consideriamo un reticolo per cui l' origine è un punto del reticolo e l' area dei parallelogrammi base è d, allora esiste un punto del reticolo differente dall' origine le cui coordinate x e y soddisfano la seguente relazione:* $x^2 + y^2 \leq \frac{4d}{\pi}$.

Dimostrazione. L' equazione $x^2 + y^2 = \frac{4d}{\pi}$ descrive il cerchio di centro l' origine e raggio $2\sqrt{\frac{d}{\pi}}$, che ha area $4d$. Siamo dunque nelle ipotesi del Teorema 6.3, deve pertanto esistere un altro punto interno o di frontiera diverso dall' origine che sia un punto del reticolo. □

Dimostriamo ora un risultato che insieme con quelli precedenti ci consentirà di dare una dimostrazione alternativa del Teorema 2.1. A tal fine ricordiamo il Teorema di Wilson, che assicura che se p è un numero primo allora

$$(p-1)! + 1 \equiv 0 \,(mod\, p) \tag{6.5}$$

Proposizione 6.5. *Per ogni primo p della forma* $4k+1$ *esiste un intero c tale che* $c^2 + 1 \equiv 0 (mod\, p)$.

Dimostrazione. Notando che $p - j \equiv -j (mod\, p)$ con $j = \frac{p-1}{2}, \frac{p-1}{2} - 1, \ldots, 2, 1$ possiamo riscrivere il Teorema di Wilson nel seguente modo:

$$(-1)^{\frac{p-1}{2}} \left(\left(\frac{p-1}{2} \right)! \right)^2 + 1 \equiv 0 \,(mod\, p)$$

Se p è della forma $4k+1$ allora -1 è elevato a una potenza pari, e quindi $(-1)^{\frac{p-1}{2}} = 1$; l' uguaglianza diventa dunque

$$\left(\left(\frac{p-1}{2} \right)! \right)^2 + 1 \equiv 0 \,(mod\, p).$$

Ponendo $c = \left(\frac{p-1}{2}\right)!$ abbiamo dimostrato il teorema. □

Dimostriamo ora il Teorema 2.1 già anticipato nel Capitolo 2.

Teorema 6.6. *Tutti i primi della forma* $4k+1$ *e* 2 *possono essere scritti come somma di due quadrati. I primi della forma* $4k+3$ *non possono essere scritti in questo modo.*

Dimostrazione. L' ultima affermazione è ovvia. Per dimostrarla basta osservare che il quadrato di un numero dispari è congruo 1 modulo 4, mentre il quadrato di un numero pari è congruo 0 modulo 4. Quindi la somma di due quadrati può essere congrua 0, 1 o 2, ma mai 3 modulo 4; pertanto i numeri della forma $4k+3$ (che sono congrui 3 modulo 4) non possono essere scritti come somma di due quadrati.
Dalla Proposizione 6.5 sappiamo che per i primi della forma $4k+1$ esiste un naturale a tale che $a^2+1 \equiv 0(mod\, p)$ (se $p=2$ basta considerare $a=1$). Consideriamo allora il reticolo descritto dalla seguente rappresentazione:

$$\begin{cases} x = up + va \\ y = v \end{cases}$$

con u e v interi. In questo reticolo l' area del parallelogramma base è $d = |p\cdot 1 - a\cdot 0| = p$, e la somma dei quadrati delle coordinate dei punti del reticolo è $x^2+y^2 = (up+va)^2+v^2 = p(pu^2+2auv)+v^2(a^2+1)$ che è divisibile per p per la scelta di a. Per la Proposizione 6.4 esiste un punto del reticolo tale che $x^2+y^2 < \frac{4p}{\pi} < 2p$. Poichè il punto non è l' origine (quindi $x^2+y^2>0$) e abbiamo dimostrato che la somma dei quadrati delle sue coordinate è divisibile per p deve essere che $x^2+y^2=p$. Abbiamo dunque dimostrato il teorema. □

Capitolo 7

Generalizzazione delle terne pitagoriche

Nel Capitolo 1 abbiamo studiato le n–ple pitagoriche come generalizzazione naturale delle terne pitagoriche, giungendo infine a una loro completa parametrizzazione. In questo capitolo studieremo una generalizzazione alternativa delle terne pitagoriche: studieremo quando una potenza n–esima si può scrivere come somma di n potenze n–sime, ovvero quando l' equazione

$$y^n = x_1^n + \ldots + x_n^n \tag{7.1}$$

ammette soluzione negli interi. Notare che le terne pitagoriche sono le soluzioni nel caso $n = 2$.

Non esiste una teoria completa su tale argomento, e pertanto in questa sede ci limiteremo a mostrare i risultati ottenuti per i primi valori di n.

7.1 $n = 3$

Per $n = 3$ l' equazione considerata diventa

$$y^3 = x_1^3 + x_2^3 + x_3^3. \tag{7.2}$$

Ad oggi non esiste una parametrizzazione che dia *tutte* le soluzioni intere. Eulero e Vieta trovarono per primi la generica soluzione razionale. Hardy e Wright nel 1979 diedero una

soluzione basata sulle seguenti identità:

$$a^3(a^3+b^3)^3 = b^3(a^3+b^3)^3 + a^3(a^3-2b^3)^3 + b^3(2a^3-b^3)^3 \tag{7.3}$$
$$a^3(a^3+2b^3)^3 = a^3(a^3-b^3) + b^3(a^3-b^3)^3 + b^3(2a^3+b^3)^3 \tag{7.4}$$

Ramanujan diede la seguente classe di soluzioni:

$$(3x^2+5xy-5y^2)^3 + (4x^2-4xy+6y^2)^3 + (5x^2-5xy-3y^2)^3 = (6x^2-4xy+4y^2)^3 \tag{7.5}$$

che per $x = 1$ e $y = 0$ ci fornisce una particolare soluzione: $3^3 + 4^3 + 5^3 = 6^3$. La parametrizzazione trovata da Ramanujan è in realtà un caso particolare di una più generale identità:

$$(ax^2 + v_1xy + bwy^2)^3 + (bx^2 - v_1xy + awy^2)^3 + (cx^2 + v_2xy + dwy^2)^3 + \tag{7.6}$$
$$+ (dx^2 - v_2xy + cwy^2)^3 = (a^3+b^3+c^3+d^3)(x^2+wy^2)^3 \tag{7.7}$$

con $v_1 = -(c^2-a^2), v_2 = a^2-b^2$ e $w = (a+b)(c+d)$. La parametrizzazione di Ramanujan si ottiene ponendo $a^3 + b^3 + c^3 + d^3 = 0$.

Riportiamo di seguito le prime più piccole soluzioni positive dell' equazione (7.2):

$$3^3 + 4^3 + 5^3 = 6^3 \tag{7.8}$$
$$1^3 + 6^3 + 8^3 = 9^3 \tag{7.9}$$
$$3^3 + 10^3 + 18^3 = 19^3 \tag{7.10}$$
$$7^3 + 14^3 + 17^3 = 20^3 \tag{7.11}$$
$$4^3 + 17^3 + 22^3 = 25^3 \tag{7.12}$$

Ci sono anche casi di uguaglianze multiple, come per esempio nei casi:

$$2^3 + 17^3 + 40^3 = 41^3 = 6^3 + 32^3 + 33^3 \tag{7.13}$$
$$3^3 + 36^3 + 37^3 = 46^3 = 27^3 + 30^3 + 37^3 \tag{7.14}$$

A tal proposito è rimarchevole la soluzione trovata da Kohmoto:

$$2100000^3 = 2046000^3 + 882000^3 + 216000^3 \tag{7.15}$$
$$= 1979600^3 + 1145400^3 + 85000^3 \tag{7.16}$$
$$= 2081000^3 + 628110^3 + 1890^3 \tag{7.17}$$
$$= 2043150^3 + 901200^3 + 30450^3 \tag{7.18}$$
$$= 2002280^3 + 1072480^3 + 30360^3 \tag{7.19}$$
$$= 1960480^3 + 1199520^3 + 15200^3 \tag{7.20}$$
$$= 1948800^3 + 1229760^3 + 30240^3 \tag{7.21}$$
$$= 2078160^3 + 658812^3 + 13188^3 \tag{7.22}$$
$$= 2009112^3 + 1048040^3 + 13888^3. \tag{7.23}$$

(Da notare che dalla (7.15) otteniamo anche la soluzione $2100^3 = 2046^3 + 882^3 + 216^3$).

7.2 $n = 4$

Per $n = 4$ l' equazione (7.1) diventa

$$y^4 = x_1^4 + x_2^4 + x_3^4 + x_4^4. \tag{7.24}$$

Non si sa se esista una parametrizzazione che dia tutte le soluzioni intere di questa equazione, tuttavia esiste la parametrizzazione (dovuta a Jacobi e Madden, nel 2008) che da le soluzioni del caso particolare:

$$x_1^4 + x_2^4 + x_3^4 + x_4^4 = (x_1 + x_2 + x_3 + x_4)^4 \tag{7.25}$$

Riportiamo di seguito le più piccole soluzioni della (7.24):

$$30^4 + 120^4 + 272^4 + 315^4 = 353^4 \tag{7.26}$$
$$240^4 + 340^4 + 430^4 + 599^4 = 651^4 \tag{7.27}$$
$$435^4 + 710^4 + 1384^4 + 2420^4 = 2487^4 \tag{7.28}$$
$$1130^4 + 1190^4 + 1432^4 + 2365^4 = 2501^4 \tag{7.29}$$
$$850^4 + 1010^4 + 1546^4 + 2745^4 = 2829^4 \tag{7.30}$$

Da notare la soluzione $(955, 1770, 2634, 5400, 5491)$ dovuta a Brudno (1964) che soddisfa anche la relazione: $955 + 1700 - 2364 + 5400 = 5491$.

7.3 $n = 5$

Per $n = 5$ la (7.1) diventa

$$y^5 = x_1^5 + x_2^5 + x_3^5 + x_4^5 + x_5^5. \tag{7.31}$$

Sastry, nel 1934, trovò una paramterizzazione delle soluzioni di tale equazione:

$$(75v^5 - u^5)^5 + (u^5 + 25v^5)^5 + (u^5 - 25v^5)^5 + (10u^3v^2)^5 + (50uv^4)^5 = (u^5 + 75v^5)^5 \tag{7.32}$$

Lander e Parkin nel 1967, sfruttando il risultato di Sastry, trovarono le più piccole soluzioni positive, alcune delle quali sono elencate di seguito:

$$19^5 + 43^5 + 46^5 + 47^5 + 67^5 = 72^5 \tag{7.33}$$
$$21^5 + 23^5 + 37^5 + 79^5 + 84^5 = 94^5 \tag{7.34}$$
$$7^5 + 43^5 + 57^5 + 80^5 + 100^5 = 107^5 \tag{7.35}$$
$$78^5 + 120^5 + 191^5 + 259^5 + 347^5 = 365^5 \tag{7.36}$$
$$79^5 + 202^5 + 258^5 + 261^5 + 395^5 = 415^5 \tag{7.37}$$

(da notare che la soluzione (7.35) è ottenuta dalla formula (7.32) per $v = 1$ e $u = 2$).

7.4 $n = 6$

Per $n = 6$ la (7.1) diventa

$$y^6 = x_1^6 + x_2^6 + x_3^6 + x_4^6 + x_5^6 + x_6^6. \tag{7.38}$$

Ad oggi non si conoscono soluzioni intere di tale equazioni sebbene si conoscano invece soluzioni delle equazioni:

$$y^6 = x_1^6 + x_2^6 + x_3^6 + x_4^6 + x_5^6 + x_6^6 + x_7^6 \tag{7.39}$$

e anche

$$y_1^6 + y_2^6 = x_1^6 + x_2^6 + x_3^6 + x_4^6 + x_5^6 + x_6^6. \tag{7.40}$$

7.5 $n = 7$

Per $n = 7$ la (7.1) diventa

$$y^7 = x_1^7 + x_2^7 + x_3^7 + x_4^7 + x_5^7 + x_6^7 + x_7^7. \tag{7.41}$$

Non esiste una parametrizzazione delle sue soluzioni, e quelle conosciute sono molto poche, la più piccole delle quali è la seguente:

$$127^7 + 258^7 + 266^7 + 413^7 + 430^7 + 439^7 + 525^7 = 568^7 \tag{7.42}$$

dovuta a Dodrill e Guy alla fine degli anni novanta.

7.6 $n = 8$

Per $n = 8$ la (7.1) diventa

$$y^8 = x_1^8 + x_2^8 + x_3^8 + x_4^8 + x_5^8 + x_6^8 + x_7^8 + x_8^8. \tag{7.43}$$

Si conosce una sola soluzione di tale equazione, ovvero:

$$90^8 + 223^8 + 478^8 + 524^8 + 748^8 + 1088^8 + 1190^8 + 1324^8 = 1409^8 \tag{7.44}$$

dovuta a Chase e Meyrignac.

7.7 $n = 9$

Per $n = 9$ la (7.1) diventa

$$y^9 = x_1^9 + x_2^9 + x_3^9 + x_4^9 + x_5^9 + x_6^9 + x_7^9 + x_8^9 + x_9^9. \tag{7.45}$$

Non si conosocno soluzioni di tale equazione. Si conoscono invece soluzioni dell' equazione

$$y^9 = x_1^9 + x_2^9 + x_3^9 + x_4^9 + x_5^9 + x_6^9 + x_7^9 + x_8^9 + x_9^9 + x_{10}^9, \tag{7.46}$$

la più piccola delle quali è

$$917^9 = 42^9 + 99^9 + 179^9 + 475^9 + 542^9 + 574^9 + 625^9 + 668^9 + 822^9 + 851^9. \tag{7.47}$$

Bibliografia

1. P. Erdös, J. Surànyi, *Topics in the theory of numbers*, Springer (2003);
2. D. Zagier, *A one sentence proof that every prime* $p \equiv 1 (mod\, 4)$ *is a sum of two squares*, Amer. Math. Monthly **97** (1990);
3. J. Stillwell, *Elements of number theory*, Springer (2003);
4. G.A. Jones, J. M. Jones, *Elementary number theory*, Springer (1998);
5. M. Curzio, P. Longobardi, M. Maj, *Lezioni di algebra*, Liguori editore (1994);
6. G. Everest, T. Ward, *An introduction to number theory*, Springer (2005);
7. Piezas, Tito III and Weisstein, Eric W., *Diophantine Equation–3rd Powers*, MathWorld–A Wolfram Web Resource, http://mathworld.wolfram.com/DiophantineEquation3rdPowers.html;
8. Piezas, Tito III and Weisstein, Eric W., *Diophantine Equation–4th Powers*, MathWorld–A Wolfram Web Resource, http://mathworld.wolfram.com/DiophantineEquation4thPowers.html;
9. Weisstein, Eric W. *Diophantine Equation–5th Powers*, MathWorld–A Wolfram Web Resource, http://mathworld.wolfram.com/DiophantineEquation5thPowers.html;
10. Weisstein, Eric W. *Diophantine Equation–6th Powers*, MathWorld–A Wolfram Web Resource, http://mathworld.wolfram.com/DiophantineEquation6thPowers.html;
11. Weisstein, Eric W. *Diophantine Equation–7th Powers*, MathWorld–A Wolfram Web Resource, http://mathworld.wolfram.com/DiophantineEquation7thPowers.html;

12. Weisstein, Eric W. *Diophantine Equation–8th Powers*, MathWorld–A Wolfram Web Resource,
http://mathworld.wolfram.com/DiophantineEquation8thPowers.html;

13. Weisstein, Eric W. *Diophantine Equation–9th Powers*, MathWorld–A Wolfram Web Resource,
http://mathworld.wolfram.com/DiophantineEquation9thPowers.html;